

UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

STUDIJSKI PROGRAM
SAVREMENE INFORMACIONE TEHNOLOGIJE

ANALIZA ZAŠTITE INFORMACIONIH TOKOVA
U SAVREMENIM BEŽIČNIM MREŽAMA

- M A S T E R R A D -

Mentor:

prof. dr Milan Milosavljević

Kandidat:

Vladan Jonić

2012/410610

Beograd, 2015.

SADRŽAJ

1.	UVOD.....	5
2.	METODOLOGIJA	6
2.1	Predmet rada.....	6
2.2	Hipoteza	6
2.3	Ciljevi rada	6
2.4	Korišćene naučne metode.....	6
3.	CLOUD COMPUTING.....	7
4.	BEŽIČNI GRID	10
5.	WIRELESS CLOUD	13
6.	RANJIVOSTI I PRETNJE U WIRELESS CLOUD OKRUŽENJU	15
7.	ZAŠTITA BEŽIČNIH OBLAKA	21
8.	AUTENTIFIKACIJA.....	23
9.	AUTORIZACIJA	26
9.1	Funkcija uspostavljanja	26
9.2	Operativne funkcije.....	27
9.3	Funkcije upravljanja	29
10.	KONTROLA PRISTUPA	31
11.	PREPORUKE ZA BEŽIČNE CLOUD MREŽE	33
11.1	Politika upravljanja identitetima i pristupom	33
11.2	Enkripcija, upravljanje ključevima i uključivanje kriptografije	34
11.3	Poreklo	35
11.4	Problemi privatnosti u toku razvoja/izbora provajdera bežičnih cloud servisa	35
12.	BEŽIČNE MESH MREŽE	37
12.1	Mesh ruteri.....	37
12.2	Mesh klijenti	37
12.3	Bežična mesh mrežna arhitektura.....	38
12.3.1	Infrastrukturna/backbone WMN	38
12.3.2	Klijentska WMN.....	39
12.3.3	Hibridna WMN	40
13.	KARAKTERISTIKE WMN.....	41
13.1	Razlike između WMN i AdHoc mreža	41
13.1.1	Bežična infrastruktura/backbone.....	41

13.1.2	Integracija.....	42
13.1.3	Specifičnosti rutiranja i konfiguracije.....	42
13.1.4	Višestruki radio standardi	42
13.1.5	Mobilnost	42
13.1.6	Oblasti primene.....	42
13.2	Tehnologija WMN	43
13.2.1	Mesh rutiranje.....	43
13.2.2	Mrežna topologija	44
14.	MREŽNO UPRAVLJANJE U WMN	45
14.1	Upravljanje greškama.....	45
14.2	Upravljanje konfiguracijom	45
14.3	Upravljanje naložima.....	46
14.4	Upravljanje performansama	46
14.5	Upravljanje bezbednošću.....	46
15.	ANALIZA RADIO STANDARDA KOJI SE KORISTE U MESH MREŽAMA.....	47
15.1	802.11a.....	47
15.1.1	802.11a prednosti	47
15.1.2	Bezbednost i upotreba 802.11a	47
15.2	802.11b.....	47
15.2.1	802.11b prednosti	48
15.2.2	Bezbednost i upotreba 802.11b	48
15.3	802.11g.....	48
15.3.1	802.11b prednosti	48
15.3.2	Bezbednost i upotreba 802.11g	49
15.4	802.11n.....	49
15.4.1	802.11n prednosti	49
15.4.2	Bezbednost i upotreba 802.11n	49
16.	ANALIZA STANDARDA 802.11s.....	50
16.1	802.11s Topologija	50
16.1.1	Mesh portal (MPP)	50
16.1.2	Mesh Point (MP).....	51
16.1.3	Mesh AP (MAP)	51
16.1.4	Station (STA).....	51
16.2	Bezbednost u 802.11s	52

