



UNIVERZITET SINGIDUNUM
Departman za poslediplomske studije

**Zaštita podataka u bežičnim WLAN i
WAN računarskim mrežama**

Magistarski rad

Mentor:
Prof. dr. Mladen Veinović

Kandidat:
Vladan Josipović dipl.inž.

Beograd, 2009.

Abstrakt:

Zaštita podataka u računarskim mrežama je uvek aktuelna tematika. Zbog pogodnosti koje pružaju bežične računarske mreže se pogotovo naglo šire. Istovremeno u njima je lako dostupan medijum za prenos podataka pa su još izloženije na napade. Iz tih razloga postaje neophodno posvetiti više pažnje njihovoj bezbednosti.

Pri implementaciji bežičnih mreža postavlja se pitanje definicije politike bezbednosti, pre svega koju opremu i metode zaštite podataka odabrati.

U ovom radu su, kao teoretska osnova, iznete neke od osnovnih postavki teorije informacija. Navedeni su najčešće korišćeni standardi za bežične računarske mreže, a standardi IEEE 802.11x. i IEEE 802.16 su detaljnije obrađeni. Razmotreni su mehanizmi zaštite podataka i u okviru njih detaljnije analizirane slabosti i pretnje po bezbednost. Korišćeni su dostupni softverski alati sa interneta za prikupljanje i analizu bežičnog mrežnog saobraćaja. Sa tim alatima je praktično isprobano nekoliko mogućnosti ugrožavanja bezbednosti bežične mreže.

Pored napretka i dalje postoji nebezbednost u 802.11x. Mogući su napadi uskraćivanjem resursa i lažiranjem zaglavlja paketa. Možda je potrebno redizajniranje celog skupa protokola? Za sada bežične mreže nije preporučljivo koristiti u okruženjima koja ne tolerišu nepouzdanost ili nedostupnost.

Ključne reči: *Bezbednost podataka, WLAN, WAN, Kriptovanje*

Abstract:

Data security in computer networks are very actual thematic. Accommodation provided by wireless network causes their spiral expansion. In the other hand easy connection to the medium for transmission of data making this networks much exposed to the attacks. Because of that it is necessary to pay much attention about data security in this networks.

During the implementation of wireless networks we must decide how to define security policy and as part of this question we must decide what is equipment and data security method best for selection.

In this paper as theoretical base are exposed some basic thesis in information theory. There are named often used standards for wireless networks, and standards IEEE 802.11x. and IEEE 802.16 are detailed presented. There are discussed mechanism for data protection, and in this frame work detailed analysed weakness and threats for data security. It is used from web available software tools for gathering and analyse wireless network traffic. With this tools are practice proved some possibilities for threat wireless network security.

No considerate for the well being there are much unsecurity in 802.11x. There are many possibilities for attack type denial of service and masquerade header. Maybe it is necessary to redesign set of protocols? In this moment it is not recommended to use wireless network in conditions where no tolerance for unreliability or unavailability.

Keywords: *Data security, WLAN, WAN, Encrypting*

Sadržaj

Uvod	5
1. Informacija i informacioni sistem	6
1.1 Informacioni sistem	6
1.2 Bezbedan informacioni sistem	7
1.2.1 Semantička definicija informacije	7
1.2.2 Observacija neodređenosti u informacijama	9
1.2.3 Bezbedna informacija	10
1.2.4 Bezbedan informacioni sistem	12
2. Pregled bežičnih računarskih mreža	14
Uvod	14
2.1 Bluetooth IEEE 802.15	14
2.2 ZigBee IEEE 802.15.4	15
2.3 UWB 802.15.3	15
2.4 HSDPA Mobile Fi IEEE 802.20	15
2.5 2G	15
2.6 2.5 G	16
2.7 3G	16
3. Prikaz standarda IEEE 802.11	16
3.1 IEEE 802.11 Logical Link Control (LLC)	17
3.2 IEEE 802.11 Media Access Control (MAC)	17
3.3 IEEE 802.11 tehnologija fizičkog sloja (WLAN PHY metode)	18
3.3.1 Procedura za pristup na fizičkom nivou (Physical Layer Convergence Procedure - PLCP)	18
3.3.2 FHSS PMD (GFSK modulacija)	18
3.3.3 Gradivni elementi fizičkog sloja (PHY)	18
3.4 Metod frekventnih skokova (FHSS)	19
3.5 Tehnike rada u proširenom spektru (DSSS)	20
3.6 OFDM Modulacija	22
3.7 Pregled razvoja standarda IEEE 802.11	24
3.8 Hardverska oprema WLAN-a	26
3.8.1 Pristupna tačka (Access point - AP) i WLAN ruter	26
3.8.2 Računarske platforme	27
3.8.3 Bežična mrežna karta	27
3.8.4 Antena	28
3.8.5 Pojačavač	29
4. Prikaz standarda IEEE 802.16	29
4.1 WiMAX	29
4.2 Razvoj IEEE 802.16 protokola	30
4.2.1 IEEE 802.16-2001	30
4.2.2 IEEE 802.16a-2003	31
4.2.3 IEEE 802.16c-2002	31
4.2.4 IEEE 802.16-2004	32
4.2.5 IEEE 802.16e i kasnije verzije	32
4.3 Odnos IEEE 802.16 i IEEE 802.11	32

5. Načini identifikacije WLAN mreža	33
5.1 Analiza WLAN mrežnog saobraćaja	33
5.1.1 Informacije od svih okvira	33
5.1.2 Informacije od okvira podataka	34
5.1.3 Informacije od upravljačkih okvira	34
5.1.4 Zaključak	35
6. Softverski alati za analizu bežičnih mreža	36
6.1 Kismet	36
6.2 TCP Dump	43
6.3 Ethereal	44
6.4 Netstumbler	44
6.5 Programi za izmenu MAC adrese	44
7. Probijanje zaštite bežičnih mreža	46
7.1 Protokol za pridruživanje na 802.11 mrežu (Connection Access)	46
7.2 Wired Equivalent Privacy (WEP)	47
7.2.1 Osnova	47
7.2.2 Narušavanje poverljivosti	48
7.2.2.1 Dobijanje WEP ključa-slabost deljenog ključa u algoritmu RC4	48
7.2.2.2 Dobijanje Passphrase Seeded WEP ključa	50
7.2.2.3 Dvostruko kriptovanje (double encryption)	52
7.2.2.4 Napad pomoću poznatog otvorenog teksta	53
7.2.2.5 Inicijalni vektor (IV) i baza sekvence ključa	55
7.2.2.6 Preusmeravanje paketa	55
7.2.2.7 Napad grubom silom na WEP ključ	56
7.2.3 Narušavanje autentikacije	57
7.2.3.1 Mehanizam za autentikaciju	57
7.2.3.2 Jednostrana autentikacija	58
7.2.3.3 Bilo ko se može autentikovati	58
7.2.3.4 Zamena MAC adrese (Spoofing)	59
7.2.4 Ubacivanje Paketa (Packet Injection)	58
7.2.5 Ubrzano prikupljanje inicijalnih vektora	60
7.2.5.1 Retransmisija paketa	61
7.2.5.2 Forsiranje ponovne autentikacije	62
7.2.5.3 Upotreba poznate sekvence ključa	62
7.2.5.4 Pokretanje saobraćaja u praznoj mreži	62
7.3 Wireless Protected Access (WPA)	63
7.3.1 Osnove WPA i slabosti WPA	63
7.3.2 Probijanje WPA – rečnički napad	64
7.3.3 Probijanje WPA ako se koristi TKIP	65
7.3.4 Mehanizam zaštite WPA2	67
7.4 Ugrožavanje bezbednosti podataka u WAN mrežama	68
8. Ratna vožnja (wardrive)	71
8.1 Pojam ratne vožnje	71
8.2 Eksperimenti i ratna vožnja	72
9. Napad putem ometanja servisa (DoS)	74

10. Mere za poboljšanje bezbednosti WLAN	80
10.1 Upravljačke mere za zaštitu bežičnih mreža	80
10.2 Operativne mere za zaštitu bezbednosti bežičnih mreža	82
10.3 Tehničke mere za zaštitu bezbednosti bežičnih računarskih mreža	83
10.3.1 Uopšte o tehničkim merama zaštite bežičnih računarskih mreža	83
10.3.2 Honeypot tehnologija za zaštitu bežične mreže	84
10.3.3 IDS sistemi za zaštitu bežične mreže	87
10.3.3.1 Vrste sistema za detekciju upada u bežičnu mrežu (IDS)	87
10.3.3.2 Neuronske mreže i IDS	88
10.3.3.3 Sistemi za vizualizaciju podataka kao podrška IDS	90
10.3.3.4 Sistemi za prevenciju upada u mrežu IPS	91
10.3.3.5 IDS na osnovu hardverskih karakteristika opreme – fingerprint ..	92
10.3.4 Zaštita bežične mreže od napada ometanjem servisa	93
10.3.5 VPN u bežičnoj mreži	95
10.3.6 Zaštita podataka kriptovanjem na diskovima u mreži	99
Zaključak	102
Literatura	103
Rečnik pojmova	105
Spisak slika	106
Spisak tabela	107
Prilog 1: Izvorni kod programa SHA-1 za dobijanje hash vrednosti	108
Prilog 2: Izvorni kod programa za primenu RIJNDAEL algoritma kriptovanja ..	113
Prilog 3: Izvorni kod programa za realizaciju RC4 algoritma	122

Uvod:

Pogodnosti koje pruža bežična računarska mreža su je učinile popularnom pa se ona danas veoma često koristi. Na primer u poslovnom okruženju, univerzitetima, na javnim mestima, a takođe i u privatnim kućama. Bezbednost podataka koji se u bežičnim računarskim mrežama prenose je sve češće pitanje koje opredeljuje korisnike. Medijum za prenos informacija je eter, što znači da bilo ko sa radio prijemnikom i predajnikom može da prima i šalje podatke. To je pretnja po poverljivost informacija koje se u takvim mrežama prenose. Da bi se otklonila takva pretnja, na samom početku razvoja bežičnih računarskih mreža, prema standardu IEEE 802.11, kao rešenje je usvojen mehanizam za kriptovanje podataka pod nazivom WEP (*engl.* Wired Equivalent Privacy). Kao što samo ime govori taj mehanizam treba da pruži zaštitu podataka jednaku onoj koju ima žična računarska mreža. U vreme kada je WEP prihvaćen, postojala su značajna ograničenja u hardverskim mogućnostima opreme i ceni njene proizvodnje što je dovelo do prihvatanja ovakvog mehanizma zaštite podataka. WEP se pokazao kao ranjiv na nekoliko vrsta napada i sada se smatra da ima malu vrednost kao mehanizam za zaštitu poverljivosti podataka. U ovom radu je prikazano kako WEP radi i nekoliko načina za probijanje zaštite koju on pruža. Da bi se poboljšala bezbednost, i iskoristila postojeća oprema koja je korišćena sa WEP mehanizmom, zaštita je unapređena WPA mehanizmom. To je bilo prelazno rešenje, sa još uvek nedovoljno efikasnom bezbednošću. Tek WPA2 uz AES i novi sistem autentikacije konačno obezbeđuje potreban nivo bezbednosti podataka.

Aktuelni sistemi zaštite su proizvod ljudskog rada, namenjen drugim ljudima. Do grešaka u primeni zaštite podataka najčešće dolazi zbog nerazumevanja koncepta na kojem se zasnivao razvoj takvih sistema. Da bi se to prevazišlo razvijaju se novi inteligentni sistemi zaštite podataka uz primenu obsevera i inteligentnog softvera.

Struktura rada:

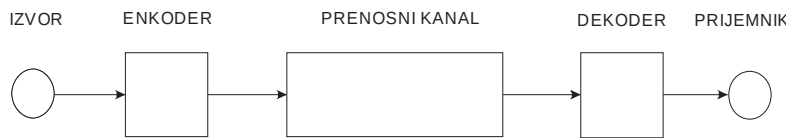
U prvom delu su date teorijske osnove o informaciji i informacionom sistemu, kao i pojam bezbednosti informacije. Osnova za razvoj i primenu bežičnih računarskih mreža su standardi za koje su navedene osnovne karakteristike. Detaljnije su prikazani standardi IEEE 802.11 i IEEE 802.16. Standard IEEE 802.11 za WLAN je analiziran kroz nivoe OSI modela. Razmotrene su tehnike modulacije sa aspekta zaštite od ometanja. Dat je pregled razvoja standarda, kao i hardverske opreme za realizaciju bežičnih računarskih mreža. Za standard IEEE 802.16 – WAN su navedene osnove arhitekture, bezbednosna rešenja, tipovi servisa za QoS, i prikazane su važnije verzije ovog standarda. Poglavlje 5 se odnosi na načine identifikacije WLAN mreža, tj. pregled informacija koje se mogu dobiti iz pojedinih paketa podataka prisluškivanjem saobraćaja u WLAN mreži. Da bi se prikupio i analizirao saobraćaj u bežičnoj mreži potreban je softverski alat za tu namenu. Neki od tih alata i njihove mogućnosti su prikazani u poglavlju 6. Poglavlje 7 je o načinu probijanja zaštite bežičnih mreža. Data su objašnjenja postupaka kao i nekoliko praktičnih primera. Obuhvaćeno je probijanje mehanizama WEP, WPA kao i ugrožavanje bezbednosti WAN mreže. Prikupljanje statističkih podataka o bežičnoj mreži pod nazivom ratna vožnja je tema poglavlja 8. Napadi putem ometanja mrežnih servisa (DoS) su tema poglavlja 9. U poglavlju 10 su sistematizovno prikazane mere za poboljšanje bezbednosti podataka u bežičnim računarskim mrežama i detaljnije su opisane neke od tehničkih mera.

1. Informacija i informacioni sistem

Informacija može biti predstavljena kao funkcija verovatnoće, pod pretpostavkom da informacija raste kada verovatnoća događaja opada i obrnuto. Pošto informacija eliminiše neodređenost, tako da većoj verovatnoći odgovara veća neizvesnost i manje očekivanje. Prikladna definicija informacije bi mogla biti da informacija predstavlja stepen slobode u izboru poruke iz skupa mogućih poruka.

1.1. Informacioni sistem

Uopšteno informacioni sistem se sastoji od izvora informacije, enkodera informacije, komunikacionog (prenosnog) kanala, dekodera i prijemnika informacije.



Slika 1.1.1 Informacioni sistem uopšteni prikaz [1]

Izvor informacije se može definisati kao skup parova $\{x_i, p(x_i)\}$, $i = 1, 2, \dots, n$, gde x_i predstavlja jednu od n poruka, koja se može pojaviti u izvoru, dok $p(x_i)$ predstavlja verovatnoću pojavljivanja te poruke. Ako logaritam za osnovu 2 zapišemo kao $\log_2$, količina informacija se može predstaviti kao: [2]

$$I(x_i) = -\log_2 p(x_i) = -\log p(x_i) \quad (1.1.1)$$

Srednja količina informacija na izvoru je:

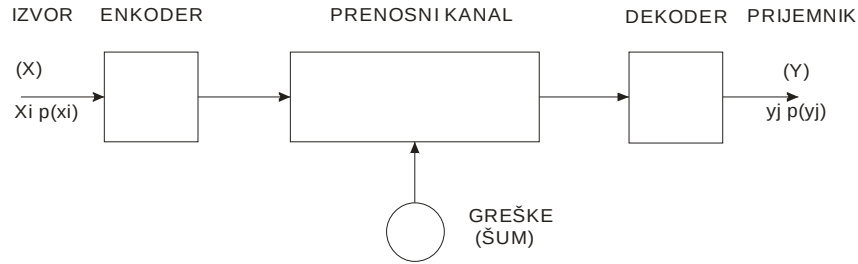
$$I(X) = -\sum_{i=1}^n p(x_i) \log p(x_i) = H(X) \quad (1.1.2)$$

Srednja količina informacija je ona količina informacija koja je neophodna da bi se odredio svaki pojedinačni simbol ili poruka iz skupa X svih mogućih simbola ili poruka koje se prenose kroz komunikacioni kanal. Količina $I(X)$ se naziva entropijom diskretnog slučajnog signala X i izražava se kao $H(X)$.

Kvalitet komunikacije se može izraziti preko kvantiteta informacionog toka, koji može biti prenet kroz komunikacioni kanal sa greškama (smetnjama). To je količina informacija koja pripada skupu primljenih poruka $\{Y\}$ i jednoznačno je povezana sa skupom poslatih poruka $\{X\}$. Količina informacija poslata kroz komunikacioni kanal sa greškama se može prikazati kao uzajamna informacija:

$$I(X; Y) = I(X) - I(X / Y) = I(Y) - I(Y / X) \quad (1.1.3)$$

Par $\{x_i, p(x_i)\}$, $i = 1, 2, \dots, n$, opisuje skup poruka na ulazu $\{X\}$, dok par $\{y_i, p(y_i)\}$, $j = 1, 2, \dots, m$, pripada skupu poruka $\{Y\}$ na izlazu iz komunikacionog kanala prikazano na Slici (1.1.2).



Slika 1.1.2 Komunikacioni kanal sa greškama

Izraz (1.1.3.) predstavlja gubitak ulaznih informacija na osnovu grešaka/šuma u komunikacionom kanalu, gledano sa strane ulaza ili izlaza tog kanala. To se može predstaviti pomoću uslovne verovatnoće $p(x_i/y_j)$ ili $p(y_j/x_i)$ što daje količinu izgubljenih informacija. [2]

$$I(X/Y) = - \sum_{i=1}^n \sum_{j=1}^m p(x_i) p(y_j/x_i) \log p(x_i/y_j) \quad (1.1.4)$$

$$I(Y/X) = - \sum_{j=1}^m \sum_{i=1}^n p(y_j) p(x_i/y_j) \log p(y_j/x_i) \quad (1.1.5)$$

1.2 Bezbedan informacioni sistem

1.2.1 Semantička definicija informacije

Kada pokušavamo da definišemo informaciju, semantički treba da uključimo u to observer (čoveka ili uređaj) [2]. Observer posmatra izvor informacije S . Uzmimo da se posmatrani izvor informacije S može predstaviti kao uređeni par, tj. $S = \{\Omega, \Omega^*\}$. Ω je skup simbola tj. sintaksni prostor, dok je Ω^* skup značenja tj. semantički prostor. Skup Ω sadrži elemente α_i , dok skup Ω^* sadrži elemente a_i . Postoji relacija između elemenata skupa Ω i skupa Ω^* . Uređeni par $\{\alpha_0, a_0\}$ koji se naziva *lexma*, označava da su simbol i njegovo značenje povezani. Gledano sa druge strane element a može biti posmatran kao objekat u stvarnom svetu, dok se element α može posmatrati kao slika elementa a . To je statička definicija.

Dinamička definicija se može predstaviti uvođenjem procesa observacije. Pretpostavimo da observer O observira jedan objekat i apsolutna observacija je predstavljena parom $\{\alpha, a\}$. Elementi α i a su observirani u isto vreme kada se pokušava odrediti njihova tačna vrednost. Observacija elemenata α i a se ne može vršiti odvojeno. Observer koristi α da bi odredio a , i obrnuto. Takođe postoji pretpostavka da postoji apsolutna simetrija između observiranog para varijabli, tj. proces observacije se može predstaviti kao rekurzivna šema $\alpha \rightarrow a$ i $a \rightarrow \alpha$. Simbol predstavlja značenje i značenje predstavlja simbol.

Da bi se izmerio prikazani proces observacije neophodno je pridružiti numeričke vrednosti varijablama α i a . Pretpostavimo da se α i a menjaju kontinualno u nekom skupu. Sa matematičke tačke gledano može se uzeti da su kontinualne promenljive α i a elementi skupa R , gde je R skup realnih brojeva. Tada se može pretpostaviti da se za promenljive α i a može izračunati neodređenost pomoću Šenonove diferencijalne entropije.

$$H(X) = - \int_{-\infty}^{+\infty} p(x) \ln p(x) dx \quad (1.2.1)$$

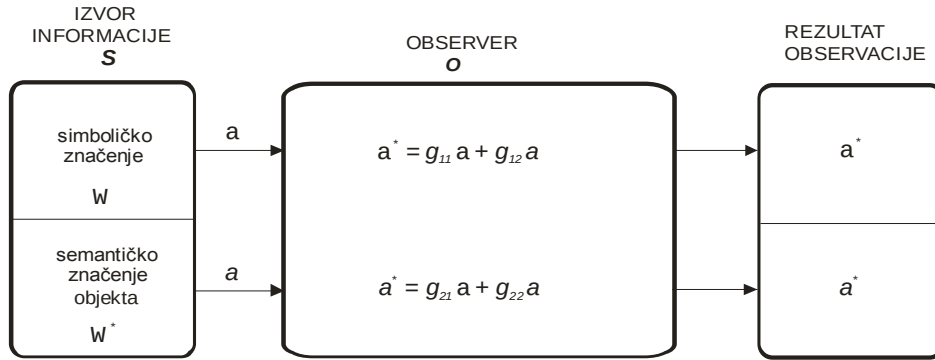
Postoji četiri aksioma, kojima se opisuje proces observacije [2]

Aksiom 1 Glavni zadatak observera O je da odredi tačnu vrednost α i a . Svakako, da rezultat observacije može biti samo više ili manje približna vrednost observiranih promenljivih. Observirane vrednosti α^* i a^* su linearne kombinacije od α i a :

$$\alpha^* = g_{11}\alpha + g_{12}a \quad (1.2.2)$$

$$a^* = g_{21}\alpha + g_{22}a \quad (1.2.3)$$

Aksiom 1 U osnovi govori da postoji relacija između α i a na nivou observacije. Uopštena forma ove relacije je nelinearna, t.j. $\alpha^* = f_1(\alpha, a)$ i $a^* = f_2(\alpha, a)$. Za lokalne observacije funkcije $f_1(\alpha, a)$ i $f_2(\alpha, a)$ mogu biti aproksimirane pomoću linearnih transformacija, tako da se **Aksiom 1** održava za observacije sa malim promenama observiranih parametara.



Slika 1.2.1 Model observera

Aksiom 2 Proces observacije se odvija na način kojim se ne uništavaju informacije niti se proizvode nove informacije. Ako je par $\{\alpha_0, a_0\}$, nastao na izvoru informacije observiran, proces observacije nema uticaja na konačno dobijenu informaciju dostupnu na izvoru informacija. To je pretpostavka očuvanja informacija.

Aksiom 3 Za specijalan slučaj kada je $\alpha \equiv a$, proces observacije se svodi na:

$$\alpha^* = G \cdot \alpha \quad (1.2.4)$$

Gde je G stalno pojačanje.

Aksiom 4 Postoji pretpostavka da se neodređenost informacije može izmeriti pomoću Šenonove entropije. Entropija observirane varijable α je $H(\alpha)$, od varijable a je $H(a)$. Međusobna entropija para $\{\alpha, a\}$ je $H(\alpha, a)$. Entropija za gore definisani proces observacije se može predstaviti kao:

$$H(\alpha^*, a^*) = H(\alpha, a) + \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} p(\alpha, a) \ln |g_{11} \cdot g_{22} - g_{12} \cdot g_{21}| d\alpha da \quad (1.2.5)$$

Ako Aksiom 2 o pretpostavci očuvanja informacija važi, onda je $H(\alpha^*, a^*)$ isto što i $H(\alpha, a)$, što znači da je drugi deo izraza (1.2.5) jednak nuli, pa je:

$$|g_{11} \cdot g_{22} - g_{12} \cdot g_{21}| = 1 \quad (1.2.6)$$

Više funkcija može ispunjavati uslov (1.2.6). Sledeće funkcije mogu biti odabrane za tražene koeficijente g_{ij} :

$$g_{11} = \cosh \omega, \quad g_{12} = \sinh \omega, \quad g_{21} = \sinh \omega, \quad g_{22} = \cosh \omega \quad (1.2.7)$$

gde je ω elemenat iz skupa R , skupa realnih brojeva, ω je parametar za podešavanje osobina observera. Jednakosti (1.2.2) i (1.2.3) se mogu pisati kao:

$$\alpha^* = \alpha \cosh \omega + a \sinh \omega \quad (1.2.8)$$

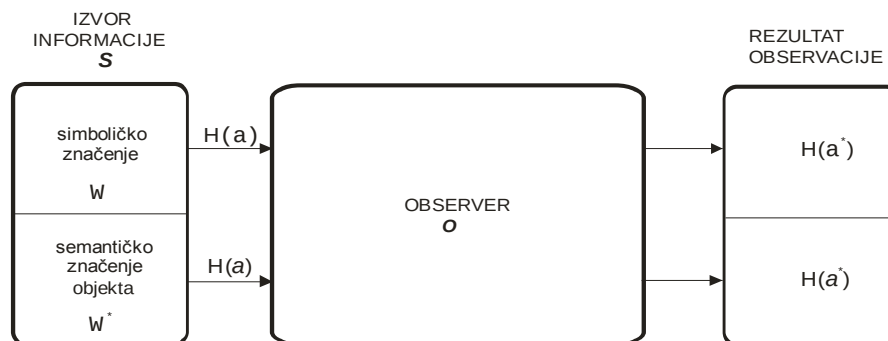
$$a^* = \alpha \sinh \omega + a \cosh \omega \quad (1.2.9)$$

Ako observer O observira par varijabli $\{\alpha, a\}$, gde su α i a elementi skupa R i vidi $\{\alpha^*, a^*\}$ kao rezultat observacije, tada postoji ω , koje je takođe elemenat skupa R , tako da su jednakosti (1.2.8) i (1.2.9) zadovoljene. Parametar observacije ω predstavlja faktor greške. Ako je $\omega=0$ observirane varijable odgovaraju tačno onima koje su proizvedene na izvoru informacije i tada nema greške u observaciji. Izbor parametra ω određuje odstupanje $\Delta\alpha$ i Δa observiranih varijabli od onih koje su nastale na izvoru informacije. Za male vrednosti $|\omega|$ transformacije u jednakostima (1.2.8) i (1.2.9) su linearne. Jednačine observacije (1.2.8) i (1.2.9) se mogu primeniti na bilo koji par simbola i odgovarajućeg značenja $\{\alpha, a\}$.

1.2.2 Observacija neodređenosti u informacijama

Pretpostavljamo da je α simbol koji označava reč u nekom od svetskih jezika i da je a neki realan ili abstraktan objekat (koji se vezuje za značenje reči). Tako uređeni par $\{\alpha, a\}$ nema brojčanu vrednost. Pretpostavimo takođe da observer može direktno da uočava količinu neodređenosti sadržanu u α i a . Tada se može reći da je observer osetljiv na promenu količine entropije $H(\alpha)$ i $H(a)$. Proces koji je opisan odgovara uobičajenoj situaciji koja se javlja u komunikaciji kada observer prima lexmu (jezički gledano) t.j. reč α i njeno značenje a . Jasno je da se α i a ne mogu izraziti numerički, tako da se gore navedena četiri aksioma mogu primeniti samo indirektno. Promenljive koje se mogu izraziti numerički su entropije $H(\alpha)$ i $H(a)$.

Observer procenjuje količinu neodređenosti vezano za pojavljivanje reči α nezavisno od neodređenosti koja je povezana sa pridruženim značenjem a . Na taj način observer (prijemnik informacija) koristi verovatno značenje reči da bi otkrio njeno simboličko značenje i obrnuto, t.j. observer može koristiti poznavanje simbolike primljene reči da bi otkrio njenu semantiku.



Slika 1.2.2 Model observacije neodređenosti informacije

Aksiomi opisani ranije se mogu primeniti na observiranje entropija, gde su $H(a^*)=H_r(a)$ i $H(a^*)=H_r(a)$ relativne entropije. Primenujući jednačine observacije (1.2.8) i (1.2.9) dobijamo nove jednakosti:

$$H_r(\alpha) = H(\alpha) \cdot \cosh \omega + H(a) \sinh \omega \quad (1.2.10)$$

$$H_r(a) = H(\alpha) \cdot \sinh \omega + H(a) \cosh \omega \quad (1.2.11)$$

1.2.3 Bezbedna informacija

Osnovni servisi bezbednosti su poverljivost, integritet i dostupnost informacije.

Poverljivost (*engl.* confidentiality) je jedan od glavnih motiva za uvođenje kriptografskih sistema. Ona znači kontrolu objavljivanja informacija i zaštitu od neovlašćenog pristupa informacijama. Da bi opravdali svoju upotrebu kriptografski sistemi moraju biti efikasni u obezbeđenju poverljivosti podataka. Ta efikasnost se naziva snaga: jak kriptografski sistem je teško „razbiti“. Umesto snage, često se koristi pojam radnog faktora (work factor) algoritma: on približno određuje vreme koje je neophodno za „razbijanje“ nekog kriptografskog sistema. Smatra se da je kriptografski sistem slab ako dozvoljava upotrebu slabih ključeva, ako poseduje propuste u dizajnu ili ako se može lako dekriptovati. Veliki broj današnjih sistema je dovoljno snažan za poslovnu i ličnu upotrebu, ali je nedovoljno jak za osjetljive vojne i vladine aplikacije.

Utvrdjivanje postojanja eventualnih izmena poruke tokom prenosa predstavlja drugi osnovni zadatak kriptografskih sistema. Integritet podataka se obezbeđuje dodavanjem zasebnih podataka u vidu kontrolne sume ili drugih redundantnih podataka koji će biti iskorišćeni u procesu dekriptovanja. Dodavanjem koda za autentičnost poruke (*engl.* Message Authentication Code - MAC) predstavlja uobičajeni način za proveru njenog integriteta. MAC se dobija na osnovu sadržaja same poruke i ključa. MAC se obično kriptuje sa samom porukom, i tako šalje, čime se dodaje još jedan sloj provere integriteta. Prijemna strana takođe na identičan način proračunava MAC vrednost i poredi svoj rezultat sa vrednošću koja je poslata uz poruku. Integritet je obezbeđen ukoliko su te dve vrednosti iste. MAC vrednost je neka vrsta ključa koja se dobija pomoću heš algoritma, SHA, MD5 ili slično. Ključ je obično simetričan, pa se isti proces odvija na oba kraja veze primenom identične funkcije.

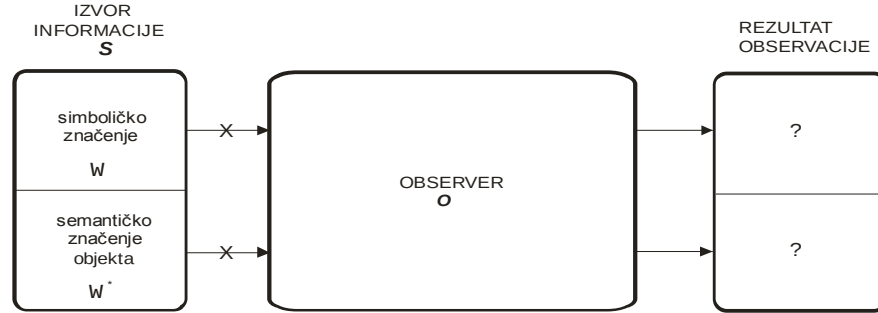
Kontrola pristupa (*engl.* access control) označava metode, procese i mehanizme za sprečavanje neovlašćenih pristupa kriptografskim sistemima. Kriptografski ključevi su osjetljivi na krađu, gubitke i ljudske propuste. Kontrola pristupa mora regulisati i fizičke i operativne mere zaštite resursa.

Kada je pretnja po bezbednost informacija ostvarena, kažemo da se desio incident. Incident se definiše kao akcija koja verovatno dovodi do ozbiljnih posledica. Jezikom IT to je bilo šta što se dogodi sa informacijama, a da nije poželjno. Prema ranije usvojenom značenju incident bi mogao biti napad u opsegu od relativno bezazlenih pokušaja, kao što je probijanje passworda, neautorizovanih pokušaja prijavljivanja na sistem sa udaljenog mesta, do mnogo ozbiljnijih napada kakvi su kreiranje, ubacivanje virusa ili napada tipa ometanja servisa, itd.

Svaki incident je u stvari kršenje Aksioma 2, koji pretpostavlja zaštitu informacija. Kada se incident dogodi, tada je prekinuta veza između izvora informacije S i

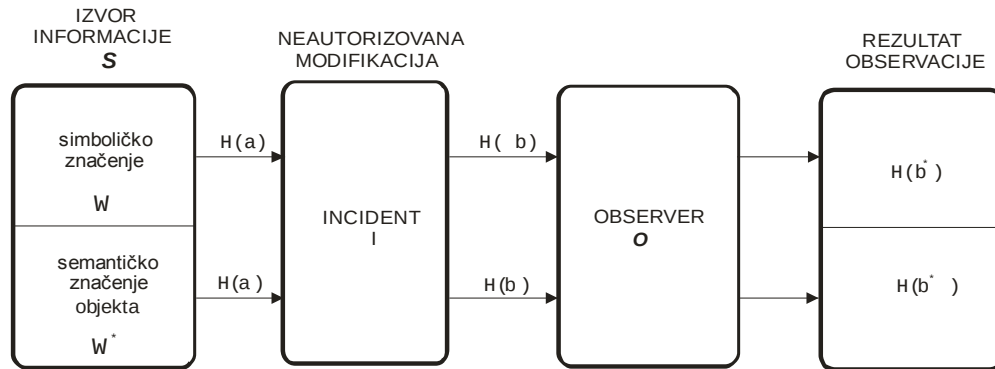
observera O i umetnuta je neautorizovana izmena informacije. Tada se dešavaju dva moguća slučaja:

- *DoS (engl. Denial of Service)*, gde je veza sa izvorom informacije potpuno prekinuta ili je informacija uništena i observer ne prima nikakve informacije od izvora.



Slika 1.2.3.1 Denial of service (DoS) napad

- *Neautorizovana modifikacija*, je kada observer prima informacije koje su, bez saglasnosti, modifikovane u prenosu od izvora informacije do observera.



Slika 1.2.3.2 Neovlašćena modifikacija informacija

U slučaju, neovlašćene modifikacije observer prima informaciju sa neodređenim sadržajem koja se može opisati preko entropije $H(\beta)$ i $H(b)$. Observirane entropije $H(\beta^*)$ i $H(b^*)$ više nisu funkcije primarnih parametara observacije ω , što znači da jednakosti (1.2.10) i (1.2.11) više ne važe. Tada se razmatraju novi parametri observacije kao što je θ . Tada se jednakosti (1.2.10) i (1.2.11) menjaju u:

$$H(\beta^*) = H_r(\beta) = H(\beta) \cdot \cosh \theta + H(b) \sinh \theta \quad (1.2.12)$$

$$H(b^*) = H_r(b) = H(b) \cdot \sinh \theta + H(\beta) \cdot \cosh \theta \quad (1.2.13)$$

pa se bezbednost informacija može izraziti preko ranije navedenih aksioma:

- *Aksiom 1*, kojim se kaže da postoji relacija između simbola (reči) α i njenog značenja a što se smatra normalnom situacijom u razmeni informacija između izvora informacija i observera.

- **Aksiom 2**, koji govori o tome da informacija ne može biti uništena u procesu observacije niti je procesu observacije dozvoljeno da kreira nove informacije, je najvažniji aksiom što se tiče bezbednosti informacija. Poverljivost, integritet i dostupnost informacija, koje karakterišu bezbednu informaciju, mogu biti sačuvane samo ako se Aksiom 2 striktno poštuje tokom čitavog procesa observacije.

- **Aksiom 3**, kojim se opisuje redukovani proces observacije, nije toliko važan za bezbednost informacija.

- **Aksiom 4**, koji objašnjava kako se neodređenost informacije može izmeriti Šenonovom entropijom, je takođe važan za bezbednost informacija, zato što daje formalni alat za merenje neodređenosti informacije preko jednakosti koje opisuju proces observacije.

Postoji još jedan aksiom koji se može dodati već navedenim.

- **Aksiom 5**, koji kaže da ako neovlašćena modifikacija informacije nastane, tada observer mora biti sposoban da uoči (i eventualno koriguje) neželjenu modifikaciju.

Posledice **Aksioma 5** su sledeće:

- observer mora biti u mogućnosti da uoči razliku između $H(\beta^*)$, $H(b^*)$ i $H(\alpha^*)$, $H(a^*)$, respektivno

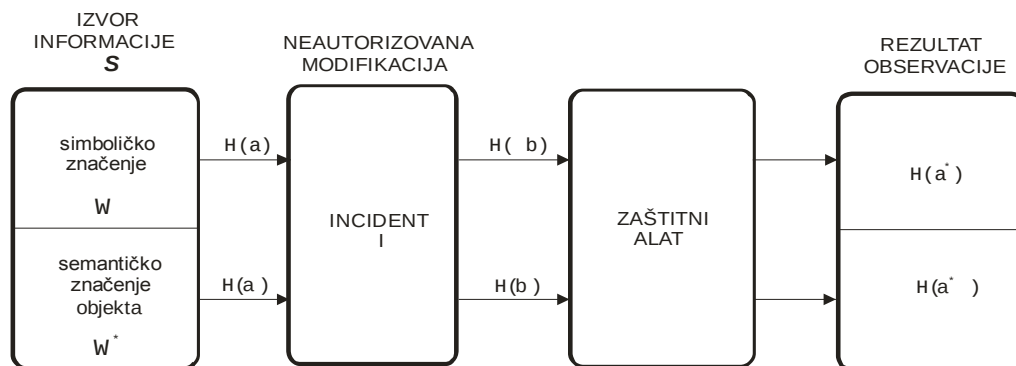
- observer mora uočiti razliku između parametra observacije ω i θ , i (ako je moguće) korigovati pogrešan parametar tako da se postigne minimalna razlika, da bude $\omega = \theta$

- observer treba da ima neka prethodna znanja o očekivanim rezultatima observacije da bi bio sposoban da uoči razliku između korektne i nekorektne informacije.

1.2.4 Bezbedan informacioni sistem

Pretnje bezbednosti u informacionom sistemu su u ovom radu dosada predstavljane kao šum u komunikacionom kanalu. Takav koncept nije uključivao semantički aspekt informacije. Bio je opterećen time što je teško razlikovati „normalne“ i „nenormalne“ aktivnosti u današnjim informacionim sistemima, delom i zato što bitan deo pretnji po bezbednost dolazi od samog informacionog sistema. To je zato što informacioni sistemi nisu kreirani još od samog početka stvaranja tako da zadovolje zahteve bezbednosti.

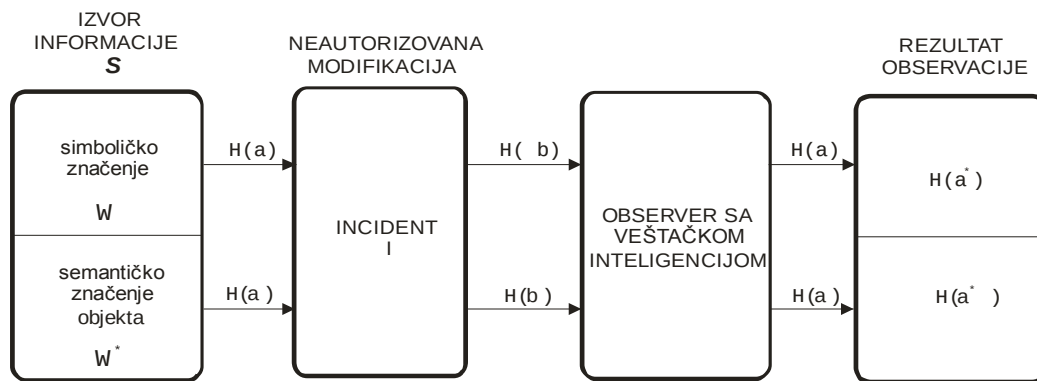
Postojeći sistemi zaštite su uglavnom pravljeni tako da rade nezavisno od informacionih sistema. Taj pristup u osnovi nije pogrešan sve dok korisnik (observer) informacionog sistema koji prima informacije postupa korektno. Na slici (1.2.4) je prikazana situacija kada je observer O izostavljen, ali je implicitno prisutan kroz rezultate observiranja.



Slika 1.2.4 Napadnuti informacioni sistem sa alatima za zaštitu

Bilo koji, pa i najbolji današnji alat za zaštitu može da pogreši. Slika (1.2.4) prikazuje idealnu situaciju kada je alat za zaštitu u mogućnosti da potpuno vrati primarnu informaciju sa izvora informacije. Nažalost danas ne postoji tako idealan alat za zaštitu. Koncept automatskih adaptivnih sistema zaštite je najbliži ovom konceptualnom dizajnu idealnog alata za zaštitu. Ipak, čak i ovo rešenje ima nekoliko tehničkih poteškoća u implementaciji. Najvažnije su raspoznavanje i problemi sa brzinom obrade.

Idealan alat za zaštitu bi morao da zadovolji gore pomenutih pet aksioma. [2] Najvažniji su svakako *Aksiom 2* i *Aksiom 5*. Uvođenjem *Aksioma 5* zahteva se novi kvalitet alata za zaštitu. Više nije dovoljno da alat bude automatizovan i adaptivan (da bi prebrodio greške korisnika). Alat se mora ponašati kao inteligentni observer, sposoban da prepozna „nenormalan“, oblik ponašanja informacionog toka. On takođe mora biti sposoban da donosi neke odluke i da bude u stanju da potpuno rekonstruiše informaciju kakva je bila pre neovlašćenih izmena. Slika (1.2.5) prikazuje takvu situaciju.



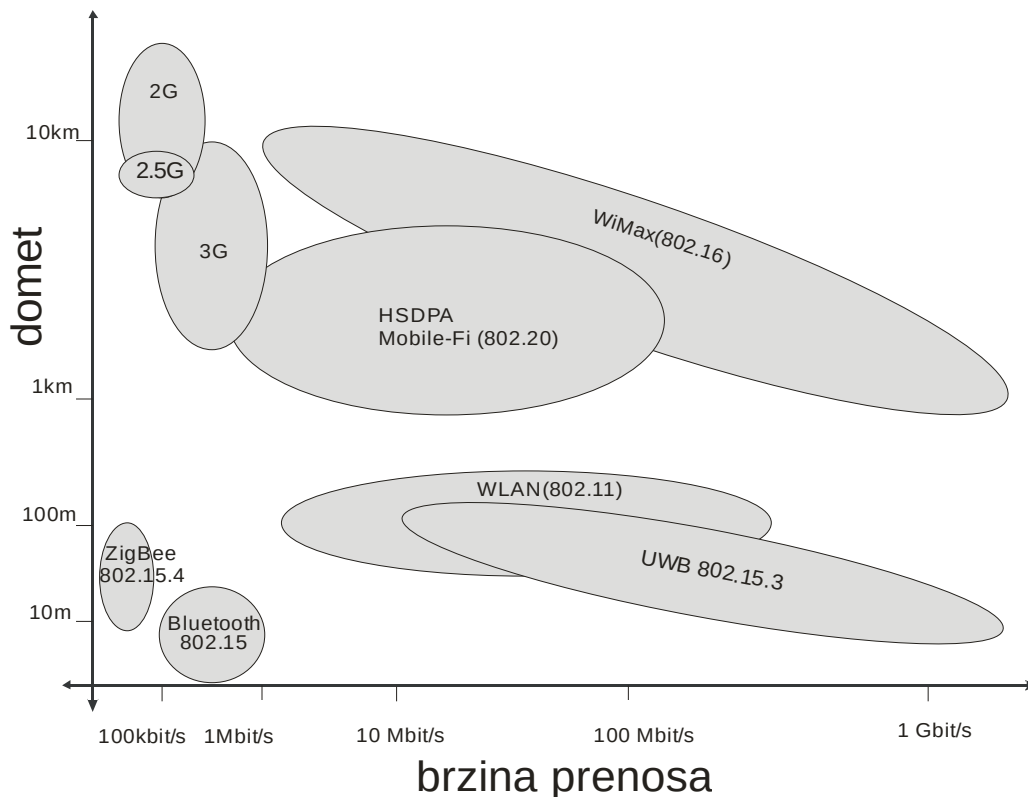
Slika 1.2.5 Napadnuti informacioni sistem sa inteligentnim observerom

Jedan inteligentni observer nije dovoljan da bi potpuno zaštitio informacioni sistem. Potrebno je više inteligentnih observera uvezanih u jedan sistem raspoređenih unutar informacionog sistema koji štite, sa mogućnošću da međusobno komuniciraju.

2. Pregled bežičnih računarskih mreža

Uvod

Bežične računarske mreže prema standardima IEEE 802.11 i IEEE 802.16 su osnovna tema ovog rada ali radi potpunije predstave, treba navesti još neke bežične mreže za prenos podataka, slične namene i karakteristika. One su razvijane da bi zadovoljile specifične potrebe, kao što je komunikacija u bliskom okruženju, ili podrška prenosu informacija i govora na veće udaljenosti. Pri tom tačke između kojih se razmenjuju podaci mogu biti stacionarne ili mobilne. IEEE 802.1x grupa obuhvata više protokola bežične komunikacije.



Slika 2.1.1. Odnos brzine prenosa i dometa za neke od standarda bežičnih mreža

2.1 Bluetooth IEEE 802.15 je protokol za bežičnu razmenu podataka na malim udaljenostima sa fiksnih i mobilnih uređaja, što čini lične bežične mreže, personal area networks (PAN). Nastao je kao alternativa RS232 prenosu podataka pomoću kabla. Moguća je konekcija više uređaja na bluetooth mrežu, uz prevazilaženje problema sinhronizacije. Razvojem specifikacije za ovaj standard se bavi Bluetooth Special Interest Group. Od 1994 god. do sada je bilo više verzija ovog standarda, verzije 1.0 i 1.0B su nekompatibilne sa ostalim verzijama a verzije 1.1, 1.2, 2.0 i 2.1 su međusobno kompatibilne. Bezbednost Bluetooth komunikacije je prema objavljenim radovima, na više načina ugrožavana. Prednosti ovakvog načina komunikacije su niska cena uređaja, mala snaga zračenja, koje je u principu štetno za ljudsko zdravlje, i niska potrošnja energije.

2.2 ZigBee IEEE 802.15.4 je specifikacija za komunikacioni protokol koji koristi digitalni radio prenos sa niskom potrošnjom energije. Zasnovana je na IEEE 802.15.4 standardima i namenjena je za bežične personalne mreže (WPANs). Tehnologija definisana ZigBee specifikacijom je namenjena da bude jednostavnija i jeftinija od ostalih WPAN, kao što je Bluetooth, i primenjuje se kao RF prenos za mali protok podataka, dug vek baterijskog napajanja i kao bezbedna mreža. Zig Bee Alliance je grupa firmi koje održavaju i publikuju Zig Bee standard, slično WiFi alijansi za standard IEEE 802.11. ZigBee radi na ISM opsegu 868 MHz u Evropi i 915 MHz u SAD i Australiji, kao i na 2.4GHz u celom svetu. Jednostavna rešenja u tehnologiji donose niže cene uređaja. Proizvodjači opreme nude integrisane varijante sa radio uređajem procesorom ili mikrokontrolerom, čak i sa kompletnim softverom. Najnovija verzija ZigBee specifikacije iz 2007 godine ima dva profila. Jedan za kućnu i manje zahtevnu komercijalnu upotrebu koji koristi manje RAM memorije, i drugi tzv. ZigBee Pro koji pruža znatno veće mogućnosti kao što je multi-casting, rutiranje many-to-one i poboljšanu bezbednost korišćenjem Symmetric-Key Key Exchange (SKKE). Oba profila rade u mesh mrežama i rade sa svim ostalim profilima ZigBee uređaja. Izrazita primena ovog standarda je u senzorskim mrežama.

2.3 UWB 802.15.3 standard IEEE 802.15.3 je nastao kako bi se omogućilo bežično povezivanje sa velikom brzinom prenosa podataka, niskom potrošnjom energije, malom cenom uređaja, za prenos multimedijalnih sadržaja, prenosivim uređajima koji su široko dostupni na tržištu. Ovaj standard omogućava brzine prenosa podataka od 11 do 55 Mb/s na udaljenosti veće od 70 m uz održavanje kvaliteta prenosa (QoS) za tok podataka. Kao dodatak, ovaj standard daje mogućnost jednostavnog ad-hoc povezivanja koje uređajima dozvoljava automatsko formiranje mreže i razmenu podataka bez intervencije korisnika. Privatnost i integritet je za podatke i komande obezbeđena sa 128-bitnom AES enkripcijom uz korišćenje CCM moda. Ovaj standard takođe omogućava različite tehnike koje se koriste za istovremenu primenu 802.15.3 piconet mreža sa drugim bežičnim mrežama. [3]

2.4 HSDPA Mobile Fi IEEE 802.20 Mobile Broadband Wireless Access (MBWA) je IEEE standard koji omogućava razvijanje mreža sa mobilnim širokopojasnim bežičnim pristupom. Standard važi za ceo svet i koristi opremu različitih proizvođača. Odobren je od strane IEEE 802 grupe u junu 2008 godine. Zahtevi koji su predloženi za ovaj standard su daleko viši od bilo kojih dosadašnjih u mobilnoj arhitekturi. Optimizovan je za punu mobilnost do brzina od 250 km/h, radi u licenciranom opsegu 3.5 GHz, koristi paketnu arhitekturu, koristi novi MAC i PHY sa IP i adaptivnim antenama. Najveća brzina prenosa je 1Mbit/s.

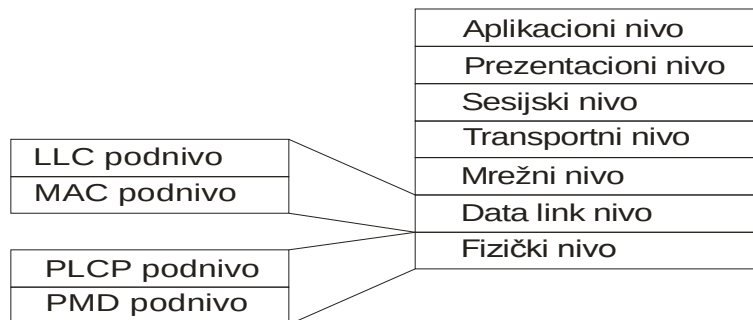
2.5 2G je tehnologija bežičnih telefona druge generacije. Prvi put je uvedena u Finskoj 1991. god. kao GSM standard. Osnovna prednost 2G u odnosu na prethodnu generaciju bežičnih telefona je digitalna enkripcija komunikacije telefona sa baznom stanicom. Ovom tehnologijom je poboljšana efikasnost u korišćenju frekventnog spektra, smanjena je snaga predajnika, smanjena potrošnja baterija kod prenosnih uređaja, smanjene dimenzije uređaja, i sve to dovodi do prodora ove tehnologije na tržištu. Novi servis su SMS poruke. U zavisnosti od toga koji je tip multipleksa primenjen razlikuju se TDMA (Time Division Multiplex Access) i CDMA (Code Division Multiplex Access).

2.6 2.5 G je stepenica u razvoju između 2G i 3G. Prvi važan korak je bilo uvođenje General Packet Radio Service (GPRS) u postojeću 2G infrastrukturu, GSM ili CDMA mreže. Iako je uvedena paketna razmena podataka, brzina prenosa je još uvek mala i kreće se u opsegu 56 Kbit/s do 114 Kbit/s. Takva tehnologija je zaživela zbog potrebe na tržištu za servisima kao što je Wireless Application Protocol (WAP), Short Message Service (SMS), Multimedia Messaging Service (MMS), Internet servis kao što je e-mail i World Wide Web. Tada je počela praksa naplaćivanja usluga prema količini prenetih podataka umesto ranijeg načina prema vremenu provedenom na vezi. Primenom kodovanja 8PSK i protokola kao što je EDGE za GSM i CDMA2000 1x-RTT za CDMA, brzina prenosa raste preko 144 Kbit/s, što je još uvek nekoliko puta sporije od 3G, i naziva se 2.75G servisom.

2.7 3G mreža je definisana prvobitnim standardom organizacije ITU, IMT-2000. Kasnija dopuna standarda od strane organizacije 3GPP je dovela do sistema Universal Mobile Telecommunications System (UMTS) koji se naziva i W-CDMA. Bezbednost u 3G mrežama je poboljšana u odnosu na 2G. Uvedena je autentikacija mreže prema korisniku tako da je korisnik siguran da se prijavljuje baš na željenu mrežu. 3G mreže koriste KASUMI blok kriptografski sistem umesto starog A5/1 kriptovanja toka podataka. Pojavila su se brojna ozbiljna upozorenja po pitanju bezbednosti KASUMI kripto sistema. Kao reakcija na to, dodata je zaštita na aplikativnom nivou, od kraja do kraja veze. Takva vrsta zaštite se ne primenjuje isključivo na 3G mreže.

3. Prikaz standarda IEEE 802.11

Ustanovljen je od strane IEEE LAN/MAN komiteta (IEEE 802). Standard IEEE 802.11 je za bežične LAN mreže, Ethernet kompatibilne, namenjen uređajima malog dometa. Obezbeđuje specifikaciju za *fizički* i *data link* nivo OSI modela.



Slika 3.1.1 OSI model sa podnivoima 802.11 tehnologije

U okviru Data link nivoa postoje LLC i MAC podnivoi OSI modela 802.11 tehnologije.

3.1 IEEE 802.11 Logical Link Control (LLC) je gornji podnivo Data Link nivoa. On omogućava mehanizme za multipleks i kontrolu toka što omogućava da nekoliko mrežnih protokola (IP, IPX) istovremeno postoje u okviru multipoint mreže i da se prenose preko istog mrežnog medijuma. LLC podnivo je interfejs između MAC podnivoa i mrežnog nivoa. On je isti za različite fizičke medijume (kao što su Ethernet, Token Ring i WLAN).

3.2 IEEE 802.11 Media Access Control MAC podnivo je komplikovaniji od 802.3 MAC podnivoa, zato što treba rešiti probleme vezane za pristup medijumu.

Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
2 Bytes	2 Bytes	6 Bytes	6 Bytes	6 Bytes	2 Bytes	6 Bytes	0-2312 Bytes	4 Bytes

Slika 3.2.1 802.11 generalni MAC okvir

Frame Control je dužine 2 bajta i sadrži 11 potpolja. *Duration/ID* polje ima vrednost u zavisnosti od toga u kom je režimu stanica koja pristupa medijumu. *Adress 1,2,3 i 4* polja se razlikuju u zavisnosti od tipa okvira i podtipa. *Sequence control* polje nosi broj sekvence i broj fragmenta okvira. *FCS* polje sadrži vrednost 32 bitnog cyclic redundancy broja koji je izračunat za sva polja MAC zaglavlja i tela okvira.

Svi 802.11 okviri odgovaraju osnovnom 802.11 okviru. Sve tri kategorije MAC podnivoa odgovaraju i koriste određene delove generalnog MAC okvira za njihove posebne uloge.

Postoje tri kategorije okvira u 802.11 MAC podnivou.

Kontrolni okviri, kontrolišu protok okvira sa podacima u toku normalnih 802.11 razmena podataka. Postoji šest jedinstvenih kontrolnih okvira: Power save poll (PS-Poll), RTS, CTS, ACK, Contention-free End (CF-End), CF-End + contention free acknowledgment (CF-End + CF-ACK).

Upravljački okviri upravljaju WLAN vezama, procesom provere identiteta (authentication) i statusom. Imaju polja iz generičkog MAC okvira. Takođe koriste strukturu podataka koja je poznata kao informacioni element (IE) i fiksna polja. Uloga IE i fiksnih polja je omogućavanje fleksibilnosti za definisanje mogućnosti postojećih okvira i obezbeđivanje proširivog metoda za proširenje funkcionalnosti MAC upravljačkih okvira.

Okviri podataka prenose podatke stanice između predajnika i prijemnika. Specifikacija standarda opisuje osam jedinstvenih okvira podataka.

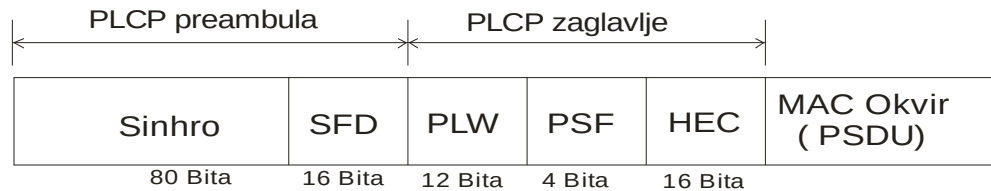
3.3 IEEE 802.11 tehnologija fizičkog sloja

MAC sloj kod svih 802.11 tehnologija je isti, a fizički sloj je ono po čemu se one razlikuju. Razlikujemo dva fizička podsloja:

- Physical Layer Convergence Procedure (PLCP)
- Physical Medium Dependant (PMD).

3.3.1 Physical Layer Convergence Procedure (PLCP)

Kada MAC sloj prosledi MAC okvir podataka, poznat i kao PLCP Physical Service Data Unit (PSDU), u PLCP podsloj, PLCP dodaje dva polja na početak okvira da bi se formirao PPDU okvir. Na slici je prikazan format PLCP okvira.



Slika 3.3.1 Format PLCP okvira

PLCP preambula se sastoji iz dva podpolja. Podpolje SYNC je dugačko 80 bita i predstavlja niz sačinjen od nula i jedinica, a započinje sa nulom. Prijemna stanica koristi ovo polje da bi donela odluku o izboru antene u različitim primenama, da bi se načinila korekcija nekog frekvencijskog pomeranja i radi sinhronizacije paketa. Potpolje „start of frame delimiter - SFD“ (graničnik početka okvira) je dugačko 16 bita i sastoji se od specijalnog bit niza (0000 1100 1011 1101, prvi bit levo) kojim se obezbeđuje tajming okvira za prijemnu stanicu.

PLCP zaglavlje se sastoji od tri podpolja: PSDU length word je polje dugačko 12 bita i određuje veličinu MAC okvira (PSDU) u oktetima. PLCP signaling polje (PSF) dugačko je 4 bita, i ukazuje na brzinu prenosa okvira. Kreće se od 1 Mbit/s do 4.5 Mbit/s korakom od 0.5 Mbit/s. Header error control (HEC) predstavlja ITU-T Cyclic Redundancy Check (CRC-16) vrednost za zaglavlje PLCP. Predajnik generiše checksum vrednost, a zatim prijemnik koristi tu vrednost da bi utvrdio postojanje greške u primljenim poljima PLW i PSF.

PSDU prolazi kroz blok za kriptovanje da bi se ulazna sekvenca bitova transformisala u oblik koji je slučajno generisan. U rezultujućem PSDU između svakog bloka od 32 simbola umeću se tzv. „stuff“ simboli. Ovi simboli uklanjaju bilo kakvo odstupanje u podacima, višak jedinica u odnosu na nule ili obrnuto, što bi moglo da ima neželjeni efekat u toku kasnije obrade modula.

3.3.2 FHSS PMD (GFSK modulacija)

PLCP konvertuje okvir u binarni tok bitova (stream) i prosleđuje ga u PMD podsloj. FHSS PMD podsloj moduliše ovaj tok podataka upotrebom GFSK metode (Gaussian Frequency Shift Keying).

3.3.3 Gradivni elementi fizičkog sloja (PHY)

Da bi se razumeli različiti PMD podnivoi, koje obezbeđuje svaki od PHY slojeva različitih 802.11 tehnologija, potrebno je razumeti osnovne gradivne elemente PHY sloja, a to su:

- **Kriptovanje** (Scrambling) je metod pomoću koga se obezbeđuje da podaci koje primite imaju, što je više moguće karakter slučajnog broja, a to se postiže mapiranjem između sekvenci bitova. Često se koristi termin „ubeljivanje toka podataka“. Većina metoda kriptovanja vrši samostalnu sinhronizaciju, što znači da je uređaj za dekriptovanje u stanju da se sinhronizuje sa uređajem za kriptovanje.

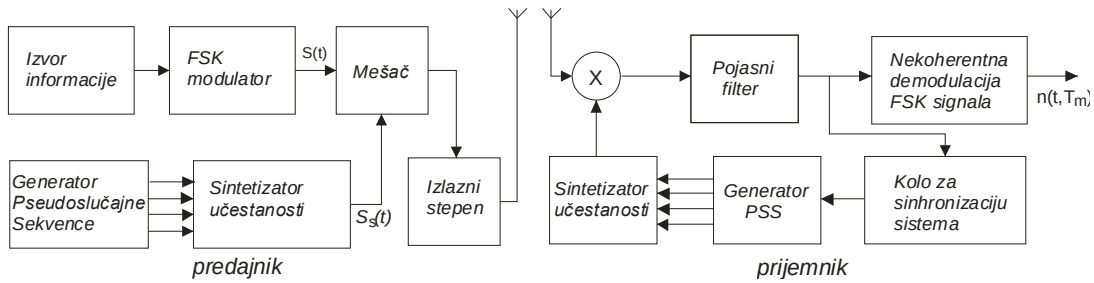
- **Kodiranje** (Coding) je mehanizam koji omogućuje prenos podataka velikim brzinama kroz kanale koji poseduju šum. Ovo se postiže zamenom sekvence bitova

dužom sekvencom koja omogućuje da se prepozna i koriguje oštećeni bit. Najčešći tip kodiranja u današnjim komunikacionim sistemima je *konvolucioni koder*, zato što je hardverska implementacija takvog koda prilično pojednostavljena upotrebom kola za kašnjenje i sabirača.

- Umetanje (Interleaving) se uvodi da bi pogrešno preneti bitovi bili razmešteni u grupe gde nastaju greške, tako da deluju nezavisno. Bilo da se umetanje vrši softverski ili hardverski cilj je da se susedni bitovi razdvoje umetanjem nesusednih bitova.

- Mapiranje simbola i modulacija. Proces modulacije preslikava sekvencu bitova na noseći talas u radnom frekventnom opsegu. Proces modulacije se može vršiti nad amplitudom, frekvencijom ili fazom. Iako se sekvenca bitova može direktno modulisati u noseći signal upotrebom amplitudne, frekventne ili fazne modulacije, mapiranjem grupe bitova u simbole može se preneti više bitova u slobodni propusni opseg nosioca. Mapiranje u simbole je proces u kome se bitovi grupišu i mapiraju u kvadratnu i faznu komponentu. Obično se predstavlja u Kartezijanskom koordinatnom sistemu, gde je na x osi fazna komponenta, a na y osi kvadratna komponenta i to se naziva *konstelacija*.

3.4 Metod frekvencijskog skakanja FHSS



Slika 3.4 Blok šema FHSS modulacije

Izvor informacije je u digitalnom obliku. Na izlazu iz FSK (Frequency Shift Keying) digitalno frekventnog modulatora dobija se signal $S(t)$.

$$S(t) = A \cos[\omega_1 + (2\mu - 1)\Delta\omega] \cdot t \quad (3.3.1)$$

Pri tome je $\mu = 1$ ako se na izlazu izvora informacije nalazi binarna jedinica, odnosno $\mu = 0$ ako se na njegovom izlazu nalazi binarna nula. Sintetizator učestanosti zajedno sa generatorom pseudoslučajne sekvence generiše prostoperiodični signal čija se učestanost skokovito menja po zakonu koji je određen pseudoslučajnom sekvencom $S_s(t)$.

$$S_s(t) = 2 \cos(\omega_2 + M\Delta\omega) \cdot t \quad (3.3.2)$$

Pri tome je M slučajan broj koji može da ima N različitih vrednosti ($1 \leq N \leq L$). Period T_f između dve sukcesivne promene broja M je određen nejednakošću $1/T_e > 1/T_f > LT_e$. Izlazni signal mešača čiji je izlazni filter podešen na učestanost

$\omega_1 + \omega_2 + (M_{\max}\Delta\omega)/2 = \omega_0 + (M_{\min}\Delta\omega)/2$ može se predstaviti u sledećem obliku:

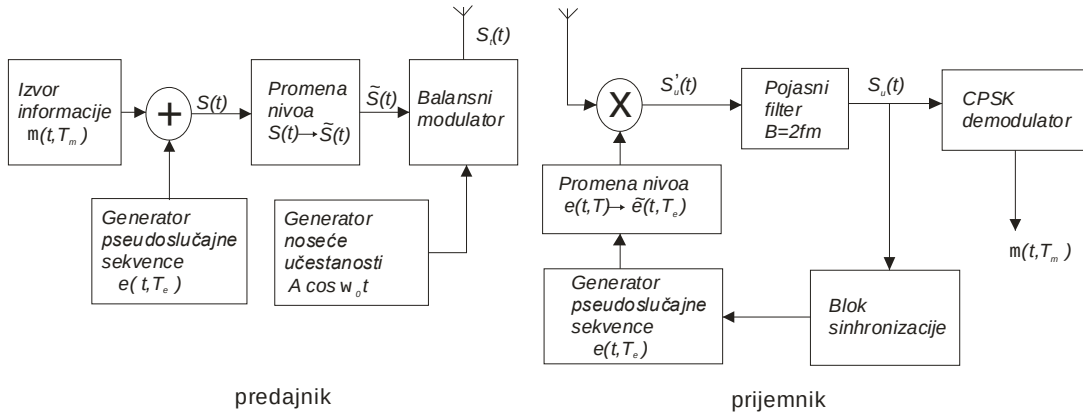
$$S_t(t) = A \cos[\omega_1 + (2\mu - 1)\Delta\omega + \omega_2 + M\Delta\omega] \cdot t = A \cos[\omega_0 + (2\mu - 1)\Delta\omega + M\Delta\omega] \cdot t \quad (3.3.3)$$

Učestanost ovako dobijenog signala se menja u diskretnim vremenskim intervalima, kao rezultat delovanja binarnog signala koji nosi informaciju i pseudoslučajne sekvence. Širina spektra signala zavisi od maksimalne vrednosti broja M i iznosi $(M_{max} + 2)\Delta\omega$. U procesu mešanja FSK signala koji nosi informaciju i izlaznog signala sintetizatora učestanosti, izvršena je ekspanzija spektra korisnog signala koji zauzima frekventni opseg $2\Delta\omega$ u novi frekventni opseg $(M_{max} + 2)\Delta\omega$. U prijemniku sistema se generiše identična pseudoslučajna sekvenca koja je tačno u sinhronizmu sa sekvencom u predajniku sistema. Pošto signal sintetizatora u prijemniku ima isti oblik kao i signal sintetizatora u predajniku može se opisati relacijom (3.3.2.). Posle mešanja ulaznog signala sa sinhronim lokalno generisanim signalom sintetizatora na izlazu pojasnog filtera mešača dobija se signal čija je učestanost jednaka razlici učestanosti ulaznih signala.

$$S_u(t) = A \cos[\omega_0 - \omega_2 + (2\mu - 1)\Delta\omega + M\Delta\omega - M\Delta\omega] = A \cos[\omega_1 + (2\mu - 1)\Delta\omega] \quad (3.3.4)$$

Tom operacijom je na ulazu prijemnika izvršena kompresija spektra širokopojasnog signala opsega $(M_{max} + 2)\Delta\omega$ u mnogo užu opseg korisnog signala koji zauzima frekventno područje širine $2\Delta\omega$. Pri tome je snaga korisnog signala na ulazu u FSK-demodulatora ista kao i u slučaju klasičnog digitalnog prenosa informacije, ali je prenos ostvaren sa mnogo manjom gustinom snage. U praktičnim realizacijama proces FSK modulacije se realizuje u sintetizatoru.

3.5 Tehnike rada u proširenom spektru (DSSS)



Slika 3.5 Blok šema DSSS modulacije

Izvor informacije generiše binarni signal $\mu(t, T_m)$, generator pseudoslučajne sekvence generiše pseudoslučajni signal $e(t, T_e)$. Binarni simbol ima periodu T_m i amplitudu $\mu(t, T_m) = 1$ ako se prenosi binarna jedinica odnosno amplitudu $\mu(t, T_m) = 0$ ukoliko se prenosi binarna nula. Pseudoslučajna sekvenca ima takođe jediničnu amplitudu ali je perioda binarnih simbola unutar nje mnogo manja $T_m \gg T_e$. DSSS signal se dobija tako što se prvo sabiranjem po modulu 2 informacionog i pseudoslučajnog signala dobije novi signal kojim se vrši CPSK modulacija talasa nosioca koji ima učestanost ω_0 . Postupak CPSK modulacije se realizuje tako što se unipolarni signal $s(t) = m(t, T_m) \oplus e(t, T_e)$ promenom nivoa prvo pretvori u bipolarni signal amplitude ± 1 a zatim se prostim množenjem na balansnom modulatoru generiše CPSK signal. Pošto

je operacija binarnog sabiranja po modulu 2 unipolarnih binarnih signala sa promenom nivoa resultantnog signala radi njegovog prelaska u bipolarni oblik, ekvivalentna množenju istih binarnih signala u bipolarnom obliku, signal predajnika DSSS sistema može se pisati kao

$$S_t(t) = A\tilde{s}(t)\cos\omega_0t = A \cdot \tilde{\mu}(t, T_m) \cdot \tilde{e}(t, T_e)\cos\omega_0t \quad (3.5.1)$$

Pri tome su sa $\tilde{s}(t) = 2s(t) - 1$, $\tilde{\mu}(t, T_m) = 2\mu(t, T_m) - 1$, $\tilde{e}(t, T_e) = 2e(t, T_e) - 1$ obeleženi bipolarni ekvivalenti unipolarnih signala $s(t)$, $\mu(t, T_m)$ i $e(t, T_e)$. Na osnovu relacije (3.5.1) može se formalno smatrati da je signal $S_t(t)$ nastao tako što je prostoperiodični talas nosilac $A\cos\omega_0t$ amplitudno modulisan (sa potisnutim nosiocem) sa svakom spektralnom komponentom pseudoslučajnog signala a nakon toga svaka spektralna komponenta novodobijenog signala amplitudno modulisana sa signalom $\hat{\mu}(t, T_m)$ koji ima kontinualni spektar. Izvršena je ekspanzija spektra signala koji nosi informaciju u mnogo širi frekventni opseg određen frekventnom učestanošću f_e sa kojom se generišu binarni simboli u pseudoslučajnoj sekvenci. Time se postiže da emitovani signal ima veoma malu i relativno konstantnu gustinu spektra snage u veoma širokom frekventnom području. Ovakav signal podseća na spektar širokopojasnog Gaussovog šuma, što znači da ga je dosta teško uočiti pošto liči na šum. Ovakav sistem je takođe otporan na smetnje uzrokovane prisustvom pojedinačnih spektralnih komponenti koje potiču od drugih sistema.

U prijemniku sistema DSSS signal se množi sa identičnom bipolarnom (PSS) pseudoslučajnom sekvencom $\tilde{e}(t, T_e)$ koja je tačno sinhronizovana sa PSS koju primljeni DSSS signal nosi u sebi sa predajnika. Pretpostavimo da se na ulazu prijemnika nalazi samo signal $S_t(t)$ bez ikakve dodatne smetnje. Nakon množenja sa lokalno generisanom pseudoslučajnom sekvencom dobija se signal

$$S'_u(t) = S_t(t) \cdot \tilde{e}(t, T_e) = A\tilde{\mu}(t, T_m)[\tilde{e}(t, T_e)]^2 \cos\omega_0t \quad (3.5.2)$$

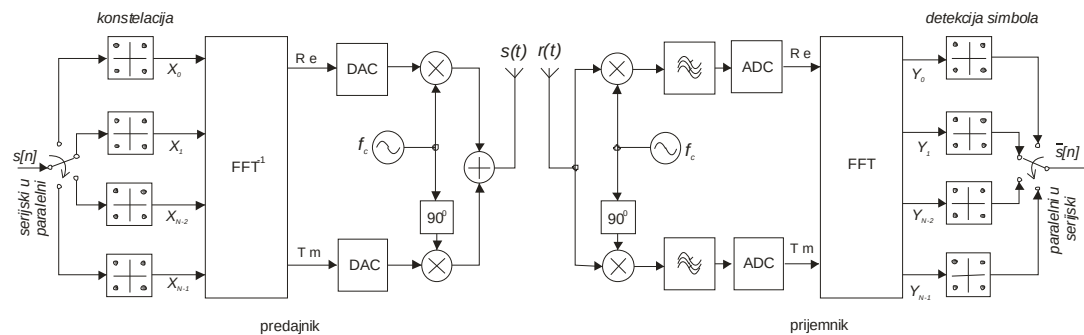
Imajući u vidu da je $[\tilde{e}(t, T_e)]^2 = 1$ ulazni signal pojasnog filtra postaje

$$S'_u(t) = A\tilde{\mu}(t, T_m)\cos\omega_0t = A[2\mu(t, T_m) - 1]\cos\omega_0t \quad (3.5.3)$$

Pojasni filter ima simetričnu prenosnu karakteristiku u odnosu na centralnu učestanost ω_0 i propusni opseg dovoljan da signal $S'_u(t)$ prođe na ulaz CPSK demodulatora bez znatnih deformacija. Množenjem ulaznog DSSS signala sa sinhronizovanom, lokalno generisanom pseudoslučajnom sekvencom, postiže se efekat kompresije spektra signala čime je od širokopojasnog DSSS signala dobijen klasični CPSK signal iste snage ali lociran u mnogo užem frekventnom opsegu koji je određen impulsnom učestanošću f_m sa kojom se generiše digitalni signal koji nosi informaciju. U procesu ekspanzije i kompresije spektra, srednja snaga korisnog signala ostaje nepromenjena. Međutim, ovim se postupkom nivo snage ometajućeg signala, koji prolazi do ulaza CPSK demodulatora, u velikoj meri redukuje čime se imunost ovako koncipiranog sistema za prenos informacija na ometanje u velikoj meri povećava.

3.6 OFDM Modulacija

OFDM je osnova za standard 802.11a. Kao tehnologija OFDM (engl. Orthogonal Frequency Division Multiplexing) je patentirana 1970. To je multikanalna modulacija, kreirana da bi se podaci prenosili pod jakom međusobnom interferencijom (intersymbol interference - ISI). Slično načinu modulacije FHSS signala na odgovarajuću frekvenciju nosioca, kanal se rastavlja na N nezavisnih kanala. Za dati propusni opseg kanala, što je veće N koje se izabere, to će biti duži period za signal i uži podkanal. To znači da ako broj podkanala raste ka beskonačnom to se ISI smanjuje tj. teži nuli. U 802.11a kanal od 20 MHz je podeljen u 52 podkanala širine 312.5 kHz i koji rade u osam standardnih kanala. Za kreiranje nezavisnih simbola, koristan alat je brza Furijeova transformacija (FFT), koja predstavlja efikasnu implementaciju diskretne Furijeove transformacije (DFT). Ona konvertuje signal iz vremenskog domena u frekventni domen i obratno. Obrada signala u frekventnom domenu je jednostavnija, ali u prijemu treba da bude prijemni signal u kanalu, u kružnoj konvoluciji a ne samo u konvoluciji. U frekventnom domenu se generiše N 4-QAM (Quadrature Amplitude Modulation) simbola, koji se zatim konvertuju u vremenski domen upotrebom inverzne brze Furijeove transformacije (IFFT). Ako se iznos transformacije podesi da bude jednak stepenu dvojke, time se omogućava jednostavna i efikasna implementacija. OFDM radi sa četiri modulacije BPSK, QPSK, 16-QAM i 64-QAM. Signali podkanala su ortogonalni, što znači da se svaki može izdvojiti u prijemu bez interferencije sa drugim podkanalima. To je moguće zato što matematičke osobine ortogonalnih talasnih oblika osiguravaju da je proizvod bilo koja dva podkanala nula. To takođe dozvoljava prijemu kraj da rekonstruiše oštećene delove primljenog signala. OFDM tehnologija se primenjuje i u drugim sistemima, kao što je Asymmetric Digital Subscriber Line (ADSL), Digital Audio Broadcasting (DAB), Digital Video Broadcasting Terrestrial (DVB-T), i 802.11g



Slika 3.6. Blok šema OFDM modulacije

OFDM signal je zbir više ortogonalnih podkanala, sa baznopojasnim podacima u okviru svakog podkanala koji je nezavisno modulisan korišćenjem neke od vrsta modulacije, engl. Quadrature Amplitude Modulation (QAM) ili engl. Phase Shift Keying (PSK). Taj sumarni signal se koristi za modulisanje glavnog RF nosioca.

U predajnik dolazi $s[n]$ serijski niz binarnih signala. Inverznim multipleksiranjem, koje demultipleksira u N paralelnih tokova, i svaki od njih mapira u tok simbola koristeći neku od konstelacija (QAM, PSK). Inverzna brza Furijeova

transformacija se računa za svaki skup simbola, dajući skup uzoraka u vremenskom domenu. Ti uzorci se zatim poprečno mešaju u propusnom opsegu na standardni način. Realne i imaginarne komponente se prvo konvertuju u analogni domen koristeći DAC (digital to analog convertor). Analogni signal se koristi za modulaciju $\cos$ i $\sin$ talasnih oblika na nosećoj frekvenciji, f_c , respektivno. Ti signali se sumiraju i daju signal na izlazu iz predajnika, $s(t)$.

Prijemnik dobija signal $r(t)$, koji se poprečno meša dole na osnovnu frekvenciju koristeći $\cos$ i $\sin$ talasne oblike na nosećoj frekvenciji. To takođe pravi signale sa osnovnom frekvencijom $2f_c$, ali se niskopropusni filteri koriste da ih odbace. Osnovni signali se tada uzorkuju i digitalizuju korišćenjem ADC Analognog digitalnih konvertora. Brza Furijeova transformacija se koristi da ih vrati nazad u frekventni domen. To daje N paralelnih tokova, od kojih se svaki konvertuje u binarni tok korišćenjem odgovarajućeg signal detektora. Ti tokovi signala se vraćaju u serijski tok, $\hat{s}[n]$, koji je estimacija originalnog binarnog toka u predajniku.

Matematička osnova:

Ako se koristi N podkanala, i svaki podkanal je modulisan korišćenjem M različitih simbola, OFDM symbol alfabet se sastoji od M^N kombinovanih simbola.

Niskopropusni ekvivalent OFDM signala se može predstaviti kao:

$$v(t) = \sum_{k=0}^{N-1} X_k e^{j2\pi kt/T}, 0 \leq t < T, \quad (3.6.1)$$

Gde su $\{X_k\}$ simboli podataka, N je broj podkanala i T je *OFDM* period simbola. Podkanalni $1/T$ ga čini ortogonalnim u odnosu na svaki period simbola, što se piše:

$$\frac{1}{T} \int_0^T (e^{j2\pi k_1 t/T})^* (e^{j2\pi k_2 t/T}) dt = \frac{1}{T} \int_0^T e^{j2\pi (k_2 - k_1) t/T} dt = \delta_{k_1 k_2} \quad (3.6.2)$$

Gde $(.)^*$ označava operaciju kompleksne konjugacije i δ je Kronekerovo delta.

Da bi se sprečila međusimbolna interferencija zbog slabljenja signala usled fadinga, zaštitni interval dužine T_g se umeće pre OFDM bloka. U toku tog intervala, ciklički prefiks je prenet tako da je signal u intervalu $-T_g \leq t < 0$ jednak signalu $T - T_g \leq t < T$. OFDM signal sa cikličkim prefiksom je prema tome:

$$v(t) = \sum_{k=0}^{N-1} X_k e^{j2\pi kt/T}, -T_g \leq t < T \quad (3.6.3)$$

Niskopropusni signal iznad može biti vrednovan u realnom ili u kompleksnom domenu. Realna komponenta niskopropusnog signala se uglavnom koristi kod širokopojasnih žičnih komunikacija kao što je DSL. Za bežične aplikacije, niskopropusni signal ima uglavnom kompleksnu vrednost; u kom slučaju, je signal prenet na noseću frekvenciju f_c . Uopšteno se preneti signal može predstaviti kao:

$$s(t) = \Re\{v(t)e^{j2\pi f_c t}\} = \sum_{k=0}^{N-1} |X_k| \cos(2\pi [f_c + k/T] \cdot t + \arg[X_k]) \quad (3.6.4)$$

3.7 Pregled razvoja standarda IEEE 802.11

IEEE 802.11 ili WLAN standard je usvojen 1997. god. Ostale ekstenzije su dopune standarda - izuzev praktičnih preporuka pod nazivom 802.11F i 802.11T. Ovaj standard obuhvata tri fizička nivoa, infracrveni opseg IC 250 ns sa brzinom prenosa 1 Mbit/s, i dva u opsegu radio frekvencija RF koji koriste ISM (*engl.* Industrial Scientist Medical) band 2.4 GHz koji je slobodan za nelicencirane korisnike. Prvi je sa modulacijom FHSS (*engl.* Frequency Hoping Spread Spectrum), i drugi DSSS (*engl.* Ddirect Sequence Spread Spectrum). Oba rade sa brzinom prenosa 1 Mbit/s ili 2 Mbit/s. Zbog zastarelosti ovaj standard ima dosta modifikacija.

IEEE 802.11a koristi data link nivo i format okvira kao i originalni standard, ali sa tehnikom modulacije OFDM (*engl.* Orthogonal Frequency-Division Multiplexing) na fizičkom nivou. Prenos signala je u 5GHz pojasu, sa maksimalnom brzinom prenosa od 54 Mbit/s i dodatkom koda za korekciju greške. To daje prihvatljivi protok od 20 Mbit/s. Zbog povećane absorpcije elektromagnetnih talasa, na višim frekvencijama, smanjen je domet.

IEEE 802.11b poznat kao Wi-Fi. Omogućava povećanje brzine protoka na 5.5Mbit/s i 11 Mbit/s što ga uz smanjenje cena bežičnih mrežnih kartica, na tržištu mrežnih uređaja dovodi u ravan sa 10 Mbit Ethernetom.

IEEE 802.11c Definiše operacije sa mrežnim mostovima (*engl.* Bridges), uključeno u standard IEEE 802.1D.

IEEE 802.11d Međunarodni standard za roming bežičnih računarskih mreža..

IEEE 802.11e Proširenje vezano za upravljanje performansama (QoS), uključuje i razbijanje paketa.

IEEE 802.11f Definiše komunikaciju između pristupnih tačaka.

IEEE 802.11g Radi na frekvencijama 2.4 GHz. Koristi novi način modulisanja OFDM kao kod 802.11a i ima maksimalni protok od 54 Mbit/s. Kartice su kompatibilne unazad sa 802.11b. Kao i 802.11b osetljiv je na interferenciju od drugih uređaja kao što su mikrotalasne rerne, bluetooth uređaji, celularni telefoni i sl.

IEEE 802.11h Ovo proširenje uvodi DFS (*engl.* Dynamic Frequency Selection) i TPC (*engl.* Transmit Power Control) što omogućava štednju energije kod mobilnih baterijski napajanih uređaja. Rešava probleme kao što je interferencija sa satelitima i radarima koji koriste 5GHz band. Mada je razvijan za potrebe Evropske unije koristi se u mnogim drugim zemljama. Integrisan je u IEEE 802.11-2007 standard.

IEEE 802.11i Određuje nove sigurnosne mehanizme za bežičnu mrežu, staru odredbu autentikacija i privatnost menja sa novom detaljnijom odredbom security. Nove komponente su 802.11X za autentikaciju, RSN (*engl.* Robust Security Network) za praćenje pridruživanja na mrežu i na AES (*engl.* Advanced Encryption Standard) zasnovan CCMP za obezbeđivanje poverljivosti, integriteta i autentikaciju korisnika.

IEEE 802.11j Posebno prilagođen Japanskom tržištu. Radi u opsegu 4.9 do 5GHz.

IEEE 802.11-2007 Verzija standarda koja objedinjuje ekstenzije a,b,d,e,g,h,i,j.

IEEE 802.11k Definiše upravljanje radio resursima. Ukoliko je signal neke pristupne tačke AP jači od ostalih, neće se svi korisnici prijavljivati na tu AP. Po ovom standardu izvršiće se raspodela korisnika i na druge pristupne tačke, tako da se ukupne performanse sistema poboljšavaju.

IEEE 802.11l Rezervisano, ali se neće koristiti.

IEEE 802.11m Objedinjene i sistematizovane sve prethodne verzije standarda, tako da poslednja revizija ovog proširenja prerasta u IEEE 802.11-2007.

IEEE 802.11n Nastao dodavanjem na fizičkom nivou (PHY) Multiple input multiple output (MIMO) tehnologije koja koristi više antena u prijemu i predaji kako bi povećala performanse sistema. I operacije spajanja kanala na 40 MHz, gde se koriste istovremeno dva nepreklapajuća kanala za prenos podataka. Primenjuje se agregacija okvira na MAC nivou. Navedene izmene daju značajno povećanje protoka sa 54Mbit/s do maksimalnih 600 Mbit/s. Konačna verzija ovog standarda se očekuje u Novembru 2009 god. ali već su dostupne neke draft verzije kod nekih proizvođača opreme.

IEEE 802.11o Rezervisano, ali se neće koristiti.

IEEE 802.11p Je predlog dopune standarda, kako bi se omogućila komunikacija sa vozilima u pokretu i između vozila u pokretu u okviru licenciranog opsega 5.9 GHz (5.85-5.95GHz). Ovaj standard je u vezi sa standardom IEEE 1609. Njegova konačna verzija je urađena u Aprilu 2009 god.

IEEE 802.11q Rezervisano, ali se neće koristiti zbog sličnosti naziva sa IEEE 802.1Q VLAN.

IEEE 802.11r Omogućava neprekidnu povezanost sa bežičnim uređajem u pokretu, uz brzi i bezbedan prelazak sa jedne pristupne tačke na drugu. To je podrška aplikaciji VoIP, za prenos govora.

IEEE 802.11s Predlog dopune standarda za kreiranje mreže. Definiše kako se bežični uređaji mogu povezati da kreiraju ad-hoc mrežu. Putanje za prenos kroz takvu mrežu se utvrđuju nekim od protokola za rutiranje, a preporučeni je HWMP (Hybrid Wireless Mesh Protocol). Ovaj standard uključuje i mehanizme za omogućavanje determinističkog mrežnog pristupa, kontrolu zagušenja i štednju energije za napajanje uređaja.

IEEE 802.11T Standardizacija metoda za predviđanje karakteristika bežične mreže Wireless Performance Prediction (WPP), metode testiranja i preporuke za merenja performansi wireless mreže.

IEEE 802.11u Povezivanje sa mrežama koje nisu pod IEEE 802 standardom npr. celularne mreže.

IEEE 802.11v Skup pravila koja služe za upravljanje bežičnom mrežom. Ta pravila se koriste i u verzijama 802.11a, 802.11b, 802.11g, i 802.11n i time se omogućava konfigurisanje klijentskih uređaja koji su povezani na IEEE 802.11 mrežu.

IEEE 802.11w Predlog poboljšanja zaštite prenosa upravljačkih okvira, koji se prema izvornom standardu šalju bez zaštite, što ih čini ranjivim.

IEEE 802.11x Rezervisano, ali se neće koristiti, zbog sličnosti naziva sa IEEE 802.1x mrežnom kontrolom pristupa.

IEEE 802.11y Radi u opsegu 3650 – 3700 MHz u SAD.

IEEE 802.11z Proširenje za Direkt Link podešavanja (DLS).

IEEE 802.11aa Podržava robusno prenošenje audio i video materijala u realnom vremenu.

3.8 Hardverska oprema za WLAN-a

Oprema kojom se uspostavlja, meri i održava WLAN je: pristupna tačka (access point), wireless ruter, računarska platforma (pc ili pda), bežična mrežna kartica, antena, pojačavač signala i skener tj. spektralni analizator. Postoji dosta proizvođača opreme čijim udruživanjem je nastala interesna organizacija WiFi. Ona ispituje usklađenost opreme sa standardom IEEE 802.11 i njenu interoperabilnost. Samo ona oprema koja prođe ispitivanje interoperabilnosti može da nosi oznaku WiFi.

3.8.1 Pristupna tačka i WLAN ruter

Pristupna tačka (engl. Access Point – AP) Slika 3.8.1- umesto Dial In servera ili Ethernet habova (skup različitih uređaja koji se ponašaju kao čvorište, tj. razvodnik). Pristupna tačka je uređaj koji služi za međusobno povezivanje klijenata i predstavlja centralni deo jedne mreže. Takođe, može da se koristi i za spajanje wireless klijenata sa LAN-om ili sa izlazom na Internet. Svaka pristupna tačka ima integrisan konektor za antenu kao i makar jedan konektor za LAN. Može raditi u nekoliko modova (čije prisustvo varira u zavisnosti od uređaja i proizvođača): *client* mod (pomoću njega se spaja na mrežu isto kao i pomoću obične kartice), *bridge* mod (koristi se za spajanje dve mreže ili više mreža u jednu celinu), *repeater* mod (repeater – ponavljač, koristi se ako je potrebno dodatno povećati domet mreže, u ovom modu uređaj ponavlja sve ono što “čuje”).

Pristupna tačka se proizvodi kao:

- Bridge - Bridž transparentno povezuje bežičnu i LAN mrežu.
- NAT ruter - NAT ruter prevodi saobraćaj sa bežične mreže na LAN mrežu, ali ne i u obrnutom smeru i obično se koristi za bežični pristup Internet-u.

NAT je skraćenica za Network Address Translation - tehniku zaštite i "skrivanja" pod mreže.

- Ruter + NAT bridge - Ova vrsta uređaja bridžem spaja bežičnu i LAN mrežu i zatim ih ruterom povezuje sa Internet-om pomoću jedne IP adrese. Ovi uređaji najčešće imaju ugrađen kablovski ili DSL modem



Slika 3.8.1 *Pristupna tačka (AP) i Ruter*

3.8.2 Računarske platforme

Notebook računari su verovatno najviše korišćena platforma za ispitivanje raspoloživih pristupnih tačaka (AP). Ručno prenosivi računari (PDA) omogućavaju veću pokretljivost i praktičniji su ako se ispitivanje raspoloživosti vrši pešice. Međutim instalacija softvera na ručno prenosivi računar kao što je na Slici (3.8.2.1), uključujući i Linux je dosta komplikovana. Za ratne vožnje (wardrives) obično se koristi notebook zato što daje odgovarajuću pokretljivost, a može se jednostavno priključiti na napajanje iz automobila.



Slika 3.8.2.1 *PDA sa Linux OS i internom bežičnom mrežnom karticom*

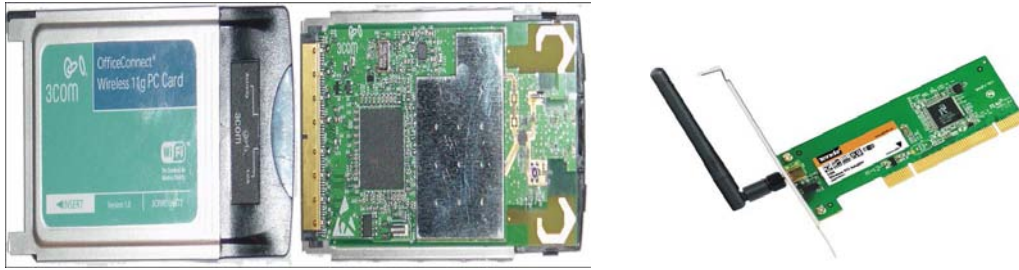


Slika 3.8.2.2 *Laptop sa internom bežičnom mrežnom karticom*

3.8.3 Bežična mrežna karta

Bežična mrežna karta je veza između računara i WLAN mreže, ili bežični mrežni interfejs. Ona ima hardverski implementiranu tehniku modulacije. Posao koji obavlja firmware koji se izvršava na kartici može da se obavi i u sklopu drajvera kartice u okviru operativnog sistema. Ali firmware je bolje rešenje, kako bi se otežala mogućnost da radio radi van licencirano odobrenog opsega i sa većom snagom. Kada se koristi spoljna antena, bežična mrežna kartica mora imati konektor za antenu. Izborom konektora, može se ograničiti izbor antena na one koje svojim pojačanjem neće prevazići jačinu signala koja je dozvoljena zakonom. Za ispitivanje bežične mreže, metodom ratne vožnje, bežična mrežna karta se postavlja u tzv. monitor mod. U tom modu, karta ne pokušava da se prijavi na bilo koju pristupnu tačku (AP). Ona

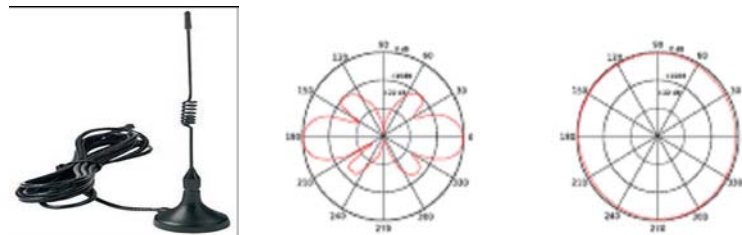
samo sakuplja pakete iz mreže i šalje ih operativnom sistemu. Novije mrežne karte mogu raditi u monitor modu, ali imaju ograničenje kada se radi o umetanju okvira.



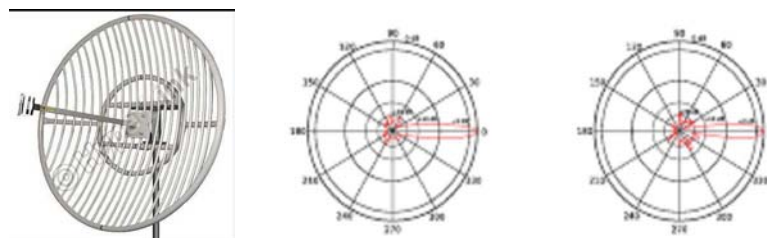
Slika 3.8.3 Bežična mrežna karta

3.8.4 Antena

Antena se koristi da usmeri ili ograniči signal koji se šalje iz bežične mrežne karte u određenom pravcu, zavisno od dijagrama zračenja. Isto tako se ponaša u slučaju prijema signala. Osnovna namena joj je da pojača signal u prijemu ili u predaji. Takođe se može koristiti za radiolokaciju. Antene se, po konstrukciji, mogu podeliti na dve osnovne vrste: usmerene i ne usmerene. Sa ne usmerenom antenom, kao što je na Slici (3.8.4.1), radio signal se prostire 360° oko antene, od čega je veliki deo nekoristan. Neusmerene antene se koriste za pristupne tačke, gde je dobro imati manje pojačanje. Na taj način se korisnici prijavljeni na AP navode da postave bolju antenu i tako je saobraćaj u oba smera brži. Usmerene antene koncentrišu radio signal, zavisno od konstrukcije, u uskom snopu od 180° do 7°, kao što je antena na Slici (3.8.4.2).



Slika 3.8.4.1 Dipol antena i njeni dijagrami zračenja, vertikalni i horizontalni



Slika 3.8.4.2 Usmerena antena i njeni dijagrami zračenja, vertikalni i horizontalni

3.8.5 Pojačavač

Pojačavač povećava izlaznu snagu signala u predajniku, i na taj način povećava domet signala. Standardna bežična mrežna karta ima snagu u predajniku od maksimalnih 100 mW. Pojačavač na Slici (3.8.5) ima izlaznu snagu od 1 W, signal je pojačan 30 dB. Ovakvi pojačivači se koriste i za ubacivanje paketa ili priključivanje na mrežu sa veće udaljenosti.



Slika 3.8.5 Pojačavač signala

4. Prikaz standarda IEEE 802.16

4.1 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) svetska intetoperabilnost za mikrotalasni pristup je telekomunikaciona tehnologija namenjena za obezbeđenje bežičnog prenosa podataka na veće udaljenosti na različite načine, od tačka-tačka povezivanja do potpuno mobilnog celularnog tipa pristupa. Zasnovan je na IEEE 802.16 standardu, koji se takođe naziva i Wireless MAN. Ime WiMAX je postalo od WiMAX Forum, koji je osnovan u Junu 2001 godine, Ovaj forum je osnovan od strane udruženih proizvođača opreme, da bi promovisao prilagođenost opreme i interoperabilnost standarda. Forum je definisao WiMAX kao tehnologiju na osnovi standarda IEEE 802.16 koja omogućava bežični širokopojasni pristup na milju od korisnika, kao alternativa kablovskom i DSL pristupu.

WiMAX podržava nekoliko sistema arhitekture, uključujući tačka-tačka, tačka-više tačaka, i opšta pokrivenost. WiMAX MAC (Media Access Control) podržava tačka-više tačaka i opšta pokrivenost servise po time shering sistemu opslužujući svakog od korisnika (Subscriber Station SS). Ako postoji samo jedan korisnik u mreži, WiMAX bazna stanica (BS) će komunicirati sa korisnikom na bazi tačka-tačka. U tom slučaju bazna stanica (BS) može da koristi usmerenu antenu kako bi povećala domet.

Bezbednosti u IEEE 802.16 je je posvećena posebna pažnja, tako da su pri pravljenju specifikacije angažovani specijalisti za tu oblast, kako bi se sveli na minimum nedostaci u metodama bezbednosti i opisanoj implementaciji. Aktuelna 802.16 (802.16-2005) bezbednosna arhitektura uključuje sledeće metode zaštite:

- Autentikacija i autorizacija. Procedura autentkacije je slična onoj koju ima WEP/WPA u pretplatničkoj stanici, kao laptop sa WiMAX kartom koja omogućava

pristup, mora prvo da dobije autorizaciju od bazne stanice pre nego što počne sa radom. 802.16 pruža mogućnost izbora između dva različita mehanizma za autentikaciju. RSA kriptografskog algoritma i EAP (*engl.* Extensible Authentication Protocol). EAP se preporučuje zato što su istraživanja ukazala na nedostatke koji postoje u RSA kod prethodnih 802.16 implementacija.

- Poverljivost i rukovanje kriptografskim ključevima PKM (*engl.* Privacy and Key Management), govori o rukovanju kriptografskim ključevima u WiMAX uređajima, ili tokom razmene ključeva između dva uređaja. Zaštita privatnih ključeva je vitalna za bezbednost WiMAX mreže i podataka na bežičnoj mreži. 802.16 nudi dve opcije, PKMv1 i PKMv2. PKM v2 je preporučena zbog uočenih nedostataka u PKM v1.

- Enkripcija podataka – 802.16e-2005 se može podestiti da koristi DES (*engl.* Data Encryption Standard) u CBC (*engl.* Cipher-Block Chaining) modu ili AES u nekom od brojnih modova. Generalno je mišljenje poznavaoa bezbednosti da AES pruža bolju zaštitu od DES-CBC i zato je preporučeni algoritam.

WiMAX QoS, WiMAX QoS se može dinamički prilagođavati za različite vrste saobraćaja. Podržava četiri tipa servisa:

1. UGS (*engl.* Unsolicited Grant Service) je pravljen da podržava real-time prenos podataka koji se sastoji od paketa fiksne dužine koji se pojavljuju u određenim vremenskim intervalima, kao što je T1/E1 i VoIP (Voice over IP).
2. Real-Time Polling Service (rtPS) je pravljen da podržava real-time prenos podataka koji se sastoji od paketa podataka promenljive dužine koji se pojavljuju u određenim vremenskim intervalima, kao što je MPEG video.
3. Non-Real-Time Polling Service (nrtPS) je pravljen da podržava prenos podataka sa tolerancijom kašnjenja pri tome su podaci u paketima promenljive dužine za šta je potrebna minimalna brzina prenosa, kao što je FTP.
4. Best Effort (BE) je pravljen da podržava tok podataka za koji nije definisan minimalni nivo servisa za prenos podataka proizvoljne dužine.

4.2 Razvoj IEEE 802.16 protokola

4.2.1 IEEE 802.16-2001

Prvi WiMAX standard koji je odobren od IEEE je bio 802.16-2001 standard. Odobren u Decembru 2001. god. Standard obezbeđuje fiksnu širokopoljasnu bežičnu mrežu kao tačka-tačka (point to point) ili kao tačka više tačaka (point to multipoint). Koristi modulaciju sa jednim nosiocem od 10 GHz do 66 GHz i za duplex u uplink i downlink kanalu podržava *engl.* Time Division Duplexing (TDD) i *engl.* Frequency Division Duplexing (FDD). Šeme modulacije koje se mogu koristiti su QPSK, 16QAM i 64QAM. Važnost korišćenja različitih modulacija i šema za korekciju greške je u tome što mreža postaje otporna na različite vremenske uslove, što dalje direktno utiče na QoS.

Bazna stanica (BS) kreira uplink i downlink mapu koja se deli svim tačkama u mreži. Ta mapa uključuje vremena predaje, trajanja i vrste modulacije. Na ovaj način je problem skrivene tačke pristupa eliminisan (hidden node). Korisnici obraćaju pažnju samo na baznu stanicu (BS) i nema potrebe za prijemom sa bilo koje druge tačke u mreži. Takođe pošto postoji tačan redosled rada na mreži, nema problema sa preuzetošću mreže.