17.	BEZBEDNOST U BEŽIČNIM MESH MREŽAMA	53
17.1	Osnovna prevencija	53
17.1.1	Poverljivost podataka	53
17.1.2	Poverljivost saobraćaja	53
17.2	Mesh bezbednost	53
17.2.1	Poverljivost	54
17.2.2	Dostupnost	54
17.2.3	Autentikacija	54
17.2.4	Autorizacija	54
17.2.5	Merenje	54
17.2.6	Integritet	55
17.2.7	Kontrola pristupa	55
17.3	Bezbednosni izazovi	55
17.4	Pregled potencijalnih napada	55
17.4.1	Flooding napad	56
17.4.2	Ometanje	56
17.4.3	Napadi usmereni ka onemogućavanju uštede energije i ispuštanju paketa (Sleep Deprivation and Packet Dropping Attacks)	56
17.4.4	Napadi na rutiranje	57
17.5	Zaštita od pretnji i napada	57
17.5.1	Centralizovani modeli	57
17.5.2	Decentralizovani modeli	58
18.	PRIMENA BEŽIČNIH MESH MREŽA	60
18.1	Širokopojasna kućna mreža	60
18.2	Umrežavanje zajednice	61
18.3	Poslovno umrežavanje	62
18.4	Gradske mreže (Metropolitan Area Networks – MAN)	63
18.5	Automatizacija zgrada	64
18.6	Medicinski sistemi	64
18.7	Mreže za obezbeđivanje komunikacija u zonama pogođenim elementarnim nepogodama	65
19.	ZAKLJUČAK	67
20.	LITERATURA	69

1. UVOD

Računarske mreže i telekomunikaciona okosnica (backbone) u većini industrija i domova širom sveta učinili su distribuciju računarske snage mogućom. Finansijska industrija preusmerava ogromne sume novca u transakcijama svaki dan koristeći postojeće mreže i tehnologije za distribuiranu obradu podataka. Vlade širom sveta čuvaju razne informacije na mrežama i u distribuiranim bazama podataka. Svaki od ovih primera predstavlja način na koji se telekomunikacione mreže i tehnologija koriste za efikasno obavljanje svakodnevnih aktivnosti. Međutim, postoje i mane. Informacije koje se čuvaju u globalnim mrežama i prosleđuju preko njih, izložene su pokušajima neovlašćenog presretanja. IT sistemi treba da budu dizajnirani tako da smanje ranjivost mreže i štite informacije sadržane u njima.

Cloud computing predstavlja ostvarenje sna o korišćenju računarskih resursa na bazi usluga. Sa svojim nemerljivim potencijalom da transformiše veliki deo IT industrije, učiniće softver još atraktivnijim omogućivši njegovo korišćenje kroz servis koji koristi resurse distribuiranog data centra. Cloud computing se može posmatrati kao nova paradigma u računarstvu jer otklanja potrebu organizacije da izgradi, upravlja i obezbedi sopstvene data centre i kompleksnu IT infrastrukturu. Cloud computing infrastruktura omogućava kompanijama da smanje sopstvene troškove iznajmljujući svoje IT resurse na privremeno korišćenje drugim kompanijama.

Dinamičan savremeni život i potreba za neprekidnom protokom informacija u svim uslovima povlače za sobom i razvoj dinamičnih ad hoc mreža. Mesh mreže se mogu predstaviti kao jedan tip mobilne ad hoc mreže (Mobile Adhoc Network – MANET). Bežične Mesh mreže (Wireless Mesh Network – WMN) imaju mnogo prednosti u odnosu na druge tipove bežičnih mreža. Obezbeđuju jednostavna podešavanja, odličnu propusnu moć i veliku otpornost na mrežne ispade. Primena WMN je veoma laka. One se dinamički samokonfigurišu i samoorganizuju sa postojećim mrežnim čvorovima automatski organizujući i održavajući vezu između njih, omogućavajući pouzdanu pokrivenost mrežnih servisa.

Ovaj rad govori o implikacijama razvoja bežičnih cloud i mesh mreža i potencijalnim bezbednosnim rizicima. Identifikovaćemo bežičnu cloud i mesh arhitekturu, moguće pretnje i ranjivosti navedenih rešenja i sagledati njihovu bezbednosnu arhitekturu.

2. METODOLOGIJA

2.1 Predmet rada

Predmet ovog rada su principi na kojima se zasniva zaštita savremenih bežičnih mreža. Imajući u vidu da se radi o relativno novim mrežnim arhitekturama, predložena su i neka rešenja koja su još uvek u fazi implementiranja a koja bi doprinela uspostavljanju potrebnog nivoa bezbednosti.

2.2 Hipoteza

Opšta hipoteza: Razvoj savremenih bežičnih mreža i njihovo masovno korišćenje uslovljava potrebu za pronalaženjem načina za njihovo bezbedno korišćenje.

Posebna/radna hipoteza: Mnogobrojne pretnje i rizici koji utiču na bezbednu upotrebu savremenih bežičnih mreža uslovljavaju neprekidnu potrebu za razvojem novih metoda i politika zaštite koje omogućavaju sigurnu i pouzdanu komunikaciju u okviru njih i bezbedno i permanentno izvršavanje svih servisa koje nude.

2.3 Ciljevi rada

Naučni cilj ovog pristupnog rada je istraživanje i sistematizacija znanja o mogućim pretnjama po savremene bežične mreže i predstavljanje najprihvatljivijih rešenja za zaštitu istih.