Korisnik (Subscriber Station SS) može pregovarati o radnoj frekvenciji pri svakoj razmeni podataka, što obezbeđuje dovoljno fleksibilnosti u rasporedu pristupa korisnika baznoj stanici. Kao što je već navedeno, šeme modulacije su QPSK, 16QAM i 64QAM. Različite SS mogu koristiti različite modulacije, a takođe i različiti okviri podataka mogu biti sa različitom modulacijom. Tako se dolazi do šeme modulacije koja obezbeđuje stabilnost rada i kvalitet konekcije.

Tabela 4.2. IEEE 802.16 Brzine prenosa i vrste modulacije [4]

Širina kanala	Brzina prenosa simbola (Megasimbola u sekundi)	QPSK (2 bita po simbolu)	16-QAM (4 bita po simbolu)	64-QAM (6 bita po simbolu)
20 MHz	16	32 Mbps	64 Mbps	96 Mbps
25 MHz	20	40 Mbp	80 Mbps	120 Mbps
28 MHz	22.4	44.8 Mbps	89.6 Mbps	134.4 Mbps

Važna osobina 802.16-2001 je sposobnost da obezbedi različiti Quality of Service(QoS) na fizičkom nivou (PHY). Identifikator toka (*engl.* Service Flow ID) obavlja proveru QoS. Identifikator toka je je opisan parametrima QoS, koji daju specifikaciju za parametre kao što su maksimalno kašnjenje i dozvoljeni jitter. Identifikator toka može biti odaslan od BS ili od SS.

802.16-2001 radi samo u uslovima direktne vidljivosti (*engl.* Line of Sight LOS), sa opremom korisnika koja je locirana na otvorenom prostoru.

4.2.2 IEEE 802.16a-2003

Sledeći standard odobren u januaru 2003. god. je 802.16-2003. Ima dosta izmena u odnosu na 802.16-2001, a najznačajnija je dodatak podrške za 2-11GHz licencirane opsege. Veoma značajan je dodatak podrške za komunikaciju bez direktne vidljivosti (None Line of Sight), koja nije bila moguća pre dodavanja podrške za rad u opsezima 2 – 11 GHz. Na ovaj način se proširila geografska pokrivenost ovom mrežom. Takođe ima izmena u šemi modulacije. Dodatak modulaciji sa jednim nosiocem, QPSK, 16QAM, 64QAM, *engl.* Orthogonal Frequency Division Multiplexing (OFDM) je jedna od opcija ovog standarda. U ovom standardu je za opsege 2-11 GHz je dodat Orthogonal Frequency Division Multiplexing (OFDMA). Značajna novina za bezbednost je da je u 802.16-2001 većina opcija koje se odnose na zaštitu podataka bila opciona, a sada su te opcije obavezne. Takođe se mogućnosti zaštite podataka koriste za autentikaciju pošiljaoca MAC poruka.

802.16a dodaje podršku za ćelijske mreže. To znači da saobraćaj može biti rutiran od jedne SS do druge. Zbog toga je uneto niz izmena u MAC nivou da bi se prenosili podaci od jedne SS koja nije vidljiva za BS, preko druge SS koja je deo ćelijske mreže.

4.2.3 IEEE 802.16c-2002

U Decembru 2002.god. je usvojena izmena standarda pod nazivim IEEE 802.16c-2002. U toj reviziji protokola, dodat je detaljni opis opsega 10-66 GHz, i takođe su ispravljene neke greške uočene u prethodnim verzijama standarda.

4.2.4 IEEE 802.16-2004

Sve prethodne verzije standarda 802.16 su ovde objedinjene i kreiran je novi standard. Ovaj standard je poznat kao 802.16-2004 ili 802.16-Revd. To je zato što je u početku ova verzija standarda objavljena kao revizija standarda pod imenom 802.16-REVD, ali su izmene bile suštinske pa je standard reizdat pod imenom 802.16-2004 i to u Septembru 2004.god. U ovoj verziji je ceo standard ratifikovan i odobren.

4.2.5 IEEE 802.16e i kasnije verzije

U ovoj verziji standarda je dodata podrška za mobilne korisničke stanice. 802.16e je prošao kroz dosta draft verzija. Zamisao je da se uključi Advanced Encryption System (AES) funkcionalnost. Provajderi su predložili WiMAX Forumu da ovu funkcionalnost (AES) uvede kao obaveznu za WiMAX sertifikaciju. Kao standard ova verzija još nije ratifikovana, pa će do tada biti verovatno još izmena. Drugi komiteti u okviru IEEE rade na novim verzijama protokola, kao što su 802.16f i 802.16g. Novine u ovim protokolima se odnose pre svega na planiranje mrežnog upravljanja (*engl.* Network Management Plane).

4.3 Odnos IEEE 802.16 i IEEE 802.11

WiMAX nije suprotnosti sa WLAN sistemom, ti sistemi su komplementarni. Zbog istog kontrolera logičke veze koji je standardizovan (IEEE 802.2) kao i kod drugih LAN i WAN mreža, WiMAX može biti premošten i povezan sa tim mrežama. WiMAX je takođe komplementaran sa žičnim ethernetom IEEE 802.3, token ringom IEEE 802.5, kao i sa ostalim ne-IEEE standardnim mrežama koje koriste isti kontroler logičke veze.

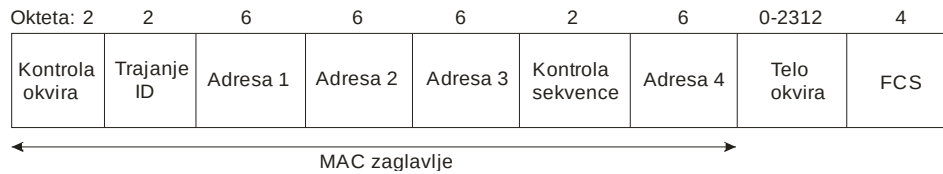
WiMAX koristi licencirani opseg da bi ostvario tačka-tačka konekciju prema internetu od nekog ISP (internet service provider) do krajnjeg korisnika. Različiti 802.16 standardi omogućavaju različite vrste pristupa, od portabl (slično celularnom telefonu) do fiksnog (kao alternativa žičnoj mreži, gde je krajnji korisnik na stalnoj lokaciji). WiMAX je prvenstveno razvijan za bežičnu mrežu tipa metropolitan area network (WMAN), sa dometom od nekoliko kilometara. WLAN koristi nelicencirani opseg, i prvenstveno je razvijan za lokalne bežične mreže dometa do 100 m.

WiMAX ima potpuno različit Quality of Service (QoS) mehanizme. Koristi mehanizam zasnovan na konekcijama između bazne stanice i korisničkog uređaja. Svaka konekcija se zasniva na specifičnom algoritmu raspodele. WLAN ima QoS mehanizam sličan žičnom Ethernetu, gde paketi imaju različite prioritete, u zavisnosti od oznake koju nose. Na primer VoIP će imati prioritet u odnosu na web pretraživač. WLAN radi na MAC CSMA/CA protokolu, koji je nezavistan od konekcije, dok WiMAX radi na konekcijski orjentisanom MAC.

Bez obzira na razlike, oba 802.11 i 802.16 rade u P2P i ad-hoc mreži, gde krajnji korisnik komunicira sa korisnicima ili serverima u drugoj lokalnoj mreži koristeći pristupnu tačku (AP) ili baznu stanicu.

5. Načini identifikacije WLAN mreža

5.1 Analiza WLAN mrežnog saobraćaja



Slika 5.1 MAC format okvira

Svaki paket prenet kroz WLAN mrežu sadrži bite informacije koji se koriste za prosleđivanje paketa kroz različite nivoe OSI modela komunikacije. Iako paketi mogu biti kriptovani u WLAN mrežama, oni uvek imaju zaglavlja sa otvorenim tekstom. Kao što je ovde prikazano, zaglavlja imaju određenu vrednost za svakog ko analizira mrežu. Čitav MAC okvir prikazan na Slici 5.1 je lako dostupan za standardni korisnički alat u Linuxu (jednostavnim postavljanjem interfejsa u monitor mod). Svi paketi u WLAN mreži su u skladu sa MAC formatom okvira podataka. Polje Frame Control pokazuje koji tip podataka MAC okvir prenosi. Postoji tri osnovna tipa paketa i mnogo različitih podtipova. Tipovi paketa su podebljani i slede njihovi podtipovi.

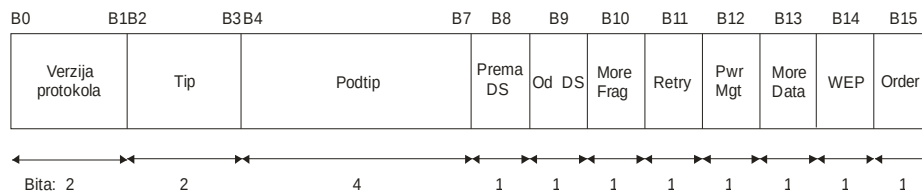
1. **Management:** Association, Probe, Beacon, i Authentication.

2. **Control:** RTS, CTS, PS'Poll, ACK, CF-Ack/Poll.

3. **Data:** Data, Data+CF-Ack/Poll i Null-function.

U sledećem odeljku će biti razmotrena samo neka polja u okvirima koja su interesantna.

5.1.1 Informacije od svih okvira



Slika 5.1.1 Polja kontrolnog okvira

Slika 5.1.1 pokazuje polja kontrolnog okvira. Iz njega se mogu dobiti sledeće informacije.

Mreža je deo WDS: Prema DS = 1 i Od DS = 1.

Mreža je u ad-hoc modu: Prema DS = 0 i Od DS = 0; i Tip = Data.

Mreža je u infrastrukturnom modu: Prema DS = 1 ili Od DS = 1 i Tip = Data.

Dodatno, svaki prikupljeni okvir nosi podatak o jačini signala izmeren u radio prijemniku. Kombinovanjem tih podataka sa koordinatama iz GPS prijemnika, moguće je predvideti:

Domet mreže: Gde se sve mogu primiti okviri poslati od pristupne tačke.

Lokacija pristupne tačke: Triangulacijom i merenjem jačine signala okvira odaslanih sa pristupne tačke a primljenih na više različitih lokacija.

Lokacija klijenta: Ista procedura kao kod lociranja pristupne tačke, samo se prate okviri poslati od odabranog klijenta.

Građevine, razne prepreke i višestruke putanje smanjuju preciznost estimacija. Pokretni klijenti ili pristupne tačke nisu deo ovakvih procedura i unosili bi prevelike greške pri estimacijama.

5.1.2 Informacije od okvira podataka

WEP ili WPA kriptovanje: B14 = 1

Tip payloada: Na primer ako je odredišna adresa broadcast adresa, i veličina payloada 68 bajta, onda je veoma verovatno da je to Address Resolution Protocol (ARP) zahtev.

Mreža je Bridge: Samo paketi podataka sa karakteristikama Prema DS=1 i Od DS=1, će biti prenošeni.

MAC adrese pristupne tačke: u MAC zaglavlju: Adrese 1,2 ili 3.

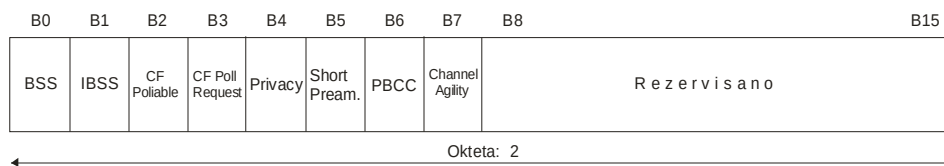
MAC adrese mobilnih klijenata: u MAC zaglavlju: Adrese 1,2,3 ili 4.

MAC adrese stanica na žičnoj mreži: u MAC zaglavlju: Adrese 1,2,3 ili 4.

Sledeća značajna stavka je vrednost IV. On se šalje sa svakim okvirom podataka u mreži sa kriptovanim prenosom podataka. IV i njegova upotreba pružaju mogućnost zaštite od okvira koji su ranije prikupljeni prisluškivanjem saobraćaja na mreži ako je šema kriptovanja WEP ili WPA. Kada se porede okviri poslati sa iste adrese, IV je različit za svaki poslati okvir u slučaju WEP kriptovanja. WPA ima iste vrednosti u 3 bajta IV polja, a samo Extended Initialisation Vector (EIV) menja vrednosti, tj nema duplikata. Payload u data okviru može biti ARP, Internet Protocol (IP), Internet Control Message Protocol (ICMP), Transport Control Protocol (TCP), Universal Datagram Protocol (UDP) itd. Svi oni su pridodati Subnetwork Access Protocol (SNAP) hederima koji su prilagođeni za ethernet. Razni tipovi paketa i poznavanje njihove strukture se koriste za napade.

5.1.3 Informacije od upravljačkih okvira

Neki od upravljačkih okvira nose u sebi puno parametara o mreži. Beacon okvir je jedan od njih. Pristupna tačka emituje beacon okvire kako bi informisala korisnike da je raspoloživa. Ti okviri nose u sebi dovoljno informacija za klijente, kako bi mogli da se pridruže mreži. Međutim upravljački okviri se striktno koriste za administriranje priključenja na mrežu. Oni ne šalju nikakve podatke sa aplikativnog nivoa. Polje capability je deo beacon okvira, a njegova struktura je prikazana na Slici 5.1.3.



Slika 5.1.3 Capability polje u beacon okviru

Iz polja capability mogu se izdvojiti sledeće korisne informacije:

Mreža je u infrastrukturnom modu: B0 = 1 i B1 = 0.

Mreža je u ad-hoc modu: B0 = 0 i B1 = 1.

WEP je uključen: B4 = 1.

Ostala polja koja se mogu izdvojiti iz tela okvira u beacon okviru su:

Beacon interval: to je vreme između slanja beacon okvira (obično $100 \cdot 1024 \mu s = 100$ ms).

Service Set Identity (SSID): string od maksimalno 32 bita karaktera koji daju ljudima čitljivu informaciju o WLAN mreži. Takođe služi i za grupisanje više pristupnih tačaka kako bi se formirala mreža pristupnih tačaka koje rade zajedno.

Podržavane brzine prenosa: lista podržavanih brzina prenosa u mreži.

Dodatne brzine prenosa: ostale podržavane brzine prenosa.

Kanali: broj kanala na kojem radi mreža.

Basic Service Set Identifier (BSSID) pokazuje informaciju o proizvođaču pristupne tačke. Prvih 16 bita u BSSID se može protumačiti na osnovu baze podataka koju održava IEEE [5].

5.1.4 Zaključak

Informacije do kojih se može doći pasivnim prikupljanjem uobičajenog WLAN saobraćaja su prikazane u Tabeli 5.1.4.

Podaci koji se mogu dobiti	Vrsta okvira sa podacima	Broj potrebnih okvira
WDS	Data	1 okvir
Ad-hoc / Infrastruktura	Beacon / Probe / Data	1 okvir
Domet mreže	Bilo koji	3 okvira i GPS lokacija
Lokacija AP ili klijenta	Bilo koji	3 okvira i GPS lokacija
WEP	Beacon / Probe / Data	1 okvir
WPA	Beacon / Probe / Data	1 okvir
SSID	Beacon / Probe	1 okvir
MAC adresa AP-a	Bilo koji	1 okvir
MAC adresa klijenta	Probe request / Data	1 okvir
MAC adresa u žičnoj mreži	Data	1 okvir
Sadržaj podataka	Data	Prema proceni

Tabela 5.1.4 Informacije koje se dobijaju analizom okvira podataka u WLAN

6. Softverski alati za analizu bežičnih mreža

6.1 Kismet

Kismet je alat otvorenog koda (open source). Prvenstveno je namenjen za detekciju pristupnih tačaka i prikupljanje raznih informacija o pristupnim tačkama. To su informacije poput identifikatora mreže, jačine signala, zaštite koja se koristi, pa čak i informacije o klijentima koji su spojeni na dotičnu pristupnu tačku. Kismet takođe čuva dosta podataka u dnevničkim datotekama (*engl. log files*) što ga čini vrlo atraktivnim. Za razliku od nekih drugih alata, Kismet ne samo da detektuje pristupne tačke, već beleži kompletni zapis svih uhvaćenih paketa. Takvi zapisi mogu se naknadno iskoristiti pomoću drugih alata (*Ethereal, Wireshark*) za dalju analizu.

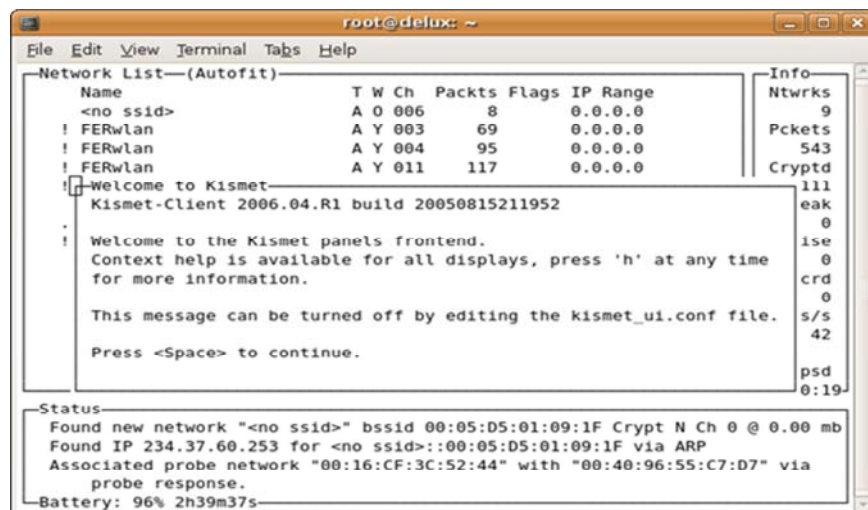
Jedna od najvećih prednosti je mogućnost rada u monitor modu što omogućava pasivno istraživanje i detekciju bežičnih mreža koje ne emituju svoj identifikator. Za razliku od aktivnog istraživanja, pasivno ne emituje nikakav signal. Umesto toga pasivni programi osluškuju radio frekvenciju za bilo koji bežični saobraćaj koji je u dometu signala bežične kartice. Ova prednost čini ga aktuelnijim od njegovih konkurenata kao na primer *NetStumbler* alata za Windowse.

Konfigurisanje Kismet alata

Uz pretpostavku da je *Kismet* alat uspešno instaliran potrebno je podesiti njegovu konfiguraciju kroz dve konfiguracione datoteke: *kismet.conf* i *kismet_ui.conf*. Uobičajeno je da se te datoteke kod većine Linux distribucija nalaze u */etc/kismet* direktorijumu.

Konfiguraciona datoteka *kismet_ui.conf*

Datoteka *kismet_ui.conf* sadrži opcije o korisničkom ekranu Kismet alata. Za većinu stvari dovoljno je ostaviti već predefinisane parametre, osim ukoliko se želi izmeniti izgled korisničkog ekrana. Prilikom pokretanja Kismet alata obično se pojavljuje pozdravna poruka (*Slika 6.1.1*).



Slika 6.1.1 Pozdravna poruka Kismet alata

Njeno pojavljivanje moguće je isključiti u *kismet_ui.conf* datoteci, postavljanjem parametra varijable *showintro* u *false*. *showintro=false*.

U ovoj datoteci takođe se može promeniti čitav niz drugih parametara kao što su boja ekrana, zvučna upozorenja, količina prikazanih informacija itd.

Konfiguraciona datoteka kismet.conf

Datoteka *kismet.conf* je konfiguraciona datoteka koja sadrži važne konfiguracione parametre kao što su parametri potrebni za ispravnu komunikaciju *Kismet* alata i bežične kartice, komunikaciju sa GPS uređajem, postavljanja privilegija rada, korišćenja određenih kanala, generisanja dnevnih datoteka itd.

Kako bi *Kismet* ispravno funkcionisao, pre prvog pokretanja potrebno je editovati ovu datoteku i ispravno postaviti informacije o okruženju i hardveru.

Za sigurniji rad *Kismet* alata potrebno je izmeniti *suiduser* varijablu. Ova varijabla definiše korisnika pod čijim privilegijama će *Kismet* raditi nakon što "prebaci" bežičnu karticu u monitor način rada.

```
# User to setid to (should be your normal user)
suiduser=roamer
```

Zatim je potrebno postaviti *source* varijablu. To je varijabla koja definše koji tip pokretačkog programa (*engl. driver*) i kartice sistem koristi, kao i okruženje na kojem je postavljena kartica. Sljedeći primer definiše izvor koji koristi *HostAP* pokretački program, karticu konfigurisanu na okruženju *wlan0*. Treći parametar varijable *source*, može biti postavljen na bilo koju vrednost. To je obično ime koje identifikuje taj izvor, naprimer *wlan*. *source=hostap,wlan0,wlan*

Ovde je nekoliko uobičajenih primera izvora za različite bežične kartice i pokretačke programe:

```
# Source line for Intel Pro Wireless 2200
source=ipw2200,eth0,ipw2200source
# Source line for wlan-ng Prism2 driver
source=prism2,wlan0,prism
# Source line for Cisco (dependent on Cisco driver used)
source=cisco,eth0,cisco
# Alternate Source line for Cisco (dependent on Cisco driver used)
source=cisco_cvs,eth1:wifi0,ciscocvs
# Source line for Hermes based cards (Orinoco)
source=orinoco,eth0,orinocosource
```

Kismet takođe nudi mogućnost korišćenja više izvora paralelno. Sve dok se koristi jedan izvor nije potrebno menjati vrednost varijable *enablesources* koja je predefinisana sa znakom komentara. Tek u slučaju korišćenja više izvora potrebno je obrisati znak komentara ispred dotične varijable i navesti listu izvora koju će *Kismet* koristiti.

Kismet predefinisano "skače" kroz kanale, što mu omogućuje da pronalazi pristupne tačke koje rade na različitim kanalima pojasa bežične mreže. To se kontroliše putem varijable *channelhop*. Sve dok nije potrebna detekcija pristupnih tačaka na samo određenom kanalu potrebno je postaviti ovu varijablu u *true*.

```
# Do we channelhop
channelhop=true
```

Tek ukoliko je poželjno da se detekcija obavlja na jednom kanalu treba postaviti varijablu `channelhop` u `flase` te postaviti parametar inicijalnog kanala u soruce varijabli. Na primer kako bi se detektovale pristupne tačke na kanalu 8:

```
source=hostap,wlan0,wlan,8
channelhop=false
```

Sledeća varijabla koju je moguće podešavati je brzina kanala. Ona određuje kroz koliko kanala će *Kismet* prolaziti unutar jedne sekunde. Predefinisano je postavljena na tri kanala u sekundi što je u većini slučajeva prihvatljivo. Da bi se povećala brzina kojom *Kismet* skače kroz kanale potrebno je povećati ovaj broj, odnosno smanjiti u slučaju da se želi usporiti brzina skakanja. Potrebno je imati na umu da je skakanjem kroz kanale moguć gubitak nekih podataka koji prolaze bežičnom mrežom.

```
# How many channels per second do we hop? (1-10)
# The following option scans each channel for 1/5 of a second
# channelvelocity=5
# The following option scans each channel for 1/2 of a second
channelvelocity=2
```

Kismet nudi mogućnost povezivanja s GPS uređajem za hvatanje koordinata položaja pristupnih tačaka. Postavke za korišćenje GPS-a nameštaju se pomoću varijabli `gps` i `gpshost`. Ukoliko je GPS aktiviran potrebno je `gps` varijablu postaviti u `true`. Varijabla `gpshost` određuje da li je *GPSd* pozadinski proces (*engl. daemon*) pokrenut na lokalnom ili nekom udaljenom računaru.

```
# Do we have a GPS?
gps=true
# Host:port that GPSD is running on. This can be localhost OR remote!
gpshost=localhost:2947
```

Sledeća opcija koju vredi pogledati je interval u kojem se zapisuju detektovane informacije u dnevničke datoteke. Parametar ove varijable je predefinisano postavljen na pet minuta. Iz razloga što je moguće da sistem ili aplikacija padnu preporučuje se ovaj parametar smanjiti na približno jedan minut.

```
# How often (in seconds) do we write all our data files
# (0 to disable)
writeinterval=60
```

Kismet generiše vrlo opsežan set dnevničkih datoteka (*Tabela 6.1*).

Dump	"Sirovi" format uhvaćenih podataka koji se mogu pregledati pomoću <i>Ethereal</i> alata ili drugih alata za analizu paketa.
-------------	---

Network	Tekstualna datoteka koja sadrži popis detektovanih pristupnih tačaka i informacija o njima.
CSV	Zarezom odvojen popis detektovanih pristupnih tačaka i informacija o njima.
XML	Detektovane mreže zapisane u XML formatu. Ovakav dnevnički zapis koristan je za uključivanje ovih zapisa u okviru drugih aplikacija.
Weak	Detektovani paketi ranjivog inicijalnog vektora (IV) zapisani u formatu pogodnom za dalju analizu pomoću <i>AirSnort</i> alata.
Cisco	Dnevnički zapis detektovanih informacija Cisco protokola koji šalju Cisco uređaji.
GPS	Dnevnički zapis GPS koordinata detektovanih pristupnih tačaka.

Tabela 6.1.1 Kismet dnevničke datoteke

Varijabla *logtype* određuje koje će sve dnevničke zapise Kismet generisati. Predefinisana opcija je prihvatljiva (*dump*, *network*, *csv*, *xml*, *weak*, *cisco*, i *gps*) iako ponekad nisu potrebni svi ti zapisi. Minimalna osnova koju je potrebno osigurati u većini slučajeva je obično *dump*, *network* i *gps* zapisi.

```
logtypes=dump,network,gps
```

Varijabla *logdefault* određuje tekst koji dolazi kao prefiks imena datoteke dnevničkog zapisa. Kismet zapisuje datoteke u formatu *[logdefault]-[date]-[sequence-number].[filetype]*. Na prmer ako je *logdefault* varijabla postavljena na *Roamer*, tada će *gps* dnevnički zapis treće sesije određenog dana biti imenovan kao *Roamer-Apr-14-2009-3.gps*. Ova opcija može biti korisna u slučaju sortiranja rezultata ukoliko se pretražuje više područja istog dana.

```
# Default log title
logdefault=MyCustomer
```

Još jedna varijabla koju je moguće menjati kroz *kismet.conf* datoteku je *logtemplate*. Ovom varijablom se kontroliše lokacija na koju se zapisuju dnevničke datoteke i njihov format. Uobičajeno je u */var/log/kismet/* direktorijumu.

Ukoliko se ova varijabla ne promeni, dnevnički zapis će biti kreiran na predefinisanim način, sa predefinisanim naslovom, unutar direktorijuma gde je *Kismet* pokrenut. Postoji sedam parametara koji su povezani s varijablom *logtemplate* (Tabela 6.1.2).

%n	Teks postavljen u varijabli <i>logdefault</i> .
%d	Trenutni datum u formatu Mesec-Dan-Godina (MM-DD-GGGG).
%D	Trenutni datum u formatu GGGGMMDD.
%t	Vreme kad je dnevnički zapis pokrenut.

%i	Inkrementalni broj dnevničkog zapisa (npr. 1 za prvi zapis u danu, 2 za drugi, itd.).
%l	Tip dnevničkog zapisa.
%h	Putanja korisničkog direktorijuma.

Tabela 6.1.2 Parametri varijable logtemplate

Na primer, ako je potrebno dnevničke zapise zapisivati u različite direktorijume prema tipu zapisa, pa ih smestiti unutar direktorijuma *PenTest* potrebno je postaviti varijablu *logtemplate* na sledeći način:

```
logtemplate=PenTest/%l/%n-%d-%i
```

Uz pretpostavku da je varijabla *logtypes* postavljena na *dump*, *network* i *gps* treba kreirati direktorijum *PenTest* sa tri poddirektorijuma: *dump*, *network* i *gps*.

Pokretanje Kismet alata

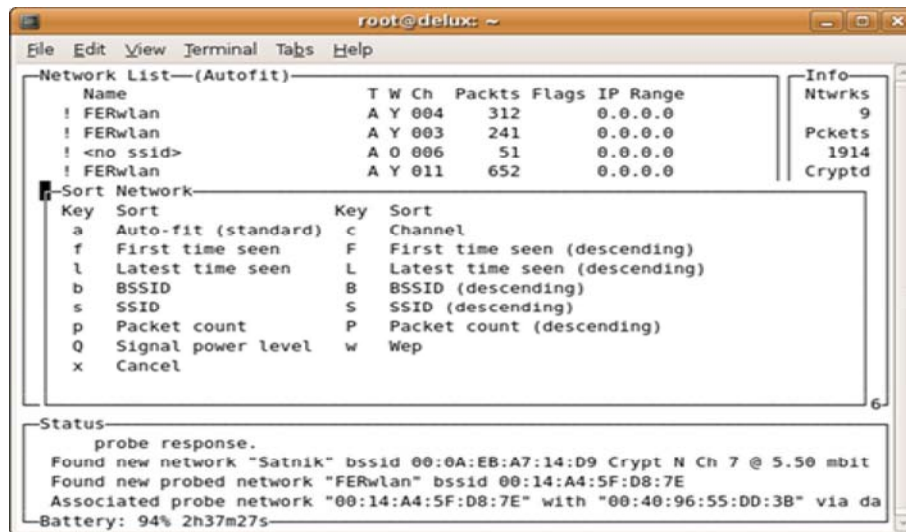
Pretpostavljajući da je *Kismet* postavljen u putanji operacionog sistema (*engl. path*), alat se pokreće jednostavnim upisivanjem *kismet* u komandnoj liniji. Može se dogoditi da prilikom pokretanja ne uspe postavljanje identifikacione datoteke procesa (*engl. pidfile*), ukoliko aplikaciju pokreće običan korisnik. To je zato što obični korisnik najčešće nema prava pisanja u direktorijum */var/run*. Postoje dva načina za rešenje tog problema tj. za uspešno pokretanje alata. Jedan od načina je promenom lokacije zapisivanja identifikacione datoteke u *kismet.conf* datoteci.

```
# Where do we store the pid file of the server?  
piddir=/home/roamer
```

Ako je prilikom konfigurisanja *Kismet* alata postavljena *suiduser* varijabla u *kismet.conf* datoteci jednostavnije je pokrenuti *Kismet* alat kao *root* korisnik. To je korisnik koji ima sve dozvole kao i dozvolu za zapisivanje identifikacione datoteke. Nakon pokretanja *Kismet* će prebaciti privilegije na korisnika definisanog *suiduser* varijablom, i na taj način izbeći potencijalne bezbednosne propuste rada aplikacije pod *root* ovlašćenjima.

Pored mogućnosti identifikovanja pristupnih tačaka, *Kismet* ima i vrlo praktičan korisnički meni. Kroz takav meni dostupna je velika količina informacija o svakoj pristupnoj tački koja je identifikovana. Neposredno je raspoloživa informacija o identifikatoru bežične mreže kao i neke druge uobičajene informacije poput tipa mreže, tipa enkripcije, kanala pristupne tačke itd. Ako se žele dobiti detaljnije dostupne informacije o otkrivenoj bežičnoj mreži treba se bliže upoznati s ostalim opcijama koje nudi *Kismet* meni.

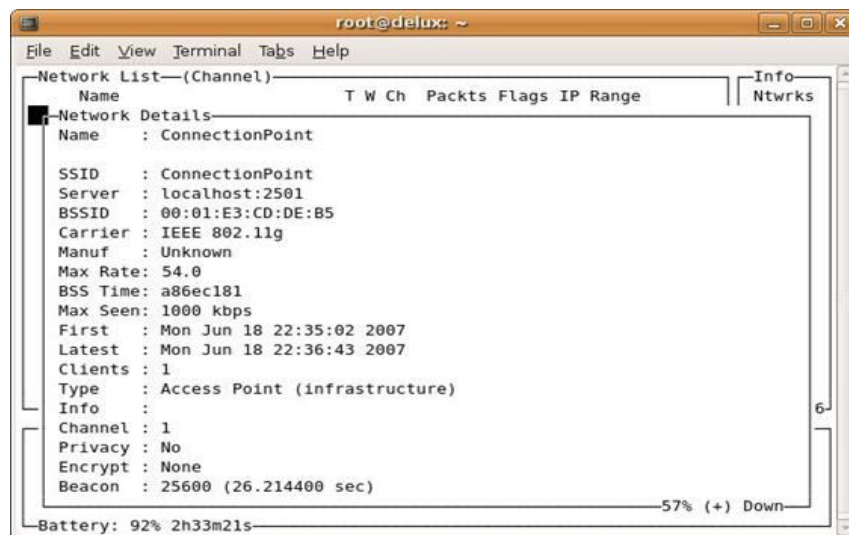
Jedna od vrlo korisnih opcija je opcija sortiranja. Standardno je *Kismet* postavljen u automatski način sortiranja. U tom načinu sortiranja ne može se dobiti mnogo informacija o različitim pristupnim tačkama. Kako bi se promenio način sortiranja, potrebno je pritisnuti taster "s" nakon čega će se pojaviti meni sa mogućim načinima sortiranja (Slika 6.1.3).



Slika 6.1.3 Opcije sortiranja Kismet alata

Postoji četrnaest različitih načina za izbor koji se koriste u zavisnosti od potreba ispitivanja. Na primer, ako su ispitivaču potrebne informacije o pristupnim tačkama specifičnog identifikacionog imena, treba odabrati opciju s kako bi se pristupne tačke sortirale prema identifikatoru.

Jednom kad je odabran metod sortiranja, može se početi s daljim ispitivanjima dodatnih informacija o pojedinoj mreži. Za dodatne informacije treba se postaviti na zapis željene pristupne tačke (korišćenjem navigacionih strelica) i pritisnuti taster "Enter" (Slika 6.1.4).

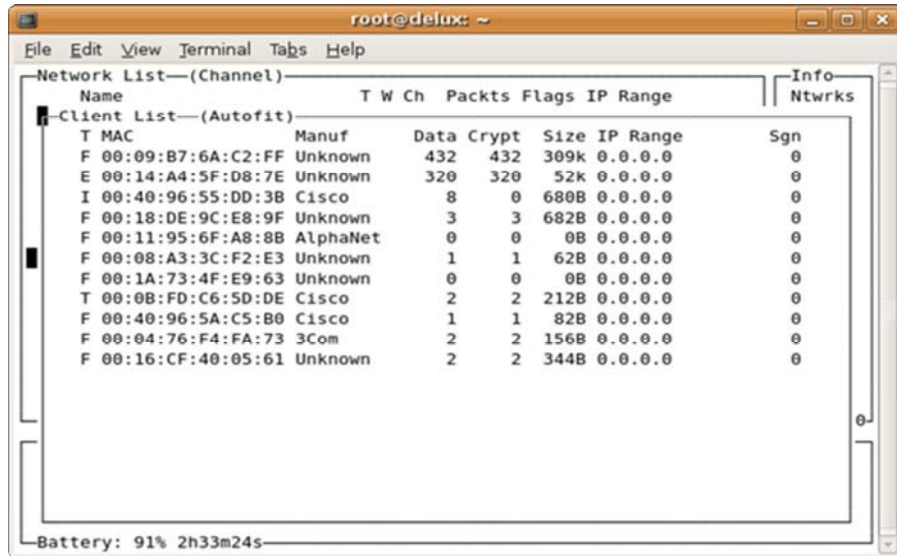


Slika 6.1.4 Detalji o odabranoj bežičnoj mreži

Takav izbor daje dodatne informacije. Osim klasičnog identifikatora (SSID) dostupna je npr. i informacija o MAC adresi pristupne tačke (osnovni identifikator, BSSID). Na osnovu maksimalne brzine prenosa koja u ovom primeru iznosi 54.0 dostupan je i

podatak da se radi o 802.11g pristupnoj tački. U nekim slučajevima Kismet će otkriti i tip proizvođača pristupne tačke. Takođe je zabeleženo i vreme kada je pristupna tačka viđena, kanal na kojem radi kao i broj aktivnih klijenata. Kroz ovaj pogled dostupna je i informacija o načinu rada pristupne tačke. Uz još mnoge druge informacije koje Kismet nudi važno je takođe spomenuti da Kismet detektuje i tip zaštite koju koriste pristupne tačke. Da bi se vratili u glavni meni potrebno je pritisnuti taster "q" za izlaz.

Korisna informacija, koju takođe možemo dobiti pomoću Kismet, alata je popis klijenata koji su spojeni na pristupnu tačku. Do takve informacije se dolazi selektovanjem određene pristupne tačke i pritiskom tastera "c" (Slika 6.1.5).



The screenshot shows a terminal window titled 'root@delux: ~' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The main window displays the 'Client List (Autofit)' table. The table has columns: T, MAC, Manuf, Data, Crypt, Size, IP Range, and Sgn. The data is as follows:

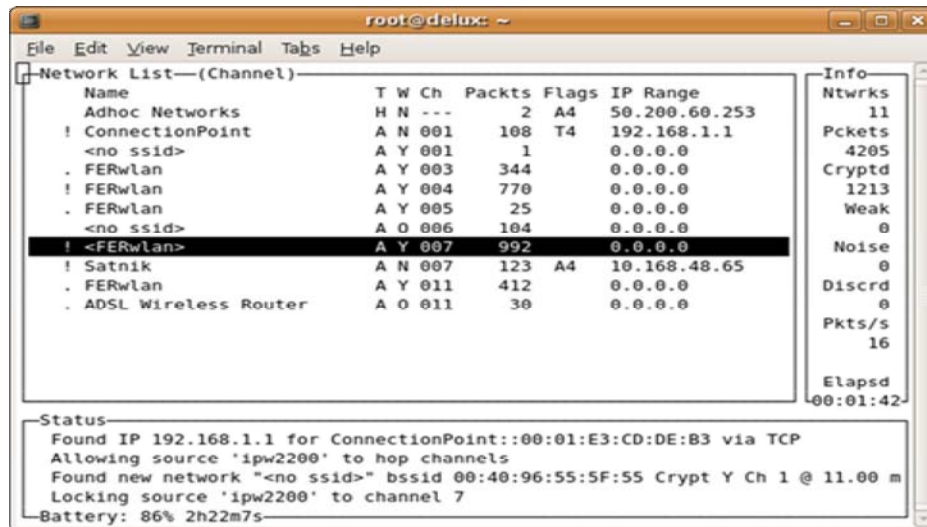
T	MAC	Manuf	Data	Crypt	Size	IP Range	Sgn
F	00:09:B7:6A:C2:FF	Unknown	432	432	309k	0.0.0.0	0
E	00:14:A4:5F:D8:7E	Unknown	320	320	52k	0.0.0.0	0
I	00:40:96:55:DD:3B	Cisco	8	0	680B	0.0.0.0	0
F	00:18:DE:9C:E8:9F	Unknown	3	3	682B	0.0.0.0	0
F	00:11:95:6F:A8:8B	AlphaNet	0	0	0B	0.0.0.0	0
F	00:08:A3:3C:F2:E3	Unknown	1	1	62B	0.0.0.0	0
F	00:1A:73:4F:E9:63	Unknown	0	0	0B	0.0.0.0	0
T	00:0B:FD:C6:5D:DE	Cisco	2	2	212B	0.0.0.0	0
F	00:40:96:5A:C5:B0	Cisco	1	1	82B	0.0.0.0	0
F	00:04:76:F4:FA:73	3Com	2	2	156B	0.0.0.0	0
F	00:16:CF:40:05:61	Unknown	2	2	344B	0.0.0.0	0

The terminal window also shows a 'Network List (Channel)' section at the top and a 'Battery: 91% 2h33m24s' status bar at the bottom.

Slika 6.1.5 Lista klijenata spojenih na odabranu pristupnu tačku

U pogledu liste klijenata dostupna je informacija o MAC adresi svakog klijenta, a u određenim slučajevima takođe je moguće dobiti informaciju o tipu kartice koju dotični klijent koristi. Identifikuje se i broj paketa koje je Kismet uhvatio i broj paketa koji su kriptovani. Kismet ima i mogućnost identifikovanja IP adrese klijenata i snage njihovog signala. Povratak u glavni meni takođe se obavlja pritiskom tastera "q".

Ponekad je korisno prikupljati informacije o pristupnoj tački samo na određenom kanalu. Kako bi onemogućili skakanje na druge kanale i prikupljali podatke na samo jednom kanalu, potrebno je odabrati željenu pristupnu tačku i pritisnuti kombinaciju tastera *Shift + L* (Slika 6.1.6). Na taj način prikupljaće se samo podaci na kanalu odabrane pristupne tačke. Za povratak potrebno je pritisnuti kombinaciju tastera *Shift + H*.



Slika 6.1.6 Prikupljanje podataka sa određenog kanala

Kismet takođe ima i robustan sistem pomoći. Tako su dodatne informacije o svakoj opciji dostupne pritiskom tastera "h". Kismet daje i statistiku kao što je distribucija upotrebe pojedinih kanala i procenat mreža koje koriste WEP i WPA.

Neke pristupne tačke rade sa onemogućenim broadcastom svojih SSID u beacon okvirima ili probe responses. Sakrivanje SSID se koristi da bi se povećala bezbednost, pošto samo oni klijenti koji znaju SSID neke AP su u mogućnosti da se pridruže na nju. Ali zato što se upravljački okviri šalju kao otvoreni tekst, SSID se takođe šalje kao otvoreni tekst kada se „autentikovani“ korisnik (koji zna SSID date AP) pridružuje na AP. Kismet koristi taj paket da prikaže postojanje AP i označava je kao „skrivenu“ u WLAN mreži.

Postoji verzija Kismet za MS Windows pod nazivom kiswin32-2005-08-R1-GPSD.

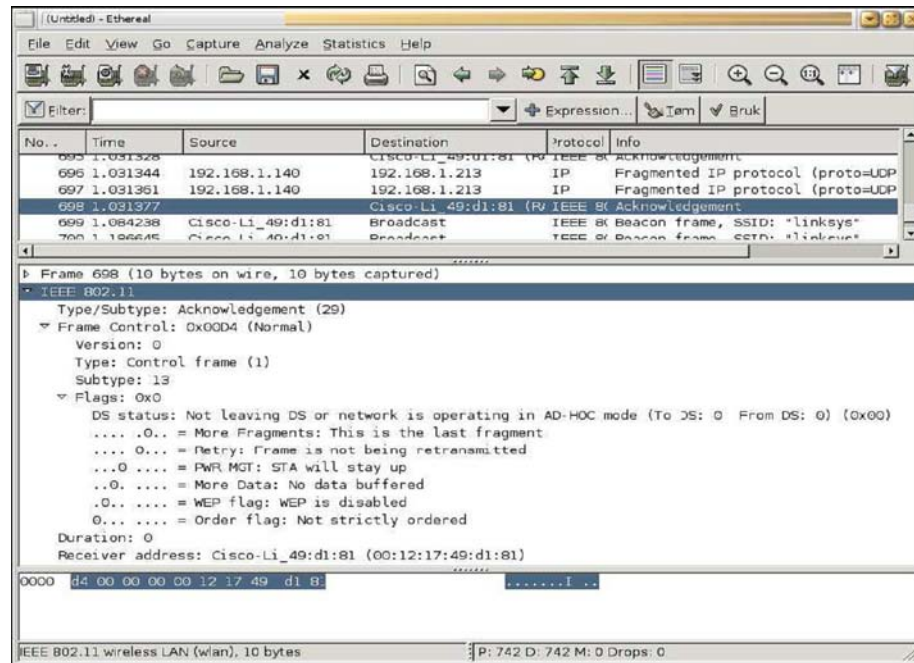
6.2 TCPCDump

TCP Dump je odličan alat za praćenje i filtriranje komunikacije u realnom vremenu. Na Slici 6.2.1 TCPCDump sluša jedan pridruženi WLAN link zbog ARP paketa. U svakoj liniji posle prve tri je opis uhvaćenog paketa. Prvi uhvaćeni paket je ARP zahtev, primljen u 11h 58 min 1.704626 sekundi. Zahtev je upućen nekome ko ima IP adresu 192.168.1.2 i treba da pošalje odgovor na IP adresu 192.168.1.213. Zahtev je ostao bez odgovora što znači da niko u mreži nema IP adresu 192.168.1.2. Kasniji zahtev prema 192.168.1.213 je dobio odgovor od mrežne karte koja ima MAC adresu 00:0e:35:a3:0f:56 i ta karta ima IP adresu 192.168.1.213

```
# tcpdump -i eth2 arp
tcpdump : verbose output suppressed , use -v or -vv for full protocol decode
listening on eth2 , link - type EN10MB ( Ethernet ), capture size 96 bytes
11:58:01.704626 arp who - has 192.168.1.2 tell 192.168.1.213
11:58:02.704491 arp who - has 192.168.1.2 tell 192.168.1.213
11:58:03.704355 arp who - has 192.168.1.2 tell 192.168.1.213
11:58:44.184709 arp who - has 192.168.1.213 tell 192.168.1.1
11:58:44.184733 arp reply 192.168.1.213 is -at 00:0 e:35: a3:0f:56 ( oui Unknown )
```

Slika 6.2.1 TCPCDump – informacije o primljenim paketima

6.3 Ethereal



Slika 6.3.1 Ethereal pod Linuxom

Ethereal se koristi za potpuniji pregled jednog paketa uključujući i sva dostupna zaglavlja. Biblioteka o strukturama pojedinih paketa daje korisniku uputstva pri analizi svakog od fragmenata u paketu. Ako Kismet ne daje dovoljno povratnih informacija korisniku o tome šta je otkrio, Ethereal se može koristiti da do najsitnijih detalja prikaže parametre mreže i komunikacije. Slika 6.3.1 je ekranski prikaz Ethereal. Prvi prozor prikazuje okvire koji su prikupljeni od strane WLAN mrežne karte. Detaljniji prikaz okvira sa potvrdom prijema je prikazan u listi ispod. Polja u okviru su prikazana tako da ih korisnik može lako pročitati. Poslednja lista na dnu je u hexa notaciji ili u ASCII notaciji.

6.4 Netstumbler

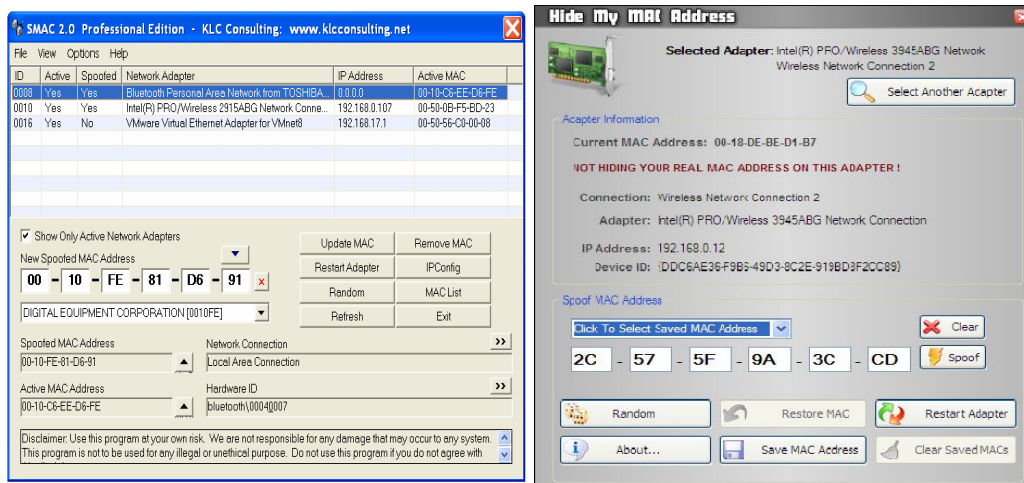
Netstumbler pokušava da se aktivno pridruži svakoj pristupnoj tački (AP) koju detektuje. Ima najveću primenu kod inženjera koji ispituju svoju WLAN mrežu. Nije naročito pogodan za wardrive, zato što je vidljiv – šalje probe request. Detaljniji opis ovog programskog paketa je dat u poglavlju 8.

6.5 Programi za izmenu MAC adrese

Tokom izrade ovog rada uočeno je da se značajan broj mreža štiti od napada tako što pristup omogućava samo uređajima koji su na listi MAC adresa kojima je dozvoljen pristup AP-u. MAC adresu određuje i u uređaj (bežičnu mrežnu karticu) upisuje proizvođač uređaja. MAC adresa je 48 bitni broj, koji je podeljen u dva jednaka dela. Prvi deo je oznaka proizvođača, a drugi deo je serijski broj koji je

uređaju dodelio proizvođač. To garantuje da nema dva uređaja sa istom MAC adresom, osim ako proizvođač pogreši. Taj 24 bitni broj se zove OUI ("Organizationally Unique Identifier"). Međutim, OUI je u stvarnosti dug 22 bita, dva bita u polju se koriste za druge namene. Jedan bit nosi informaciju o adresi - „broadcast ili multicast”, drugi bit je indikacija o tome dali je adapter lokalno preraspodeljen (ako administrator mreže dodeli drugu vrednost MAC adrese kako bi zadovoljio kriterijum iz lokalne mrežne politike).

Mehanizam za prosleđivanje MAC adrese pod Microsoft Windows OS, se može zaobići, i tako odaslati neka druga MAC adresa, koju korisnik sam odabere. Izmena koju ovakav program unese nije permanentna, ne upisuje se u sam uređaj, i postoji samo dok se operativni sistem ponovo ne pokrene. Namena ovog programa je upravljanje MAC adresama, a korisnici su najčešće velike korporacije. To se može zloupotrebiti kako bi se napadač lažno predstavio i tako dobio pristup AP-u.



Slika 6.5.1 Programi za izmenu MAC adrese

U Linux-u, promenu MAC adrese možemo obaviti `ifconfig` komandom, na primer:

`ifconfig eth0 hw ether 00:00:DE:AD:BE:EF`

ili sa kratkim C programom pozivajući `ioctl()` funkciju sa `SIOCSIFHWADDR` flegom.

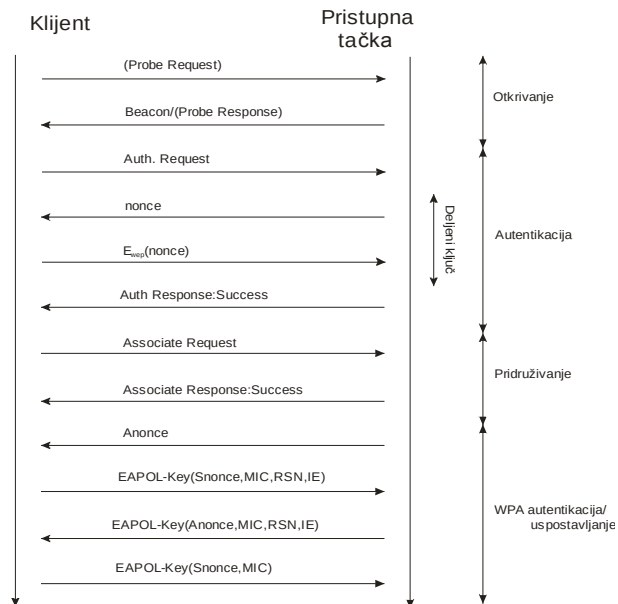
Lista proizvođača opreme i njima dodeljenih OUI kodova za MAC adrese se može pronaći na [5].

7. Probijanje zaštite bežičnih mreža

Uvod

Još od vremena kada se pojavio poznati rad na temu kako kreirati WEP ključ postoji dosta radova na temu slabosti i propusti u WEP mehanizmu zaštite bezbednosti podataka. Kao zamenu za WEP korisnici su prihvatili najpre VPN i 802.1X. Takvo rešenje je dozvoljavalo korišćenje postojeće mrežne opreme uz poboljšanje bezbednosti podataka. Zatim je usledilo privremeno rešenje u vidu WPA mehanizma. WPA je otklonio većinu poznatih bezbednosnih propusta uočenih kod WEP. Sa poboljšanjem bezbednosti raste i složenost podešavanja bezbednosnih mehanizama, a to opet uzrokuje da primena u praksi bude manja nego što se očekuje. Konačna zamena za WEP i WPA je WPA2 (IEEE 802.11i) za koji do sada u varijanti enterprise nema objavljenih slabosti po pitanju bezbednosti. Praktični primeri u ovom poglavlju su izvršavani pod Linux operativnim sistemom zbog ograničenog broja bežičnih mrežnih adaptera koji imaju potrebne funkcionalnosti. Većina navedenih primera bi se mogla izvršiti i pod Windows platformom.

7.1 Protokol za pridruživanje na 802.11 mrežu (Connection Access)



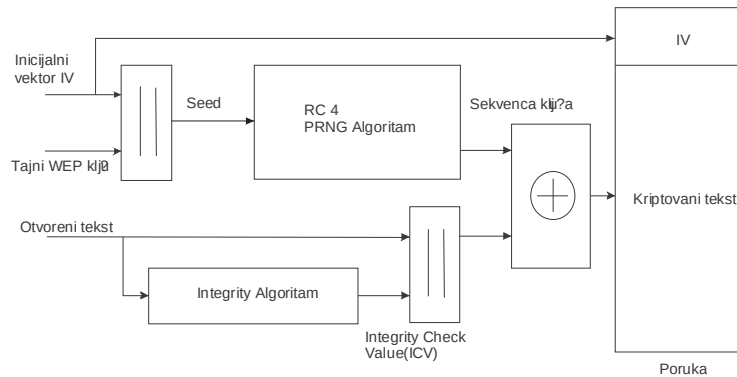
Slika 7.1.1 Protokol konekcije na WLAN

Slika 7.1.1 pokazuje osnovu protokola i toka okvira prilikom konektovanja na neku pristupnu tačku (AP). Najpre klijent detektuje pristupne tačke, bilo da šalje zahtev za ispitivanje (probe request) i dobija odgovor (probe response), ili da samo posmatra beacon okvire koje pristupne tačke često šalju. Odmah po otkrivanju, klijent može da proba autentikaciju na pristupnu tačku. Ako se uspešno autentikuje, klijent može probati da se pridruži na pristupnu tačku tako što pošalje zahtev za pridruživanje na mrežu (association request). Ako mu je dozvoljen pristup na AP, klijent će dobiti od AP-a pozitivan odgovor na zahtev za pridruživanje (association

response). Kad god je WPA aktivan, mehanizam autentikacije deljenim ključem WEP-a se izbegava (koristi se sistem otvorene autentikacije), i stvarna autentikacija se obavlja nakon pridruživanja. U toku ovog četvorostepenog procesa, važni ključevi se generišu i razmenjuju. Posle inicijalizacije, klijentu je dozvoljeno i omogućeno da šalje i prima okvire podataka od mreže i ka mreži.

7.2 Wired Equivalent Privacy (WEP)

7.2.1 Osnova



Slika 7.2.1 WEP - blok dijagram kriptovanja

Prvobitna namena WEP-a je da osigura bezbednost u bežičnoj mreži jednaku onoj u ekvivalentnoj žičnoj mreži. Iz toga se nameće pitanje, kakvu to bezbednost ima žična mreža u fizičkom smislu. U kontrolisanom medijumu kakav ima žičana mreža, osnovna ideja je da su podaci vidljivi samo pošiljaocu primaocu i na switch-u. U ranijim implementacijama žičane mreže, bilo ko od korisnika priključenih na HUB je mogao da sluša sav saobraćaj ostalih učesnika. Sa današnjim switch uređajima, to više nije slučaj, podaci su dostupni za dva entiteta koji komuniciraju, a razmena podataka se može pratiti na switch-evima i ruterima u mreži. Dakle WEP ipak ne obezbeđuje nivo bezbednosti u mreži kakav imaju današnje žične mreže. Sa WEP bilo ko od autorizovanih korisnika može da sluša sve ostale učesnike u toj mreži, što odgovara nivou bezbednosti koji su omogućavale starije žičane mreže sa HUB-om.

Ispunjavanje tri osnovne pretpostavke tajnosti, autentičnosti i kontrole pristupa, su osnovni uslovi za bezbednost, i to je definisano standardom IEEE 802.11. Može se pokazati da nezavisno od toga kako je mreža konfigurisana sa WEP, uvek je moguće narušiti ove tri pretpostavke bezbednosti. To je moguće zbog načina na koji je WEP napravljen. Kontrola pristupa nije ostvarena kao deo WEP. U izvornom tekstu standarda 802.11 postoje samo nagoveštaji o kontroli pristupa. To je smernica o korišćenju MAC adresiranja da bi se sprečio pristup autentikovanim klijentima, na primer kada korisniku nije dozvoljen pristup u određeno vreme ili kada mu ne treba dozvoliti da koristi određenu tačku pristupa (AP). Probijanje takve kontrole pristupa, zasnovane na MAC adresiranju, je u ovom radu detaljnije analizirano. Takva kontrola pristupa daje ideju da „klijenti” koji nisu autentikovani, i koji su potencijalni napadači, ne mogu slati nikakav sadržaj u mrežu. Neautorizovano ubacivanje paketa je takođe detaljnije obrađeno u ovom radu.

Prikaz rada WEP-a je dat u standardu, a Slika 7.2.1 prikazuje operacije koje se tom prilikom obavljaju. WEP koristi RC4 algoritam generatora pseudo slučajnih brojeva (PRNG) razvijen od strane RSD Data Security, Inc. Svi učesnici u mreži uključujući i pristupne tačke dele isti tajni WEP ključ. Zatim se po redosledu kriptovanja podataka, jedan inicijalni vektor IV spaja sa WEP ključem i koristi kao ulaz (seed) za RC4 PRNG algoritam. To na izlazu iz RC4 generatora daje sekvencu ključa. Ta sekvencu ključa se XOR-uje sa zbirom otvorenog teksta i vrednošću dobijenom proverom integriteta otvorenog teksta (ICV). Inicijalni vektor IV se spaja sa kriptovanim tekstom i šalje primaocu. Prijemnik ili prijemnici na drugoj strani, sledeći istu proceduru u obrnutom smeru dekriptuju poruke.

7.2.2 Narušavanje poverljivosti

Poverljivost (confidentiality) se štiti kriptovanjem svih podataka na aplikativnom nivou. Za WEP je objavljeno sedam načina kako se može dekriptovati komunikacija.

1. Dobijanje WEP ključa kao slabosti deljenog ključa u algoritmu RC4.
2. Korišćenje WEP ključa dobijenog napadom brute-force tipa uz upotrebu rečnika.
3. Dekriptovanje paketa uz pomoć poznatog inicijalnog vektora, odnosno baze podataka inicijalnog vektora.
4. Napad pomoću poznatog otvorenog teksta.
5. Dvostrukim kriptovanjem se dobija otvoreni tekst.
6. Preusmeravanje kriptovanih poruka na neku IP adresu kontrolisanu od napadača.
7. Probanje svakog mogućeg WEP ključa i provera njegove validnosti, offline.

Drugi i četvrti slučaj će raditi samo u specifičnim okolnostima. Treći slučaj traži posebnu pažnju i nekoliko gigabajta prostora na disku. Peti slučaj se mora primenjivati sa dosta istrajnosti. Šesti slučaj zahteva ciljnu mrežu kojoj će se pridružiti bežična mreža ili host računar pod kontrolom napadača, koji ima pristup internetu. Prvi ujedno i najefikasniji metod napada na bežičnu mrežu sa WEP zaštitom zahteva vremena koliko je dovoljno da pokupi kriptovane pakete. Sa „IV akceleracijom“ opisanom u ovom radu, prvi metod će imati uspeha bilo gde za vreme od jednog minuta do otprilike dvadeset minuta posle kupljenja prvog kriptovanog paketa. Ako se ne koristi aktivni napad, to može da potraje i nekoliko nedelja pri uslovima saobraćaja niskog intenziteta. Vreme potrebno za izvođenje ostalih napada se kreće od nekoliko minuta do nekoliko dana.

7.2.2.1 Dobijanje WEP ključa - slabost deljenog ključa u algoritmu RC4

Najveći nedostatak WEP je nesumnjivo to što napadaču pruža mogućnost da dobije tajni WEP ključ. Potreban je samo obezbediti prijem radio signala, standardnu malo prilagođenu oprema za bežičnu mrežu i široko dostupan open-source softver za tu namenu. Napad sa ciljem da se kompromituje ključ je prvi put opisan u radu pod naslovom „Slabosti u deljenju ključa algoritma RC4“ [6]. Ukratko, neki od ključeva koji služe kao ulaz u RC4 algoritam i generišu sekvencu ključa, sa sobom nose i prikazuju neke bitove ključa koji je korišćen. Vrednost inicijalne sekvence ključa je određena malim delom ključa. Kada se poredi veliki broj sekvenci ključa generisanih pomoću „slabih ključeva“, statistički se može pronaći određeni tajni ključ. Skup

„slabih ključeva” se može identifikovati pomoću inicijalnog vektora IV koji čini prva tri bajta za ulaz u RC4 algoritam. Rečima, postupak je sledeći:

1. Prikupljanje kriptovanih okvira.
2. Izdvajanje IV i prva dva bajta toka ključa.
3. Odbacivanje okvira ako IV ne ukazuje na „slabi” RC4 ključ.
4. Od prikupljenih informacija, odrediti verovatnu vrednost bajta tajnog ključa.
5. Ići na prvi korak ponovo dok se ne prikupi veliki broj okvira, ili dok se ne otkrije ključ.
6. Kada se prikupi dovoljan broj okvira, proveriti da li je ključ sa najvećom verovatnoćom validan.

U stvarnom napadu oko 5,000,000 jedinstvenih inicijalnih vektora IV treba da bi se pronašao tajni ključ. Kasnije 2002 god. David Hulton je u radu [7] obradio optimizaciju ovog napada. Njegova metoda napada i optimizacija zahteva samo 500,000 jedinstvenih IV, da bi se dobio tajni WEP ključ. Implementacija je dostupna u Hulton's BSD Airtols. Aircrack [8] je druga implementacija napada i optimizacije. Anonimni haker pod pseudonimom „KoreK” dalje usavršava napad u 2004. god. sa više algoritama za izračunavanje ponderisanih vrednosti (glasova) za bajtove ključa. Kada se primene ovakvi napadi, moguće je doći do WEP ključa nakon samo 300,000 prikupljenih jedinstvenih IV.

Aircrack alat je u ovom radu korišćen za prikazivanje metoda napada. Kada se koristi Aircrack, korak pre toga je podeljen između dva alata. Airodump prikuplja okvire i beleži interesantne IV i kriptovane bajtove. Aktuelni Aircrack program prolazi kroz prikupljene podatke, sačinjava bazu podataka o ponderisanim vrednostima (glasovima) i obavlja proveru validnosti isprobavanjem WEP ključeva sa najvećim brojem glasova.

```
# airodump packets eth3
BSSID CH MB ENC PWR Packets LAN IP / # IVs ESSID

00:12:17:49:D1 :81 11 48 WPA -1 289826 253343 HomeNet
00:12:17:6 F :92:33 11 48 WEP -1 4725 0 linksys
```

Slika 7.2.2.1 Listing Airodump

Listing na Slici 7.2.2.1 pokazuje sve mreže sa kojih su prikupljeni paketi u kojima su neki parametri o tim mrežama. Vrednost IV koja se vidi je od interesa, 253,343 za mrežu koja je napadnuta ; „HomeNet”.

```
# aircrack packets
aircrack 2.1
* Got 231129! unique IVs | fudge factor = 2
* Elapsed time [00:00:03] | tried 1 keys at 20 k/m

KB depth votes
0 0/ 1 2A( 57) 3D( 15) 09( 12) 5E( 12) 73( 12) DF( 12)
1 0/ 1 B1( 53) 6B( 25) 3C( 13) 58( 13) 59( 13) DC( 12)
2 0/ 1 DD( 96) 59( 15) A4( 15) AF( 12) B5( 12) 2A( 5)
3 0/ 3 37( 36) 10( 23) 97( 18) 22( 15) 5A( 15) 34( 12)
4 0/ 1 6E( 68) 1C( 21) CA( 15) A0( 13) 59( 12) 7F( 12)
5 0/ 3 93( 263) F3( 175) AD( 170) 8D( 45) 0C( 40) 0B( 38)
6 0/ 3 57( 25) 71( 16) C4( 12) 72( 11) 38( 10) F1( 10)
7 0/ 1 D7( 113) AE( 18) F6( 15) 04( 12) 91( 12) 41( 10)
8 0/ 1 7B( 116) CC( 20) 85( 18) 8F( 18) 7E( 15) BF( 14)
9 0/ 1 8D( 49) D4( 18) 08( 15) 6C( 15) E9( 15) 42( 12)
10 0/ 1 54( 37) 41( 16) E8( 16) 8F( 15) 09( 12) 0E( 12)
11 0/ 1 67( 115) BD( 22) 35( 18) 7C( 18) 29( 15) DC( 15)
12 0/ 1 B0( 38) 2C( 15) 5E( 15) 67( 15) 69( 12) 83( 11)
```

Slika 7.2.2.2 Listing Aircrack

U listingu na Slici 7.2.2.2 se vidi kakao Aircrack proba mnogo različitih ključeva kako bi video dali je neki od njih tajni WEP ključ. Bitovi u ključu koji su prikazani izabrani su preko ponderisane veličine tj. „glasova” koje su dobili. Glasovi su brojevi u zagradama odmah pored bita koji predstavljaju ključ. Broj različitih bajtova koje proba za svaki odabrani bajt je određen sa vrednošću „fudge factor”, i prikazan je na slici. Sa većom „fudge factor” vrednošću više ključeva će biti testirano. Što više glasova bajt ključa dobije to je verovatnije da će biti ispravna vrednost bajta ključa u okviru tajnog ključa. Kada se dovoljno paketa prikupi, statistika obično sa velikom verovatnoćom ukaže na ispravnu vrednost ključa. U ovom slučaju svi bajtovi ključa koji imaju najviše glasova su bajtovi ključa, pa je tako ispravna vrednost ključa: 2A-B1-DD-37-6E-93-57-D7-7B-8D-54-67-B0. U eksperimentu je oko 4800 paketa u sekundi poslato preko linka. Ova slika uključuje okvire podataka u oba smera. Otprilike 2900 paketa podataka sa jedinstvenim IV-om u sekundi znači da je ukupno vreme za napad $231\,129 / 2900 \approx 79$ sekundi. Brzina od 4800 paketa u sekundi je moguća zato što je omogućen pristup internoj mreži, paketi su prebacivani u WLAN mrežu što je brže moguće.

U situacijama koje više odgovaraju realnim uslovima, gde napadač nema dobar pristup internoj mreži, proces prikupljanja dovoljno IV-a bi uzeo više vremena. Metod koji je nazvan „IV akceleracija” omogućava napadaču da IV prikuplja brzinom koja je otprilike jednaka polovini one brzine koju je moguće postići ako postoji pristup internoj mreži. Nekoliko posebnih problema se javlja pri pokušaju ubacivanja paketa. Najveća brzina ubacivanja paketa postignuta u ovom radu je 800 ubačenih paketa u sekundi. Slučaj koji je iznad naveden, kada se primeni zajedno sa „IV akceleracijom” uzeo bi nešto manje od pet minuta za dobijanje WEP ključa.

Uglavnom je više od 231129 jedinstvenih IV-a potrebno da bi se razbio ključ. „Kvalitet” prikupljenih kriptovanih IV-a je povezan sa uspešnošću kreiranja. Ima slučajeva kada 10,000,000 jedinstvenih IV-a ne daje rezultat u dobijanju ključa. Napad je zasnovan na statističkim analizama i ponekad ta činjenica dovodi do neuspeha u kreiranju ključa. Neki skupovi IV-a i kriptovanih poruka čini se vode statistiku u pogrešnom pravcu. Ta činjenica je potvrđena od strane autora Aircrack-a pa su delovi algoritma za kreiranje ključa, posebno „KoreK” algoritma, izbačeni, posebno ako postoji mogućnost da se čistim brute-force napadima dobiju zadnja dva bajta ključa. Uzorak sastavljen od prikupljenih paketa, kriptovanih sa ključem od 40 bita, obezbeđen u [9] pokazuje da se koristi 174476 jedinstvenih IV-a za postavljanje napada, Aircrack može pronaći ključ posle testiranja 1184 ključa (8 sekundi vremena). Ali ako proširimo broj prikupljenih paketa na 331829 jedinstvenih IV-a, Aircrack će dati rezultat posle nekoliko minuta.

7.2.2.2 Dobijanje Passphrase Seeded WEP ključa

Većina WLAN opreme prihvata passphrase kada se inicijalno postavlja mreža štićena sa WEP. Ta passphrase je korišćena za generisanje WEP ključa. Proizvođači opreme imaju različite metode korišćenja passphrase da bi se došlo do konačnog WEP ključa. Jedan metod ga koristi da napravi hash od passphrase sa MD5. Pošto MD5 zahteva 128 bita kao ulaz, passphrase se proširuje. Proširenje je različito u zavisnosti od proizvođača. Dok 3com radi proširenje sa null karakterima, Lynksys ponavlja passphrase string dok ne dosegne dužinu od 128 bita. Konačno MD5 hash kod 3com opreme je 2A-B1-DD-37-6E-93-57-D7-7B-8D-54-67-B0-AC-2D-A2, a kod Lynksys

opreme je to C3-8B-C1-61-4B-EB-F4-8C-7C-E7-99-58-79-C7-AF-39. Samo se prva 104 bita koriste za WEP ključ.

To relativno direktno vodi ka rečničkom napadu. ICV se koristi za verifikaciju dali je paket dekriptovan sa ispravnim ključem. Nekoliko dodatnih paketa se može koristiti za ispitivanje kako bi se eliminisale donete greške.

Evo kako softverski alat sprovodi napad tipa brute-force:

1. Propušta WEP kriptovani paket i izdvaja IV, kriptovani tekst (uključujući ICV).
2. Bira reč iz rečnika, i radi njen hash kao što je gore objašnjeno.
3. Dodaje generisani WEP ključ izdvojenom IV-u.
4. Koristeći RC4, generiše sekvencu dugu koliko i izdvojeni kriptovani tekst payload.
5. Vrš XOR nad otvorenim tekstom i sekvencom ključa (dekriptuje).
6. Računa ICV dekriptovanih podataka.
7. Poređi izračunati ICV i ekstrakovani ICV.
8. Ako su isti, pogađani WEP ključ može biti korektan WEP ključ.
9. Dalja provera testiranjem ključa sa još WEP kriptovanih okvira, ili pregledanje dekriptovanog otvorenog teksta da bi se uočile eventualne primedbe.

WEP Lab je softverski alat koji ove korake obavlja automatski. On zahteva skup kriptovanih WEP okvira podataka i listu passphrases. Ako je ispravna passphrase u tog listi, WEPLab će ispitati da li je korektan WEP ključ, i prikazati ga. Da bi eliminisao donete greške, on ispituje ključ na 10 paketa.

```
~/ Tools /weplab -0.1.4.Vlada -w:~/ engl -stdout ./ weplab -y -d1 --attack 3 -k 128 ~/ dump/ dump2 . cap
weplab - Wep Key Cracker Wep Key Cracker (v0 .1.4) .
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users. sourceforge .net >
18 % readNot BSSID specified .
Detected one packet with BSSID : [00:13:10:9 B:47: F1]
Only packets belongs to that BSSID will be processed .
If -a option reveals other BSSIDs you can specify one with --ssid .
Total valid packets read: 11
Total packets read: 260
10 packets selected .
Packet 0 --> 86 total lenght , 58 data lenght (just encrypted data)
Packet 1 --> 86 total lenght , 58 data lenght (just encrypted data)
Packet 2 --> 86 total lenght , 58 data lenght (just encrypted data)
Packet 3 --> 116 total lenght , 88 data lenght (just encrypted data)
Packet 4 --> 104 total lenght , 76 data lenght (just encrypted data)
Packet 5 --> 104 total lenght , 76 data lenght (just encrypted data)
Packet 6 --> 368 total lenght , 340 data lenght ( just encrypted data)
Packet 7 --> 368 total lenght , 340 data lenght ( just encrypted data)
Packet 8 --> 368 total lenght , 340 data lenght ( just encrypted data)
Packet 9 --> 96 total lenght , 68 data lenght (just encrypted data)
Statistical cracking started ! Please hit enter to get statistics from Vlada.
Weplab statistics will be printed each 5 seconds
It seems that the first control data packet verifies the key ! Let 's test it
with others ....
Right KEY found !!
Key : c3 :8b:c1 :61:4 b:eb:f4 :8c:7c:e7 :99:58:79
This was the end of the dictionary attack .
```

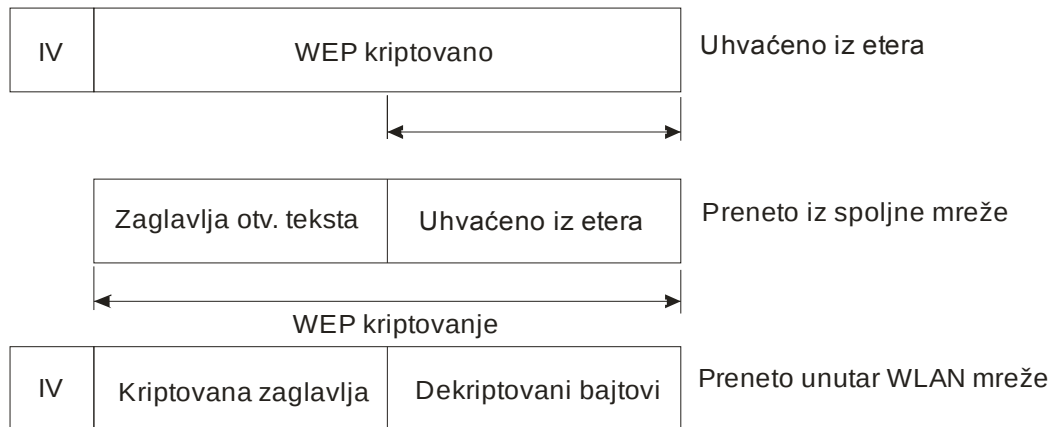
Slika 7.2.2.2 WEPLab ispitivanje passphrase seeded WEP ključeva

Listing na Slici 7.2.2.2 prikazuje WEPLab softver pri pokušaju da metodom brute-force pogodi passphrase tajnog WEP ključa. Inicijalna komanda “john -w../english -

stdout” je pokretanje popularnog alata za generisanje passworda koji se zove „John The Ripper”. On uzima reči iz Engleskog jezika sa liste, i kombinuje reči na način kako to i korisnici rade kada biraju passphrase. Generisani passphrase se prosleđuje u WEPLab koji obavlja testiranje nad ključem koji passphrase generiše. Kao što se vidi sa listinga, WEPLab najpre na izlazu štampa neke informacije kao što je BSSID i dužina podataka kriptovanih okvira koji su obezbeđeni na ulazu. Na kraju kada WEPLab pronade ispravan WEP ključ on ga prikaže. U ovom primeru passphrase je simba123 uz upotrebu 3com passphrase algoritma.

7.2.2.3 Dvostruko kriptovanje (double encryption)

WEP koristi potpuno isti mehanizam za kriptovanje i dekriptovanje. Ako klijent ili pristupna tačka greškom ponovo kriptuje već kriptovani tekst, time će praktično dekriptovati frejm i poslati otvoreni tekst na predaju. Kako se odvija napad pokazuje Slika 7.2.2.3.



Slika 7.2.2.3 Napad tipa dvostruko kriptovanje

Da bi se dekriptovao sadržaj određenog paketa, ubacivanje kriptovanog sadržaja mora da se obavi kada klijent ili tačka pristupa kriptuje koristeći isti IV kojim je odabrani kriptovani paket kriptovan. Pošto ima 224 IV-a, to napad čini sporijim. Srećom po napadača, broj je znatno manji ako klijent ili tačka pristupa odbaci delove skupa IV-a. Neki klijenti i pristupne tačke koriste sekvencijalnu šemu i tako generisanje IV-a čine predvidljivim i omogućavaju mu da ubaci paket tačno na vreme.

Znatno efikasniji način za implementaciju napada je korišćenje (Internet Control Message Protocol) ICMP echo request i echo replay paketa. Ako je moguće, poslati jedan ICMP echo request klijentu u WLAN mreži. Payload u okviru jednog echo request može biti bilo šta i može biti bilo koje veličine, u okviru ograničenja koja mreža dozvoljava. Payload može da sadrži kriptovani paket, čiji je offset jednak dužini svih zaglavlja paketa. Kada se paket pojavi u WLAN mreži, pristupna tačka će ga kriptovati. Slati što je više moguće echo request-a sve dok ih pristupna tačka kriptuje pod željenim IV. Ovaj napad čini oko dva puta bržim, to što kada klijent odgovara na zahtev, on šalje potpuno isti payload kao odgovor, samo kriptovan pod drugim novim IV.

Ofset za korišćenje u ICMP verziji napada je 40 bajta: 8 bajta SNAP zaglavlja od Etherneta, 24 bajta za IP zaglavlje i 8 bajta za ICMP zaglavlje. To znači da će sve

osim prvih 40 bajtova moći da se dekriptuje. Ako je kriptovani paket TCP/IP, onda je TCP/IP zaglavlje najmanje $24 + 32 = 56$ bajtova dugo. Što neizostavno znači da je moguće dekriptovati sve podatke u TCP/IP paketu, i $56 - 32 = 24$ zadnja bajt TCP zaglavlja-samo su izvorišni i odredišni broj porta TCP zaglavlja izgubljeni.

Postoji drugi način da se učestvuje u raspodeli mrežnog dekriptovanja podataka. U šemi challenge-response WEP autentikacije, tačka pristupa daje nonce klijentu i klijent treba da ga kriptuje koristeći klasičan WEP metod. Napadač može poslati deautentikovani okvir klijentu. Kada klijent pokuša da se ponovo autentifikuje, napadač može poslati otvoreni tekst kriptovanog paketa kao nonce. Napadač može otkriti prvih 128 bajtova kriptovanog otvorenog teksta. Sa otprilike 0.5 pokušaja u sekundi i klijentovo kriptovanje svaki put kada je novi IV, iz nefiltriranog skupa IV-a, to bi trajalo oko 9320 časa, ili oko 388 dana. 50% šanse za uspeh je posle polovine tog vremena. Samo u izuzetnim slučajevima će napadač biti istrajan u tako dugom vremenskom periodu. Ako bi to bio jedini mogući napad na WEP, to bi na primer moglo da se koristi za pronalaženje passworda iz protokola sa otvorenim tekstom, kao što su protokoli za proveru e-maila. Tačno, onaj okvir koji sadrži password, može da se izdvoji uparivanjem komunikacionih modela i veličina okvira koji su zajednički za protokol. Postoje slabosti WEP-a koje se lakše i sa više efekta mogu iskoristiti. Trenutno nema dostunih ni javno poznatih alata koji automatizuju ovu vrstu napada.

7.2.2.4 Napad pomoću poznatog otvorenog teksta

Dodatne informacije o kriptovanom tekstu dostupne su preko (kriptovanog) ICV. ICV se koristi da proveru da li je paket validan ili nije. Ako je paket validan on će biti prihvaćen od primaoca, ako nije biće odbačen. Pod tim okolnostima u WEP kriptovanoj WLAN mreži, jedan napad odabranim otvorenim tekstom može se izvesti da bi se dekriptovao jedan kriptovani okvir:

1. Prikupljanje kriptovanih paketa koji su procenjeni kao interesantni.
2. Procenjivanje sa velikom verovatnoćom prvih n bajtova podataka.
3. Izračunavanje ICV za $n-3$ bajtova.
4. Spajanje $n-3$ bajta i ICV i njihovo XOR-ovanje sa odgovarajućim sekvencom toka ključa (koja je dobijena XOR-ovanjem n bajtova sa stvarnim kriptovanim paketom).
5. Dodavanje na kraj jednog bajta, procenjenog pomoću brute-force napada.
6. Slanje paketa ka prijemnoj tački (AP).
7. Ako je paket validan, zadnji bajt je zadnji bajt ICV-a. Njegova stvarna dekriptovana vrednost je u ovom trenutku nepoznata. Međutim, kako su svi bajtovi pre poslednjeg bajta poznati, primenom (CRC) Cyclic Redundant Check na poznate podatke da bi se dobio ICV će dati pravu vrednost zadnjeg bajta – a na ovaj način i bajt sekvence ključa.
8. Ako je paket neodgovarajući, ići na korak 5 i uzeti drugu procenu zadnjeg bajta.

Napad je opisan u Real 802.11 Security [10, str. 326-329], gde je koautor Profesor William A. Arbaugh, koji je objavio rad o ovom napadu u 2001. god. On ima zatvorenu aplikaciju uz pomoć koje tvrdi da može dekriptovati okvir podataka od 1500 bajta za oko 42.8 minuta. Varijacija ovog napada je implementirana od strane anonimnog hakera „KoreK“, koji je objavio implementaciju kao softverski alat, Chopchop u 2004. god. na online diskusionom forumu [11]. „KoreK“ varijanta napada obavlja napad u obrnutom redosledu nad podacima. On počinje sa procenom zadnjeg bajta u paketu dok ne dostigne deveti bajt. Prvih devet bajtova se procenjuju na osnovu približno istih zaglavlja u paketima podataka.

Vreme koje mu je potrebno da dekriptuje okvir raste linearno sa dužinom okvira. Činjenica je da napad uvodi mogućnost da se dobije proizvoljno duga sekvenca ključa, iz bilo koje dužine okvira podataka. Na primer čak 1500 bajta sekvenca ključa iz 64 bajta dugog okvira podataka.

```
# ./aireplay -h 00:0E:35:A3:0F:56 -k eth3
Option -x not specified, assuming 256.
Seen 26 packets ...
FromDS = 0, ToDS = 1, WEP = 1
BSSID = 00:0D:54:9D:EC:4B
Src . MAC = 00:0E:35:A3:0F:56
Dst . MAC = FF:FF:FF:FF:FF:FF
0 x0000 : 0841 0000 000 d 549 d ec4b 000 e 35a3 0f56 .A....T..K ..5.. V
0 x0010 : ffff ffff ffff 1004 807 f 5300 6295 ff14 ..... S.b...
0 x0020 : ea41 744 e 6548 787 d 6cc5 0c26 c6cb c428 . AtNeHx }1 ..&...(
0 x0030 : 5802 332 e 303 e 52b8 a718 ddba a2bc bf7a X.3.0 > R ..... z
0 x0040 : be9d 58 da ..X.
Use this packet ? y
Saving chosen packet in replay_src -050622 -010218. pcap
Operating in authenticated mode.
Offset 67 ( 0% done ) | xor = 2F | pt = F5 | 235 frames written in 919 ms
Offset 66 ( 2% done ) | xor = 76 | pt = 2E | 223 frames written in 870 ms
Offset 65 ( 5% done ) | xor = 40 | pt = DD | 4 frames written in 15 ms
...
Offset 36 (91% done ) | xor = 65 | pt = 00 | 221 frames written in 863 ms
Offset 35 (94% done ) | xor = 48 | pt = 06 | 253 frames written in 988 ms
Offset 34 (97% done ) | xor = 7C | pt = 08 | 231 frames written in 903 ms
Saving plaintext in replay_dec -050622 -010218. pcap
Saving keystream in replay_dec -050622 -010218. prga
Completed in 23s (1.30 bytes /s)
# hexdump eplay_dec -050622 -010218. prga
00000000 7f80 0053 3fc8 14fc 41 ea 487 c 4965 7d70
00000010 c16a 270 c c5c6 8 bf1 5457 86 f3 2531 b852
00000020 18 a7 badd 1462 7 fbe 40 d1 2f76
0000002 c
```

Slika 7.2.2.4.1 Listing Aireplay izvršava napad otvorenim tekstom

```
# tcpdump -r replay_dec -050622 -010218. pcap
reading from file replay_dec -050622 -010218. pcap, link -type IEEE802_11 (802.11)
01:02:18.889097 arp who - has 192.168.1.5 tell 192.168.1.27
```

Slika 7.2.2.4.2 TCPDump prikazuje dekriptovane okvire

```
# hexdump eplay_dec -050622 -010218. prga
00000000 7f80 0053 3fc8 14fc 41 ea 487 c 4965 7d70
00000010 c16a 270 c c5c6 8 bf1 5457 86 f3 2531 b852
00000020 18 a7 badd 1462 7 fbe 40 d1 2f76
0000002 c
```

Slika 7.2.2.4.3 Hexdump prikazuje sekvencu ključa

Slika 7.2.2.4.1 prikazuje “aireplay” iz Aircrack kako izvršava “KoreK” verziju napada (sa parametrom -k). Namena alata je da uzme sekvencu ključa i zatim će oslušivati pakete za koje veruje da ih može dekriptovati brzo. Parametar -h 00:0E:35:A3:0F:56 će naterati aireplay da prima samo pakete poslate sa navedene MAC adrese. Posle pregledanja 26 okvira, pronalazi jedan za koji veruje da ga je moguće brzo dekriptovati. Korisnik odobrava dekriptovanje paketa, i napad počinje. Prvi bajt je pronađen pošto je isprobano 235 vrednosti za taj bajt. Drugi nakon 223, i tako redom.

Kada se dođe do svih bajtova, sekvenca ključa i otvoreni tekst se smeštaju u fajl. U datom primeru je urađeno dekriptovanje za 23 sekunde. Pобоljšanje sa pokušajem da se paralelno više različitih vrednosti proba za zadnji bajt značajno povećava brzinu napada. Dekriptovani okviri su prikazani u „TCP Dump” na Slici 7.2.2.4.2, a Slika 7.2.2.4.3 pokazuje „hexdump” i u njemu prikazanu sekvencu ključa smeštenu u .prga fajl.

Napad tipa „KoreK” koji koristi Aircrack ima nekih nedostataka. On ne radi potpuno na svim pristupnim tačkama. Neke pristupne tačke odbacuju svaki okvir koji ima payload manji od 40 bajta. Prema tome prvih 40 bajtova neće biti dekriptovano ovim napadom, ali ostali bajtovi hoće. To znači da u ovoj verziji napada prvih 40 bajtova mora biti poznato/pretpostavljeno pre nego što se dedukcijom dođe do otvorenog teksta ostalog dela podataka. Lynksys WRT54G i WAP54G pristupne tačke odbacuju sve pakete koji imaju manje od 40 bajtova podataka. Samo nekolicina pristupnih tačaka je osposobljeno da dozvoljava male korisne tekstove (payload). Primer iznad je napad tipa brute-force protiv jedne Prism54 PC kartice pod Linux OS i Prism 54 drajvera u master modu. („Master mod” je kada mrežna kartica igra ulogu pristupne tačke).

U WPA dodatni mehanizam za proveru integriteta je implementiran uz korišćenje Message Integrity Code (MIC). MIC koristi odvojene ključeve za generisanje njihovih vrednosti i zaštitu od napada.

7.2.2.5 Inicijalni vektor (IV) i baza sekvence ključa

Ako je dat IV i odgovarajuća sekvenca ključa, moguće je dekriptovati neki drugi okvir koristeći isti IV sve do isteka dužine sekvence ključa. Pravljenjem baze podataka svih mogućih IV-a i odgovarajućih sekvenci ključa, dekriptovanje bilo kojeg kriptovanog okvira postaje trivijalno. Trenutni kriptovani ključ se ne dobija, ali on nije neophodan sve dok imate sekvencu ključa i IV. Postoji 224 moguća IV-a. Najveći mogući data payload je otprilike 1500 bajta. Kompletna baza podataka će zauzeti oko 24GB.

Najbolji način da se napravi takva baza je da se iskoristi prednost dobijena napadom odabranim otvorenim tekstom iz predhodnog stava i ICMP echo request na isti način kao što se koristi u napadu dvostrukim kriptovanjem u odeljku 7.2.2.3. Korišćenjem napada odabranim otvorenim tekstom, može se dobiti čitava dužina sekvence ključa. Sa tom jednom sekvencom ključa, ostatak sekvenci ključa sa njihovim jedinstvenim IV se jednostavno dobija. Ubacivanjem pune dužine ICMP echo request-a prema svakom klijentu u mreži, oni će odgovoriti sa potpuno istim ICMP podacima kao što su u ubačenom paketu. Na ovaj način je otvoreni tekst i kriptovani tekst postao poznat, pa tako i sekvenca ključa postaje poznata.

Sa brzinom ubacivanja od 800 paketa/sekundi i 800 ICMP odgovora u sekundi, kompletna baza podataka IV-a i sekvenci ključeva se može napraviti za $224/800 \approx 20,972$ sekundi, što je oko 6 časova. Ako nekoliko mreža koristi isti ključ, napad se može obavljati paralelno što značajno skraćuje vreme.

Obično tačke pristupa i klijenti odbacuju IV za koje pretpostavljaju da su „slabi”. Rezultat toga je da se smanjuje broj jedinstvenih IV koji se koriste, na mnogo manji broj nego što ih ukupno ima. Real 802.11 Security [10] preporučuje još agresivnije smanjenje IV prostora na 218 što je 262,144 jedinstvena IV-a. Baza podataka o njima se može napraviti za pet minuta, sa stvarno velikom brzinom ubacivanja. 262144 je najmanje jedinstvenih IV koje napad kreiranja WEP ključa može da zahteva. Međutim agresivno filtriranje nije očigledno kod bilo koje opreme testirane tokom

izrade ovog rada. Još se niko nije potrudio da ovaj napad implementira za javnu upotrebu. Jedna od prednosti ovog napada je potpuna nezavisnost od veličine WEP ključa. Čak ni 1Mbit ne bi imao efekta protiv ovog napada.

7.2.2.6 Preusmeravanje paketa

Istaknuti integritet nije nešto što WEP obezbeđuje, ali realno to ne obezbeđuje ni ekvivalentna žična mreža. Pošto IEEE 802.11 standard [12], Sekcija 8.2.3, naglašeno tvrdi da postoji ICV izračunat nad otvorenim tekstom “da bi štitio od neautorizovanih modifikacija”. ICV je implementiran kao CRC koji ne obezbeđuje zaštitu od zlonamernih izmena. Napadač je u mogućnosti da komplementira bite u polju podataka zajedno sa pridodatim ICV da izmeni podatke tako da primalac ne primeti da je postojala modifikacija. Način kako se sprovodi korekcija ICV posle modifikacije podataka je iznet u dodatku Real 802.11 Security [10].

Napadač može da pokuša sa promenom odredišta paketa tako da on stigne na neku mašinu koju on kontroliše. On pri tome mora znati dve stvari pre nego što pristupi napadu; to je pozicija odredišne adrese u paketu, i vrednost odredišne adrese. Ako to ima, on može da uradi XOR originalne odredišne adrese i kriptovanom adresom da bi dobio sekvencu ključa za taj bajt. Tada može da uradi XOR sekvence ključa i adrese na koju namerava da preusmeri paket i rezultat postavi zajedno sa ostalim kriptovanim originalnim bajtovima. Sada još mora modifikovati kriptovani ICV tako da bi frejm ostao validan.

Kao prvo, ovaj napad zahteva od napadača da bude u poziciji man-in-the-middle. Samo napadač može da vidi originalni saobraćaj, pošto pristupna tačka prima samo modifikovane okvire, bez ijednog originalnog. Napadač može da pokupi saobraćaj, modifikuje zaglavlja, i vrati ponovo u mrežu u bilo koje vreme. Ima dosta složenih problema koje pri tome treba rešiti kao što je pitanje prolaska paketa kroz ruter ili firewall. Nema javno poznatog softvera koji služi za napad preusmeravanjem ili modifikaciju paketa. Razlog za to je svakako mogućnost primene jednostavnijih napada kao što je krekovanja WEP ključa koji se koristi umesto ovog napada.

7.2.2.7 Napad grubom silom na WEP ključ

WEPLab kao što je već pomenuto u ovom radu takođe omogućava jednostavan način za testiranje svakog mogućeg WEP ključa na validnost. On proverava preko 300000 ključeva u sekundi na prosečnom PC računaru. Za 104 bitni ključ to bi trajalo 2,143,836,631,537,678,676 / 2 godina. A 40 bitni ključ bi verovatno mogao da se sa verovatnoćom od preko 50% otkrije za 21 dan. To vreme nije nedostižno pa je zbog toga 40 bita bila granica za odobravanje izvoza osetljive opreme iz SAD. Nije nerealna pretpostavka da dobro opremljenje agencije i vladine službe imaju mogućnost da razbiju 40 bitni ključ skoro u realnom vremenu.

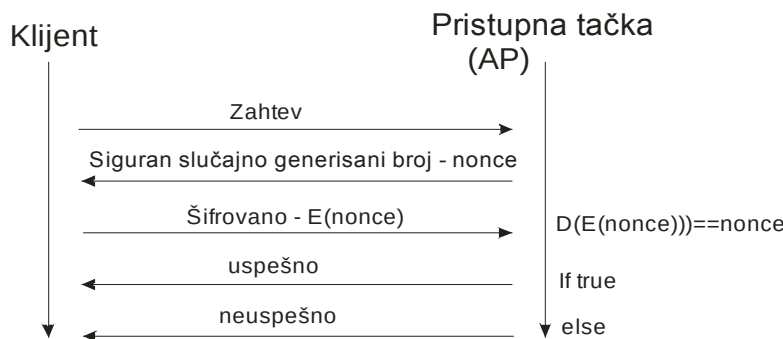
Na slici 7.2.2.7 je početak napada tipa brute-force na 40 bitni ključ WEPLab je pokrenut sa parametrima -b i -64 da bi se napad usmerio na 40 bitni ključ. Najpre se vrši učitavanje velikog broja prikupljenih paketa koji su smešteni u fajl dump.cap, onda se odabere 10 od njih da bi se uradila validacija ključa koji se proverava. Na kraju proces pogađanja ključeva počinje, poslednja linija pokazuje dokle se stiglo sa testiranjem 16,941,566 ključ pri brzini od 308,028 ključa/sekundi i trenutno se testira ključ fd:81:02:01:00.

```
weplab -b -d 1 -k 64 dump.cap
weplab - Wep Key Cracker Wep Key Cracker (v0 .0.8 - beta ).
Jose Ignacio Sanchez Martin - Topo[LB] topolb@users.sourceforge.net
Total valid packets read : 333539
Total packets read : 1149079
10 packets selected .
Packet 0 --> 60 total lenght , 32 data lenght (just encrypted data)
Packet 1 --> 60 total lenght , 32 data lenght (just encrypted data)
Packet 2 --> 60 total lenght , 32 data lenght (just encrypted data)
Packet 3 --> 60 total lenght , 32 data lenght (just encrypted data)
Packet 4 --> 60 total lenght , 32 data lenght (just encrypted data)
Packet 5 --> 60 total lenght , 32 data lenght (just encrypted data)
Packet 6 --> 60 total lenght , 32 data lenght (just encrypted data)
Packet 7 --> 60 total lenght , 32 data lenght (just encrypted data)
Packet 8 --> 60 total lenght , 32 data lenght (just encrypted data)
Packet 9 --> 269 total lenght , 241 data lenght (just encrypted data)
Launched process number 0
Process number : 0 ==>> 16941566 keys tested [308028 c/s] >>> Key : fd :81:02:01:00
```

Slika 7.2.2.7 WEPLab kreiranje 40 bitnog ključa metodom grube sile

7.2.3 Narušavanje autentikacije

7.2.3.1 Mehanizam za autentikaciju



Slika 7.2.3 Protokol za autentikaciju sa deljenim ključem

Postoje dva moda za autentikaciju:

Otvoreni sistem: Dozvoljava bilo kome da se pridruži na pristupnu tačku (AP).

Deljeni ključ: Dozvoljava pridruživanje samo klijentima koji znaju deljeni ključ.

Otvoreni sistem za autentikaciju je null mehanizam autentikacije. Ovim načinom autentikacije tačka pristupa nije u mogućnosti da utvrdi da li je klijent validan. Ovaj nedostatak predstavlja sigurnosnu slabost ukoliko u WLAN-u nije primenjen WEP. Čak i sa statičnim WEP-om, omogućenim kod klijenta i tačke pristupa, otvorena autentikacija ne pruža način utvrđivanja ko koristi WLAN uređaj. Autorizovani uređaj u rukama neautorizovanog korisnika predstavlja pretnju po bezbednost mreže jednaku onoj koju omogućuje i mreža bez sigurnosnih mehanizama.

Autentikacija deljenim ključem (Shared Key) koristi pojednostavljenu challenge-response šemu, kao što je prikazano na Slici 7.2.3. Kada klijent pokuša da se konektuje na pristupnu tačku, on prima niz karaktera otvorenog teksta, koji se naziva nonce ili challenge-text. Kao preduslov da bi se klijent autentikovao potrebno je da zna WEP ključ, i kriptovanjem ključa koristeći klasično WEP kriptovanje: $E(nonce)$ na

slici. Klijent zatim šalje tako kriptovan odgovor. Pristupna tačka dekriptuje odgovor $D(E(\text{nonce}))$, i poredi rezultat sa nizom koji je poslala kao nonce. Ako su identični pristupna tačka šalje odgovor klijentu sa pristankom na konekciju, ako nonce ne odgovara, odgovor pristupne tačke je negativan.

Autentikacija deljenim ključem može da se obavlja u obe vrste, WEP kriptovanim mrežama i u mrežama gde nema kriptovanja. U mrežama gde nema kriptovanja WEP i tajni WEP ključ se još uvek zahteva, osim ako se sav saobraćaj ne šalje kao otvoreni tekst.

Provera autentičnosti deljenim ključem zahteva od klijenta da koristi unapred podešen WEP ključ za kriptovanje teksta (challenge) dobijenog od tačke pristupa. Proces razmene teksta se obavlja preko bežične veze i podložan je riziku da se dođe do sadržaja teksta (napad poznat kao plaintext attack). Ova slabost autentikacije deljenim ključem se bazira na matematičkom principu koji stoji iza procesa kriptovanja. Proces kriptovanja se obavlja primenom matematičke operacije ekskluzivno ili (XOR). Ukoliko se na čist tekst i njemu odgovarajući kriptovani tekst primeni operacija XOR, rezultat je tok ključa za WEP ključ i IV par.

7.2.3.2 Jednostrana autentikacija

Dobro poznati nedostatak protokola je da se samo sa jedne strane vrši autentikacija. Klijent se autentikuje pred pristupnom tačkom, ali se pristupna tačka ne autentikuje klijentu. Tako je moguće postaviti lažnu pristupnu tačku koja bi se prikazivala kao prava, i prihvatala klijente umesto prave pristupne tačke. Imitacija pristupne tačke je poznata pod nazivom rogue access point. Ako bi u prvom okviru koji šalje klijent stajao zahtev pristupnoj tački da se ona autentikuje, a nakon toga bi se klijent autentikovao prijemnoj tački, to bi bila dvostrana autentikacija.

7.2.3.3 Bilo ko se može autentikovati

Ali postoje još ozbiljniji propusti od jednostrane autentikacije. Svako ko ima sekvencu ključa i IV za zadnjih 136 bajta se može autentikovati na pristupnu tačku. Na osnovu Slike 7.2.1. i jednakosti (7.2.3.3.1), (7.2.3.3.2) i (7.2.3.3.3) se vidi kako klijent može da napravi odgovor.

$$\text{Sekvenca ključa} = \text{RC4}(\text{IV} \parallel \text{WEP key}) \quad (7.2.3.3.1)$$

$$\text{ICV} = \text{CRC32}(\text{nonce}) \quad (7.2.3.3.2)$$

$$E(\text{nonce}) = (\text{nonce} \parallel \text{ICV}) \oplus \text{Sekvenca_ključa} \quad (7.2.3.3.3)$$

Pri tome se korak u relaciji (7.2.3.3.1) može izostaviti ako su već poznati sekvenca ključa i IV. Uslov da je poznat WEP ključ je eliminisan. U zavisnosti od implementacije na pristupnoj tački, može se pokupiti validna challenge – response sesija i tako obezbediti sekvenca ključa. Dobre implementacije ne dozvoljavaju da se IV koristi više od jednog puta, ikada. Međutim 802.11 standard implicira da je to dozvoljeno. Ako je korišćenje IV dobijenog na osnovu prethodne sesije challenge-response odbijeno, postoji drugi način da se dođe do sekvence ključa.

Slabost sledi iz činjenice da klijent stvarno ne dokazuje pristupnoj tački da on zna WEP ključ. Klijent samo dokazuje da je u mogućnosti da napravi paket sa određenim

sadržajem, što nije tako teško ako ima sekvencu ključa i IV. Napad je takođe opisan u Real 802.11 Security [10, str. 330].