Društveni ciljevi su:

- da se projektanti budućih savremenih bežičnih mreža upoznaju sa rizicima i pretnjama koje mogu da utiču na pouzdanost i bezbednost njihovih rešenja i da u procesu planiranja implementiraju trenutno najbolja rešenja za zaštitu,
- da se korisnici upoznaju sa rizicima i pretnjama po bezbednost njihovih podataka koje šalju kroz bežične mreže i da steknu osnovna saznanja o bezbednosnim zahtevima koje pružaoci usluga moraju prema njima ispoštovati.

2.4 Korišćene naučne metode

Prilikom istraživanja korišćene su sledeće metode:

- opšte analitičke metode pri prikupljanju i proučavanju dostupne literature
- hipotetičko-deduktivne i
- uporedne metode

Metodologija istraživanja svela se na korišćenje dostupne literature iz oblasti bežičnih komunikacija. Imajući u vidu da se radi o relativno novijim mrežnim arhitekturama a i o bezbednosti računarskih komunikacija, dosta truda je uloženo u prikupljanje validnih podataka.

3. CLOUD COMPUTING

Termin „Cloud computing“ je relativno nov termin i nastao je na temelju višedecenijskog istraživanja u oblastima virtuelizacije, distribuirane obrade, a u skorije vreme i umrežavanja, web i softverskih servisa. Cloud computing predstavlja model koji omogućava jednostavan mrežni pristup deljenim računarskim resursima .

Kao što je prikazano na slici 1, cloud computing je nastao kao nova računarska paradigma koja objedinjuje ogroman broj računara u centralizovane računске centre sa ciljem isporučivanja web aplikacija, aplikativnih platformi ili usluga preko utility modela [15, 34]. Nacionalni institut za standarde i tehnologiju (National Institute of Standards and Technology - NIST) je identifikovao četiri modela za cloud servise:

- **privatni cloud** - cloud infrastruktura se koristi isključivo za organizaciju. Njime može upravljati ili organizacija ili treće lice, a fizički se može nalaziti na lokaciji organizacije ili van nje,
- **community cloud** - cloud infrastrukturu deli nekoliko organizacija i ona podržava određenu zajednicu koja deli ista interesovanja. Njime mogu upravljati organizacije ili treće lice, a fizički se može nalaziti na lokaciji organizacija ili van nje,
- **javni cloud** - cloud infrastruktura je dostupna javnosti ili velikim industrijskim grupacijama i u vlasništvu je organizacije koja prodaje cloud usluge i
- **hybrid cloud** - cloud infrastruktura je sastavljena od dva ili više oblaka (privatni, community, ili public) koji ostaju sami za sebe jedinstveni subjekti, ali su povezani standardizovanom ili sopstvenom tehnologijom koja omogućava međusobnu prenosivost podataka i aplikacija.

Pod okriljem cloud computinga postoji raznovrsna ponuda usluga i implementiranih modela. Ovi modeli, kao što je prikazano u tabeli 1, mogu se grupisati u sledeće tri kategorije:

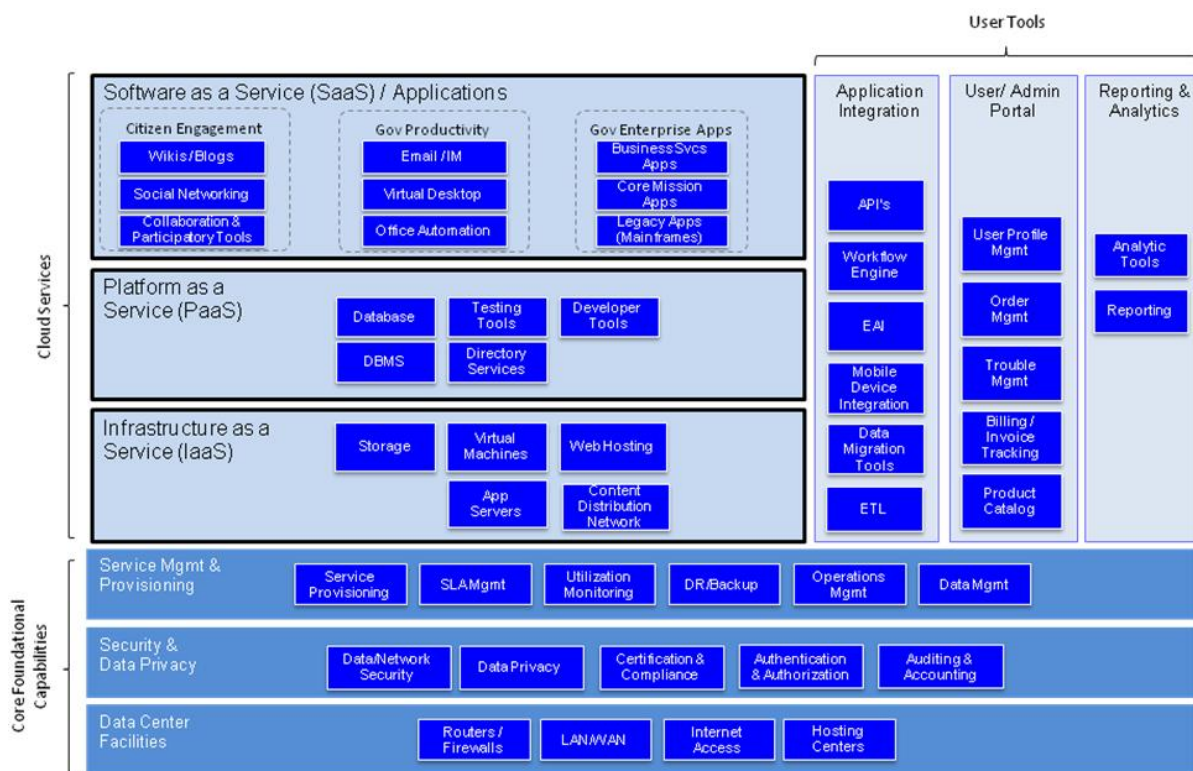
- Infrastruktura kao servis (Infrastructure as a Service - IaaS), koja pruža mogućnost da se zakupe usluge kao što su skladištenje i računarski resursi (npr. Amazon Simple Storage Service¹ i Elastic Compute Cloud²) [6],
- platforma kao servis (Platform as a Service - PaaS), koja pruža mogućnost da se zakupi okruženje za razvoj aplikacija (npr. Microsoft Azure Services Platform³) i
- softver kao servis (Software as a Service - SaaS), koji nudi mrežno dostupne aplikacije (npr. Google docs⁴). Ovi modeli obezbeđuju različite resurse korisnicima u rasponu od opštih infrastrukturnih usluga koje obezbeđuje IAAS do ciljano prilagodljivih aplikacija koje obezbeđuju provajderi SaaS usluga. [40].

¹ Amazon Simple Storage Service: <http://aws.amazon.com/s3/>

² Amazon Elastic Compute Cloud: <http://aws.amazon.com/ec2/>

³ Microsoft Windows Azure: www.microsoft.com/windowsazure

⁴ Google Docs: <https://docs.google.com>



Slika 1 – Cloud computing radno okruženje

Modeli	Opis
Infrastruktura kao servis (IaaS)	Uključuje osnovne elemente, kao što su skladištenje podataka, instance operativnih sistema, mrežu i upravljanje identitetima, na koje razvojne platforme i aplikacije mogu da budu oslonjene; mogućnosti koje su obezbeđene korisnicima su da iznajme obradu, skladištenje, mrežu i druge osnovne računarske resurse i gde su sami u mogućnosti da primenjuju i pokreću proizvoljan softver [6, 40].
Platforma kao servis (PaaS)	Cloud sistemi mogu ponuditi dodatni nivo apstrakcije: umesto da obezbeđuju virtuelizovanu infrastrukturu, oni mogu da obezbede softversku platformu na kojoj će sistem da radi. Zauzimanje hardverskih resursa koje zahtevaju usluge za svoje izvršavanje vrši se na transparentan način [6, 40].
Softver kao servis (SaaS)	Izgrađen na Paas modelu da ponudi kompletne aplikacije delimično prilagodljive od strane korisnika i zasnovan na sigurnosnom modelu razvijenom od strane provajdera; usluge od potencijalnog interesa za širok spektar korisnika hostovane su na Cloud sistemima, što je drugi način lokalnog izvršavanja aplikacija. Primer za to su online alternative tipičnih kancelarijskih aplikacija, kao što su obrada teksta, Google Docs, itd [6, 40]