7.2.3.4 Zamena MAC adrese (Spoofing)

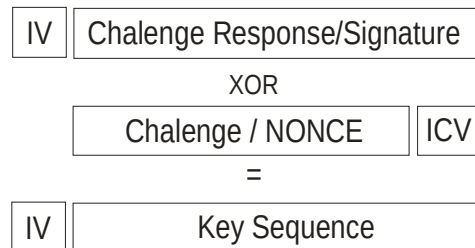
Ako je autentikacija omogućena a kriptovanje nije, autentikacija je podložna narušavanju u svakom slučaju. Čak i da je mehanizam autentikacije potpuno savršen, on ne može da zaustavi nikoga ko potura MAC adresu korisnika koji je već autentikovao. To znači da je dobijanje pristupa isto što i zaobilaženje MAC adresnog filtera.

7.2.4 Ubacivanje Paketa (Packet Injection)

Moguće je ubaciti kriptovane pakete proizvoljnog tipa i podatke. Jedan IV i njemu odgovarajuća sekvenca ključa se mora poznavati da bi bilo moguće takvo ubacivanje. U odeljku 7.2.2 se govori o načinima za dobijanje sekvence ključa. Postoje još neki načini da se dođe do sekvence ključa, npr. preko inicijalnog mehanizma autentikacije. Sekvenca ključa se može koristiti nekoliko puta, čak i uzastopno. To je zato što nema pravila za određivanje vrednosti IV – IV nije redni broj kao što bi trebalo da bude, a to je tako i kod WPA kriptovanja.

Jednom kada se dobije odgovarajući tok ključa, bilo koji podaci nešto manje dužine od toka ključa se mogu ubaciti. Ako je tok ključa kratak, on se može produžiti pomoću napada poznatim otvorenim tekstom. ICV je izračunat i dodat podacima i rezultat toga se XOR-uje sa sekvencom ključa a na kraju ubačen u data okvir sa odgovarajućim IV.

Kao što je navedeno u odeljku 7.2.2.1, najmanje $2900/2=1450$ paketa/sekundi je moguće ubaciti. Međutim u eksperimentima sa retransmisijom i ubacivanjem paketa neke pristupne tačke (kao što je Linksys WRT54G) dolaze u potpuno zagušenje kad god im prispe više od 800 paketa/sekundi. Tada pristupna tačka ne može da nastavi sa radom dok se ne uradi resetovanje prekidom napajanja. U tom periodu će odgovor AP-a na sve prispele okvire biti deautentikovao okvir. Najverovatnije da je razlog za to što odgovor od pristupne tačke nije nikada potvrđen sa acknowledgement okvirom od napadača. Tako pristupna tačka vidi da nešto nije u redu. Neke kompletnije implementacije uspevaju da pošalju potvrdu prijema, ali i one imaju poteškoća sa vremenom potrebnim za softversku obradu prispelih paketa, što opet ne pomaže da se poveća broj ubačenih paketa u sekundi.



Slika 7.2.4.1 Dobijanje sekvence ključa tokom inicijalne autentikacije

Dobijanje sekvence ključa je trivijalno kada je tajnost narušena, kao što je pokazano u odeljku 7.3.2. Drugi način za dobijanje sekvence ključa je kada je omogućena autentikacija deljenim ključem. Nonce i E(Nonce) na slici 7.2.3 su

otvoreni tekst i njemu odgovarajući kriptovani tekst. Posle međusobnog XOR-ovanja daju napadaču mogućnost dobijanja sekvence ključa koja je duga 136 bajtova. IV se uvek šalje kao otvoreni tekst. U slučaju kada je kriptovanje dodato autentikaciji, nema nikakvog razloga za upotrebu autentikacije sa deljenim ključem. Kriptovanje samo po sebi obezbeđuje isti nivo autentikacije zato što samo klijent koji zna tajni WEP ključ može da kriptuje pakete i komunicira. Potpuno u suprotnosti sa intuitivnim shvatanjem, autentikacija deljenim ključem mora biti isključena iz bezbednosnih razloga! Otvoreni sistem autentikacije je podrazumevani mehanizam autentikacije, ali iako je definisan precizno ovaj metod dobijanja sekvence ključa retko daje rezultate. Sa lažnom pristupnom tačkom, moguće je naterati klijenta da se autentikuje, mada to zavisi i od podešenja bezbednosnih parametara koja korisnik ima.

Sve do IEEE 802.11 standarda iz 1999. god. postojala je mogućnost neautorizovanog otkrivanja sekvence ključa u toku postupka autentikacije. Preporuka koju ovaj standard daje je izbegavanje korišćenja istih parova sekvence ključa i IV u narednim okvirima. Ova preporuka ne pomaže protiv preuzimanja sekvence ključa, ali je sredstvo za odbranu od preuzimanja autorizacije. Međutim to nema većeg značaja, napadač iako preuzme autorizaciju ponovnom upotrebom prethodno uočenog challenge response, nadalje nema pristupa kriptovanoj komunikaciji.

```
# ./prgasnarf -i eth3
Auth Frame : Auth Type: Shared -Key - 00 01:00:01:00
Auth Frame : Auth Type: Shared -Key - 01 01:00:02:00 :seq = 02 : Challenge
Frame ? Auth Frame : [3] Encrypted Auth Response
Auth Frame : [4] responder OK with auth
BSSID : 00121749 d181 SourceMAC : 000 e35a30f56
Created 136 byte PRGA for IV: 4b:39: fd
Created prgafile .dat in current directory
```

Slika 7.2.4.2 listing PRGASnarf

Softverski paket pod nazivom WEPWedgie stoji na prijemu čekajući authentication okvire sa challenge response. Jednom kada ih pronade, izdvaja sekvencu ključa i čuva je u fajlu zajedno sa IV. U listingu na Slici 7.2.4.2 PRGASnarf iz paketa WEPWedgie nadzire WLAN interfejs eth3 očekujući sesiju autentikacije. Prve četiri linije opisuju svaki okvir za autentikaciju koji je uhvatio, prvo zahtev, zatim nonce, pa kriptovani odgovor i na kraju pozitivan odgovor za autentikaciju. BSSID i MAC adresa autentikovanog klijenta su prikazani u sledećoj liniji. Zadnje dve linije daju informacije o veličini sekvence ključa, njegovom IV-u i u koji fajl su smešteni.

7.2.5 Ubrzano prikupljanje inicijalnih vektora

Postoji mogućnost za ubrzavanje procesa prikupljanja IV i odgovarajućeg kriptovanog teksta koji su neophodni za kreiranje WEP ključa. Klijent ili pristupna tačka su prevareni i šalju kriptovane okvire podataka, svaki sa novim IV. Da bi obavio posao, napadač mora da ubacuje pakete i za to ima opcije:

- Ponovno slanje prikupljenih paketa prema redosledu da bi primio nove odgovore,
- Slanje paketa deautentikacije prema klijentu tako da on mora ponovo da se autentikuje.

- Pravljenje paketa, njihovo kriptovanje sa poznatom sekvencom ključa i njihovo slanje da bi se dobio odgovor na njih. Povezivanje sa klijentom preko spoljne mreže.

Retransmisija je metod koji koristi Aircrack. Usiljena reautentikacija je sporiji proces u poređenju sa ostalim opcijama. Ubacivanje paketa zahteva dodatno poznavanje mreže kao što su IP adrese. Povezivanje sa klijentom preko spoljne mreže zahteva dosta znanja i nije praktično u realnim uslovima napada na WLAN, zato se takav napad retko primenjuje.

7.2.5.1 Retransmisija paketa

Napadač može da izvrši retransmisiju (slanje primljenih paketa) onih paketa koje je uhvatio od validnog klijenta ili pristupne tačke. Za to su najpogodniji paketi koji nose podatke u connection-less protokolima. Kod protokola orjentisanih ka konekciji, duplirani paketi mogu biti otkriveni i uništeni. UDP i ARP paketi su odličan izbor. Određeni tipovi paketa imaju neke osobine na osnovu kojih napadač može da ih identifikuje sa velikom verovatnoćom. IEEE 802.11 okviri koji nose ARP zahtev su dugi 68 bajta i adresirani na broadcast MAC adresu (FF:FF:FF:FF:FF:FF). ARP zahtev može biti potpuno pojednostavljen i opšti ako se ARP keš tabela osvežava veoma često od strane bilo kojeg klijenta u mreži. ARP zahtev sledi kada se klijenti konektuju i diskonektuju često na mrežu, što je slučaj kod bežičnih mreža. Zbog toga što je ARP zahtev broadcast, zahtevi odaslati u žičnoj mreži dopiru do bežične mreže iako striktno gledano nebi trebali da se nadju tu.

```
# tcpdump -i eth2 arp
tcpdump : verbose output suppressed , use -v or -vv for full protocol decode
listening on eth2 , link - type EN10MB ( Ethernet ), capture size 96 bytes
06:15:34.747002 arp who - has 192.168.1.1 tell 192.168.1.116
06:15:34.748811 arp reply 192.168.1.1 is -at 00:12:17:49: d1 :7f (oui Unknown )
06:15:39.744364 arp who - has 192.168.1.116 tell 192.168.1.1
06:15:39.744386 arp reply 192.168.1.116 is -at 00:0 d:54:9 d:ec:4b ( oui Unknown )
06:19:49.663522 arp who - has 192.168.1.1 tell 192.168.1.140
06:19:54.660989 arp who - has 192.168.1.116 tell 192.168.1.1
06:19:54.661011 arp reply 192.168.1.116 is -at 00:0 d:54:9 d:ec:4b ( oui Unknown )
06:20:34.767898 arp who - has 192.168.1.1 tell 192.168.1.116
06:20:34.769336 arp reply 192.168.1.1 is -at 00:12:17:49: d1 :7f (oui Unknown )
06:25:29.790841 arp who - has 192.168.1.1 tell 192.168.1.116
06:25:29.792594 arp reply 192.168.1.1 is -at 00:12:17:49: d1 :7f (oui Unknown )
06:25:34.787133 arp who - has 192.168.1.116 tell 192.168.1.1
06:25:34.787157 arp reply 192.168.1.116 is -at 00:0 d:54:9 d:ec:4b ( oui Unknown )
06:26:45.241247 arp who - has 192.168.1.116 tell 192.168.1.1
06:26:45.241282 arp reply 192.168.1.116 is -at 00:0 d:54:9 d:ec:4b ( oui Unknown )
06:27:00.255980 arp who - has 192.168.1.116 tell 192.168.1.140
06:27:00.256002 arp reply 192.168.1.116 is -at 00:0 d:54:9 d:ec:4b ( oui Unknown )
```

Slika 7.2.5.1.1 listing ARP saobraćaj

Na Slici 7.2.5.1.1 se vidi ARP saobraćaj jedne male mreže koja se sastoji od jednog bežičnog klijenta (.116), jedne pristupne tačke (.1), i klijenta spojenog na pristupnu tačku preko žične mreže (.140). Ništa posebno se ne dešava u mreži što bi izazvalo ARP saobraćaj, ali se ARP paketi pojavljuju veoma često. To je zbog trajanje keša na pristupnoj tački od samo jednog minuta. Posle isteka tog vremena klijent više nije na mreži. Čak i kada računar ne radi ništa, uobičajeno je da instalirani softver povremeno traži konekciju ka internetu, pa se zbog toga šalju ARP zahtevi ka pristupnoj tački ili ka internet gateway.

```
# aireplay -x 800 -3 -b 00:12:17:49:D1 :81 -h 00:0E :35: A3 :0F :56 ath0
Saving ARP requests in replay_arp -0530 -060850. cap
```

You must also start airodump to capture replies .
Read 11922 packets (got 1024 ARP requests), sent 5720 packets ...)

Slika 7.2.5.1.2 Aircrack prosleđuje prikupljene ARP zahteve

Na Slici 7.2.5.1.2 je prikazana sesija gde Aireplay vrši retransmisiju prikupljenih ARP zahteva. -x 800 govori Aireplay da radi retransmisiju okvira 800 puta u sekundi, -3 omogućava mod retransmisije, -b 00:12:17:49:D1:81 je BSSID koji treba napasti, i -h 00:0E:35:A3:0F:56 je MAC adresa klijenta u WLAN mreži. U zadnjoj liniji Aireplay daje status o tome koliko je okvira prikupio, i koliko od njih je verovatno ARP paketa.

7.2.5.2 Forsiranje ponovne autentikacije

```
Use -c to target a specific station .  
# ./ aireplay -0 5 -a 00:13:10:9 B:47: F1 ath0  
16:01:04 Sending DeAuth to broadcast -- BSSID : [00:13:10:9 B:47: F1]  
16:01:04 Sending DeAuth to broadcast -- BSSID : [00:13:10:9 B:47: F1]  
16:01:05 Sending DeAuth to broadcast -- BSSID : [00:13:10:9 B:47: F1]  
16:01:09 Sending DeAuth to broadcast -- BSSID : [00:13:10:9 B:47: F1]  
16:01:12 Sending DeAuth to broadcast -- BSSID : [00:13:10:9 B:47: F1]
```

Slika 7.2.5.2.1 Aircrack ubacuje okvire za deautentikaciju

Drugi metod prikazan na slici 7.2.5.2.1 izvršen prema listingu, je ubacivanje deauthentication okvira klijentu i tako ga prisiliti da se ponovo autentikuje i kriptuje novi challenge. Pri eksperimentisanju ovaj metod se nije pokazao efikasnim. Kada je kao klijent korišćen Intel IPW2915ABG Mini-PCI adapter sa ipw-1.0.4 Linux drajverom, postoji vremenska pauza pre nego što klijent pokuša se ponovnom autentikacijom. Tako vreme za prikupljanje jednog IV-a postaje predugačko, oko pola IV-a za sekundu. Uz to napad nije prikriven pošto prekida žrtvu u radu odbijajući da mu dozvoli pristup u bežičnu mrežu.

7.2.5.3 Upotreba poznate sekvence ključa

Sekvenca ključa i IV se mogu koristiti za ubacivanje paketa. Koristeći dodatno znanje o mreži ili sa nekoliko procena, ICMP zahtev se može napraviti i ubaciti. Za ICMP zahtev treba imati dve IP adrese, izvorišnu i odredišnu. Odredišna adresa mora da pripada klijentu u mreži, a odredište može da bude bilo koja IP adresa u opsegu adresa za WLAN. Pogađanje prave izvorišne adrese može da bude veoma teško obzirom da postoji 232 moguće vrednosti. Sreća po napadača je da većina pristupnih tačaka drži svoje klijente u posebnoj klasi IP adresa, 10.0.0.0/24 ili 192.168.0.0/16 opsezima. Pristupna tačka obično ima prvu adresu u opsegu, npr. 1192.168.0.1, i WLAN klijentima daje adrese u opsegu do 192.168.0.100.

Softverski alat za pravljenje i ubacivanje paketa podesan za ubrzano prikupljanje IV nije javno dostupan. ARP retransmisija je jednostavnija za primenu pošto su ARP zahtevi dostupni i lako prepoznatljivi.

7.2.5.4 Pokretanje saobraćaja u praznoj mreži

Pristupna tačka može samo da prima okvire koji dolaze od autentkovanih klijenata. Šta ako nema klijenta koji je konektovan na pristupnu tačku? Još uvek je moguće pokrenuti pristupnu tačku da počne sa slanjem kriptovanih paketa. Onoliko dugo koliko je mod za autentikaciju u mreži otvoren (ili ranjiv kao što je prikazano u

Sekciji 7.2.3) napadač može da se autentikuje i pridruži mreži. Pristupna tačka će tada prosleđivati saobraćaj namenjen njenoj MAC adresi ili broadcast adresi. Opet se ARP javlja kao spas. ARP paketi od klijenata u žičnoj mreži završavaju u WLAN dok ih pristupna tačka prosleđuje lažnom klijentu. Sada retransmisija može da počne kao što je opisano u odeljku 7.2.5.1.

7.3 Wireless Protected Access (WPA)

7.3.1 Osnove WPA i slabosti

Kada je postalo jasno da postoje ozbiljne bezbednosne slabosti u WEP mehanizmu zaštite i korisnici i proizvođači opreme su tražili bolje rešenje. Tada je počeo rad na standardu 802.11i (poznat i kao WPA2). Izrada standarda je tekla presporo, a trebalo je iskoristiti postojeći hardver uz poboljšanje bezbednosti. Standard 802.11i je predvideo primenu AES umesto RC4 za kriptovanje, što stari hardver nije mogao da podrži. Zbog toga je WiFi alijansa napravila novi bezbednosni sistem pod nazivom Wireless Protected Access (WPA) zasnovan na delovima 802.11i standarda, ali sa mogućnošću da koristi hardver na kojem je radio WEP. Da bi se kreirao jak bezbednosni mehanizam zasnovan na hardveru koji je radio pod WEP-om uključen je novi protokol nazvan Temporal Key Integrity Protocol (TKIP) sa svoja tri elementa. Ti elementi su novi Message Integrity Code (MIC) poznatiji kao Michael, novi sekvencijalni brojač paketa i nova funkcija mešanja ključeva za svaki paket. WPA koristi RC4 sa 128 bita osnovnim ključem i 64 bita ključem za autentikaciju zajedno sa 48 bita IV i sa već pomenutom funkcijom za mešanje ključeva. Michael štiti podatke o izvornoj i odredišnoj adresi određuje redosled IV a protokol IEEE 802.11X upravlja ključevima. Po zatom algoritmu se izračunava MIC na strani predajnika koristeći funkciju sa ključem i podacima kao ulazom. Takav proizvod algoritma se šalje zajedno sa korisnim podacima ka prijemniku. Na strani prijemnika se izvodi ista operacija i rezultat se poredi sa MIC koji je primljen zajedno sa korisnim podacima. Klasičan MIC (kao što je HMAC-SHA1 koji se koristi u IPsec) ne može se koristiti na postojećem hardveru zato što zahteva veću procesorsku snagu. Zato je napravljen Michael za WPA. Sa takvim MIC algoritmom postoje degradacije performansi ali nema poznatog algoritma koji sa tako malom procesorskom snagom obezbeđuje takav nivo bezbednosti. Michael koristi šiftovanje XOR i sabiranje da bi napravio 64 bita dug dodatak za autentikaciju koji se šalje zajedno sa korisnim podacima. Nivo bezbednosti se meri u bitima, i Michael ima nivo bezbednosti od samo 20 bita, što ga čini veoma nesigurnim. Da bi prevazišao taj problem WPA zahteva nove ključeve u slučaju greške u validaciji sa MIC. To menjanje ključeva je ograničeno na jednom u minuti, kako bi se sprečio napad ponavljanjem (replay attack) u WPA. WEP je proširen sa 48 bita dugim rednim brojem, koji je pomešan sa ključem za kriptovanje iz razloga vezanih za implementaciju. Na ovakav način nastaje ICV (Integrity Check Value). U cilju sprečavanja FMS (Fluhrer-Martin-Shamir) napada kao u slučaju WEP-a postoji funkcija za mešanje ključeva za svaki paket. Ova funkcija koristi osnovni ključ, MAC adresu predajnika i redni broj paketa kao ulaz na osnovu kojeg pravi ključ za dati paket. 802.11X se koristi da obezbedi WPA sa novim ključevima za kriptovanje (128 bita osnovni ključ) i 64 bita ključ za autentikaciju koji koristi Michael prilikom svake nove asocijacije.

Dok su sa razvojem WPA korigovani problemi uočeni kod WEP, otkrivene su nove slabosti [13]. U literaturi ima mišljenja da je WPA (sa PSK) lakši za kreiranje

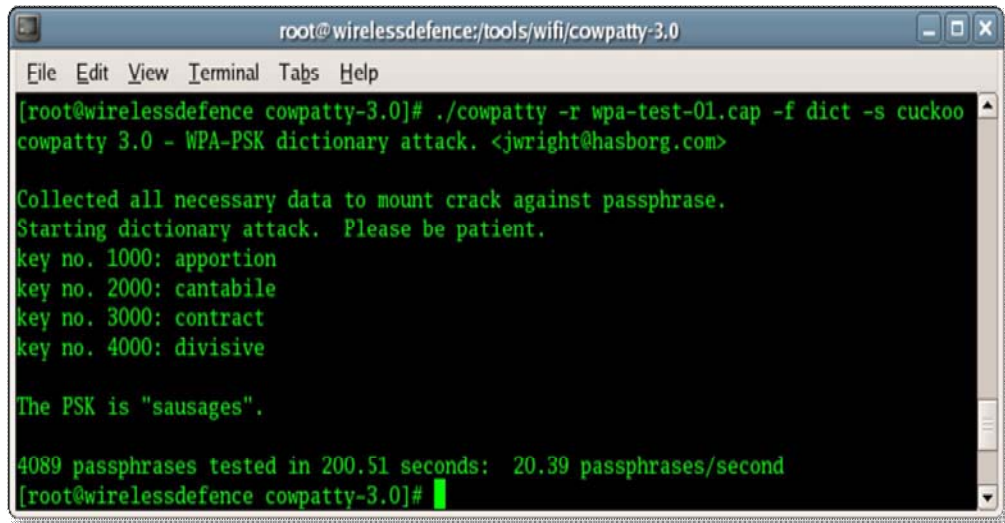
nego WEP. Sa unapred pripremljenim rečnikom postiže se velika brzina rečničkog napada. Slabost vezana za Michael algoritam (koji se koristi sa WPA), se odnosi na prekid rada pristupne tačke (AP) u slučaju otkrivanja dva pokušaja ometanja u roku od jednog minuta. To pruža mogućnost za jednu vrstu DoS napada, ali obzirom da postoje DoS napadi koji se lakše izvode a zasnovani su na slabosti standarda 802.11 to se ne uzima kao veliki nedostatak. Na početku prenosa podataka kada se koristi WPA-PSK dešava se četvorostruki handshake kako bi se uspostavio sistem šifrovanja. Informacije poslate u okviru četvorostrukog handshake se mogu iskoristiti za offline rečnički napad. U tom procesu privremeni ključ se koristi da napravi hesh okvir. Neki od brojnih programa za offline rečnički napad se može modifikovati da koristeći informacije od handshake izvede napad. Prema WPA standardu korisnik bi trebalo da izabere password koji je duži od 20 karaktera, ali većina ljudi to nerado čini iz sasvim praktičnih razloga, a kratki passwordi se ne mogu odupreti offline rečničkim napadima.

7.3.2 Probijanje WPA – rečnički napad

WPA i WPA2 su podložni rečničkom napadu kada rade u Pre Shared Key (PSK) modu. Napadač može da uhvati saobraćaj iz već uspostavljene WPA/WPA2 sesije i da primeni rečnički napad kako bi dobio PSK. To je čisti rečnički napad, a može se predupređiti upotrebom relativno jakih korisničkih šifara i njihovom periodičnom rotacijom [14]. WPA i WPA2 u Enterprise modu nije podložan ovakvim napadima budući da koristi 802.11X. Za rečnički napad na WPA/WPA2 mreže u PSK modu zasnovane na TKIP protokolu može se koristiti open source softverski alat „coWPAtty“ autora Joshua Wright [15]. Alat radi pod Linux-om. Koristi se tako što se posle preuzimanja sa interneta (poslednja verzija je coWPAtty-4.2) iskopira u /tools/wifi. Nakon toga raspakuje se arhiva komandom `tar zxvf cowpatty-4.2.tgz`, pređe na direktorijum `cowpatty-4.2` i uradi `make`, time je završena instalacija. Kako bi izveli rečnički napad treba obezbediti fajl sa uhvaćenim saobraćajem koji u sebi sadrži i TKIP četvorostruki handsake, fajl sa rečnikom koji sadrži moguće pasworde i SSID za mrežu koja se napada. Prilikom prikupljanja četvorostrukog handshake mora se čekati trenutak kada se klijent pridružuje na mrežu ili se preporučuje da se klijent navede na forsirano ponovno pridruživanje na mrežu i to pomoću alata kao što je `void11` ili `aireplay` i da se prikupi handshake koristeći `kismet`, `ethereal` ili `airodump`.

Primer komande za pokretanje `cowpatty` alata je u sledećem redu.

`./cowpatty -r wpa-test-01.cap -f dict -s cuckoo`



```
root@wirelessdefence:/tools/wifi/cowpatty-3.0
File Edit View Terminal Tabs Help
[root@wirelessdefence cowpatty-3.0]# ./cowpatty -r wpa-test-01.cap -f dict -s cuckoo
cowpatty 3.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against passphrase.
Starting dictionary attack. Please be patient.
key no. 1000: apportion
key no. 2000: cantabile
key no. 3000: contract
key no. 4000: divisive

The PSK is "sausages".

4089 passphrases tested in 200.51 seconds: 20.39 passphrases/second
[root@wirelessdefence cowpatty-3.0]#
```

Slika 7.3.2.1 coWPAtty alat za WPA-PSK rečnički napad

Kao što se vidi ovaj rečnički napad traje oko 3 minuta, a može se dodatno ubrzati ako se ranije izračuna WPA-PMK kako bi se krekovao WPA-PSK.

wpa-test-01.cap je fajl koji sadrži četvorostruki handshake,

dict je fajl sa passwordima,

cuckoo je SSID za napadnutu mrežu.

Na internetu se mogu pronaći fajlovi kao što je lookup tabela za 1000 SSID sa preko 170,000 reči koje se koriste za passworde. Rezultujuća tabela je veličine oko 7 GB [16]. Za komercijalne svrhe postoje tabele veličine i do 33 GB.

Postoje i drugi - komercijalni alati za ovu vrstu napada, kao što je WPA Key Recovery (WPAKR) koji je dodatak alatu CommView a oba su proizvod iste firme[17]. Ovaj softver ima mogućnost paralelnog procesiranja na više računara u mreži, kao i mogućnost dodatnog definisanja pravila od strane korisnika za menjanje ponuđenih reči iz rečnika na osnovu kojeg se traži password.

Rečnički napad na WPA traje zavisno od pozicije tražene reči u rečniku kojim raspolazemo, a može biti i neuspešan ako reči koja čini password nema u rečniku (uključujući i njene permutacije). Kod napada na WEP ključ nije potreban rečnik već treba prikupiti nekoliko stotina hiljada paketa saobraćaja i uspeh je zagarantovan. U rečničkom napadu na WPA/WPA2 u PSK modu uspeh napada nije zagarantovan.

7.3.3 Probijanje WPA ako se koristi TKIP

WPA standardno ima dva moda u kojima se korisna informacija (payload) štiti tokom prenosa. To su Temporal Key Integrity Protocol (TKIP) i (AES) CCMP. Posebno je interesantan TKIP, koji je neznatno modifikovana verzija WEP. TKIP implementira usavršenu verziju funkcije za mešanje ključa sesije sa inicijalnim vektorom za svaki paket. To onemogućava sve trenutno poznate napade usmerene ka otkrivanju ključa, zato što svaki bajt ključa za paket zavisi od svakog bajta ključa sesije i inicijalnog vektora. Dodatno je uključen u svaki paket, 64 bita dug Message Integrity Check (MIC) - Michael, da bi sprečio napade na slabi mehanizam CRC32 zaštite integriteta, poznat još od WEP. Da bi sprečio jednostavni napad ponavljanjem, sekvencijalni brojač (TSC) se koristi i dozvoljava prijem paketa samo prema redosledu slanja.

TKIP je napravljen tako da se postojeći hardver, koji podržava WEP, može modifikacijom firmware ili drajvera iskoristi. Tako je RC4 kriptovanje toka podataka ostalo u upotrebi i ICV je i dalje ostao uključen u svaki paket.

Može se pokazati da je moguće dekriptovati saobraćaj chop chop metodom i zatim odaslati paket sa sadržajem kakav šalje korisnik. Za ovo je potrebno da budu zadovoljene sledeći uslovi:

- Mreža koja je napadnuta koristi TKIP za komunikaciju klijenta sa pristupnom tačkom (AP).
- Koristi se IPv4 protokol sa IP opsegom gde je većina bajta u IP adresi poznata napadaču (npr. 192.168.0.X).
- Primenjen je dug interval izmene ključeva za TKIP, na primer 3600 sekundi.
- Mreža podržava IEEE 802.11e mogućnosti za Quality of Service kojima se omogućava 8 različitih kanala (koji se zovu TID traffic identifier) za različite tokove podataka.
- Da je korisnik trenutno u komunikaciji sa mrežom.

Ove uslovi su potpuno realni za većinu mreža koje su u upotrebi. Napadač najpre prisluškuje saobraćaj, sve dok ne uoči ARP zahtev ili odgovor. Takvi paketi se lako uočavaju zbog svoje karakteristične dužine. Uz to, izvorna i odredišna ethernet adresa nisu zaštićene WEP i TKIP pa se zahtev uvek šalje na broadcast adresu u mreži. Većina otvorenog teksta u ovom paketu je poznata napadaču, izuzev poslednjeg bajta izvorišne i odredišne IP adrese, 8 bajta Michael MIC i 4 bajta ICV checksum. MIC i ICV formiraju poslednjih 12 bajta otvorenog teksta.

Sada napadač može da primeni modifikovani chop chop napad kao protiv WEP mreže da bi dekriptovao nepoznate bajtove otvorenog teksta. TKIP uglavnom ima dve protivmere za napade tipa chop chop:

- Ako je paket sa neispravnom ICV vrednošću primljen na strani klijenta, greška u prenosu je simulirana i dobijeni paket će nečujno biti odbačen. Ako je vrednost ICV ispravna, ali MIC verifikacija nije prošla, simuliran je napad i pristupna tačka (AP) će biti upozorena slanjem MIC okvira sa izveštajem o grešci (failure report frame). Ako se više od 2 MIC greške u verifikaciji pojave za manje od 60 sekundi, komunikacija se prekida, i svi ključevi se obnavljaju posle 60 sekundi zastoja u komunikaciji.

- Kada paket pristigne ispravno, TSC brojač za kanal u okviru kojeg je primljen paket se ažurira. Ako primljeni paket ima manju vrednost nego što je aktuelna vrednost TSC brojača, onda je narušen redosled i paket biva odbačen.

Međutim i pored ovih protivmera moguće je izvršiti napad tipa chop chop. Napadač će napad izvršavati na različitim kanalima QoS u odnosu na kanal po kojem je paket primljen. Obično je to kanal na kojem je slab saobraćaj ili ga nema, gde je stanje TSC brojača što manje. Ako je pretpostavka o vrednosti zadnjeg bajta tokom chop chop napada pogrešna, paket se odbacuje bez izdavanja upozorenja o tome. Ako je pretpostavka tačna, klijent šalje MIC okvir sa izveštajem o grešci ali se TSC brojač ne inkrementira. Tada napadač mora da sačeka 60 sekundi posle slanja MIC okvira sa izveštajem o grešci kako nebi došlo do pokretanja protivmera za zaštitu mreže. U okviru 12 minuta napadač može da dešifruje poslednjih 12 bajtova otvorenog teksta (MIC i ICV). Da bi odredio ostale nepoznate bajtove (i izvukao IP adrese pošiljaoca i primaoca), napadač može da pretpostavi vrednosti i da ih proveriti na osnovu dekriptovanog ICV.

Pošto su MIC i otvoreni tekst paketa poznati, napadač može da primeni Michael algoritam reverzno i da dobije MIC ključ koji je korišćen za zaštitu paketa koji je

pristupna tačka poslala prema klijentu. Michael algoritam nije napravljen da bude jednosmerna funkcija pa je reverzni algoritam uspešan koliko i algoritam unapred.

Na ovoj tački, napadač ima MIC ključ i tok ključa koji koristi pristupna tačka za slanje paketa ka klijentu. On je sada u stanju da pošalje uobičajeni paket prema klijentu na bilo kom QoS kanalu, gde je TSC brojač još uvek manji od vrednosti uzete za pokupljeni paket. U većini mreža koje se koriste u stvarnoj upotrebi sav saobraćaj se obavlja preko kanala 0, tako da je napadač u mogućnosti da šalje 7 uobičajenih paketa prema klijentu. Pošto izvrši i ovu fazu napada, napadač je u mogućnosti da dobije preostali tok ključa u roku od 4-5 minuta, zato što samo treba da dešifruje 4 bajta ICV koristeći chop chop. Bajtovi IP adresa se mogu pretpostaviti, MIC se može izračunati koristeći poznati MIC ključ i može se verifikovati na osnovu ICV.

Da bi izazvao štetu, napadač može na primer poslati poruku kojim pobuđuje IDS sisteme koji rade na IP nivou. Alternativno, sobraćaj može biti prerutiran koristeći lažne ARP odgovore. Napadač može da pokuša uspostavu bidirekcionog kanala sa klijentom, ako je klijent konektovan na internet koristeći firewall blokiranje dolaznog saobraćaja, ali dozvoljavajući odlazni saobraćaj. Odgovor od klijenta napadač ne može da primi bežično i da razume, ali se on može ruturati ka napadaču koristeći internet.

Čak iako IEEE 802.11 ne podržava QoS mogućnosti, napad ove vrste je i dalje moguć. Tada napadač treba da onemogući klijentu prijem paketa podataka koje je odabrao za chop chop napad, i mora da diskonektuje klijenta sa pristupne tačke za vreme napada, tako da se TSC brojač ne inkrementira pri prijemu paketa. Pošto napadač uspešno izvrši chop chop napad, on može poslati jedan paket podataka klijentu. Za sada nije objavljeno da je razvijen softver za ovu vrstu napada.

Ako bi napadač bio u mogućnosti da dobije tok ključa validan za QoS kanale i MIC ključ za oba smera komunikacije (prethodno opisani napad omogućava dobijanje toka ključa i MIC ključa za komunikaciju samo u smeru od AP-a do klijenta), on bi mogao da dobije neograničeni tok ključa i tako šalje neograničeno pakete podataka sa proizvoljnim otvorenim tekstom.

Mere za sprečavanje ovakvog napada bi mogle da budu smanjenje vremena za obnavljanje ključeva, na primer na 120 sekundi ili manje. Za 120 sekundi, napadač može samo da dešifruje deo ICV vrednosti na kraju paketa. Alternativno se može onemogućavanjem slanja MIC okvira sa izveštajem o grešci kod klijenata takođe zaštititi mreža od napada ove vrste. Najbolje rešenje je onemogućavanje TKIP i korišćenje CCMP.

Primer ovakvog napada pokazuje da WPA sa jakim šiframa nije potpuno siguran i da se u realnim uslovima može uspešno napadati. Premda ovaj napad nije takav da daje kompletan ključ, moguće je da proizvođači opreme u okviru firmwarea implementiraju zaštitu od ovakvih napada. Zato što se problemi mogu uočiti na višem nivou protokola, ove izmene je moguće ostvariti razvijanjem i isporukom novih drajvera.

7.3.4 Mehanizam zaštite WPA2

WPA2 je deo standarda IEEE 802.11i, zajedno sa WPA. Između ta dva mehanizma za kriptovanje postoji značajna razlika. WPA je nastao kao prelazno-kompromisno rešenje koje omogućava poboljšanje zaštite podataka u bežičnoj mreži uz mogućnost korišćenja opreme na kojoj je radio WEP. WPA2 koristi novi metod za kriptovanje CCMP (*engl.* Counter Mode with CBC-MAC Protocol), zasnovanom na

AES (engl. Advanced Encryption Standard), koji je kriptografski jači od dotadašnjeg RC4.

WPA2 sam ne može da obezbedi potpunu zaštitu, ali u kombinaciji sa IEEE 802.1X portovski orijentisanim autentikacijskim protokolom za kontrolu pristupa može eliminisati većinu bezbednosnih pretnji. To ne znači da je postignuta zaštita od prevara putem socijalnog inženjeringa, DoS napada ili napada interferencijom.

Mod za autentikaciju kod WPA i WPA2 može biti personal i enterprise. WPA2 personal mod generiše 256 bita dug ključ od otvorenog teksta passworda, koji se naziva PSK, ili preshared key. PSK zajedno sa SSID i njegovom dužinom formira matematičku osnovu za PMK (pairwise master key) koji se koristi za četvorostruki handshake (razmenu) i generiše PTK (pairwise transient key) ili ključ sesije koja se uspostavlja između korisničkog uređaja i pristupne tačke. WPA2-personal trpi osporavanja u pogledu distribucije ključeva i održavanja, što ga čini dovoljnim za manje kancelarijske primene ali ne i za veće mreže.

WPA2-Enterprise mod, kontrolu pristupa obavlja na bazi naloga i to na posebnom serveru za autentikaciju. Ovaj mod zahteva uverenja kao što su korisničko ime i password, certifikat, ili password za jednokratnu upotrebu, a autentikacija se obavlja na relaciji korisnički uređaj-centralni server za autentikaciju. Pristupna tačka u ovom slučaju nadgleda konekciju i usmerava pakete za autentikaciju ka odgovarajućem serveru, obično je to RADIUS server. Okvir za ovo je IEEE 802.1X, koji podržava autentikaciju korisnika i uređaja, sa kontrolom na bazi porta, to radi objedinjeno za obe vrste mreža: žičnu i bežičnu.

U internet forumima se mogu naći rasprave o slabostima WPA i WPA2. Preko njih se može doći do informacija da na tržištu postoji komercijalni softverski paket za napad grubom silom, koji koristi procesorsku snagu dve GeForce GTX280 video kartice [18]. Mreža tako opremljenih računara u paralelnom radu, prema navodima proizvođača, može da izvrši „oporavak izgubljenog ključa” za WPA ili WPA2 u roku od nekoliko dana ili nedelja.

7.4 Ugrožavanje bezbednosti podataka u WAN mrežama

Iako se o bezbednosti podataka u standardu IEEE 802.16 vodilo računa još od samog početka stvaranja standarda, bezbednosni mehanizam u IEEE 802.16 (WiMAX) ima još nerešenih pitanja. WiMAX je relativno nova tehnologija, koja nije tako raširena da bi se sa dovoljno primera iz prakse potkrepili dokazi o pretnjama, rizicima i slabostima u realnim situacijama.

U WiMAX pretnje po bezbednost se odnose na PHY i MAC nivo. Mogući napadi na PHY nivou uključuju ometanje (jamming) radio spektra, izazivanja otkaza servisa (DoS) na svim stanicama, i preplavljivanje stanica sa okvirima podataka kako bi ispraznile svoje baterije. Trenutno nema efikasne tehnike koja bi sprečila ovakve napade. Ipak fokus bezbednosti WiMAX je potpuno na MAC nivou [19]. 802.16 bezbednost je implementirana kao podnivo na dnu MAC nivoa sa zadatkom da zaštiti razmenu podataka između MAC i PHY nivoa. U suštini to ne štiti sam PHY nivo od napada koji su usmereni na slabosti svojstvene bežičnim linkovima. Ometanje i izvrtnje signala (scrembing) mogu biti oblici napada na PHY sloj od kojih se WiMAX 802.16 ne može braniti.

Ometanje (jamming) se ostvaruje unošenjem izvora šuma dovoljno jakog da značajno smanji kapacitet WiMAX kanala. Informacije i opremu za izvođenje napada ometanjem nije teško nabaviti.

Izvrtnje signala (scrambling) je slično ometanju ali se ono obično izvodi u kratkom vremenskom intervalu i usmereno je na specifične WiMAX okvire ili delove okvira podataka. WiMAX izvrtnje signala se može selektivno izvoditi na kontrolne ili upravljačke poruke sa ciljem da se održi privid o normalnom funkcionisanju mreže. Delovi razmene podataka koji su usmereni ka jednoj korisničkoj stanici mogu biti skremblovani selektivno, prisiljavajući ih na retransmisiju.

Drugi karakterističan napad na PHY nivo, takozvani napad vodenom torturom (water torture attack), primorava korisničku stanicu da isprazni svoje baterije ili da nepotrebno koristi svoje računarske resurse šaljući joj lažne okvire sa podacima. Ova vrsta napada, naročito na mobilne stanice može biti znatno destruktivnija od klasičnog Denial-of-Service (DoS) napada na uređaje u žičnoj mreži zato što prenosni uređaji imaju ograničene resurse za napajanje.

U ćelijskom modu 802.16 je podlozan na napade ponavljanjem (replay) u okviru kojeg napadač zlonamerno ponovo šalje ispravne okvire sa podacima koje je primio u okviru relejnog prenošenja podataka, i tako dovodi mrežu u zagušenje.

Napadi na PHY nivo mogu biti predupređeni ili oslabljeni pomoću nekoliko jednostavnih mera. Povećanjem izlazne snage signala može se pružiti otpor na napad ometanjem. Posebna oprema, odmah po detektovanju radio ometanja (praćenjem nivoa signala) povećava snagu izlaznih signala do nivoa kada je delovanje malicioznog signala anulirano. U skladu sa [19], širina opsega se može povećavati koristeći tehnike modulacije kao što je FHSS ili DSSS, čime se smanjuje uticaj napada ometanjem. Poseban sofisticirani mehanizam koji odbacuje falsifikovane okvire sa podacima je potreban da bi sprečio praznjenja baterija ili prekomernu upotrebu računarskih resursa i tako anulirao napad vodenom torturom. Novija verzija 802.16 standarda ima podršku za mobilnu komunikaciju sa korisničkom stanicom. To 802.16/WiMAX čini još osetljivijim kada su u pitanju napadi na PHY nivo zato što napadač više ne mora da deluje sa jedne pozicije pa nadgledanje anomalija postaje znatno otežano. Iako je nameran napad skremblovanjem znatno kompleksniji od napada ometanjem, mogućnost da se skremblovanje izvodi je uslovljena prekidanjem prirodnim šumom što određuje periode kada je napad moguć. Ovi napadi se mogu uočiti praćenjem odstupanja performansi sistema od uobičajenih vrednosti.

Postoji nekoliko značajnih nedostataka po pitanju bezbednosti koji su implementirani u MAC nivou 802.16 standarda. Da bi konačno uspostavio bezbednu konekciju za prenos podataka, 802.16 koristi sekvencijalne dvostrane transakcije za kontrolu, autorizaciju i autentikaciju. Prvi problem je što se tokom osnovne i primarne konekcije, MAC upravljačke poruke šalju kao otvoreni tekst i nisu na odgovarajući način autentikovane. Na ovaj način, upravljačke poruke mogu biti presretnute u eteru i izmenjene od strane napadača (man in the middle attack). Na taj način se napadač može pripremiti za buduće napade. Drugi problem 802.16 je korišćenje X.509 sertifikata, standarda za PKI, koji definiše putanju za validaciju sertifikata da bi se identifikovala prava-validna korisnička stanica. On koristi RSA kriptovanje sa SHA-1 hash funkcijom. Uglavnom je sertifikat korisničke stanice unapred zadat od strane proizvođača opreme i kao stalna vrednost postoji u okviru opreme. To pruža mogućnost za krađu i falsifikovanje sertifikata ako se oprema ne čuva na odgovarajući način. Dosta ozbiljnih pretnji po bezbednost proizilazi iz ovakve šeme autentikacije. WiMAX podržava jednostranu autentikaciju na nivou uređaja, kakva postoji i kod WLAN mreža, a zasnovana je na filtriranju MAC adresa. Pretraživanje MAC adresa i njihovo poturanje čine napad putem lažnog predstavljanja sasvim mogućim. Takođe nedostatak obostrane autentikacije omogućava napad tipa čovek u sredini sa lažne bazne stanice. Takav napad nije jednostavno izvesti, zbog upotrebe TDMA modela za

deljenje medijuma u WiMAX. Napadač mora da emituje u isto vreme kada i bazna stanica umesto koje se predstavlja i to sa znatno većom izlaznom snagom predajnika kako bi „prekrio“ njen signal. Nadalje, WiMAX podržava obostranu autentikaciju u mreži na nivou korisnika zasnovanu na izvornom EAP. Podržane su varijante EAP-TLS (Transport layer security) na bazi X.509 sertifikata i EAP-SIM (Subscriber identity module – SIM kartica). Prisluškiivanje upravljačkih poruka je ozbiljna pretnja za korisnike i glavna pretnja za sistem. Na primer, napadač može iskoristiti tu slabost da se uveri u prisutnost žrtve ne njenoj lokaciji pre nego što izvrši napad. Takođe se može iskoristiti od strane konkurencije za mapiranje mreže. Sledeća slabost je kriptovanje zasnovano na data encryption standard (DES). 56 bita DES ključ se može probiti novijim sistemima za napad grubom silom. Pored toga DES sistem kriptovanja ne uključuje funkcionalnost za zaštitu integriteta poruke i zaštitu od napada ponavljanjem (replay attack) pa te slabosti omogućavaju aktivni napad ili napad ponavljanjem. AES mod kriptovanja je u prednosti u odnosu na DES. Prisluškuju se najčešće informacije koje se prenose, što retko uzrokuje sistemske smetnje. Pretnje lažnim predstavljanjem kao bazna stanica ili korisnička stanica su moguće kada su prisutne slabosti u autentikaciji. Krađa identiteta i lažna bazna stanica su tehnike specifične za napad lažnim predstavljanjem (masquerading). Krađa identiteta je ozbiljna pretnja za neautorizovane servise koje pruža WiMAX. Uređaj koji se lažno predstavlja može da koristi hardversku adresu drugog, registrovanog, uređaja do koje se dolazi prijemom okvira sa upravljačkim porukama iz etera. Kad to jednom uspe, napadač može da imitira legitimnu BS (baznu stanicu) sa lažnom BS i tako zbuni njoj pridružene SS (pretplatničke stanice). Te SS pokušavaju da dobiju WiMAX servise od lažne BS, što dovodi do degradacije servisa ili potpunog prekida rada tih servisa. Za poređenje se može uzeti, WiFi mreža koja koristi CSMA (carrier sense multiple access), i to postaje jedna od najvećih bezbednosnih pretnji. Napadač može lako da uhvati identitet legitimne pristupne tačke tako što sluša CSMA proces koji sam otkriva informacije o identitetu AP. Napadač može da napravi maliciozne poruke koristeći identitet legitimne AP, a zatim čekajući da medijum bude slobodan, može da ih distribuira. To je još jedna mogućnost za DoS napad, zato što operacije autentikacije pokreću procedure koje dugo traju. Efekti ovakvog napada se klasifikuju kao srednje teški po sistem zato što se radi o gubitku vremena, ali za korisnika ti efekti mogu biti znatno ozbiljniji.

Može se zaključiti da WiMAX obezbeđuje robusnu autentikaciju korisnika, kontrolu pristupa, tajnost i integritet podataka, koristeći naprednu tehnologiju autentikacije i kriptovanja. WiMAX ima napredan skup bezbednosnih protokola implementiranih na dobar način kao i mehanizam za alokaciju propusnog opsega, što ga čini ozbiljnim kandidatom za aplikacije u poslovnoj primeni. Sa druge strane, pokazuje se da u okviru WiMAX postoje propusti koji omogućavaju ometanje, prisluškiivanje kao i modifikaciju upravljačkih poruka, lažno predstavljanje BS, i DoS napade. To ukazuje na obilnost sa kojim treba pristupati izradi svake sledeće verzije standarda 802.16, kako bi se izbegle greške koje su se javile u prehodnim verzijama kao i u standardu 802.11.

8. „Ratna vožnja“ (Wardrive)

8.1 Pojam „ratne vožnje“ (Wardrive)

Ratna vožnja je prikupljanje statističkih podataka o bežičnim računarskim mrežama u datoj geografskoj oblasti tako što se WLAN prijemnikom oslušuju njihovi javno dostupni broadcast okviri. Bežične pristupne tačke (AP) objavljuju svoje prisustvo prema zadatom intervalu (obično 100 ms) šaljući u eter pakete podataka koji sadrže njihove identifikatore servisa (SSID) i još drugih podataka. Softverski alat za ratnu vožnju se pokreće na portabl računaru ili na nekom od prenosnih računara (laptop ili PDA). U toku ratne vožnje, krećete se u automobilu dok pokrenuti softver prikuplja podatke koje emituju obližnje pristupne tačke (AP). Većina softverskih alata namenjenih za ratnu vožnju ima mogućnost dodavanja informacija u log fajl o trenutnoj poziciji koje preuzima sa GPS-a. To omogućava da se pozicija uočenih pristupnih tačaka sačuva i nacrtu u obliku elektronskih mapa softverom kakav je npr. Microsoft MapPoint.

Softverski alat koji se dosta koristi za wardrive je Network Stumbler (neformalno, NetStumbler). Ovim alatom se prikupljaju samo oni podaci koje je pristupna tačka učinila javno dostupnim. Nema mehanizma za snifovanje paketa, reverzni inženjering šifara ili za priključivanje na nezaštićenu mrežu. Netstumblerom se poštuju ograničenja vlasnika mreže, ako je onemogućen AP beacon broadcast mreža neće biti detektovana. Netstumbler se koristi uglavnom za 1) wardriving, 2) otkrivanje lažnih pristupnih tačaka u velikim mrežama sa mnogo korisnika 3) direktno merenje pokrivenosti radio polja neke pristupne tačke. Za ovaj alat je neophodno da bežični mrežni adapter ima podršku, što prvo proveravamo pri instalaciji NetStumblera. Lista direktno podržanih adaptera je u readme fajlu uz instalaciju NetStumblera a može se naći i na internetu. Postoji dosta sličnih adaptera koji nisu direktno podržani, ali često mogu da rade sa dostupnim drajverima.

Wardriving kako ga mi sada poznajemo je prvi put razvijen i korišćen od strane Pete Shipley u Aprilu 2001 god. Pre toga je bilo osluškivanja beacon paketa sa pristupnih tačaka (AP) i o tome su pravljene beleške (često na papiru). Pete je prvi automatizovao taj proces prikupljanja podataka softverom napravljenim za tu namenu, i takođe je prvi integrisao podatke sa GPS-a sa bazom podataka o detektovanim AP.

Postavlja se pitanje legalnosti ratne vožnje. Ima mišljenja da je ona sama po sebi nelegalna. Ono što je u suštini nelegalno je konektovanje i korišćenje mreže bez dozvole vlasnika te mreže (što se naziva upadom u mrežu). Dešava se da ratna vožnja bude pomenuta u novinskim natpisima u negativnom kontestu. To je onda kada krekeri koriste alate za ratnu vožnju kako bi locirali mreže u koje kasnije upadaju. Ova materija je u pravnom smislu još uvek nova, pa oblast računarskih mreža još uvek nije dovoljno precizno obrađena. Da bi se u primeni ratne vožnje zadržali u okviru zakona važno je da poštujemo pozitivnu pravnu regulativu koja je trenutno na snazi. Drugim rečima, 1) ne istraživati sadržaj mreže, 2) ne dodavati, brisati, ili menjati bilo šta na mreži i 3) nikada ne koristiti mrežnu Internet konekciju za surfovanje na web-u, razmenu e-maila, chat, FTP ili bilo šta drugo. Pošto je javna percepcija o pitnju legalnosti ratne vožnje izuzetno važna, medijima koji o tome izveštavaju kad god je moguće treba ukazati na razliku između legalne primene softverskih alata za ratnu vožnju i njihove zloupotrebe od strane krekeri.

Vožnja automobilom tokom wardrivinga treba da bude što sporija, idealno bi bilo oko 50-60 km/h, pošto Stumbler programima treba vremena da uoče stanice i

naprave zapis o tome u log fajl. Ako se krećemo prebrzo dosta stanica koje treba detektovati neće biti dovoljno dugo u dometu.

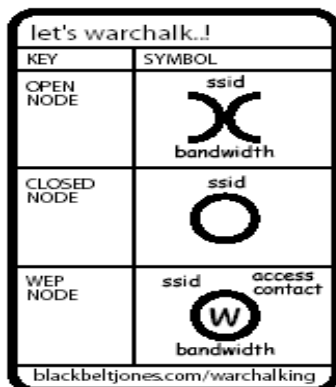
Detektovanje onih koji obavljaju ratnu vožnju, kao način da se štiti bežična mreža se može u principu obavljati na dva načina. Prvi metod je efikasan za detektovanje korisnika NetStumblera, dok drugi metod detektuje NetStumbler, MiniStumbler i MacStumbler. Nijedan od ovih metoda ne detektuje Kismet, zato što je on pasivni skener. Oba metoda zahtevaju računar sa bežičnim mrežnim adapterom i na njemu pokrenut Kismet koji radi neprekidno. Taj računar nije prijavljen na bežičnu mrežu, i neprekidno je na prijemu.

Metod 1: Osluškivanje paketa koje emituje NetStumbler pošto detektuje neku bežičnu mrežu. Ti paketi sadrže karakteristike koje se mogu identifikovati pomoću Kismet programa.

Metod 2: Znatno manje precizan metod za otkrivanje upada u mrežu je jednostavno osluškivanje prekomernog emitovanja 802.11b zahteva za ispitivanje mreže (probe request). Tako se ne mogu sa sigurnošću pozitivno identifikovati svi napadi na mrežu, zato što i legitimni klijenti na mreži emituju zahteve za ispitivanje mreže. Ali ako se zna koji uređaji legitimno koriste mrežu, može se zaključiti koji zahtevi za ispitivanje mreže potiču od potencijalnog napadača tj. nelegitimnih korisnika.

Zaključak:

Ratna vožnja je aktivnost koja se može sprovoditi sa minimalnim sredstvima i tehničkim znanjem. U toku te aktivnosti se prikupljaju podaci o imenu, lokaciji i bezbednosnom podešenju pristupnih tačaka. Rezultati najčešće ukazuju da veliki broj pristupnih tačaka nema nikakvu zaštitu. Iako postojeće zaštite bežičnih mreža nisu savršene, treba ih koristiti kako bi većina potencijalnih napadača bila odvrćena od napada.



Slika 8.2 Simboli koji u gradovima ukazuju na bežične mreže

8.2 Eksperimenti i „ratna vožnja“

U toku izrade ovog rada, za praktičnu realizaciju bežične mreže i ratnu vožnju korišćena je sledeća oprema i softver:

- 1) Notebook: hp Compaq nc6320 ,
Intel PRO/Wireless 3945ABG
MAC adresa 00.18.DE.BE:D1:B7
OS Windows: XP SP2 i Knopix 3.4

sw: NetStumbler ver.0.4.0 (Build 554)

- 2) Desktop PC: Dell Opti plex GXa 256 MB RAM,
Gigabyte AirCruiser GN-WP01GS 802.11b/g,
OS Linux: Mandriva 10.0 i Windows XP SP2
- 3) Wireless Broadband Router W541R
- 4) GPS: Nokia N79, OS: Symbian serija 60 ver 3.

U cilju boljeg upoznavanja sa WLAN tehnologijom, u laboratorijskim uslovima, na desktop PC računaru je instaliran OS Linux i odgovarajući softverski alati. Notebook računar pod OS Windows XP, kao i mobilni telefon Nokia N79, su imali ulogu korisnika. Stim što su sa mobilnog telefona Nokia N79 uzimani i podaci o lokacijama a na Notebook računaru pod OS Knopix vršeno je i prikupljanje paketa podataka.

U terenskim uslovima sa Notebook računom prikupljeni su podaci o pristupnim tačkama koje emituju svoj SSID i izvršena su merenja jačine signala. Vizuelnim osmatranjem mesta na kojima se nalaze antene za bežičnu mrežu lociran je izvestan broj pristupnih tačaka. Na osnovu brzine prenosa podataka, vidi se da većina pristupnih tačaka koristi opremu kompatibilnu sa standardom IEEE 802.11 a/b (Slika 8.1). Samo manji deo njih može da ostvari brzinu od 54 Mb/s. Neke pristupne tačke za kriptovanje podataka koriste WEP. Na osnovu SSID lako je pretpostaviti kome pristupna tačka pripada. Prikazani su podaci o MAC adresama svih pristupnih tačaka, kao i o kanalu na kojem rade.

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc.	SNR	Signal+	Noise-	SN
002163B18508	HG520s		7	54 Mbps	(Fake)	AP		7	-93	-100	7
00026F441593	8iPuk1		11	11 Mbps	Senao Intl	AP		5	-94	-100	6
001D0FB86926	VAVWireless AP5		8	54 Mbps	(Fake)	AP			-88	-100	12
0019E08C5E2B	mic23		5	11 Mbps	(Fake)	AP			-93	-100	7
002163B18A3F			1	54 Mbps	(Fake)	AP	WEP	10	-90	-100	10
002163ACCD93	HG520s		1	54 Mbps	(Fake)	AP			-94	-100	6
00026F32F30F	TOD 11		1	11 Mbps	Senao Intl	AP			-90	-100	10
002163AFC08C	HG520s		1	54 Mbps	(Fake)	AP			-91	-100	9
00005E000101	VAVWireless AP2		11	54 Mbps	(Fake)	AP			-79	-100	21
002163B01407	HG520s		1	54 Mbps	(Fake)	AP			-94	-100	6
0014789E3F6C	GGC		6	54 Mbps	(Fake)	AP	WEP		-95	-100	5
000C4226949E	mic13		11	11 Mbps	(Fake)	AP		14	-86	-100	14
0014789E3F6C			5	54 Mbps	(Fake)	AP			-85	-100	15
004F620A3673	NumLock		3	11 Mbps	(Fake)	AP			-92	-100	8
0050FCD56A9			8	11 Mbps	Edimax	AP	WEP	10	-89	-100	11
0019E00FE168	MaxiNet Pamjaca1		8	11 Mbps	(Fake)	AP		13	-87	-100	13
002127D947E8	Z_Cuda		9	54 Mbps	(Fake)	AP		13	-85	-100	15
000C4226949E	mic12		1	11 Mbps	(Fake)	AP			-89	-100	11
001478115812	mic5		11	11 Mbps	(Fake)	AP			-90	-100	10
00304F38ED26	BRD054		4	11 Mbps	PLANE...	AP			-82	-100	18
0006B8D98795	valjevo-mw			54 Mbps		AP			-89	-100	11
0202C91CF6A4	edvaljevo		7	11 Mbps	(User-d...	Peer	WEP	11	-84	-100	16
00026F302655	marsh5		6	11 Mbps	Senao Intl	AP		22	-78	-100	22
002163AFC48E	moja_mreza		11	54 Mbps	(Fake)	AP	WEP		-90	-100	10
0080484709A5	MaxiNetPopare2		4	2 Mbps	Compex	AP		11	-85	-100	15
001D0FBCDFFE	AP1		6+	54 Mbps	(Fake)	AP			-87	-100	13
00147810C59B	mic2		10	11 Mbps	(Fake)	AP		11	-87	-100	13
0014788F66A7	mic2		2*	11 Mbps	(Fake)	AP		22	-76	-100	24

Slika 8.1 Netstumbler program - ratna vožnja



Slika 8.2 Snimak područja na kojem je vršena detekcija AP-a

9. Napadi na WLAN mrežu putem ometanja servisa

Kada autorizovani korisnici ne dobiju zahtevani servis u okviru definisanog maksimalnog vremena čekanja, kaže se da je u toku Denial of Service (DoS) napad, tj. napad u kome se vrši otkaz svih servisa mreže ili sistema.

Infrastruktura međusobno spojenih sistema i mreža sastoji se od ograničenih resursa. DoS napadi su napravljeni na način da zauzmu dovoljno slobodnih resursa koje žrtva poseduje, kao što su bandwidth, CPU ili mesto za čuvanje podataka. Na taj način DoS napadi uskraćuju usluge legalnim korisnicima. Napadi mogu biti usmereni prema bilo kojem mrežnom uređaju ili bilo kojem drugom mrežnom resursu.

Rani DoS napadi koristili su jednostavne alate koji su generisali i slali pakete s jednog izvora na jedno odredište. Tokom vremena, alati su unapređeni da izvode napade s jednog izvora na više odredišta, s više izvora na jedno odredište ili s više izvora na više odredišta.

DoS napad ili napad sa uskraćivanjem usluge je pokušaj da se resursi računara učine nedostupnim ili nekorisnim za legalne korisnike. To je tip bezbednosnog propusta računarskih sistema koji nužno ne rezultira krađom informacija ili bilo kojim drugim materijalnim gubitkom.

DoS napadi imaju dve glavne forme. Jedna od njih je prisiljavanje računara žrtve da zauzme svoje resurse tako da više ne može pružati potrebne usluge. Drugi način je narušavanje načina komunikacije između legalnih korisnika i računara žrtve na način da oni više ne mogu komunicirati.

Iako najčešće namerni i zlonamerni, DoS napadi mogu se dogoditi i sasvim slučajno.

Ometanje bežične računarske mreže se najčešće vrši tako što se emituje jak signal prema prijemnoj anteni na istom opsegu, ili podopsegu, učestanosti kao što emituje i predajnik u regularnoj komunikaciji. Bitno je napomenuti da ovo ometanje ne utiče na predajnik, već samo na prijemnik sa druge strane komunikacionog linka. Tu se javlja problem za onoga ko vrši ometanje, a sastoji se u tome da samo lokacija predajnika može da se otkrije, ali ne i lokacija prijemnika koji želi da se ometa. Lokacija prijemnika mora biti poznata jer i ometač ima konačnu izlaznu snagu signala.

Ometanje je uspešno kada ometački signal dovoljno uništi korisnost komunikacionog linka, odnosno kada koristan signal bude neupotrebljiv. U digitalnim komunikacijama to se postiže kada verovatnoća greške prevazilazi dozvoljeni procenat, tj. kada mehanizmi za otklanjanje grešaka postaju neefikasni. Uspešno ometanje podrazumeva da je nivo snage ometačkog signala jednak ili veći od nivoa snage korisnog signala na prijemnoj strani. Efekat ometačkog napada zavisi od odnosa jamming-to signal (J/S), tipa modulacije, kodiranja kanala i interleavinga koji se primenjuje na sistemu koji se ometa. Ako ometač nema dovoljan nivo izlazne snage da emituje ometački signal u širokom opsegu kontinualno, onda se pribegava principu impulsnog ometanja punom snagom. Prilikom impulsnog ometanja ometa se takođe široki opseg frekvencija, ali deo po deo (podopseg po podopseg) u kratkim vremenskim intervalima.

Jamming-to-signal odnos, ako se zanemare propagacijski efekti, može da se izračuna prema sledećem izrazu: [20]

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j} \quad (9.1)$$

gde su:

P_j - snaga ometačkog predajnika

P_t - snaga komunikacionog predajnika

G_{jr} - dobitak antene – ometač - komunikacioni prijemnik

G_{rj} - dobitak antene – komunikacioni prijemnik – ometač

G_{rt} - dobitak antene – prijemnik – predajnik

G_{tr} - dobitak antene – predajnik – prijemnik

B_r - širina opsega komunikacionog prijemnika

B_j - širina opsega ometačkog predajnika

R_{tr} - rastojanje komunikacioni predajnik – prijemnik

R_{jr} - rastojanje ometački predajnik – komunikacioni prijemnik

L_j - slabljenje ometačkog signala

L_r - slabljenje komunikacionog signala

Prema izrazu (9.1) vidi se da ERP (Effective Radiated Power) ometača, koje je proizvod dobitka antene i izlazne snage, treba da je što veći ako se želi što efikasnije ometanje. S druge strane, u cilju zaštite od ometanja, dobitak antene prema komunikacionom partneru treba da je što veći, a prema ometaču što manji. Prema izrazu (9.1), model antene, odnos između azimuta i dobitka, je vrlo bitan faktor prilikom ometanja. Rastojanje između predajnika i prijemnika ima veliki uticaj na slabljenje signala. Ako se ometač nalazi na dva puta većem rastojanju od prijemnika, on mora da ima četiri puta veći izlazni nivo da bi kod prijemnika imao isti nivo kao i koristan signal. Većina digitalnih komunikacionih sistema zahtevaju da se i sinhronizacioni signal prenosi između uređaja koji komuniciraju. Ometač može da se podesi da ometa taj sinhronizacioni signal i da na taj način ometa kompletnu komunikaciju. Sistemi sa sinhronizacijom su inače vrlo osetljivi na ometanje jer se sinhronizacija vrši stalno po istom kanalu. Kada se jednom sinhronizacija izgubi, tada

ometać može da prekine emitovanje, pa da ponovo počne sa emitovanjem signala kada se sinhronizacija ponovo uspostavi, mada je za ometača vrlo teško da prepozna kada se to dogodilo. Klasičan ometački signal predstavlja, u stvari, običan signal šuma u određenom opsegu. Krajnji cilj je da se učestanost ometačkog signala što više približi učestanosti komunikacionog signala, tj. da korisni komunikacioni signal utone u interferencijski signal. Najbolje je za ometanje koristiti talasni oblik sličan signalu koji se želi ometati.

IEEE 802.11 standard za WLAN definiše dve tehnike prenosa u proširenom spektru (Spread-Spectrum – SS) u okviru radio-veza i tehniku za infracrveni (Infrared - IR) prenos. U okviru tehnike proširenog spektra može da se koristi prenos sa frekvencijskim skakanjem ili sa direktnom sekvencom (Frequency Hopping – FH i Direct Sequence - DS). IR WLAN se ovde ne razmatra, već samo WLAN sistemi sa radio prenosom. Radio-veze koriste ISM (Industrial, Scientific and Medical) opseg učestanosti 2.4 – 2.4853 GHz. Ovaj frekvencijski opseg spada u ne licencirane opsege. Ovo znači da svako ima pravo da koristi ovakvu opremu dok god se pridržava definisanih nivoa izlazne snage i frekvencijskog opsega. IEEE 802.11 standard koji definiše WLAN sisteme, propisuje izlaznu snagu za ovaj opseg u intervalu 1-100 mW. U WLAN sistemima frekvencijski opseg je podeljen na 79 kanala širine po 1 MHz. Predajnik i prijemnik se na početku svake konekcije dogovaraju oko sekvence skakanja ako se radi o FHSS. Svaka konekcija sa mrežom vrši se po drugoj sekvenci, koje se definišu tako da se otkloni mogućnost da dva korisnika istovremeno koriste isti kanal. FHSS koristi 2FSK ili 4FSK (Frequency Shift Keying) modulaciju. FH ograničava transportni kapacitet u WLAN sistemima na 3 Mb/s zbog širine od 1MHz svakog pojedinačnog kanala. Na signal se dodaje overhead koji se koristi za ARQ proceduru, kojom se ispravljaju grške nastale prilikom propagacije signala. Kod uređaja koji koriste DSSS, frekvencijski opseg se deli na 3 kanala širine po 22 MHz. Ovi kanali su međusobno razdvojeni sa po 5 MHz. Maksimalna brzina prenosa sa DSSS je 11 Mb/s. Po IEEE 802.11b standardu, ovi uređaji koriste Barkerov kod dužine 11 bita za kodovanje svih signala koji se emituju u etar. Svaka sekvenca od 11 bita pretvara se u simbol za prenos kroz slobodan prostor i predstavlja 1 bit korisnog signala. Simboli se šalju brzinom 1 Mb/s. DSSS koristi dva tipa modulacije (DBPSK i DQPSK) u zavisnosti koliki se protok sistema želi ostvariti. Za protoke 11 i 5.5 Mb/s ne koristi se Barkerov kod dužine 11 bita, već se koristi metoda Complementary Code Keying – CCK. CCK se sastoji od 64 kodne reči od po 8 bita, koje čine jedan set kodnih reči. Svaki set ima jedinstvenu matematičku karakteristiku, pomoću koje se signal na prijemnoj strani izdvaja iz šuma. IEEE 802.11 koristi Dynamic Rate Shifting - DRS koji omogućava automatsko podešavanje protoka ukoliko dođe do pogoršanja uslova propagacije. To znači da će ometač biti efikasan isključivo ako je u mogućnosti da ometa komunikaciju i na protocima od 1 Mb/s. Prema standardu, DSSS sistem koji koristi ISM frekvencijski opseg mora da ima minimalno 10 dB procesno pojačanje. Treba napomenuti da je signal sa većim protokom podložniji ometanju, interferenciji i izobličenjima koje unose filtri, od signala sa nižim protocima zbog zahtevanog većeg odnosa signal/šum (E_s/N_o). Tako da je procesno pojačanje razlog zbog čega su DS sistemi otporniji na ometanje.

Savremeno ometanje se takođe koristi u pozitivne svrhe. U mirnim i tihim sredinama, kao što su biblioteke ili koncertne sale, ometanje se koristi da mobilni telefoni ne bi radili, da ne bi ometali ostale posetioce. U bolnicama, GSM i ostali slični digitalni signali mogu da prouzrokuju smetnje u radu medicinskih instrumenata.

DoS napadi izvode se korišćenjem alata koji šalju mnogo paketa ciljanom serveru. Ti paketi preplave (*engl.* flood) resurse servera i na taj način server postaje

nekoristan. Svaki sistem koji je spojen na Internet i koji je opremljen mrežnim uslugama zasnovanim na TCP (*engl.* Transmission Control Protocol) protokolu potencijalna je žrtva napada.

DoS napadi mogu se podeliti na softverska iskorišćavanja i preplavlјivanja. Napadi preplavlјivanjem se zasnivaju na jednom jednostavnom pravilu: onaj ko upravlja najvećim širinom opsega (*engl.* bandwidth) pobeđuje. Napadi preplavlјivanjem mogu se podeliti na napade s jednog izvora, napade s više izvora ili napade sa refleksijom.

U napadima s jednim izvorom postoji jedan napadač koji preplavlјuje žrtvu, dok u napadima sa više izvora postoji više napadača. U oba slučaja mogu se koristiti dodatni „zombie” računari. „Zombie” je računar koji je zaražen pomoću iskorišćavanja neke ranjivosti. Takav računar sadrži skriveni program koji omogućava upravljanje računarom sa daljine. Najčešće se koriste za izvođenje napada na neki drugi računar.

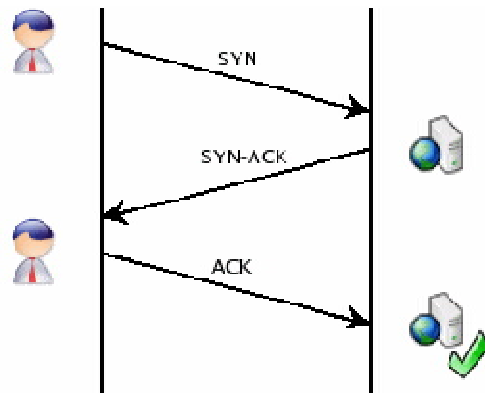
Napadi s refleksijom su specijalni slučajevi napada sa više izvora. Koriste se za skrivanje identiteta pravog napadača ili za pojačavanje napada. Reflektor je bilo koji računar koji odgovara na zahteve. Bilo koji računar može se koristiti kao reflektor dodavanjem IP adrese računara žrtve u izvorno polje zahteva. Dodavanjem te informacije računar reflektor će poslati odgovor žrtvi umesto napadaču. Ako postoji mnogo računara reflektora rezultat će biti efikasan DoS napad.

Glavna razlika između „zombie” računara i računara reflektora je ta što su reflektori legalni serveri Internet usluga. Zbog toga je napade sa refleksijom jako teško suzbiti.

Najčešće metode DoS napada su opisane u nastavku poglavlja.

SYN flood

SYN flood ili SYN preplavlјivanje je metod DoS napada u kojoj napadač iskorišćava malu veličinu bafera u toku rukovanja u tri koraka (*engl.* three way handshake). Ovaj metod sprečava server da prihvati ulazne TCP veze. Normalno TCP rukovanje prikazano je na Slici 9.1.

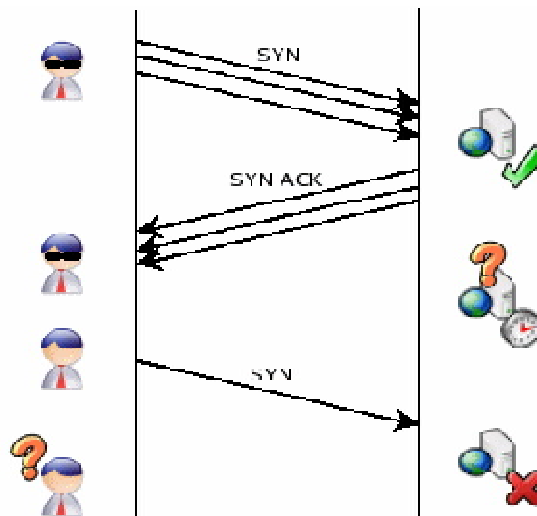


Slika 9.1 TCP rukovanje u normalnom slučaju

Ovaj metod napada je poznat već duže vreme i nije primenjiv na moderne mreže. Napad je iskoristiv samo ako server zauzme sve resurse pošto primi SYN poruku, ali pre nego što je primio ACK poruku.

Postoje dva metoda izvođenja ovog napada. Oba metoda uključuju ne primanje ACK poruke od strane servera. U prvom metodu zlonamerni klijent preskače slanje poslednje ACK poruke. Drugi metod uključuje lažiranje izvorišne IP adrese u SYN poruci. Zbog toga što server šalje SYN-ACK poruku prema pogrešnoj IP adresi

nikada ne dobije ACK poruku. Veze koje nisu završile rukovanje zovu se polu otvorene veze. Preplavljivanje mreže takođe može biti uzrok nepostojeće ACK poruke. Iz tog razloga server će neko vreme čekati poruku koja nedostaje (Slika 9.2).



Slika 9.2 SYN flood: nekoliko veza je polu otvoreno, server je preplavljen i druge veze su onemogućene

Ako polu otvorene veze koriste resurse na serveru, moguće je zauzeti sve resurse na serveru slanjem SYN poruka. Jednom kada se svi resursi zauzmu od strane polu otvorenih veza, ni jedna nova veza (legalna ili ne) nije moguća.

Teardrop je tip DoS napada koji iskorišćava način na koji IP protokol (*engl. Internet Protocol*), deli na fragmente paketa koji su preveliki za router. U fragmente paketa upisuje se udaljenost od početka prvog paketa, što omogućuje ponovno sastavljanje paketa na drugoj strani. U ovom napadu napadač postavlja zbunjujuću vrednost udaljenosti u jedan od fragmenata (veću od dozvoljene). Ako server koji prima takav paket nema plan za takav slučaj rezultat će biti pad sistema.

Distribuirani reflektujući DoS napad uključuje slanje lažnih zahteva velikom broju računara koji će odgovoriti na zahtev. Korišćenjem maskiranja IP adrese, izvorišna adresa se postavlja na adresu računara žrtve. Zbog toga što će svi odgovori otići prema maskiranoj IP adresi računar žrtva će biti preplavljen.

Dve glavne komponente smurf napada su korišćenje lažnih ICMP (*engl. Internet Control Message Protocol*) *echo* zahteva i smer paketa prema IP broadcast adresi.

U ovom metodu napada, napadač šalje IP *ping* zahtev. *Ping* paket određuje da će biti poslat većini servera unutar lokalne mreže primaoca. Paket takođe pokazuje da zahtev dolazi sa drugog izvora, računara koje će postati žrtva DoS napada. Rezultat će biti velika količina *ping* odgovora koji će preplaviti žrtvu. Ako je preplavljivanje dovoljno veliko, žrtva više neće moći da razlikuje pravi saobraćaj od zlonamernog.

Napad zasnovan na ICMP *echo* zahtevima smatra se jednom vrstom reflektujućeg napada, pošto preplavljeni server šalje *echo* zahteve na broadcast adresu nepravilno

konfigursanih mreža. Posledica toga je podsticanje velikog broja računara da šalju *echo* odgovore žrtvi. Raniji DDoS programi su implementirali distribuirani način ove vrste napada.

Fraggle napad je napad sličan smurf napadu. Umjesto ICMP-a koristi UDP (*engl. User Datagram Protocol*).

Računarski virusi takođe mogu biti metod DoS napada. Žrtva u ovom slučaju nije unapred izabrana, nego je to najčešće računar koji je slučajno dobio virus. Zavisno od virusa, DoS napad može biti jedva primetan ili katastrofalan.

Land napad je DoS napad koji se sastoji od slanja posebnih zaraženih paketa računaru. Posledica primanja tih paketa je zaključavanje računara. Napad uključuje slanje maskiranih TCP SYN paketa sa odredišnom IP adresom i *open portom* kao izvorišnom i odredišnom adresom. Ovaj metod napada je efikasan zato što računar odgovara samom sebi beskonačno.

SQL ubacivanje je ranjivost sistema koja se događa kada aplikacija ne filtrira korisničke podatke na dobar način, pre nego što ih pošalje sistemu za upravljanje bazama podataka (*engl. Data Base Management System*). Korisnik-napadač ubacuje zlonameran kod u aplikaciju koja koristi SQL naredbe. Ako aplikacija korisnikov unos ne filtrira na dobar način, zlonamerni kod u vidu SQL naredbe se šalje sistemu za upravljanje bazama podataka i izvodi napad.

Distribuirani DoS napadi (DDoS) događaju se kada više zaraženih sistema preplavljuje propusni opseg ili resurse sistema žrtve.

Ako napadač izvodi *smurf* napad sa jednog izvora, takav napad će biti prepoznat kao DoS napad. Bilo koji napad na dostupnost podataka će biti prepoznat kao DoS napad.

Ako napadač koristi hiljade „*zombie*” sistema da istovremeno izvedu *smurf* napad, napad će biti prepoznat kao DDoS napad.

Napadi izgladnjivanjem resursa pokušavaju zauzeti sve resurse na računaru žrtvi. Na taj način ti resursi postaju nedostupni legalnim korisnicima. Postoje tri načina ovog napada.

CPU izgladnjivanje je specifično za aplikacije. Jedan paket poslan od napadača rezultuje slanjem više paketa prema žrtvi.

Izgladnjivanje memorije se oslanja na operacioni sistem ili aplikaciju.

Izgladnjivanje diska javlja se kada je na primer veza zbog razmene podataka ostala otvorena ili ako je pronađen FTP server na kojem je dozvoljeno pisanje. Jedan od najpoznatijih napada ovog tipa je bombardovanje e-mailovima. To se postiže slanjem velikog broja e-mail poruka korisniku, što dovodi do popunjavanja e-mail inboxa.

Poplavljivanje na aplikativnom nivou je još jedan vid napada. Ranjivosti zbog popunjavanje bafera nastaju zbog programskih grešaka. To su ujedno i najčešće programske greške. Zbog toga je najčešći metod DoS napada generisnje većeg prometa prema mreži nego što baferi mogu prihvatiti.

Jedan tip napada popunjavanja bafera iskorišćava manu u implementaciji ICMP-a. Napadač ne mora znati ništa o računaru koji napada, osim njegove IP adrese. Ovaj metoda napada poznat je i kao „*ping of death*”. Ovaj napad uključuje slanje

zlonamerne *ping* poruke računar. U normalnom slučaju *ping* je veličine 64 okteta. Mnogi sistemi ne mogu obraditi *ping* zahtev koji je veći od maksimalne veličine IP paketa. Slanje *ping* paketa te veličine nije dozvoljeno u mrežnim protokolima, ali je moguće poslati fragmentisani paket te veličine. Kada računar primi takav paket i ponovo ga složi može doći do popunjavanja bafera, što često dovodi do pada sistema. Izgladnjivanje *bandwidtha* se oslanja na činjenicu da napadač ima na raspolaganju veći *bandwidth* nego žrtva. Takvi napadi danas se izvode putem DDoS napada koristeći *botnet*-ove.

Takozvani “banana napad” uključuje preusmeravanje odlaznih poruka klijenta prema tom istom klijentu. Time se onemogućava slanje poruka ka drugim računarima, a postiže se preplavljanje klijenta. Napadač koji ima pristup računar žrtve može usporiti računar do nivoa njegove neupotrebljivosti ili do pada sistema koristeći “*fork*” bombu.

Pulsirajući *zombie* je termin koji se odnosi na posebnu vrstu DoS napada. Mreži se šalje velika količina *ping* poruka, tokom dužeg perioda. Posledica toga je znatno smanjen kvalitet usluge i povećano korišćenje mrežnih resursa. Ovu vrstu napada teže je otkriti od tradicionalnih DoS napada.

Najnoviji trend u DoS napadima su botneti. Botnet je skup autonomnih softverskih robota. Termin botnet se koristi za skup kompromitovanih računara koji izvode programe sa zajedničkom naredbom i zajedničkom kontrolnom infrastrukturom. Noviji roboti mogu automatski skenirati okruženje u kojem se nalaze i širiti se koristeći pronađene ranjivosti. Najpopularnije korišćenje botneta za izvođenje DoS napada je korišćenje istih za slanje spam poruka.

Slanje spam poruka takođe je jedan od načina za izvođenje DoS napada. Slanjem enormne količine beskorisnih poruka korisnicima, korisne poruke i resursi mogu biti izgubljeni. Crvi i virusi takođe mogu biti poslani putem spama da bi stvorili početni skup zaraženih računara, koja šalju viruse ostalim računarima. Zaraženi računari mogu se koristiti kao zombiji, da bi slali dodatne spamove ili izvodili DoS napade.

Prema “The Communications Research Network’s” VoIP bi mogao postati nova meta DoS napada. Sposobnost zvanja unutra i van VoIP *overlay*-a dozvoljava kontrolu aplikaciji kroz govornu mrežu i na taj način pronalazak izvora napada čini gotovo nemogućim. Kriptovanje, P2P i super-peer sistemi pomažu u preusmeravanju poziva i NAT/firewall dodatno maskiraju saobraćaj.

Problem DoS napada nije se značajno promenio tokom proteklih godina. Mrežni resursi ostaju ograničeni i ranjivi. Od DoS napada, zbog svoje prirode, se teško obraniti. Zbog toga će ostati atraktivan metod napada.

Količina DoS problema, u kojima su mreže “padale” zbog preplavljanja elektronskom poštom, teško se može proceniti. Mnogi napadi nisu prijavljeni zbog straha organizacija da će izgubiti poverenje u njihovu bezbednost. Broj zombie računara koji se koriste u DDoS napadima je takođe nepoznat, ali se procenjuje da ih ima nekoliko miliona. Naredba za napad najčešće dolazi putem *instant messaging*. Internet provajderi za sada mogu kontrolisati *instant message* servere. Ali ako se ta kontrola kompromituje, biće jako teško pronaći krivca za DoS napade.

Iako se ukupan broj elektronskih napada smanjio, još uvek postoji velika pretnja od budućih DoS napada. Oni će postati automatizovaniji, sofisticiraniji i biće ih teško iskoreniti.

10. Mere za poboljšanje bezbednosti WLAN

Mere za zaštitu bežične računarske mreže se mogu sprovesti na upravljačkom, operativnom i tehničkom nivou.

10.1 Upravljačke mere za zaštitu bezbednosti WLAN

Upravljačke mere za zaštitu bezbednosti počinju sa obuhvatnom politikom bezbednosti. Politika bezbednosti je dokument na osnovu kojeg su ostale mere bezbednosti, operativne i tehničke usklađene i implementirane. Bezbednost bežične mreže uključuje sledeće odrednice:

Ovlašćenja i odgovornosti korisnika - Politika prikazuje šta je sve u nju uključeno, zašto je ona neophodna i šta se dešava ako se ona prekrši. Ona takođe definiše odgovornost službi i pojedinaca, posebno korisnika uopšte, odeljenja IT i kontrolora.

Sredstva koja se štite - Politika bezbednosti može identifikovati ili ukazati na osetljive informacione resurse, komunikacione kanale i sisteme koje treba zaštititi u bežičnoj mreži.

Pretnje i slabosti - Politika bezbednosti može da uključi i deo u kojem se identifikuju pretnje po bežičnu mrežu.

Analiza napada - Politika bezbednosti može identifikovati posledice koje nastanu u slučaju narušavanja bezbednosti bežične mreže.

Postupci i odgovornosti - Politika bezbednosti bi trebalo da identifikuje i definiše bezbednosne procedure za sledeće slučajeve:

- Kreiranje naloga za nove korisnike.
- Politiku lozinki i njihovo obnavljanje.
- Autentikaciju.
- Pristup opremi i prostorijama.
- Izveštavanje o narušavanju bezbednosti.
- Raspolaganje sa osetljivim podacima.

Planiranje odgovora na narušavanje bezbednosti - Može biti opisano uključujući i planove odgovora na različite incidente, spisak osoba koje treba pozvati u slučaju incidenta i njihovu odgovornost, proces ispitivanja uzroka incidenta, proces oporavka sistema, popis izveštaja koji se moraju podneti posle incidenta.

Prihvatljivo korišćenje - Politika bezbednosti može da se kreira tako što bi bile definisane dozvoljene aktivnosti na bežičnoj mreži (npr. pristup internetu, razmena elektronske pošte i poslovna primena). Politika takođe može da definiše aktivnosti koje su izričito zabranjene na bežičnoj mreži sa objašnjenjem potrebe da se zaštite resursi korisnika i održi integritet mreže.

Bezbednost na krajnjim tačkama - Kontrola bezbednosti na radnim stanicama, laptop računarima, PDA i drugim bežičnim uređajima koji su uključeni u politiku bezbednosti bežične mreže. Zahtevi za često čak i dnevno ažuriranje softvera, namensko korišćenje bezbednosnog softvera (npr. VPN klijenti, anti-virus i firewall), treba da budu uključeni. Lista za kontrolu bezbednosti može da ima razne oblike prema mogućnostima pristupa krajnjoj opremi, na lokaciji opreme ili preko mreže.

Uputstvo za uvođenje WLAN - Politika treba da obezbedi uputstvo za implementaciju i razmeštaj delova bežičnih sistema. Treba da odredi ko može da instalira pristupne tačke i drugu bežičnu opremu i da obezbedi ograničenja za lokacije

i fizičku bezbednost za pristupne tačke. Takođe može da obezbedi podrazumevane konfiguracije za pristupne tačke (koristeći WPA2/802.11i) i krajnje uređaje (koristeći VPN), autentikaciju (koristeći autentikaciju na osnovi 802.11X) i mehanizam poverljivosti, zahteve za upravljanje ključevima, i zahteve za fizičko raspoređivanje uređaja i mreže.

Politika razvijanja - Trebalo bi povesti računa o uvođenju promena u već razmeštenoj infrastrukturi, kao što je registracija uređaja, procedure za dogradnju uređaja, uklanjanje i dodavanje uređaja, kao i testiranje interoperabilnosti uređaja.

Verifikacija i usaglašavanje - Politika treba da uključuje zahteve za dnevnik revizije i obračuna troškova, uključujući i specifikacije akcija i događaja koje treba zabeležiti, kao i učestalost pregleda dnevnika. Politika treba da sadrži predviđenu učestalost i opseg bezbednosnih procena za uključivanje pristupne tačke.

Nametanje politike – Politika treba da definiše odgovornost za nadziranje zaposlenih, i treba da do detalja definiše aktivnosti na disciplinovanju prekršioca i ponovljenih prekršioca.

Obaveze prema regulativi – Politika bezbednosti WLAN mora uzeti u obzir bilo koji relevantni industrijski standard (npr. Payment Card Industry Data Security Standard (PCI-DSS)) ili uputstva za očuvanje i zaštitu privatnosti podataka.

Obuka i podizanje nivoa svesti o bezbednosti – Zajedno sa jasnim delokrugom politike bezbednosti, organizacije koje koriste WLAN treba takođe da obezbede da svo kritično osoblje bude na odgovarajući način obučeno za korišćenje bežične tehnologije. Administratori mreže treba da budu potpuno svesni bezbednosnih rizika koje sa sobom nose mreža i uređaji. Oni moraju da rade kako bi garantovali primenu politike bezbednosti i da znaju koje korake treba da preduzimaju u slučaju napada. Svi korisnici WLAN treba da budu upozoreni na svoju odgovornost kada koriste bežične mreže unutar organizacije na koju se odnosi politika bezbednosti ili kada koriste mobilne bežične uređaje za povezivanje na druge bežične mreže, van organizacije.

10.2 Operativne mere za zaštitu bezbednosti WLAN

Fizička bezbednost je osnovna mera kojom se obezbeđuje da samo autorizovani korisnici imaju pristup bežičnoj računarskoj opremi. Fizička bezbednost podrazumeva mere kao što su:

- **Kontrola pristupa** – Identifikacija propusnicama, pristup uz identifikaciju putem čitača kartica, identifikacija biometrijskim uređajima su metode koje smanjuju mogućnost neovlašćenog pristupa opremi za bežičnu računarsku mrežu.

- **Lična identifikacija.**

- **Zaštita na više nivoa** – zaključavanje vrata, instalacija video nadzora za nadgledanje prostora oko objekata u kojima je postavljena WLAN. Na taj način se odvrćaju potencijalni napadači na pristupne tačke.

Svaka od navedenih mera je važna, ali napadač na bežičnu mrežu se može nalaziti van objekta u kojem se koristi bežična mreža, a da ipak bude u dometu te mreže, sa mogućnošću upada u nju. Da bi se to sprečilo, koristi se alat za procenu bezbednosti bežične mreže (npr. procena povredivosti) i sprovođenje bezbednosne procene se obavlja redovno. Bezbednosne procene se vrše kako bi se osigurala usaglašenost opreme i ponašanja zaposlenih sa politikom bezbednosti. Testiranje na probijanje zaštite bežične mreže se takođe pojavljuje kao mogućnost da se bezbednost bežične mreže održi u okviru predviđene tolerancije rizika.

10.3 Tehničke mere za zaštitu bezbednosti WLAN

10.3.1 Uopšte o tehničkim merama zaštite WLAN

Tehničke mere zaštite obuhvataju korišćenje hardverskih i softverskih rešenja. Softverske mere zaštite uključuju pravilno konfigurisanje pristupnih tačaka (AP), instaliranje softverskih zakrpa i nadgradnju softvera, autentikacija, sistemi za detektovanje upada (IDS), lični firewall za bežične uređaje i kriptovanje komunikacija. Hardverska rešenja uključuju smart kartice, virtualne privatne mreže (VPN), infrastrukturu sa javnim ključem (PKI), segregaciju mreže, i biometrijske metode zaštite. Treba primetiti da se neka od ovih rešenja pojavljuju i kao hardverska i kao softverska. Tehničke mere zaštite bi trebalo da uključuju podršku kriptovanjem i kontrolu autentikacijom što je opisano u svakom od standarda za bežične mreže. Kriptovanje u bežičnim komunikacijama se koristi prvenstveno da zaštiti poverljivost poruka i podataka za podešavanje konekcije koji se šalju preko mreže. Autentikacija u bežičnim mrežama se pojavljuje da bi se proverila veza između jednog i drugog uređaja, ili da se potvrdi da je korisnik ovlašćen da se konektuje na određenu mrežu.

Protokoli za kriptovanje koji se koriste u starijim standardima za bežične mreže su bili implementirani na neodgovarajući način a kao posledica toga je njihovo lako probijanje (npr. WEP RC4). Korišćenje najnovije verzije standarda za bežične mreže je preporučljivo, pošto one imaju tendenciju da koriste protokole za kriptovanje koji nisu podložni probijanju (npr. WPA2, AES). Izbor protokola za kriptovanje zavisi od raspoložive infrastrukture. Postojeći uređaji, nasleđeni od ranije, mogu samo da podrže WEP/TKIP, ali ne i WPA/WPA2. AES zahteva veću procesorsku snagu. Najbolja praksa po pitanju bezbednosti WLAN-a je korišćenje WPA2 i AES.

Mnoge bežične tehnologije dozvoljavaju upotrebu više modova za autentikaciju, čime se nudi različita čvrstina autentikacije. Na primer WPA i WPA2 se mogu postaviti u lični ili kompanijski mod. Lični mod koristi slabiju PSK autentikaciju, a kompanijski mod zahteva mnogo čvršći 802.1x/EAP metod. U zavisnosti od poslova koji se obavljaju, može se odrediti prikladnost svake od metoda autentikacije. Za veće mreže koje zahtevaju više upravljanja, centralizovana autentikacija i upravljanje korišćenjem 802.1X uz odgovarajući izbor EAP se preporučuje. Za male privremene mreže, metoda deljenog ključa može da obezbedi odgovarajuću zaštitu. Najbolja autentikacija u praksi za WLAN je trenutno WPA2 uz korišćenje 802.1X/EAP.

Stariji sistemi ili uređaji nisu kompatibilni sa većinom novijih standarda, i ostala infrastruktura (npr. server za autentikaciju) može takođe biti ograničenje za uspešnu implementaciju bezbednosnih protokola novije generacije.

Dobra praksa je onemogućavanje network service set identifer SSID broadcast. Na taj način se pristupna tačka čuva od nepotrebnog oglašavanja svog prisustva.

Dodatne mere bezbednosti se mogu primenjivati pored već uključenih bezbednosnih funkcionalnosti prema bezbednosnim standardima i njima pridruženim tehnologijama. U mnogim slučajevima, ti dodaci mogu značajno da povećaju nivo bezbednosti. Dodatne mere uključuju:

- Korišćenje virtualne privatne mreže (VPN) kojom se dodaje još jedan nivo bezbednosti za daljinski pristup. Kada se koristi bežična mreža ili hotspot koji ne pripadaju organizaciji (npr. kućna ili javna WLAN), upotreba VPN je veoma preporučljiva. Taj dodatni nivo zaštite omogućava jaču autentikaciju i kriptovanje za korisnike koji imaju daljinski pristup.

- Sistem za detekciju upada u bežičnoj mreži (IDS) je tehnologija iskorišćena da detektuje napade karakteristične za bežičnu mrežu. Korišćenje bežičnog IDS sistema

dozvoljava organizaciji koja štiti svoju mrežu da reaguje na napad što je ranije moguće i tako minimizuje bilo koje oštećenje na mreži. Bežični IDS se dalje može koristiti da poveća mogućnost predviđanja napada i za upravljanje procedurom isključenja korisnika, kao što je blokiranje ili deautentikacija sumnjivih korisnika, ili promena bežičnih kanala kako bi se iskoristilo slabljenje signala, i tako onemogućio pristup napadaču.

- Kriptovanje podataka na hard disku je veoma preporučljivo za osetljive informacije koje se čuvaju na nekom od uređaja koji ima pristup bežičnoj mreži.

- WEP nije siguran, nije dizajniran kao potpuno rešenje za obezbeđivanje mreže, već mu je namena samo da podigne nivo bezbednosti na nivo kakav je postojao u ranijim kablovskim mrežama. Postoji veliki broj programa koji "provaljuju" WEP algoritam a lako su dostupni na internetu. Ako oprema nije zastarela preporučuje se WPA2 umesto WEP-a.

- Kada se radi o mreži sa mnogo korisnika, preporuka je da se izvrši njena segmentacija. To je tehnika koja predstavlja razdvajanje računarske mreže u podmreže. Tako se postižu bolje performanse i povećava bezbednost takvih podmreža, zato što se postavljaju dodatna pravila za deo mreže u kojem se nalaze kritične komponente. Segmentacija se najčešće ostvaruje pomoću mrežnih uređaja bridge, switch, i router.

- Ako se omogućava broadcast SSID, ne koristiti imena firme ili imena po kojima bi neko lako mogao da utvrdi o čijoj se mreži radi za SSID (service set identifier) i AP. Ta imena se ne šifruju u hederu 802.11x paketa podataka, tako da svako može da ima podatak o kojoj se mreži radi, a napadaču je značajno olakšan posao kada tačno zna gde i šta treba napasti.

- Ne dozvoliti da bilo ko vidi MAC adresu AP-a iako mnogi proizvođači opreme ugrađuju mogućnost automatskog prepoznavanja adrese.

- Menjanje ključa s vremena na vreme ne donosi neku zaštitu jer hakeri ključ mogu "provaliti" u roku od par minuta, a promena se mora ručno izvršiti na svakom AP-u u mreži. Iz tog razloga su razvijeni automatski izmenjivači ključa koji ga menjaju dosta često na svim AP-ovima istovremeno.

- Postaviti AP tako da pokriva svu potrebnu površinu ali da signal što manje napušta zgradu ili okruženje u kojem se radi.

- Pre prve instalacije AP-a obavezno promeniti šifru i IP adresu.

- Ne koristiti DHCP (Dynamic Host Configuration Protocol) na WLAN-u.

Pronalaženje postojeće IP adrese u mreži kada se koristi DHCP je veoma jednostavno.

- Postoji mogućnost korišćenja boja za zidove koje blokiraju wireless signal. Boja sadrži okside gvožđa i aluminijuma i apsorbira talase frekvencije do 128 GHz. [21]

- Merenjem jačine signala pomoću više prijemnika, utvrđuje se lokacija klijenta koji se prijavljuje na AP i na osnovu toga dozvoljava ili odbija pristup mreži. Postoje HW/SW alati za takvu zaštitu, koriste se za zaštitu velikih bežičnih mreža.

10.3.2. Honeypot tehnologija za zaštitu bežične mreže

Za razliku od firewall-a ili IDS, honeypot ne rešava samo jedan specifičan problem. To je veom fleksibilan alat kojim se mogu obavljati poslovi od otkrivanje napada na IPv6 mrežama do hvatanja prevara sa kreditnim karticama on-line. Uopštena definicija koja pokriva sve manifestacije, honeypot je resurs informacionog sistema

čija je vrednost u neovlašćenom korišćenju tog resursa. Kao i svaki koncept i ovaj ima svoje prednosti i nedostatke.

Prednosti honeypot tehnologije:

- Mali skup podataka od velike važnosti: Honeypot prikuplja veoma malo podataka. Skup podataka koje prikupi za jedan dan ne prelazi veličinu reda MB (kod drugih sistema je to reda GB). Prosečno generiše desetak upozorenja dnevno. Honeypot prikuplja samo maliciozne i neautorizovane aktivnosti. To značajno smanjuje potrebno vreme i troškove analize podataka.
- Novi nestandardni alat i taktika odbrane od napada na mrežu.
- Zahteva upotrebu minimalnih resursa: Računar klase PII sa 128 MB RAM-a može bez poteškoća da opslužuje mrežu klase B na ovim poslovima.
- Kriptovanje ili IPv6: Za razliku od većine drugih tehnologija (kao što su IDS sistemi) honeypot radi bez problema u kriptovanom ili IPv6 okruženju. Bez obzira kakve podatke napadač ubacivao u honeypot, on će ih detektovati i sakupiti.
- Jednostavnost: Konceptualno je honeypot veoma jednostavan. Nema složenih algoritama u razvoju, glomaznih tabela za održavanje niti dodataka i ispravki za update. Što je jednostavnija tehnologija to je manje mogućnosti za greške ili pogrešno konfigurisanje alata za zaštitu.

Nedostatci honeypot tehnologije:

- Ograničen opseg vidljivosti: Honeypot može da registruje aktivnosti koje su direktno ka njemu usmerene, a ne može da registruje napade na druge sisteme oko sebe, ako nije i sam obuhvaćen tim napadom.
- Rizik: Sve tehnologije za zaštitu bezbednosti su obuhvaćene rizikom. Firewall je pod rizikom da bude probijen, kriptovanje da bude razbijeno, IDS senzori mogu da propuste registrovanje napada. Honeypot ima rizik da bude iskorišćen od strane napadača za napad na druge sisteme. Taj rizik zavisi od vrste honeypot sistema i njegove konfiguracije.

Vrste honeypot zaštita:

Honeypot se pojavljuje u više oblika i veličina kako bi se otežalo prepoznavanje ovih sistema od strane napadača. Generalno postoje dve kategorije, sa niskom interakcijom i sa visokom interakcijom. Interakcija definiše nivo aktivnosti koji honeypot dozvoljava napadaču.

Honeypot sa niskom interakcijom radi sa emulacijom servisa i operativnih sistema. Aktivnosti napadača su ograničene na nivo emulacije, na primer emulirani FTP servis sluša na portu 21 i može samo da emulira FTP prijavljivanje i eventualno još nekoliko jednostavnijih komandi u FTP. Prednost ovakvog sistema je njegova jednostavnost, lako se instalira i održava, sa minimalnim rizikom. Uvođenje ovakvih honeypot obuhvata instalaciju softvera, izbor operativnih sistema i servisa koje treba emulirati kao i monitor aktivnosti napadača. Sve ovo je veoma jednostavno i dostupno širem krugu zainteresovanih organizacija koje štite svoju bežičnu mrežu. Emulacija servisa smanjuje rizik od neželjenih aktivnosti napadača, tako da on ne može preuzeti ovakav honeypot tj. njegov operativni sistem i sa te pozicije dalje napadati ostatak štićene mreže. Glavni nedostatak honeypot sa niskom interakcijom je što beleži samo ograničen skup informacija već unapred poznatih aktivnosti koje napadač sprovodi.

Napadač, ako je iskusen, jednostavno otkriva ovakav honeypot, bez obzira koliko su dobre emulacije. Primeri honeypot sa niskom interakcijom su Specter, Honeyd i KFSensor.

Honeypot sa visokom interakcijom je obično komplikovano rešenje koje zahteva stvarno instaliran operativni sistem i aplikacije. Prednost ovakvog rešenja se ogleda u dve stvari. Prvo, može se prikupiti veoma mnogo informacija. Davanjem napadaču realnog sistema sa kojim će biti u interakciji, može se naučiti dosta o navikama napadača, o metodama napada i softverskom alatu koji koristi. Drugo, nema pretpostavki o tome kako se napadač ponaša, zato što je obezbeđeno realno okruženje u kojem se registruju sve aktivnosti. Sve ovo značajno povećava rizik od preuzimanja honeypot sistema od strane napadača i njegovo korišćenje za napad na ostatak mreže. U tom smislu su razvijene nove metode koje se implementiraju kako bi zaštitile honeypot od preuzimanja. Samim tim je i instalacija i održavanje ovakvog honeypot sistema znatno složenija. Primeri honeypot sa visokom interakcijom su Symantec Decoy Server i Honeynets. [14].

Honeyd - primer honeypot sa niskom interakcijom:

Autor Honeyd-a je Niels Provos, to je Open Source projekat namenjen pre svega za Linux (mada je portovan i za Windows). Honeyd radi na principu monitoringa neiskorišćenog IP prostora. Kad god uoči pokušaj konekcije na neku od neiskorišćenih IP adresa, on prihvata konekciju i u interakciji sa napadačem nastoji da bude žrtva. Honeyd detektuje i beleži bilo koju konekciju na bilo kom UDP ili TCP portu. Dodatno se mogu konfigurisati emulacije servisa za nadgledanje željenih portova, kao što je emulacija FTP servera nadgledanjem TCP porta 21. Kada se napadač konektuje na emulirani servis, pored prijavljivanja na sistem beleži se i sva ostala aktivnost napadača, username i password, komande koje je izdavao, eventualno se može otkriti i namera napadača pa čak i njegov identitet. Količina i vrsta informacija koje se mogu prikupiti zavise od nivoa na kojem je izvedena emulacija. Većina emulacija radi slično, prema očekivanom načinu ponašanja, unapred su zadate reakcije honeypot. U slučaju da napadač uradi nešto nepredviđeno, reakcija je najčešće u vidu generisanja poruke o grešci. Neki honeypot, kao što je Honeyd, ne emuliraju samo servise, već i operativne sisteme. Honeyd se pred napadačem može pojaviti kao Cisco router, WinXP webserver ili Linux DNS server. To je prednost, zato što se honeypot bolje prilagođava sistemu pored kojeg radi. Može se ciljati na specifičnog napadača, tako što mu se omogući napad na sistem i servise koje on najčešće napada. Postoje dva elementa pri emulaciji operativnog sistema. Prvi je emulacija servisa. Kada se napadač konektuje na emulirani servis, tada servis radi kao što bi se ponašao u određenom operativnom sistemu. Na primer, ako imamo servis emulacije web servera, i ako se želi da honeypot emulira Win2000 server, tada se mora emulirati ponašanje IIS webservera. Za Linux bi to bilo ponašanje Apache webservera. Većina honeypot emulira operativne sisteme na ovaj način. Neki napredniji honeypot emulaciju obavljaju za jedan korak naprednije (kao i Honeyd). Ne emuliraju samo na nivou servisa, već i na nivou IP steka. Ako neko koristi metodu „active fingerprinting“ da bi odredio pod kojim je tipom operativnog sistema honeypot, većina honeypot će odgovoriti sa IP stekom karakterističnim za operativni sistem pod kojim je instaliran honeypot. Honeyd i još neki napredniji honeypot će obmanuti napadača ne samo emulacijom servisa već i emulacijom IP steka. Nivo emulacije dakle zavisi od izbora honeypot tehnologije.

Honeynets - primer honeypot sa visokom interakcijom:

Honeynets nije gotov softverski proizvod koji se može instalirati na računaru. To je arhitektura čitave mreže računara koja je napravljena da bi služila kao meta napada. Ideja je da se postavi arhitektura u okviru koje je izuzetno kontrolisana mreža, i gde su sve aktivnosti kontrolisane i registrovane. U okviru te mreže se postavlja potencijalna žrtva napada, to je stvarni računar na kojem radi isto tako stvarna aplikacija. Napadač pronalazi, napada i ulazi u taj sistem na svoju inicijativu. Dok to radi nije svestan da je unutar Honeynets. Sve njegove aktivnosti, od kriptovane SSH sesije do emaila i spuštanja fajlova se registruju bez njegovog znanja. To se radi pomoću ubačenih modula u kernel sistema koji predstavlja žrtvu. U isto vreme Honeynets kontroliše aktivnost napadača. To se obavlja uz pomoću Honeywall gejtvaja. Taj gejtvaj dozvoljava ulazni saobraćaj prema sistemu koji predstavlja žrtvu, ali kontroliše odlazni saobraćaj primenom tehnologije sprečavanja upada. To daje napadaču slobodu interakcije sa sistemom koji predstavlja žrtvu, ali sprečava napadača da naškodi drugim računarima koji nisu u Honeynet mreži.

Primenljivost Honeypot tehnologije:

Postoje generalno dve kategorije honeypot sistema, kao što je već navedeno, ali prema načinu upotrebe honeypot sistemi se mogu podeliti na primenjene i istraživačke. Primenjeni honeypot sistemi se koriste za zaštitu bežičnih mreža što uključuje prevenciju, detekciju i odgovor na napad, to su uglavnom honeypot sistemi sa niskom interakcijom. Istraživački honeypot sistemi se koriste za prikupljanje informacija o trendovima u aktivnostima napadača, ranom upozoravanju na mogućnosti napada, kao i za potrebe prikupljanja dokaza u sprovođenju zakona. Istraživački honeypot sistemi su uglavnom sistemi sa visokom interakcijom.

10.3.3 Sistemi za detekciju upada u bežične mreže (IDS)

10.3.3.1 Vrste sistema za detekciju upada u bežičnu mrežu (IDS)

Upad u mrežu je kada neko, obično napadač, pokušava da naudi ili zloupotrebi bežičnu računarsku mrežu. Sistem za zaštitu od upada služi da detektuje i signalizira takve aktivnosti na mreži. Većina ovakvih sistema je sposobna da signalizira i napade tipa ometanja servisa (DoS). U nekim slučajevima IDS sistem je sposoban da odgovori na napad, tako što rekonfiguriše firewall sa ciljem da blokira saobraćaj sa IP adrese ili porta sa kojeg dolazi pretnja ili napad. Treba uočiti razliku između IDS koji prati saobraćaj unutar mreže i firewalla koji reaguje na saobraćaj ka drugim mrežama.

Način na koji IDS sistemi rade u okviru bežične mreže se znatno razlikuje od IDS u okviru žične LAN, najpre zato što u žičnoj mreži postoji potpuna kontrola o tome koja vrsta saobraćaja se odvija kroz mrežu. U WLAN-u eter je medijum kroz koji se prenose paketi i nema potpune kontrole saobraćaja, pa je potrebno nadziranje unutar mreže i van mreže.

Sistemi za zaštitu od upada u bežičnu mrežu se mogu podeliti u tri kategorije:

- IDS na bazi računara domaćina (*engl. host-based*), procenjuje informacije koje dobija od jednog ili više računara, uključujući informacije od operativnog sistema, sistemskih i aplikativnih fajlova.
- IDS na bazi mreže (*engl. network-based*), procenjuje informacije prikupljene iz mrežne komunikacije, analizirajući tok paketa koji se prenose kroz mrežu. Paketi se prikupljaju uz pomoć senzora raspoređenih na pogodna mesta u

mreži. Osnovna poteškoća kod ovakvih sistema je obrada svih paketa koji prolaze kroz mrežu u realnom vremenu, što zahteva posebna hardverska rešenja.

- IDS na bazi procene podložnosti napadu (*engl. vulnerability-assessment*), detektuje slabosti unutar same mreže i firewall-a. Postoje dva primarna modela za analizu događaja uz pomoć kojih se detektuju napadi:
 - Detektovanje na osnovu greške (*engl. misuse detection model*): IDS detektuje upad u mrežu na osnovu zapažanja aktivnosti koje su u vezi sa prepoznatljivim znakovima upada u mrežu ili nekih slabosti mreže.
 - Detektovanje na osnovu izuzetaka (*engl. anomaly detection model*) IDS detektuje upad u mrežu na osnovu uočavanja izuzetaka u mrežnom saobraćaju. Detekcija na osnovu izuzetaka u okviru računara domaćina ili na bazi mreže uključuje: Detekciju na osnovu prekoračenja zadate vrednosti uočavajući neuobičajene aktivnosti na serveru ili mreži, na primer neprimerenu upotrebu CPU resursa na nekom od servera, povećanje zasićenja saobraćaja na mreži. Detekcija na osnovu statističkih merenja, zasnovana na ranije uočenim vrednostima koje se posmatraju. Merenja na osnovu zadatih pravila, što uključuje ekspertski sistem. Detekcija na osnovu nelinearnih algoritama kao što su neuralne mreže ili genetski algoritmi.

Većina komercijalnih IDS alata se bazira na detektovanju na osnovu greške, tako da karakteristike upada u mrežu moraju biti stalno dopunjavane od strane proizvođača ovakvih IDS.

IDS zasnovani na detektovanju na osnovu izuzetka imaju mogućnost da detektuju simptome napada bez određivanja modela napada, ali su veoma podložni lažnim alarmima.

Ocenjivanje komercijalnih IDS je vršeno u laboratoriji u Los Alamosu i za tu namenu je utvrđen kriterijum po osnovu sledećih karakteristika:

1. prikladnost za IDS arhitekturu ili šemu upravljanja
2. fleksibilnost ili sposobnost prilagođavanja određenoj mreži koja se nadgleda
3. zaštita od zlonamernog ubacivanja grešaka
4. interoperabilnost sa ostalim mrežnim upravljačkim i bezbednosnim alatima
5. obuhvatnost, sa mogućnošću da se proširi koncept IDS na blokiranje Java appleta ili Active-X kontrola, nadgledanje e-mail sadržaja, blokiranje određenih URL
6. upravljanje događajima, kao što je upravljanje i izveštavanje o praćenju događaja, dopunjavanje baze podataka o napadima
7. aktivan odgovor kada dođe do napada, kao što je rekonfiguracija firewalla ili rutera
8. podrška za isporučeni proizvod.

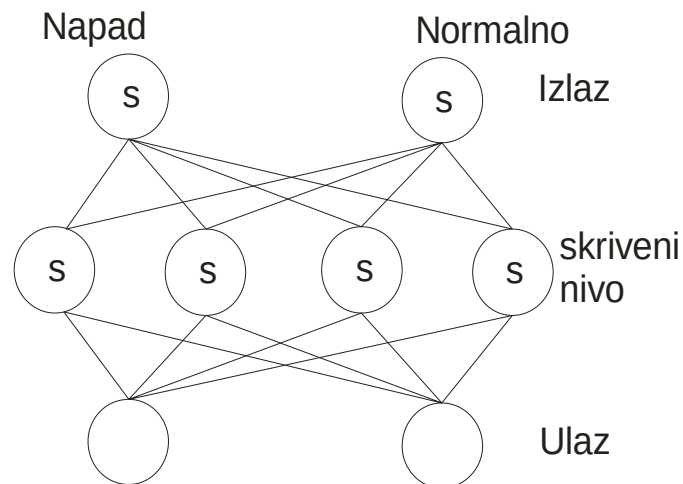
10.3.3.2 Neuronske mreže i IDS

Neuronska mreža sa veštačkom inteligencijom se sastoji od skupa postupaka kojim se transformiše skup ulaza u skup traženih izlaza kroz skup jednostavnih procesnih jedinica ili čvorova i njihovih međusobnih veza. Podskupovi su ulazni čvorovi, izlazni čvorovi i čvorovi koji između ulaza i izlaza formiraju skrivene nivoe. Veze između dva čvora imaju određenu vrednost, što se koristi za određivanje njihovog međusobnog uticaja. Izdvajaju se dva tipa arhitekture neuronskih mreža:

- Nadgledani algoritmi za obučavanje gde u fazi obučavanja, mreža uči željene izlaze za zadate ulaze ili modele. Poznata arhitektura nadgledane neuronske mreže je (*engl.* Multi-Level Perception MLP); koja se koristi za rešavanje problema prepoznavanja uzoraka.
- Nenadgledani algoritmi za obučavanje kod kojih se, mreža obučava bez zadavanja željenih izlaza. (*engl.* Self-Organizing Maps SOM) je popularan nenadgledani algoritam; SOM pokušava da pronađe topološko preslikavanje sa ulaznog prostora na klastere. Koristi se za rešavanje problema klasifikacije.

Najvažnija osobina neuronskih mreža je automatsko učenje/menjanje koeficijenata u neuronskoj mreži u skladu sa ulaznim i izlaznim podacima. Prilikom uvođenja neuronske mreže u IDS, prvo se prikazuju podaci koji važe za normalno stanje, a zatim se podešavaju koeficijenti koji važe za stanje napada na nadgledanu računarsku mrežu. Ispitivanje performansi sistema se vrši u uslovima realnog saobraćaja i napada na mrežu. Neuronske mreže su dosta zastupljene u rešavanju složenih problema kao što su prepoznavanje uzoraka, prepoznavanje rukom pisanog teksta, statističke analize.

Ovde navodimo četiri aplikacije sa neuronskim mrežama koje su primenjene u IDS, dve za model sa detektovanjem greške i dve za model detektovanjem na osnovu anomalija.



Slika 10.3.3.2 Prikaz percepcije sa jednim skrivenim nivoom

U okviru Georgia Technical research institute (GTRI) sprovedeno je istraživanje na primeni Multi –Level Perception (MLP) modela i MLP/SOM (Self-Organizing Maps) za detektovanje zloupotreba na mreži. MLP prototip je sa karakteristikama: 4 potpuno povezana nivoa, 9 ulaznih čvorova i 2 izlazna čvora (normalno i napad). Sa tim prototipom, simulirani su specifični napadi kao što je ISS skeniranje, SATAN skeniranje i SYNflood, i svaki napad je jasno prepoznat u okviru normalnog saobraćaja. MLP/SOM prototip je napravljen da detektuje disperzivne napade i napade gde je moguće pomaganje iznutra. U fazi obučavanja, neuronska mreža je napredovala veoma brzo. Početni rezultati pokazuju da je čak i neuspešno FTP prijavljivanje ispravno detektovano kao napad.

Istraživanje neuronskih mreža u IDS u okviru MIT Lincoln laboratorije je dovelo do testiranja primene neuronskih mreža u modelu detekcije zloupotrebe, traženjem za

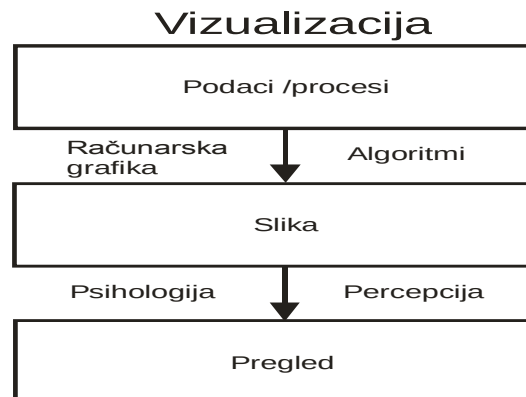
napad karakterističnih reči u mrežnom saobraćaju. Oni su koristili MLP za detektovanje napada na Unix host računare, i napada za dobijanje root privilegija na serveru. Generičke ključne reči su odabrane za detektovanje pripreme napada i akcija koje se izvode posle toga. Percepcija na dva nivoa je napravljena sa k ulaznih čvorova, 2k skrivenih čvorova i 2 izlazna čvora (normalno i napad); prostiranje unazad u fazi obučavanja detektuje vrednost veza u okviru neuronske mreže. Dobre performanse za detektovanje napada su postignute sa skupom od 30 odabranih ključnih reči, kao što su „cat”, „uudecode”, ili za novi root shell „uid=0”, „bash”

U okviru Reliable Software Technologies Corp. koristili su pristup neuronske mreže sa modelom detektovanja anomalija i analizom profila ponašanja programa za IDS. Profili ponašanja programa su napravljeni hvatanjem sistemskih poziva koje obavlja program. Njihov IDS je sa jednim skrivenim nivoom MLP, oni su takođe koristili takozvani Lucky Bucket algoritam da bi zadržali u memoriji trenutne vrednosti koje karakterišu tek izvršene nenormalne događaje, i tako upravljali brojačem: za normalno stanje, brojač teži ka nuli, a za stanje kada postoji napad brojač teži ka jedinici. Performanse ovog sistema su testirane sa DARPA bazom podataka. Primenjen na detekciju anomalija, sistem detektuje sa dobrim performansama poznate i nove napade (77% napada je detektovano sa 3% lažnih alarama), ali aplikacija sa detekcijom na osnovu greške ima znatno više lažnih alarma, izuzev kada se radi o primeni u komercijale svrhe.

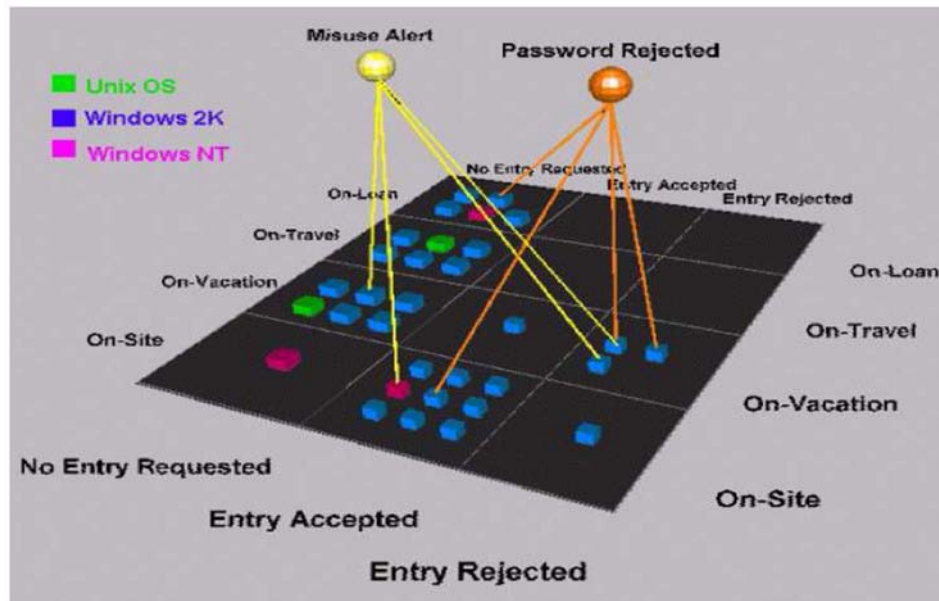
Sa namerom da iskoristi model sa detekcijom na osnovu izuzetka, A.Ghosh je testirao metodu detekcije upada sa drugačijom topologijom neuronske mreže, tzv. Elmanova mreža za raspoznavanje mogućnosti za rekurentno izvršavanje programa. Elmanova mreža je zasnovana na feed-forward topologiji sa dodatkom zadržavajućih čvorova koji sadrže informacije od prethodnih ulaza. Primenjena na DARPA bazu podataka, Elmanova mreža je u stanju da detektuje 77% napada bez ijednog lažnog alarma, poboljšavajući tako rezultate postignute sa MLP tehnologijom.

10.3.3.3 Sistemi za vizualizaciju podataka kao podrška IDS

Sistemi za grafičko prikazivanje podataka o stanju u mreži se koriste kao pomoć profesionalcima koji online nadgledaju velike računarske mreže. Proces grafičkog prikazivanja stanja u mreži je dat na slici 10.3.3.3.1.



Slika 10.3.3.3.1 Proces grafičkog prikazivanja stanja u mreži



Slika 10.3.3.2 Grafički prikaz napada na datu računarsku mrežu

Problem prikupljanja velike količine informacija u veoma kratkom vremenu, u odnosu na optimalno vreme za reagovanje na incident, je postavio zahtev za automatizaciju procesa prikupljanja obrade i prikazivanja podataka. Što duže taj proces traje - to će napadač imati više vremena da učini štetu pre nego naiđe na odgovarajuću reakciju. Iz tog razloga, čisti podaci sami po sebi obezbeđuju malo relevantnih informacija na vreme. Slike dinamičkih događaja koje se pojavljuju u okviru nekoliko prozora za nadgledanje mreže predstavljaju znatno lakši način da se dođe do informacija o saobraćaju na mreži.

10.3.3.4 Sistemi za prevenciju upada u mrežu IPS

Sa specijalnim hardverom (ASICs, FPGAs, mrežnim procesorima) koji je sada dostupan, prevencija upada u mrežu je realnost. Intrusion Prevention System (IPS) je bolje implementirati kao prefabrikovani deo mreže nego kao pasivni deo koji se nakandno dodaje mreži. Kako svaki paket dolazi u mrežu, on se potpuno analizira i tada se donosi odluka prolazi-ne prolazi. Ako je paket zlonameran, on se odbacuje tako da nikada ne dospe do potencijalne žrtve. Važno je da se odluka donosi pre nego što paket dospe do žrtve. Postoje proizvođači koji pokušavaju da adaptiranjem IDS naprave IPS. To rade tako što koriste TCP resetovanje i prepodešavanje firewala. Problemi koji se tada javljaju su brojni. TCP reset je signal koji se šalje napadaču i žrtvi tako da prekine konekciju pre nego što dođe do zloupotrebe. Problem je u tome što IDS/IPS vidi napad u isto vreme kada i žrtva napada, tako da je šteta često već pričinjena u vreme kada se šalje signal za reset. Takođe TCP reset nije efikasan protiv napada koji se ne zasnivaju na TCP. Primer je Slammer crv zasnovan na UDP, koji je potpuno neosetljiv na TCP reset. Prepodešavanje firewall-a je signal koji IDS/IPS šalje firewall-u (ili ruteru) da bi blokirali saobraćaj sa IP adrese odakle dolazi napad. Ovaj metod ima iste slabe strane kao i TCP reset. Dodatno, ometanjem napada koji liči na saobraćaj od legitimnog korisnika, napadač izaziva promenu pravila na firewall-u tako da se blokira legitimni korisnik. U osnovi napadač tako izaziva napad ometanjem servisa (DoS).

Kada se pravilno implementira, IPS zasnovan na hardverskoj platformi dozvoljava izuzetno precizne i procesorski dobro podržane definicije zlonamernog saobraćaja. To pomaže da se prevaziđe interesovanje za IDS. Za uspešnu primenu IPS dobro je da implementator što bolje poznaje mrežu koju štiti, tj. da zna koja vrsta saobraćaja je uobučajena za tu mrežu.

Mrežni procesori mogu da obrađuju saobraćaj do brzina reda Gb/s, što je sasvim prihvatljivo. I kada je uključena potpuna zaštita IPS ima zadržku od 215 milisekundi. Pouzdanost mrežnih uređaja za IPS, koji se vezuju redno, je važan faktor. Niko ne želi da ima još jednu tačku otkaza u mreži. Sprečavanje neželjenog uticaja IPS na pouzdanost rada mreže se vrši odgovarajućim izborom protokola za rutiranje koji obavlja prerutiranje u slučaju otkaza nekog od elemenata u mreži. Druga mogućnost je postavljanje redundantnog IPS sistema u režimu vruće rezerve, koji bi trenutno preuzeo sve funkcije primarnog sistema. Na kraju, postoji mogućnost da se IPS podese tako da u slučaju otkaza ili preopterećenja propušta sav saobraćaj bez provere.

10.3.3.5 IDS na osnovu hardverskih karakteristika opreme – fingerprint

Oprema za WLAN koju proizvođači isporučuju, kao što se i očekuje, odgovara standardu IEEE 802.11, a to potvrđuje i WiFi asocijacija. Pa ipak proizvodi mogu da variraju kada je u pitanju implementacija ovog standarda. Svaka implementacija se sastoji od softvera (drajveri za uređaj), hardvera (radio čipset), i firmware za taj čipset. Kombinacija ove tri komponente je jedinstvena za svaku implementaciju pa se ona tako može identifikovati. Nepromenljivo, implementacija ispoljava isto ponašanje koje se može uočiti ili izmeriti i ono je jedinstveno. To ponašanje se naziva njenim 802.11 otiskom (*engl. fingerprint*). Takvi otisci nam omogućavaju da identifikujemo implementacije. Postoje dve vrste identifikacije otiska implementacije, aktivna i pasivna.

Aktivna identifikacija se zasniva na posmatranju varijacija implementacije 802.11 standarda. Dve aktivne tehnike se razmatraju. Jedna tehnika uzima u obzir odziv 802.11 implementacije na CTS pakete koji pokušavaju da koriste virtual carrier sense mehanizam da bi rezervisali pristup medijumu. Druga tehnika je efikasnija i obuhvata modifikacije paketa koji se razmenjuju tokom tipičnog odziva autentikacija i pridruživanje kada se klijent prijavljuje na AP. Kada se jednom obavi razmena podataka rezultat se može kategorizovati i potražiti u tabeli. Ova tehnika zahteva bar jedan pokušaj od strane implementacije za koju treba uraditi otisak, da se pridruži pristupnoj tački, koja je modifikovana tako da šalje posebnu vrstu okvira sa podacima za pridruživanje i autentikaciju kao odgovor. Ovi okviri sa podacima izazivaju različito reagovanje od strane 802.11 implementacije. Otisak u ovom slučaju je odgovor 802.11 implementacije na poslate specijalne okvire podataka.

Pasivna identifikacija se obavlja pomoću offline algoritma. Algoritam uzima kao ulaz prikupljene 802.11 pakete koje je poslala 802.11 implementacija koja se ispituje. Ona poredi određene karakteristike prikupljenih paketa sa bazom podataka koja je ranije prikupljena, i vraća informaciju o tome koja je implementacija najverovatnije generisala to što je prikupljeno.

Alati i tehnike ovde opisane rade sa neočekivano malom količinom informacija, koje se čuvaju u tzv. print database. Tu postoji otisak za svaku implementaciju. Otisak je baza podataka koja se sastoji od rekorda u formi (packet_type, duration-value, count) sa kojim daje za dati tip paketa broj pojavljivanja paketa sa određenim trajanjem. Svi

okviri sa podacima i upravljački okviri se posmatraju dok se kontrolni paketi odbacuju.

10.3.4 Zaštita bežične mreže od napada ometanjem servisa

Kada se DoS napad već dogodio, male su šanse da se brzo zaustavi. Ipak postoji nekoliko koraka koji mogu pomoći u ublažavanju posledica napada. Ako je napad bio usmeren na samo jedan računar, najbolje je promeniti IP adresu tog računara.

Ako je napad nesofisticiran, može se uočiti specifičan saobraćaj. Ispitivanje uhvaćenih paketa može otkriti neki podatak na kojem se mogu zasnivati ili ACL (*engl.* Access Control List) rutera ili pravila firewall-a. Velika količina podataka može dolaziti od specifičnog davaoca Internet usluga ili *core* rutera. U tom slučaju može se privremeno blokirati sav saobraćaj koji dolazi od tih izvora. Nažalost blokirće se i legalan saobraćaj, ali to je neizbežno.

Alternativna opcija je dodavanje novog hardvera ili povećanje propusnog opsega i čekanje da napad prođe. Ovo možda nije najbolje rešenje, ali može pružiti privremenu zaštitu. Poslednja metoda bi bila fizičko isključivanje servera sa mreže, što administratoru daje vremena da reši problem, ali u tom slučaju ni jedna usluga neće biti dostupna legalnim korisnicima.

Najlakši način za preživljavanje DoS napada je planiranje odbrane od njega. U tom pogledu, formiranje odvojenog bloka IP adresa za hitne slučajeve može biti korisno.

Najbolji način obrane od SYN napada su SYN kolačići (*engl.* cookies). Oni menjaju upravljanje TCP protokolom tako da usporavaju zauzimanje resursa dok se ne proverí IP adresa klijenta.

Firewall nije efikasan protiv DoS napada. Većina firewall rešenja ne može da razlikuje legalan saobraćaj od saobraćaja koji se koristi kod DoS napada. Novija firewall rešenja imaju ugrađenu mogućnost razlikovanja legalnog od zlonamernog saobraćaja. Oni potvrđuju TCP veze pre prosljeđivanja na mrežu. Ova mogućnost zove se "*Defender*".

Neki switch uređaji pružaju automatsko i/ili *system-wide rate-limiting*, oblikovanje saobraćaja, *delayed binding (TCP splicing)*, proveravanje paketa i filtriranje IP adresa da bi otkrili i ispravili štetu koju su naneli DoS napadi kroz automatsko filtriranje i WAN *link failover* i balansiranje.

Ruteri su jako slični switch-u kada su u pitanju DoS napadi. Oni takođe imaju *rate-limiting* i ACL sposobnosti. Većina switch-eva se može lako preopteretiti tokom DoS napada, tako da nisu efikasni u borbi protiv DoS napada.

Front end hardver analizira pakete podataka prilikom ulaza u sistem i identifikuje ih kao prioritetne, regularne ili opasne.

Sistemi za prevenciju nedozvoljenog ulaženja (*engl.* Intrusion-prevention systems - IPS) jako su efikasni ako napadi imaju specifične tragove ili potpise. IPS sistemi koji rade na principu raspoznavanja uzoraka ne mogu blokirati DoS napade koji su zasnovani na ponašanju.

ASIC (*engl.* Application Specific Integrated Circuit) zasnovani IPS sistemi mogu otkriti i blokirati DoS napade jer imaju mogućnost analiziranja napada i ponašaju se kao automatizovani uređaji.

Rate-based IPS sistemi moraju analizirati granularnost saobraćaja i stalno nadgledati uzorak saobraćaja da bi otkrili bilo kakve anomalije. Oni moraju dozvoliti prolaz legalnom saobraćaju, a blokirati DoS napade.

Otpornost bežičnih računarskih mobilnih mreža na ometanje može se povećati: [38]

1. trenutno se infrastruktura bežičnih mreža sastoji i od radio-relejnih linkova. Ako bi se ovi linkovi zamenili optičkim vlaknima, mogućnost za ometanje bi se svela na ometanje interfejsa između bazne stanice i korisničkih jedinica
2. upotreba što usmerenijih antena sa velikim potiskivanjem bočnih listova sprečava radio ometanja iz svih ostalih pravaca osim direktnog. Vrlo je malo verovatno da se ometač nalazi tačno na liniji propagacija glavnog snopa
3. veličina ćelija treba da je što manja zbog vrlo striktnog ograničenja izlaznog nivoa na uređajima. Mala veličina ćelija povećava mogućnost za *handover* između ćelija, što smanjuje efikasnost ometanja
4. upotreba frekvencijskog skakanja prisiljava ometača da svoju izlaznu snagu proširi na veći oseg kanala, ako želi da uspe u ometanju. Detekcija pravca je takođe otežana usled procesnog pojačanja, zbog slabijeg odnosa S/N, kao i zbog toga što više predajnika mogu da emituju signal istovremeno
5. obaranje brzine protoka povećava otpornost na ometanje;
6. prednosti impulsnog ometanja se mogu poništiti upotrebom interleaving procedure kao i upotrebom nekog od Forward Error Corection (FEC) algoritama
7. arhitektura kanala bi trebalo da se isprojektuje tako što će ideja o ometanju stalno biti prisutna. Sekvenca skakanja i pseudoslučajna sekvenca za širenje spektra ne bi trebali da se prenose da se pre toga na neki način ne kodiraju
8. sinhronizacija bi trebalo da se tako projektuje da bude najteža za ometanje.

10.3.5 VPN u bežičnoj mreži

Virtuelna privatna mreža (VPN) predstavlja privatnu mrežnu konekciju koja se obavlja preko javne mreže. Privatna mreža obezbeđuje zaštićeni prenos preko neobezbeđenog okruženja, kao što je bežična računarska mreža. Krajnji učesnici u VPN se ponašaju kao da su povezani lokalno. VPN zahteva instalaciju specijalnog hardvera ili VPN softverskih paketa na serveru i u radnim stanicama. VPN koristi protokol tunelovanja, kao što su Layer 2 Tunneling Protocol (L2TP), IPsec ili Point-to-Point Tunneling Protocol (PPTP). IPsec nudi najviši stepen zaštite, pa se sve više koristi u sigurnim VPN okruženjima.

IPsec (*engl.* IP Security) je grupa protokola koji je razvila organizacija IETF (*engl.* Internet Engineering Task Force) kako bi zaštitila razmenu podataka preko IP sloja u mrežnom protokolu koji se koristi na Internetu. IPsec se koristi kod implementacije virtualne privatne mreže (*engl.* Virtual Private Network). Dakle osnovna namena IPsec protokola je mogućnost uspostavljanja sigurne komunikacije između dva računara preko nesigurnog medijuma kao što je Internet, lokalna mreža ili bežična mreža.

IPsec ima dva osnovna načina rada:

- Transportni način (*transport mode*)
U ovom načinu rada šifrjuje se samo teret (*payload*) koji nosi paket, ne i njegovo zaglavlje (*header*).
- Tunelski način (*tunnel mode*)
U ovom načinu rada šifrjuje se i teret i zaglavlje paketa. Smatra se sigurnijim od transportnog načina.

Takođe postoje i dva protokola koji se koriste u IPsec-u:

- AH (*engl.* Authentication header)
Koristi se samo za autentifikaciju svakog pojedinog paketa.
- ESP (*engl.* Encapsulating Security Payload)

Obavlja autentifikaciju i enkripciju svakog pojedinog paketa.

Dakle iz prethodno navedenog može se videti da korisnik koji želi autentifikovati primljeni paket ima ukupno četiri različita načina na raspolaganju:

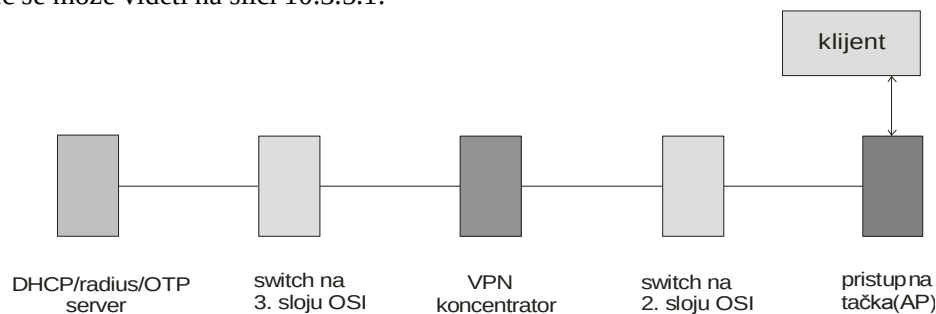
- Transportni način/AH
- Tunelski način/AH
- Transportni način/ESP ukoliko se ne koristi enkripcija
- Tunelski način/ESP ukoliko se ne koristi enkripcija

Međusobna razlika je minorna tako da je praktično svejedno koji će se način koristiti. Ali to donosi sa sobom i pitanje zašto su nam onda potrebna dva protokola koji se koriste. Misao vodilja kreatora IPsec-a je bila da se AH koristi kada je potrebna autentifikacija, a ESP kada je uz autentifikaciju potrebno i pakete zaštititi enkripcijom. Na prvi pogled se vidi kako je transportni način rada ustvari deo tunelskog načina rada, gledajući iz perspektive mreže. Jedina prednost korišćenja transportnog načina rada je u nešto manjem opterećenju mreže, ali i to se da popraviti ukoliko se u tunelskom modu primene neke metode kompresije zaglavlja paketa. Nameće se zaključak da se transportni način rada može izbaciti iz protokola i može, bez ikakvih posledica, koristiti samo tunelski način rada.

U transportnom načinu rada bolje je koristiti AH protokol jer on autentifikuje i zaglavlje paketa. U tunelskom načinu rada najčešće se koristi ESP protokol.

AH protokol ima i neke nedostatke. Najveći nedostatak je to da on autentifikuje zaglavlja i nižih mrežnih slojeva što je direktno kršenje načela modularnosti u izradi mrežnih protokola. Zbog toga AH protokol mora poznavati sve tipove podataka koji se koriste u zaglavlju nižih mrežnih slojeva. Ukoliko se dogode izmene u standardu koji opisuju neki od nižih mrežnih protokola to će dovesti do problema sa AH protokolom u IPsec-u. Tunelski način rada u kombinaciji sa ESP-om otklanja navedeni problem ali je on i zahtevniji na širinu propusnog opsega (*engl.* bandwidth).

Osnovna ideja korišćenja IPsec-a u bežičnim mrežama jeste da bežičnu mrežu smatramo kao i javnu (nesigurnu) mrežu. Dakle bežičnu mrežu treba staviti izvan intraneta organizacije i na taj način povećati bezbednost mreža. Kada se želi primeniti IPsec u bežičnoj mreži prvi korak je instalacija klijentskog programa (ukoliko već sam operativni sistem nema podršku) koji podržava IPsec na svaki računar u bežičnoj mreži. Na taj način se osigurava da klijent mora pre nego što se pridruži bežičnoj mreži uspostaviti IPsec tunel do žične mreže i samo kroz njega može komunicirati sa drugim računarima. Saobraćaj se filtrira na više slojeva, na 2. i 3. sloju OSI modela i na taj način se osigurava komunikacija isključivo preko sigurnog tunela. Model mreže koja koristi IPsec se može videti na slici 10.3.5.1.



Slika 10.3.5.1: Model mreže sa IPsec

Na slici su vidljivi bitni entiteti:

- Klijentska programska i hardverska podrška koja omogućava komunikaciju klijenta i pristupne tačke (mrežna kartica, antena, odgovarajući programi...)
- VPN klijentska programska podrška sa ličnim firewall-om omogućava uspostavljanje sigurnog tunela od kraja do kraja tj. od klijentskog računara do VPN koncentratora. Firewall štiti korisnika od raznih opasnosti sa mreže
- Pristupna tačka pruža usluge spajanja klijentima, ali i vrši filtriranje po IP adresama između klijenta i mreže
- Switch na drugom sloju OSI modela spaja lokalnu mrežu sa pristupnom tačkom. Neki noviji modeli imaju mogućnost korištenja VLAN ACL (VACL) koja dodaje još jedan sloj u filtriranju adresa
- Switch na trećem sloju OSI modela ima ulogu usmeravanja IP paketa prema raznim modulima a pruža i uslugu filtriranja IP paketa sa bežične mreže
- RADIUS server se koristi pri autentifikaciji korisnika žične/bežične mreže Opcionalno komunicira sa OTP serverom.
- OTP (*engl.* One-Time Password) server ima ulogu autorizacije OTP informacija koje šalje RADIUS server
- DHCP server daje adrese VPN klijentima pre i poslije uspostavljanja VPN-a
- VPN koncentrator ima ulogu autentifikacije klijenata, a može i dodeljivati IP adrese klijentima (one koje je dobio od DHCP servera).

Kao što vidimo uvođenje VPN-a u neku organizaciju zahteva nove, velike investicije. Na svakoj organizaciji je da proceni isplati li se uvoditi tako kompleksan sistem s obzirom na njihove potrebe.

IPsec otklanja nekoliko vrsta opasnosti:

- **Krađa paketa**

Krađa paketa je nemoguća jer se koristi jaka enkripcija svih podataka koji se šalju u eter. Novija programska podrška dopušta da se tunel automatski digna čim korisnik pokuša da se spoji na mrežu tj. kada mu se dodeli ispravna IP adresa. Na ovaj način je izbegnuto da korisnik mora ručno podizati tunel, on je oslobođen svih tehničkih detalja

- **Napad čovek-u-sredini**

Ovaj tip napada je onemogućen korištenjem enkripcije i autentifikacije klijenata

- **Neovlašćen pristup**

Kako je jedino inicijalnim protokolima (DHCP za dodelu privremene IP adrese, IKE (*engl.* Internet Key Exchange) koji se brine o raspodeli ključeva i ESP kojim se uspostavlja siguran tunel) dozvoljen prolazak preko filtera nije moguće da bi napadač mogao doći do podataka iz lokalne mreže preko pristupne tačke. Dodatno se mogu pojačati mere bezbednosti na VPN koncentratoru zavisno od vrste korisnika koji se žele spojiti

- **Umetanje i krađa IP paketa**

Napadač može snimiti IP paket ali ga ne može ponovno iskoristiti jer neće proći proveru i autentifikaciju kroz sve filtre

- **Umetanje i krađa ARP paketa**

Moguće je da napadač snimi ARP saobraćaj na mreži ali ne može doći do nikakvih podataka jer se koristi jaka i sigurna enkripcija (3DES ili u novije vreme AES)

- **Otkrivanje topologije mreže**

Kako su dozvoljeni protokoli samo IKE, DNS, DHCP i ESP napadač ne može prodrati sa ICMP (*engl.* Internet Control Message Protocol) paketima u mrežu, a tako ne može ni otkriti topologiju mreže.

Ovom se protokolu zamera velika kompleksnost. Kompleksnost sistema je u suprotnosti sa njegovom bezbednošću jer što je sistem kompleksniji veća je i mogućnost da se dizajnerima potkradu greške. Sistem je kompleksan ponajpe jer je na njegovom dizajnu radilo mnogo ljudi pa se nastojalo da se sve strane zadovolje nauštrb jednostavnosti dizajna sistema. Ranije je napomenuto da se može transportni način rada, uz manje prepravke, u potpunosti izbaciti i koristiti samo tunelski način rada. Isto bi se moglo zaključiti i za AH protokol koji vrši samo autentikaciju korisnika - i on bi se mogao zameniti sa ESP protokolom koji dozvoljava autentikaciju i enkripciju. Nadalje većina stručnjaka smatra da bi trebalo autentikaciju u ESP protokolu učiniti obaveznom, a ne kako je sada, opcionom. Opciona bi trebalo da ostane samo enkripcija.

Možemo zaključiti da je IPsec/VPN tehnologija najbolji izbor za maksimalnu bezbednost bežičnih računarskih mreža i uprkos visokoj ceni uvođenja i kompleksnosti sistema trebalo bi je koristiti u svakoj važnijoj bežičnoj računarskoj mreži.

Jednosmerna funkcija F ima sledeće karakteristike. Za datu vrednost x relativno je lako izračunati vrednost funkcije $F(x)$, ali ako je dato $y = F(x)$ onda ne postoji lak put za dobijanje vrednosti x , tj. $1/F(x)$ je veoma teško izračunati.

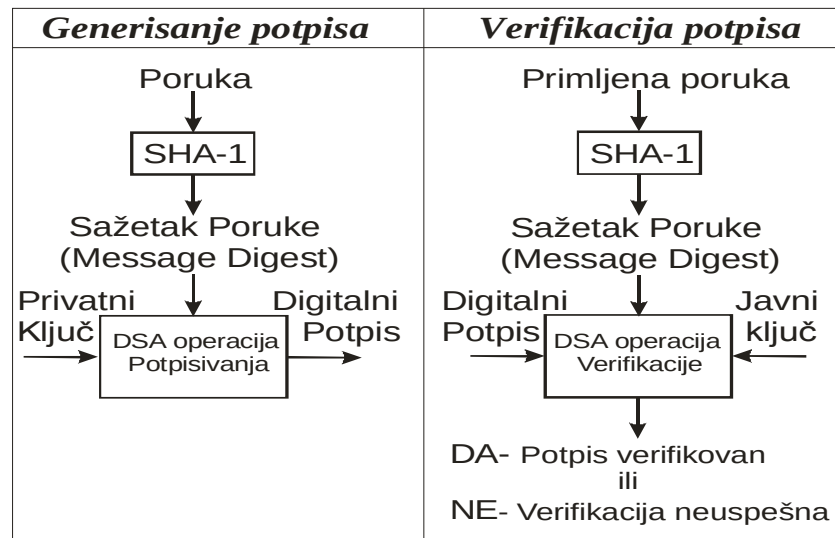
Jasno je da se može izračunati bilo koji broj odgovarajućih vrednosti x i $F(x)$ i smestiti u memoriju u tablicu u kojoj će x biti izraženo kao funkcija od y . Ako je domen funkcije vrlo veliki, nije izvodljivo formiranje inverzne funkcije. Pojam jednosmeran nije apsolutan već zavisi od toga za koliko mnogo izračunavanja kažemo da predstavlja „nemoguće veliki broj”. Kažemo da je za zadatak vrednost funkcije $F(x)$ izračunavanje vrednosti za x računskim putem neizvodljivo.

Specijalne karakteristike eksponencijalnih funkcija mogu se iskoristiti u zadatku distribuiranja ključa. U komunikaciji se dva kraja veze dogovaraju o osnovi a i o modulu p velikog prostog broja. Sve aritmetičke operacije koje slede se izvršavaju po modulu p . Mogu se primenjivati normalni aritmetički zakoni. U toj aritmetici funkcija a na x je jednosmerna funkcija od x . Drugim rečima nalazenje logaritma od x za osnovu a nije izvodljivo za skoro sve vrednosti x . To zahteva oko $2p \exp \frac{1}{2}$ množenja i otprilike istu količinu memorijskog prostora. Jedan sagovornik odabere broj x , a drugi y . Oni ove brojeve čuvaju kod sebe, a jedan drugom šalju $a \exp x$ i $a \exp y$. Sada svaki može da izračuna $a \exp xy$ stepenovanjem. Provalnik koji zna samo predete vrednosti ne može da nađe ni x ni y niti, $a \exp xy$. Vrednost $a \exp xy$ je tajni ključ koji je formiran posredstvom javne mreže.

Secure Hash Algorithm, SHA-1, služi za izračunavanje zgusnute reprezentacije poruke ili fajla sa podacima. Kada je poruka bilo koje dužine manje od 2^{64} bitnog ulaza, SHA-1 pravi 160-bitni izlaz koji se naziva **message digest**. Message digest može biti ulaz za Digital Signature Algorithm (DSA) kojim se generiše ili verifikuje potpis poruke. Potpisivanje message digest umesto potpisivanja poruke povećava efikasnost postupka zato što je message digest obično daleko manji od poruke. Isti hash algoritam mora biti upotrebljen da verifikuje digitalni potpis kao što je upotrebljen kada je pravljen digitalni potpis.

SHA-1 je nazvan sigurnosnim zato što je računarski veoma teško pronaći poruku koja odgovara datoj message digest, ili pronaći dve različite poruke koje daju istu message digest. Bilo koja promena u poruci u toku prenosa, će sa velikom verovatnoćom, proizvesti različitu message digest, i potpis će pasti prilikom verifikacije. SHA-1 je tehnički usavršeni SHA (FIPS 180). Kružno levo šiftovanje je operacija koja je dodata prema specifikaciji u odeljku 7, linija b, strana 9 FIPS 180 i njegovog ekvivalenta u odeljku 8, linija c, strana 10 FIPS 180. Ova ispravka je podigla bezbednost koju obezbeđuje ovaj standard. SHA-1 je zasnovan na

principima sličnim onima koji su korišćeni od strane prof. Ronald L. Rivest sa MIT kada je projektovao MD4 ("The MD4 Message Digest Algorithm"), napravljen neposredno posle tog algoritma.



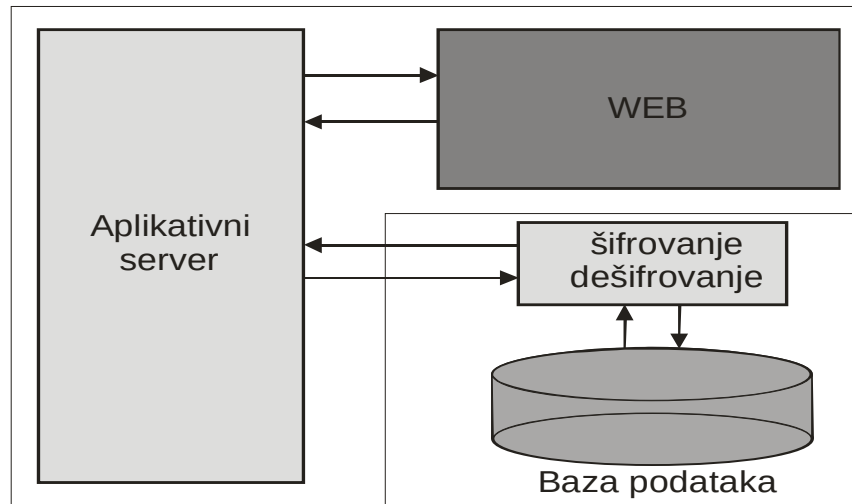
Slika 10.3.5.2 Upotreba SHA-1 sa DSA

10.3.6 Zaštita podataka kriptovanjem na diskovima u mreži

Kao još jedna mogućnost zaštite baza podataka kojima se pristupa preko mreže, dostupno je kriptovanje podataka na diskovima u mreži. Teži se da krajnji korisnici što manje osećaju prisustvo kriptografskog rešenja i da im se ne menjaju vremenski resursi. Pri tome dobro je da kriptografsko rešenje bude uz upotrebu pouzdanih nosećih softverskih komponenti čiji je izvorni kod dostupan, kako bi se što realnije mogla izvršiti procena nivoa bezbednosti rešenja. Dva su najčešća pristupa kriptovanju podataka na diskovima u mreži:

Kriptovanje unutar baze podataka:

Za realizaciju ovog rešenja lokalne zaštite često se koristi MySql baza podataka. Izvorni kod nekih od realizacija je dostupan i/ili postoji mogućnost proširenja dok su neke realizacije potpuno zatvorene. MySql SUBP ne poseduje sve funkcionalnosti kao sistemi tipa Oracle ali dovoljan skup funkcionalnosti i povoljna cena su pozitivno uticali na prihvatanje ovog softvera od strane tržišta. Danas većina programskih jezika poseduje biblioteke za korišćenje MySQL-a, a postoji i ODBC interfejs za jezike za koje nije ugrađena podrška. Mesto modula za kriptovanje kod lokalne zaštite baze prikazano je na Slici 10.3.6.1.



Slika 10.3.6.1 Kriptovanje unutar baze podataka [22]

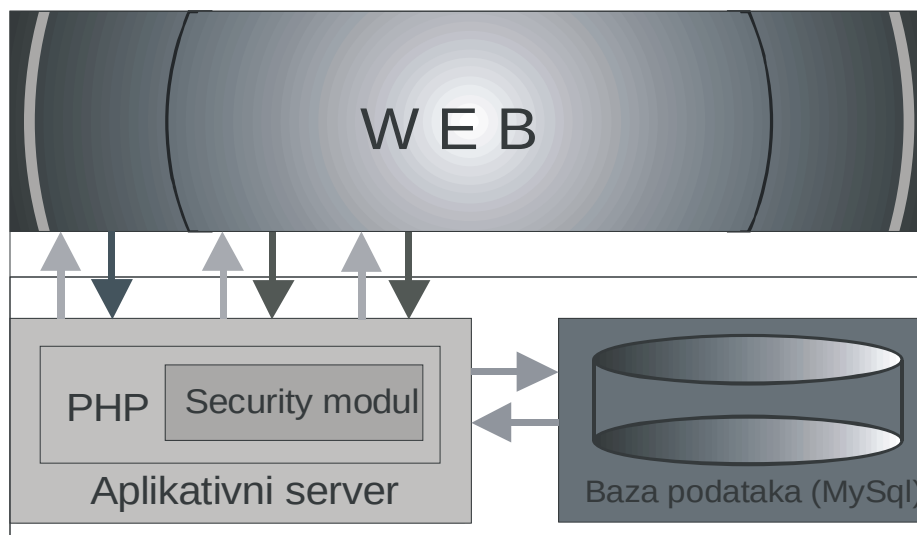
MySQL u svom kriptografskom modulu koristi dva najpoznatija algoritma za kriptovanje AES i DES. AES algoritam ("Rijndael") koristi funkcije AES_ENCRYPT() i AES_DECRYPT() za kriptovanje i dekriptovanje podataka. U ovom modulu MySQL može da koristi dužinu ključa od 128 ili 256 bita. Funkcija AES_ENCRYPT() kao rezultat vraća binarni string (šifrat), a funkcija AES_DECRYPT() vraća originalni string (otvoreni tekst). U slučaju kada se proslede pogrešni argumenti funkcijama, obe funkcije vraćaju kao rezultat nulu. Za realizaciju funkcije AES_ENCRYPT() kao argumente funkciji prosleđujemo tekst za kriptovanje i ključ algoritma dužine 128 ili 256 bita sa kojim šifrujemo, a za realizaciju funkcije AES_DECRYPT() kao argumente prosleđujemo šifrat i ključ koji smo koristili kod funkcije AES_ENCRYPT() pri kriptovanju. Prednosti ovakvog sistema kriptovanja su: realizacija AES algoritma u C programskom jeziku, podaci se u bazi čuvaju u kriptovanom obliku, a mane su nedostupnost izvornog koda, ključ se nalazi zajedno sa kriptovanim podacima, promena ključa (proces koji zahteva dekriptovanje i ponovno kriptovanje kompletne baze podataka) i to što podaci nisu zaštićeni u toku komunikacije sa bazom.

Kriptovanje na aplikativnom serveru:

Ovaj vid lokalne zaštite se postiže na klijent/server arhitekturi instalacijom kriptografskog modula na aplikativnom serveru. Komponente klijent/server arhitekture moraju se ponašati nekim osnovnim principima kako bi međusobno delovale ispravno. Ovi principi moraju biti jednoznačno upotrebljivi u komponentama klijenta, servera i komunikacionog posrednika. Principi koji moraju biti ispunjeni su: hardverska nezavisnost, softverska nezavisnost, otvoreni pristup za servise, distribucija procesa.

Klijent-server arhitektura se često koristi u vidu web aplikacija gde se može pojaviti veliki broj korisnika istovremeno, performanse i konkurentni pristup su dva pitanja na koja treba obratiti pažnju pri realizaciji. Različita serverska rešenja imaju različite pristupe za povećanje performansi. Na Slici 10.3.6.2 je ilustrovana moguća klijent server arhitektura koju je moguće iskoristiti u procesu zaštite podataka u bazama podataka. Prikazana arhitektura se sastoji od dva servera. Na jednom serveru se nalazi baza podataka, a na drugom aplikativni server. Aplikativni server implementira

php modul sa modulom za kriptovanje i dekriptovanje. Između ova dva servera postoji direktna komunikacija. Podaci koji se razmenjuju su u obliku šifrata.



Slika 10.3.6.2. Kriptovanje na aplikativnom serveru [22]

Prednosti ovog koncepta zaštite su: podaci u komunikaciji su zaštićeni, ključ se ne nalazi sa kriptovanim podacima, izvorni kod je dostupan, a mane su: realizacija AES algoritma u interpreterskom jeziku (što se odražava na performanse sistema), promena ključa (proces koji zahteva dekriptovanje i ponovno kriptovanje kompletne baze podataka).

Kod lokalne zaštite interveniše se na samoj bazi podataka uključivanjem modula za kriptovanje i dekriptovanje. Podaci u bazi su zapisani u kriptovanom obliku i obezbeđeni su od eventualne krađe hard diska ili neovlašćenog pristupa u bazi. Kod rešenja na aplikativnoj strani u okviru izabranog programskog jezika postiže se fleksibilnost sa mogućnošću selektivnog kriptovanja i dekriptovanja. Mana je što neki savremeni jezici (kao što je php) nisu optimizovani za efikasno izvršavanje kompleksnih operacija nad binarnim podacima što može da utiče na ukupne performanse sistema.

Performanse današnjih PC računara nisu dovoljne za potpuno iskorišćenje mogućnosti kriptografskih mehanizama za kriptovanje na opisanim nivoima. Postoji potreba za dodatnim hardverom za kriptovanje umesto softverskog rešenja. Time bi se omogućilo zadržavanje performansi rada sa konkretnom bazom podataka, uz kvalitetno kriptovanje na dodatnom hardverskom modulu. Eventualni pad performansi bi se odnosio samo na komunikaciju sa dodatnim hardverom.

Zaključak

U ovom radu su najpre dati osnovni pojmovi teorije informacija, bezbedne informacije i informacionog sistema. Navedeni su standardi za bežične računarske mreže a detaljnije su prikazani standardi IEEE 802.11 kao i IEEE 802.16. Kroz analizu mrežnog saobraćaja su prikazani načini identifikacije bežičnih računarskih mreža. Za analizu i poboljšanje bezbednosti, ali često i za napade na mrežu, se koriste neki od softverskih alata koji su prikazani. Da bi što bolje upoznali slabosti mehanizama zaštite, detaljnije su prikazani poznati načini za njihovo probijanje. Napad putem ometanja servisa (DoS) je takođe analiziran. Na kraju je dat sistematičan pregled mera za poboljšanje bezbednosti podataka.

Bežične računarske mreže su bezbednosni rizik za svakoga ko ih koristi. Uzroke treba tražiti u nepotpunoj primeni postojećih mehanizama zaštite kao i u još uvek važećim standardima 802.11a, 802.11b i 802.11g koji kao osnovu bezbednosti koriste WEP. On nije zadovoljio nijedan od tri cilja s kojim je stvoren: pouzdana autentifikacija korisnika, zaštita privatnosti podataka i autorizacija korisnika. Impresivan broj različitih mogućih napada, od kojih su neki i praktično uspešno izvedeni, samo potvrđuje činjenicu o nebezbednosti sadašnjeg standarda. Zbog toga se većina organizacija koje intenzivno koriste bežične mreže u svom poslovanju odlučila na skupo uvođenje IPsec tehnologije koja, iako ne bez mana, ipak značajno povećava bezbednost bežične mreže. IEEE uvidevši sve propuste u važećim standardima je počela ubrzano da radi na novim predlozima za poboljšanje bezbednosti bežičnih mreža. Prvi rezultat toga je i donošenje 802.1X standarda koji znatno poboljšava način autentifikacije korisnika i time povećava ukupnu bezbednost. Taj standard kao svoju osnovu koristi EAP koji omogućava veliki broj različitih metoda autentifikacije korisnika mreže. Sledeći korak u evoluciji bezbednosti je WPA standard koji je usvojen od strane udruženja proizvođača mrežne opreme za bežične računarske mreže (*Wi-Fi Alliance*). WPA je otklonio sve bezbednosne propuste u WEP-u, a pri tome uz manje promene drajvera radi na postojećoj opremi. Iako veliko poboljšanje WPA se smatra samo međukorakom između 802.11x standarda i najnovijeg 802.11i standarda koji se nameće kao konačno rešenje problema bezbednosti bežičnih računarskih mreža. Sam 802.11i standard je deo većeg RSN (*Robust Security Network*) standarda. 802.11i koristi kao algoritam za kriptovanje AES (*Advanced Encryption System*), a kao mehanizam autentifikacije se, iako 802.11i standard ne propisuje, koristi 802.1X standard. Za uvođenje 802.11i standarda u mreže je potrebno zameniti sadašnju bežičnu mrežnu opremu (pristupne tačke i mrežne kartice) sa novom.

Na osnovu iznetog pregleda standarda i tehnologije vidi se da primena samo komercijalnih tehnologija zaštite informacija ne može predstavljati pouzdano rešenje odbrane od potencijalnih napada. Potrebno je koncipirati i primeniti slojevit i sveobuhvatnu politiku zaštite. Ona će pored komercijalnih tehnologija zaštite obavezno uključiti i primenu sopstveno realizovanih mehanizama, kao i mehanizama kontrole pristupa i organizacionih elemenata zaštite date bežične računarske mreže.

Literatura

- [1] Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Cambridge, January 2001.
- [2] Suzana Stojaković – Čelutska. Building Secure Information Systems, dissertation. Prague. 2000.
- [3] IEEE Std 802.15.3™-2003 Specifications for High Rate Wireless Personal Area Networks (WPANs). 12.06.2003.
- [4] Thomas Maufer. Field Guide to Wireless LANs for Administrators and Power Users. Prentice Hall PTR. 2003.
- [5] IEEE lista proizvođača opreme i OUI kodova.
<http://standards.ieee.org/regauth/oui/>. 16.02.2009.
- [6] Itisk Martin Scott Fluhrer i Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. <http://www.crypto.com.papers/others/rc4.ksaproc.pdf> .
- [7] David Hulton. Practical exploitation of RC4 weakmesses in WEP environments. <http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt>. 02.2007.
- [8] Christopher Devine. Aircrack. <http://www.aircrack-ng.org>. 02.2007.
- [9] Hallvar Helleseth. Data set of WEP encrypted frames. 02 2007.
- [10] William A. Arbaugh. Real 802.11 Security. 2001.
- [11] Diskusioni forum: <http://www.netstumbler.org>. 02.2009.
- [12] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems
Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, IEEE, 28.02.2006.
- [13] Martin Beck, Erik Tews. Practical attack against WEP and WPA. 2008.
- [14] Robbie Gill. Security Note on WPA and WPA2 dictionary attacks. 2008.
- [15] <http://www.willhackforsushi.com/Cowpatty.html> . 05.06.2009.
- [16] <http://torrents.lostboxen.net/cowf-wpa-psk-hash-tables-with-cowpatty-4.0> 2006-10-19 . 03.06.2009 .
- [17] <http://www.tamos.com/>. 05.06.2009.
- [18] <http://www.elcomsoft.com>. 22.06.2009.
- [19] M. Barbeau. WiMax/802.16 Threat Analysis. ACM Press. str. 8-15, 2005.

- [20] Nenad Simić, Nenad Marić. DoS Napadi na IEEE 802.11 Radio sisteme. Telfor Beograd. 2004.
- [21] Japan Science and Technology Agency. <http://sciencelinks.jp/> 10.06.2009.
- [22] Saša Adamović, Mladen Veinović. Analiza zaštite podataka u bazama podataka na lokalnom i serverskom nivou. Telfor. Beograd. 2008.

Rečnik pojmova

Access node - Mesto na koje se mogu spajati klijenti, čini ga minimalno jedna pristupna tačka (access point).

Access Point - Uređaj koji omogućava klijentima spajanje na access node, i njegov je osnovni deo. Većina access point-a u unutrašnjosti je u stvari PCMCIA kartica sa dodatnom elektronikom, zavisno od modela.

Bridge - Uređaj koji povezuje dva ili više Access point-a odnosno node-a, ujedno i "prečišćava" - poboljšava signal.

Client node – Računar sa bežičnom mrežnom karticom koji se spaja na access point.

Kantena - Sinonim za ručno izrađenu klijent antenu.

LOS (Line of Sight) - Optička vidljivost između dve tačke bez obzira na udaljenost.

Omni antena, - Antena koja pokriva 360 stepeni. Vertikalno širenje snopa oko 8 stepeni, zavisi od proizvođača.

Parabolic antena - Usmerena antena karakterističnog rešetkastog izgleda, koja projektuje uski snop prema nekoj tački. Malo slabije karakteristike od Yagi-udo antena, no ponekad i bolje usmerenosti, do 12 stepeni.

Pigtail (jumper cable) - Komad antenskog kabla s konektorima. Na jednoj strani za antenu, a na drugoj za wi-fi karticu. Dužine od 0,5m do 5m uz velike gubitke, osim ako nije od HDF400 kabla (npr. SMC-ov 5 metarni).

PKCS (Public Key Cryptography Standards) – Skup javnih standarda čiji su autori RSA i vodeća imena iz oblasti zaštite u industriji.

PKI (Public Key Infrastructure) – Sistem kriptovanja sa dva ključa u kome se poruka šifruje privatnim a dešifruje javnim ključem.

Residential Gateway - Npr. Orinoco RG-1000 koji se softverski može prepraviti u veoma funkcionalan access point.

Repeater - Samostalni uređaj koji prima signal sa access point-a i "ponavlja" odnosno pojačava ga. Uređaj se identifikuje kao sam access point. Loša strana je smanjenje brzine prenosa podataka na polovinu.

Sector antena - "Inteligentna" antena, obično pokriva 90 stepeni.

Wi-Fi - Sinonim za IEEE 802.11b. Isto kao što je Ethernet za IEEE 802.3.

WLAN - Bežična Ethernet mreža.

MAN - Metropolitan Area Network, mreža širokih razmera.

Spisak slika:

1. Slika 1.1.1 Informacioni sistem uopšteni prikaz
2. Slika 1.1.2 Komunikacioni kanal sa greškama
3. Slika 1.2.1 Model observera
4. Slika 1.2.2 Model observacije neodređenosti informacije
5. Slika 1.2.3.1 Denial of service (DoS) napad
6. Slika 1.2.3.2 Neovlašćena modifikacija informacija
7. Slika 1.2.4 Napadnuti informacioni sistem sa alatima za zaštitu
8. Slika 1.2.5 Napadnuti informacioni sistem sa inteligentnim observerom
9. Slika 2.1.1. Odnos brzine prenosa i dometa za neke od standarda bežičnih mreža
10. Slika 3.1.1 OSI model sa podnivoima 802.11 tehnologije
11. Slika 3.2.1 802.11 generalni MAC okvir
12. Slika 3.3.1 Format PLCP okvira
13. Slika 3.4 Blok šema FHSS modulacije
14. Slika 3.5 Blok šema DSSS modulacije
15. Slika 3.6. Blok šema OFDM modulacije
16. Slika 3.8.1 Pristupna tačka (AP) i ruter
17. Slika 3.8.2.1 PDA sa Linux OS i internom bežičnom mrežnom karticom
18. Slika 3.8.2.2 Laptop sa internom bežičnom mrežnom karticom
19. Slika 3.8.3 Bežična mrežna karta
20. Slika 3.8.4.1 Dipol antena i njeni dijagrami zračenja, vertikalni i horizontalni
21. Slika 3.8.4.2 Usmerena antena i njeni dijagrami zračenja, vertikalni i horizontalni
22. Slika 3.8.5 Pojačavač signala
23. Slika 5.1 MAC format okvira
24. Slika 5.1.1 Polja kontrolnog okvira
25. Slika 5.1.3 Capability polje u beacon okviru
26. Slika 6.2.1 Pozdravna poruka Kismet alata
27. Slika 6.1.3 Opcije sortiranja Kismet alata
28. Slika 6.1.4 Detalji o odabranoj bežičnoj mreži
29. Slika 6.1.5 Lista klijenata spojenih na odabranu pristupnu tačku
30. Slika 6.1.6 Prikupljanje podataka sa određenog kanala
31. Slika 6.2.1 TCPDump – informacije o primljenim paketima
32. Slika 6.3.1 Ethereal pod Linuxom
33. Slika 6.5.1 Programi za izmenu MAC adrese
34. Slika 7.1.1 Protokol konekcije na WLAN
35. Slika 7.2.1 WEP - blok dijagram kriptovanja
36. Slika 7.2.2.1 Listing Airodump
37. Slika 7.2.2.2 Listing Aircrack
38. Slika 7.2.2.2 WEPLab ispitivanje passphrase seeded WEP ključeva
39. Slika 7.2.2.3 Napad tipa dvostruko kriptovanje
40. Slika 7.2.2.4.1 Listing Aireplay izvršava napad otvorenim tekstom
41. Slika 7.2.2.4.2 TCPDump prikazuje dekriptovane okvire
42. Slika 7.2.2.4.3 Hexdump prikazuje sekvencu ključa
43. Slika 7.2.2.7 WEPLab kreiranje 40 bitnog ključa metodom grube sile
44. Slika 7.2.3 Protokol za autentikaciju sa deljenim ključem
45. Slika 7.2.4.1 Dobijanje sekvence ključa tokom inicijalne autentikacije
46. Slika 7.2.4.2 listing PRGASnarf
47. Slika 7.2.5.1.1 listing ARP saobraćaj
48. Slika 7.2.5.1.2 Aircrack prosleđuje prikupljene ARP zahteve

- 49. Slika 7.2.5.2.1 Aircrack ubacuje okvire za deautenticaciju
- 50. Slika 7.3.2.1 coWPAtty alat za WPA-PSK rečnički napad
- 51. Slika 8.2 Simboli koji u gradovima ukazuju na bežične mreže
- 52. Slika 8.1 Netstumbler program - ratna vožnja
- 53. Slika 8.2 Snimak područja na kojem je vršena detekcija AP-a
- 54. Slika 9.1 TCP rukovanje u normalnom slučaju
- 55. Slika 9.2 SYN flood: nekoliko veza je polu otvoreno, server je preplavljen
i druge veze su onemogućene
- 56. Slika 10.3.3.2 Prikaz percepcije sa jednim skrivenim nivoom
- 57. Slika 10.3.3.3.1 Proces grafičkog prikazivanja stanja u mreži
- 58. Slika 10.3.3.3.2 Grafički prikaz napada na datu računarsku mrežu
- 59. Slika 10.3.5.1 Model mreže sa IPsec
- 60. Slika 10.3.5.2 Upotreba SHA-1 sa DSA
- 61. Slika 10.3.6.1 Kriptovanje unutar baze podataka
- 62. Slika 10.3.6.2 Kriptovanje na aplikativnom serveru

Spisak tabela:

- 1. Tabela 4.2. IEEE 802.16 Brzine prenosa i vrste modulacije
- 2. Tabela 5.1.4 Informacije koje se dobijaju analizom okvira podataka u WLAN
- 3. Tabela 6.3.1 Kismet dnevničke datoteke
- 4. Tabela 6.1.4 Parametri varijable logtemplate

Prilog 1: izvorni kod programa SHA-1

```

/*
SHA-1

Test Vektori (iz FIPS PUB 180-1)
"abc"
  A9993E36 4706816A BA3E2571 7850C26C 9CD0D89D
"abcdbcdbcdedfdefgefghfghighijhijkijklklmklmnlmnomnopnopq"
  84983E44 1C3BD26E BAAE4AA1 F95129E5 E54670F1
million ponavljanja "a"
  34AA973C D4C4DAA4 F61EEB2B DBAD2731 6534016F
*/

#define LITTLE_ENDIAN
#define SHA1HANDSOFF

#include <stdio.h>
#include <string.h>

typedef struct {
    unsigned long state[5];
    unsigned long count[2];
    unsigned char buffer[64];
} SHA1_CTX;

void SHA1Transform(unsigned long state[5], unsigned char buffer[64]);
void SHA1Init(SHA1_CTX* context);
void SHA1Update(SHA1_CTX* context, unsigned char* data, unsigned int
len);
void SHA1Final(unsigned char digest[20], SHA1_CTX* context);

#define rol(value, bits) (((value) << (bits)) | ((value) >> (32 - (bits))))

#ifndef LITTLE_ENDIAN
#define blk0(i) (block->l[i] = (rol(block->l[i],24)&0xFF00FF00) \
    |(rol(block->l[i],8)&0x00FF00FF))
#else
#define blk0(i) block->l[i]
#endif
#define blk(i) (block->l[i&15] = rol(block->l[(i+13)&15]^block->l[(i+8)&15] \
    ^block->l[(i+2)&15]^block->l[i&15],1))

/* (R0+R1), R2, R3, R4 su razlicite operacije koje se koriste u SHA1 */
#define R0(v,w,x,y,z,i)
z+=((w&(x^y))^y)+blk0(i)+0x5A827999+rol(v,5);w=rol(w,30);
#define R1(v,w,x,y,z,i)
z+=((w&(x^y))^y)+blk(i)+0x5A827999+rol(v,5);w=rol(w,30);
#define R2(v,w,x,y,z,i) z+=(w^x^y)+blk(i)+0x6ED9EBA1+rol(v,5);w=rol(w,30);

```

```
#define R3(v,w,x,y,z,i)
z+=(((w|x)&y)|((w&x))+blk(i)+0x8F1BBCDC+rol(v,5);w=rol(w,30);
#define R4(v,w,x,y,z,i) z+=(w^x^y)+blk(i)+0xCA62C1D6+rol(v,5);w=rol(w,30);

/* Izracunavanje hash za jedan blok 512-bita. Jezgro algoritma. */

void SHA1Transform(unsigned long state[5], unsigned char buffer[64])
{
    unsigned long a, b, c, d, e;
    typedef union {
        unsigned char c[64];
        unsigned long l[16];
    } CHAR64LONG16;
    CHAR64LONG16* block;
#ifdef SHA1HANDSOFF
        static unsigned char workspace[64];
        block = (CHAR64LONG16*)workspace;
        memcpy(block, buffer, 64);
#else
        block = (CHAR64LONG16*)buffer;
#endif
    /* Kopiranje context->state[] u radne varijable */
    a = state[0];
    b = state[1];
    c = state[2];
    d = state[3];
    e = state[4];

    R0(a,b,c,d,e, 0); R0(e,a,b,c,d, 1); R0(d,e,a,b,c, 2); R0(c,d,e,a,b, 3);
    R0(b,c,d,e,a, 4); R0(a,b,c,d,e, 5); R0(e,a,b,c,d, 6); R0(d,e,a,b,c, 7);
    R0(c,d,e,a,b, 8); R0(b,c,d,e,a, 9); R0(a,b,c,d,e,10); R0(e,a,b,c,d,11);
    R0(d,e,a,b,c,12); R0(c,d,e,a,b,13); R0(b,c,d,e,a,14); R0(a,b,c,d,e,15);
    R1(e,a,b,c,d,16); R1(d,e,a,b,c,17); R1(c,d,e,a,b,18); R1(b,c,d,e,a,19);
    R2(a,b,c,d,e,20); R2(e,a,b,c,d,21); R2(d,e,a,b,c,22); R2(c,d,e,a,b,23);
    R2(b,c,d,e,a,24); R2(a,b,c,d,e,25); R2(e,a,b,c,d,26); R2(d,e,a,b,c,27);
    R2(c,d,e,a,b,28); R2(b,c,d,e,a,29); R2(a,b,c,d,e,30); R2(e,a,b,c,d,31);
    R2(d,e,a,b,c,32); R2(c,d,e,a,b,33); R2(b,c,d,e,a,34); R2(a,b,c,d,e,35);
    R2(e,a,b,c,d,36); R2(d,e,a,b,c,37); R2(c,d,e,a,b,38); R2(b,c,d,e,a,39);
    R3(a,b,c,d,e,40); R3(e,a,b,c,d,41); R3(d,e,a,b,c,42); R3(c,d,e,a,b,43);
    R3(b,c,d,e,a,44); R3(a,b,c,d,e,45); R3(e,a,b,c,d,46); R3(d,e,a,b,c,47);
    R3(c,d,e,a,b,48); R3(b,c,d,e,a,49); R3(a,b,c,d,e,50); R3(e,a,b,c,d,51);
    R3(d,e,a,b,c,52); R3(c,d,e,a,b,53); R3(b,c,d,e,a,54); R3(a,b,c,d,e,55);
    R3(e,a,b,c,d,56); R3(d,e,a,b,c,57); R3(c,d,e,a,b,58); R3(b,c,d,e,a,59);
    R4(a,b,c,d,e,60); R4(e,a,b,c,d,61); R4(d,e,a,b,c,62); R4(c,d,e,a,b,63);
    R4(b,c,d,e,a,64); R4(a,b,c,d,e,65); R4(e,a,b,c,d,66); R4(d,e,a,b,c,67);
    R4(c,d,e,a,b,68); R4(b,c,d,e,a,69); R4(a,b,c,d,e,70); R4(e,a,b,c,d,71);
    R4(d,e,a,b,c,72); R4(c,d,e,a,b,73); R4(b,c,d,e,a,74); R4(a,b,c,d,e,75);
    R4(e,a,b,c,d,76); R4(d,e,a,b,c,77); R4(c,d,e,a,b,78); R4(b,c,d,e,a,79);

    /* Dodavanje radnih varijabli nazad u context.state[] */
```

```
state[0] += a;
state[1] += b;
state[2] += c;
state[3] += d;
state[4] += e;
/* Brisanje sadržaja varijabli */
a = b = c = d = e = 0;
}

/* SHA1Init – Inicijalizacija novog sadržaja */

void SHA1Init(SHA1_CTX* context)
{
    /* SHA1 inicijalizacione konstante */
    context->state[0] = 0x67452301;
    context->state[1] = 0xEFCDAB89;
    context->state[2] = 0x98BADCFE;
    context->state[3] = 0x10325476;
    context->state[4] = 0xC3D2E1F0;
    context->count[0] = context->count[1] = 0;
}

void SHA1Update(SHA1_CTX* context, unsigned char* data, unsigned int
len)
{
    unsigned int i, j;

    j = (context->count[0] >> 3) & 63;
    if ((context->count[0] += len << 3) < (len << 3)) context->count[1]++;
    context->count[1] += (len >> 29);
    if ((j + len) > 63) {
        memcpy(&context->buffer[j], data, (i = 64-j));
        SHA1Transform(context->state, context->buffer);
        for (; i + 63 < len; i += 64) {
            SHA1Transform(context->state, &data[i]);
        }
        j = 0;
    }
    else i = 0;
    memcpy(&context->buffer[j], &data[i], len - i);
}

/* Dodaje padding i vraća message digest. */

void SHA1Final(unsigned char digest[20], SHA1_CTX* context)
{
    unsigned long i, j;
    unsigned char finalcount[8];

    for (i = 0; i < 8; i++) {
```

```
        finalcount[i] = (unsigned char)((context->count[(i >= 4 ? 0 : 1)]
        >> ((3-(i & 3)) * 8) ) & 255);
    }
    SHA1Update(context, (unsigned char *)"\200", 1);
    while ((context->count[0] & 504) != 448) {
        SHA1Update(context, (unsigned char *)"\0", 1);
    }
    SHA1Update(context, finalcount, 8);
    for (i = 0; i < 20; i++) {
        digest[i] = (unsigned char)
            ((context->state[i]>>2] >> ((3-(i & 3)) * 8) ) & 255);
    }

    i = j = 0;
    memset(context->buffer, 0, 64);
    memset(context->state, 0, 20);
    memset(context->count, 0, 8);
    memset(finalcount, 0, 8);
#ifdef SHA1HANDSOFF
    SHA1Transform(context->state, context->buffer);
#endif
}

/*****/
int main(int argc, char** argv)
{
    int i, j;
    SHA1_CTX context;
    unsigned char digest[20], buffer[16384];
    FILE* file;
    if (argc > 2) {
        puts("SHA-1 implementacija ");
        puts("SHA-1 hash fajla, ili stdin ako nije odredjen fajl.");
        exit(0);
    }
    if (argc < 2) {
        file = stdin;
    }
    else {
        if (!(file = fopen(argv[1], "rb"))) {
            fputs("Ne mogu da otvorim fajl.", stderr);
            exit(-1);
        }
    }
    SHA1Init(&context);
    while (!feof(file)) {
        i = fread(buffer, 1, 16384, file);
        SHA1Update(&context, buffer, i);
    }
    SHA1Final(digest, &context);
```

```
fclose(file);
for (i = 0; i < 5; i++) {
    for (j = 0; j < 4; j++) {
        printf("%02X", digest[i*4+j]);
    }
    putchar(' ');
}

putchar('\n');
exit(0);
}
```

Prilog 2: izvorni kod programa RIJNDAEL

Standardne definicije:

```
/* 1. Standardni tipovi za AES cryptography izvorni kod */
typedef unsigned char  u1byte; /* 8 bit unsigned character type */
typedef unsigned short u2byte; /* 16 bit unsigned integer type */
typedef unsigned long  u4byte; /* 32 bit unsigned integer type */

typedef signed char    s1byte; /* 8 bit signed character type */
typedef signed short   s2byte; /* 16 bit signed integer type */
typedef signed long    s4byte; /* 32 bit signed integer type */

/* 2. Standardni interfejs za AES kriptografske rutine */
#ifdef __cplusplus
    extern "C"
    {
#endif
    char **cipher_name(void);
    u4byte *set_key(const u4byte in_key[], const u4byte key_len);
    void encrypt(const u4byte in_blk[4], u4byte out_blk[4]);
    void decrypt(const u4byte in_blk[4], u4byte out_blk[4]);

#ifdef __cplusplus
    };
#endif

/* 3. Osnovni makroi za ubrzavanje generickih operacija */

/* Cirkularno rotiranje 32 bit vrednosti */
#ifdef _MSC_VER
# include <stdlib.h>
# pragma intrinsic(_lrotl, _lrotr)
# define rotr(x,n) _lrotl(x,n)
# define rotl(x,n) _lrotr(x,n)
#else
#define rotr(x,n) (((x) >> ((int)(n))) | ((x) << (32 - (int)(n))))
#define rotl(x,n) (((x) << ((int)(n))) | ((x) >> (32 - (int)(n))))
#endif

/* Invertovanje redosleda byte u 32 bit varijabli */
#define bswap(x) (rotl(x, 8) & 0x00ff00ff | rotr(x, 8) & 0xff00ff00)

/* Izdvajanje bajta iz 32 bit vrednosti (little endian notacija) */
#define byte(x,n) ((u1byte)((x) >> (8 * n)))

/* Za invertovani redosled bajtova u input/output 32 bit reči, ako je potrebno */
#ifdef BLOCK_SWAP
#define BYTE_SWAP
```

```
#define WORD_SWAP
#endif
```

```
#ifndef BYTE_SWAP
#define io_swap(x) bswap(x)
#else
#define io_swap(x) (x)
#endif
```

/ Za invertovanje redosleda bajtova u input/output blokovima, po potrebi */*

```
#ifndef WORD_SWAP
#define get_block(x) \
    ((u4byte*)(x))[0] = io_swap(in_blk[3]); \
    ((u4byte*)(x))[1] = io_swap(in_blk[2]); \
    ((u4byte*)(x))[2] = io_swap(in_blk[1]); \
    ((u4byte*)(x))[3] = io_swap(in_blk[0])
#define put_block(x) \
    out_blk[3] = io_swap(((u4byte*)(x))[0]); \
    out_blk[2] = io_swap(((u4byte*)(x))[1]); \
    out_blk[1] = io_swap(((u4byte*)(x))[2]); \
    out_blk[0] = io_swap(((u4byte*)(x))[3])
#define get_key(x,len) \
    ((u4byte*)(x))[4] = ((u4byte*)(x))[5] = \
    ((u4byte*)(x))[6] = ((u4byte*)(x))[7] = 0; \
    switch((((len) + 63) / 64)) { \
    case 2: \
        ((u4byte*)(x))[0] = io_swap(in_key[3]); \
        ((u4byte*)(x))[1] = io_swap(in_key[2]); \
        ((u4byte*)(x))[2] = io_swap(in_key[1]); \
        ((u4byte*)(x))[3] = io_swap(in_key[0]); \
        break; \
    case 3: \
        ((u4byte*)(x))[0] = io_swap(in_key[5]); \
        ((u4byte*)(x))[1] = io_swap(in_key[4]); \
        ((u4byte*)(x))[2] = io_swap(in_key[3]); \
        ((u4byte*)(x))[3] = io_swap(in_key[2]); \
        ((u4byte*)(x))[4] = io_swap(in_key[1]); \
        ((u4byte*)(x))[5] = io_swap(in_key[0]); \
        break; \
    case 4: \
        ((u4byte*)(x))[0] = io_swap(in_key[7]); \
        ((u4byte*)(x))[1] = io_swap(in_key[6]); \
        ((u4byte*)(x))[2] = io_swap(in_key[5]); \
        ((u4byte*)(x))[3] = io_swap(in_key[4]); \
        ((u4byte*)(x))[4] = io_swap(in_key[3]); \
        ((u4byte*)(x))[5] = io_swap(in_key[2]); \
        ((u4byte*)(x))[6] = io_swap(in_key[1]); \
        ((u4byte*)(x))[7] = io_swap(in_key[0]); \
    }
}
```

```
#else

#define get_block(x) \
    ((u4byte*)(x))[0] = io_swap(in_blk[0]); \
    ((u4byte*)(x))[1] = io_swap(in_blk[1]); \
    ((u4byte*)(x))[2] = io_swap(in_blk[2]); \
    ((u4byte*)(x))[3] = io_swap(in_blk[3])
#define put_block(x) \
    out_blk[0] = io_swap(((u4byte*)(x))[0]); \
    out_blk[1] = io_swap(((u4byte*)(x))[1]); \
    out_blk[2] = io_swap(((u4byte*)(x))[2]); \
    out_blk[3] = io_swap(((u4byte*)(x))[3])
#define get_key(x,len) \
    ((u4byte*)(x))[4] = ((u4byte*)(x))[5] = \
    ((u4byte*)(x))[6] = ((u4byte*)(x))[7] = 0; \
    switch((((len) + 63) / 64)) { \
    case 4: \
        ((u4byte*)(x))[6] = io_swap(in_key[6]); \
        ((u4byte*)(x))[7] = io_swap(in_key[7]); \
    case 3: \
        ((u4byte*)(x))[4] = io_swap(in_key[4]); \
        ((u4byte*)(x))[5] = io_swap(in_key[5]); \
    case 2: \
        ((u4byte*)(x))[0] = io_swap(in_key[0]); \
        ((u4byte*)(x))[1] = io_swap(in_key[1]); \
        ((u4byte*)(x))[2] = io_swap(in_key[2]); \
        ((u4byte*)(x))[3] = io_swap(in_key[3]); \
    }
#endif
```

Listing programa rijndael.c

/* Podaci o vremenima potrebnim za izvršenje (rijndael.c)
Algoritma: rijndael (rijndael.c)

128 bit key:

Key Setup:	305/1389 cycles (encrypt/decrypt)
Encrypt:	374 cycles = 68.4 mbits/sec
Decrypt:	352 cycles = 72.7 mbits/sec
Mean:	363 cycles = 70.5 mbits/sec

192 bit key:

Key Setup:	277/1595 cycles (encrypt/decrypt)
Encrypt:	439 cycles = 58.3 mbits/sec
Decrypt:	425 cycles = 60.2 mbits/sec
Mean:	432 cycles = 59.3 mbits/sec

256 bit key:
Key Setup: 374/1960 cycles (encrypt/decrypt)
Encrypt: 502 cycles = 51.0 mbits/sec
Decrypt: 498 cycles = 51.4 mbits/sec
Mean: 500 cycles = 51.2 mbits/sec
*/

```
#include "../std_defs.h"
static char *alg_name[] = { "rijndael", "rijndael.c", "rijndael" };
char **cipher_name()
{
    return alg_name;
}
#define LARGE_TABLES
u1byte pow_tab[256];
u1byte log_tab[256];
u1byte sbx_tab[256];
u1byte isb_tab[256];
u4byte rco_tab[ 10];
u4byte ft_tab[4][256];
u4byte it_tab[4][256];
#ifdef LARGE_TABLES
    u4byte fl_tab[4][256];
    u4byte il_tab[4][256];
#endif
u4byte tab_gen = 0;
u4byte k_len;
u4byte e_key[60];
u4byte d_key[60];
#define ff_mult(a,b) (a && b ? pow_tab[(log_tab[a] + log_tab[b]) % 255] : 0)
#define f_rn(bo, bi, n, k) \
    bo[n] = ft_tab[0][byte(bi[n],0)] ^ \
            ft_tab[1][byte(bi[(n + 1) & 3],1)] ^ \
            ft_tab[2][byte(bi[(n + 2) & 3],2)] ^ \
            ft_tab[3][byte(bi[(n + 3) & 3],3)] ^ *(k + n)

#define i_rn(bo, bi, n, k) \
    bo[n] = it_tab[0][byte(bi[n],0)] ^ \
            it_tab[1][byte(bi[(n + 3) & 3],1)] ^ \
            it_tab[2][byte(bi[(n + 2) & 3],2)] ^ \
            it_tab[3][byte(bi[(n + 1) & 3],3)] ^ *(k + n)

#ifdef LARGE_TABLES

#define ls_box(x) \
    ( fl_tab[0][byte(x, 0)] ^ \
      fl_tab[1][byte(x, 1)] ^ \
      fl_tab[2][byte(x, 2)] ^ \
      fl_tab[3][byte(x, 3)] )
```

```
#define f_rl(bo, bi, n, k) \
    bo[n] = fl_tab[0][byte(bi[n],0)] ^ \
        fl_tab[1][byte(bi[(n + 1) & 3],1)] ^ \
        fl_tab[2][byte(bi[(n + 2) & 3],2)] ^ \
        fl_tab[3][byte(bi[(n + 3) & 3],3)] ^ *(k + n)

#define i_rl(bo, bi, n, k) \
    bo[n] = il_tab[0][byte(bi[n],0)] ^ \
        il_tab[1][byte(bi[(n + 3) & 3],1)] ^ \
        il_tab[2][byte(bi[(n + 2) & 3],2)] ^ \
        il_tab[3][byte(bi[(n + 1) & 3],3)] ^ *(k + n)
#else

#define ls_box(x) \
    ((u4byte)sbx_tab[byte(x, 0)] << 0) ^ \
    ((u4byte)sbx_tab[byte(x, 1)] << 8) ^ \
    ((u4byte)sbx_tab[byte(x, 2)] << 16) ^ \
    ((u4byte)sbx_tab[byte(x, 3)] << 24)

#define f_rl(bo, bi, n, k) \
    bo[n] = (u4byte)sbx_tab[byte(bi[n],0)] ^ \
        rotl(((u4byte)sbx_tab[byte(bi[(n + 1) & 3],1)]), 8) ^ \
        rotl(((u4byte)sbx_tab[byte(bi[(n + 2) & 3],2)]), 16) ^ \
        rotl(((u4byte)sbx_tab[byte(bi[(n + 3) & 3],3)]), 24) ^ *(k + n)

#define i_rl(bo, bi, n, k) \
    bo[n] = (u4byte)isb_tab[byte(bi[n],0)] ^ \
        rotl(((u4byte)isb_tab[byte(bi[(n + 3) & 3],1)]), 8) ^ \
        rotl(((u4byte)isb_tab[byte(bi[(n + 2) & 3],2)]), 16) ^ \
        rotl(((u4byte)isb_tab[byte(bi[(n + 1) & 3],3)]), 24) ^ *(k + n)
#endif

void gen_tabs(void)
{
    u4byte i, t;
    u1byte p, q;

    for(i = 0, p = 1; i < 256; ++i)
    {
        pow_tab[i] = (u1byte)p; log_tab[p] = (u1byte)i;
        p = p ^ (p << 1) ^ (p & 0x80 ? 0x01b : 0);
    }
    log_tab[1] = 0; p = 1;
    for(i = 0; i < 10; ++i)
    {
        rco_tab[i] = p;
        p = (p << 1) ^ (p & 0x80 ? 0x1b : 0);
    }

    for(i = 0; i < 256; ++i)
    {
        p = (i ? pow_tab[255 - log_tab[i]] : 0); q = p;
```

```
    q = (q >> 7) | (q << 1); p ^= q;
    q = (q >> 7) | (q << 1); p ^= q;
    q = (q >> 7) | (q << 1); p ^= q;
    q = (q >> 7) | (q << 1); p ^= q ^ 0x63;
    sbx_tab[i] = (u1byte)p; isb_tab[p] = (u1byte)i;
}

for(i = 0; i < 256; ++i)
{
    p = sbx_tab[i];

#ifdef LARGE_TABLES
    t = p; fl_tab[0][i] = t;
    fl_tab[1][i] = rotl(t, 8);
    fl_tab[2][i] = rotl(t, 16);
    fl_tab[3][i] = rotl(t, 24);
#endif
    t = ((u4byte)ff_mult(2, p)) |
        ((u4byte)p << 8) |
        ((u4byte)p << 16) |
        ((u4byte)ff_mult(3, p) << 24);
    ft_tab[0][i] = t;
    ft_tab[1][i] = rotl(t, 8);
    ft_tab[2][i] = rotl(t, 16);
    ft_tab[3][i] = rotl(t, 24);
    p = isb_tab[i];

#ifdef LARGE_TABLES
    t = p; il_tab[0][i] = t;
    il_tab[1][i] = rotl(t, 8);
    il_tab[2][i] = rotl(t, 16);
    il_tab[3][i] = rotl(t, 24);
#endif
    t = ((u4byte)ff_mult(14, p)) |
        ((u4byte)ff_mult( 9, p) << 8) |
        ((u4byte)ff_mult(13, p) << 16) |
        ((u4byte)ff_mult(11, p) << 24);
    it_tab[0][i] = t;
    it_tab[1][i] = rotl(t, 8);
    it_tab[2][i] = rotl(t, 16);
    it_tab[3][i] = rotl(t, 24);
}
    tab_gen = 1;
};
#define star_x(x) (((x) & 0x7f7f7f7f) << 1) ^ (((x) & 0x80808080) >> 7) * 0x1b
#define imix_col(y,x) \
    u = star_x(x);      \
    v = star_x(u);      \
    w = star_x(v);      \
    t = w ^ (x);        \
```

```
(y) = u ^ v ^ w;    \
(y) ^= rotr(u ^ t, 8) ^ \
      rotr(v ^ t, 16) ^ \
      rotr(t,24)

#define loop4(i)      \
{ t = ls_box(rotr(t, 8)) ^ rco_tab[i];    \
  t ^= e_key[4 * i];    e_key[4 * i + 4] = t;  \
  t ^= e_key[4 * i + 1]; e_key[4 * i + 5] = t;  \
  t ^= e_key[4 * i + 2]; e_key[4 * i + 6] = t;  \
  t ^= e_key[4 * i + 3]; e_key[4 * i + 7] = t;  \
}

#define loop6(i)      \
{ t = ls_box(rotr(t, 8)) ^ rco_tab[i];    \
  t ^= e_key[6 * i];    e_key[6 * i + 6] = t;  \
  t ^= e_key[6 * i + 1]; e_key[6 * i + 7] = t;  \
  t ^= e_key[6 * i + 2]; e_key[6 * i + 8] = t;  \
  t ^= e_key[6 * i + 3]; e_key[6 * i + 9] = t;  \
  t ^= e_key[6 * i + 4]; e_key[6 * i + 10] = t; \
  t ^= e_key[6 * i + 5]; e_key[6 * i + 11] = t; \
}

#define loop8(i)      \
{ t = ls_box(rotr(t, 8)) ^ rco_tab[i];    \
  t ^= e_key[8 * i];    e_key[8 * i + 8] = t;  \
  t ^= e_key[8 * i + 1]; e_key[8 * i + 9] = t;  \
  t ^= e_key[8 * i + 2]; e_key[8 * i + 10] = t; \
  t ^= e_key[8 * i + 3]; e_key[8 * i + 11] = t; \
  t = e_key[8 * i + 4] ^ ls_box(t);          \
  e_key[8 * i + 12] = t;                    \
  t ^= e_key[8 * i + 5]; e_key[8 * i + 13] = t; \
  t ^= e_key[8 * i + 6]; e_key[8 * i + 14] = t; \
  t ^= e_key[8 * i + 7]; e_key[8 * i + 15] = t; \
}

u4byte *set_key(const u4byte in_key[], const u4byte key_len)
{ u4byte i, t, u, v, w;
  if(!tab_gen)
    gen_tabs();
  k_len = (key_len + 31) / 32;
  e_key[0] = in_key[0]; e_key[1] = in_key[1];
  e_key[2] = in_key[2]; e_key[3] = in_key[3];
  switch(k_len)
  {
    case 4: t = e_key[3];
            for(i = 0; i < 10; ++i)
              loop4(i);
            break;
    case 6: e_key[4] = in_key[4]; t = e_key[5] = in_key[5];
            for(i = 0; i < 8; ++i)
              loop6(i);
```

```
        break;
    case 8: e_key[4] = in_key[4]; e_key[5] = in_key[5];
           e_key[6] = in_key[6]; t = e_key[7] = in_key[7];
           for(i = 0; i < 7; ++i)
               loop8(i);
           break;
    }
    d_key[0] = e_key[0]; d_key[1] = e_key[1];
    d_key[2] = e_key[2]; d_key[3] = e_key[3];
    for(i = 4; i < 4 * k_len + 24; ++i)
    {
        imix_col(d_key[i], e_key[i]);
    }
    return e_key;
};

/* kriptovanje jednog bloka teksta */
#define f_nround(bo, bi, k) \
    f_rn(bo, bi, 0, k); \
    f_rn(bo, bi, 1, k); \
    f_rn(bo, bi, 2, k); \
    f_rn(bo, bi, 3, k); \
    k += 4
#define f_lround(bo, bi, k) \
    f_rl(bo, bi, 0, k); \
    f_rl(bo, bi, 1, k); \
    f_rl(bo, bi, 2, k); \
    f_rl(bo, bi, 3, k)
void encrypt(const u4byte in_blk[4], u4byte out_blk[4])
{
    u4byte b0[4], b1[4], *kp;
    b0[0] = in_blk[0] ^ e_key[0]; b0[1] = in_blk[1] ^ e_key[1];
    b0[2] = in_blk[2] ^ e_key[2]; b0[3] = in_blk[3] ^ e_key[3];
    kp = e_key + 4;
    if(k_len > 6)
    {
        f_nround(b1, b0, kp); f_nround(b0, b1, kp);
    }
    if(k_len > 4)
    {
        f_nround(b1, b0, kp); f_nround(b0, b1, kp);
    }
    f_nround(b1, b0, kp); f_nround(b0, b1, kp);
    f_nround(b1, b0, kp); f_nround(b0, b1, kp);
    f_nround(b1, b0, kp); f_nround(b0, b1, kp);
    f_nround(b1, b0, kp); f_nround(b0, b1, kp);
    f_nround(b1, b0, kp); f_lround(b0, b1, kp);
    out_blk[0] = b0[0]; out_blk[1] = b0[1];
    out_blk[2] = b0[2]; out_blk[3] = b0[3];
};
```

```
/* dekriptovanje jednog bloka teksta */
#define i_nround(bo, bi, k) \
    i_rn(bo, bi, 0, k); \
    i_rn(bo, bi, 1, k); \
    i_rn(bo, bi, 2, k); \
    i_rn(bo, bi, 3, k); \
    k -= 4

#define i_lround(bo, bi, k) \
    i_rl(bo, bi, 0, k); \
    i_rl(bo, bi, 1, k); \
    i_rl(bo, bi, 2, k); \
    i_rl(bo, bi, 3, k)
void decrypt(const u4byte in_blk[4], u4byte out_blk[4])
{ u4byte b0[4], b1[4], *kp;
  b0[0] = in_blk[0] ^ e_key[4 * k_len + 24]; b0[1] = in_blk[1] ^ e_key[4 * k_len
+ 25];
  b0[2] = in_blk[2] ^ e_key[4 * k_len + 26]; b0[3] = in_blk[3] ^ e_key[4 * k_len
+ 27];
  kp = d_key + 4 * (k_len + 5);

  if(k_len > 6)
  {
    i_nround(b1, b0, kp); i_nround(b0, b1, kp);
  }

  if(k_len > 4)
  {
    i_nround(b1, b0, kp); i_nround(b0, b1, kp);
  }

  i_nround(b1, b0, kp); i_nround(b0, b1, kp);
  i_nround(b1, b0, kp); i_nround(b0, b1, kp);
  i_nround(b1, b0, kp); i_nround(b0, b1, kp);
  i_nround(b1, b0, kp); i_nround(b0, b1, kp);
  i_nround(b1, b0, kp); i_lround(b0, b1, kp);

  out_blk[0] = b0[0]; out_blk[1] = b0[1];
  out_blk[2] = b0[2]; out_blk[3] = b0[3];
};
```

Prilog 3: Izvorni kod za realizaciju RC4 algoritma

```
#include <iostream>
#include <fstream>
#include <iomanip>
using namespace std;
int main()
{
    fstream ulaz;
    ulaz.open("rc4.in",ios::in);
    if (!ulaz.is_open()) {
        cout << "GRESKA: Ne postoji datoteka rc4.in!" << endl;
        return 0;
    }
    char kljuc[256+1],znak;
    int j=0,i=0,velicinaTeksta=0;
    unsigned char S[256],temp;
    ulaz.getline(kljuc,256);
    ulaz >> velicinaTeksta;
    if (velicinaTeksta<1) {
        cout << "GRESKA: Pogresna velicina teksta." << endl;
        ulaz.close();
        return 0;
    }
    //KSA
    for (i=0;i<256;i++) S[i]=i;
    for (i=0;i<256;i++)
    {
        j=(j+S[i]+kljuc[i%strlen(kljuc)])%256;
        temp=S[i]; S[i]=S[j]; S[j]=temp;
    }

    //PRGA
    cout << "Kriptovan tekst:" << endl;
    for (int n=0,i=0,j=0;n<velicinaTeksta;n++)
    {
        i=(i+1)%256;
        j=(j+S[i])%256;
        temp=S[i]; S[i]=S[j]; S[j]=temp;
        ulaz >> znak;
        cout << setw(2) << setfill('0') << hex << (int)(znak^(S[i]+S[j]))%256) << " ";
    }
    cout << endl;
    ulaz.close();
    return 0;
}
```

Ulazna datoteka za program: rc4.in

kljuc

12

tajni podatak

Izlaz programa za priloženu ulaznu datoteku:

Kriptovan tekst: 10 54 15 03 16 94 da bc 53 67 fd ac