Tabela 1 – Modeli cloud servisa

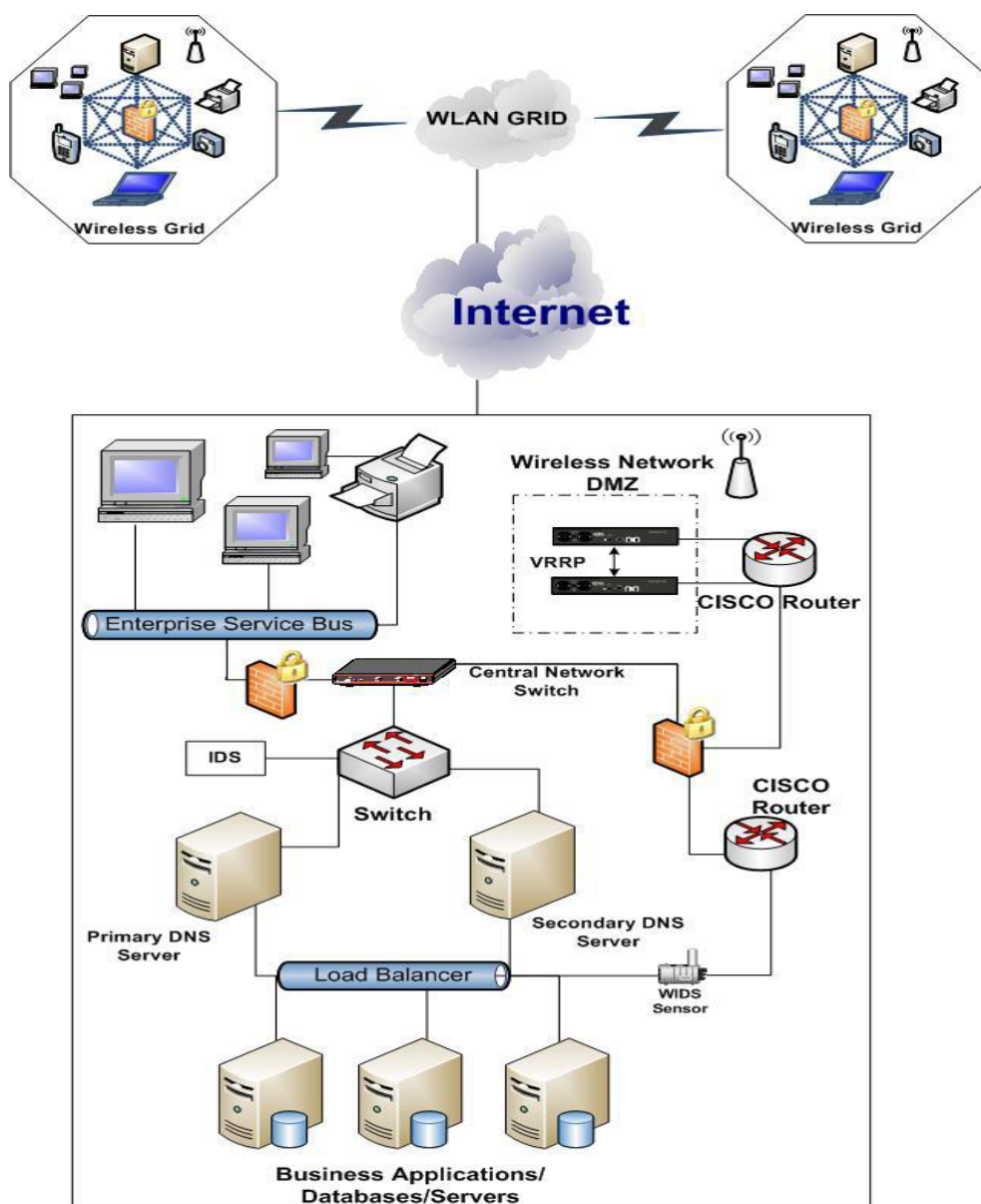
Umesto kupovine i skupog održavanja servera, IAAS cloud computing model omogućava da se dinamički i daljinski upravlja obradom, memorijom, skladištenjem podataka, mrežom i protokom izdvojenim iz ogromnih resursa, pružajući mogućnost da se na zahtev rezervišu i zauzmu računarski kapaciteti [18,20]. Ukoliko postoji potreba da se udovolji iznenadnom zahtevu, neophodni resursi mogu biti dodeljeni korisniku na korišćenje i putem web browsera. Te iste usluge pružaju se mnogobrojnim eksternim korisnicima (višestruki zakup), uz korišćenje zajedničkih resursa velikih data centara u cilju redukovanja cene koštanja samog servisa prema pojedincu. Višestruki zakup omogućava deljenje resursa (i troškova) među velikom grupom korisnika, obezbeđujući pouzdanost putem više redundantnih lokacija, što ga čini pogodnim u smislu kontinuiteta pružanja usluga. Cloud se reklamira kao jeftina alternativa superkompjuterima i specijalizovanim klasterima. Cloud platforma je mnogo pouzdanija i skalabilnija od grid platformi [30].

Tehnologije koje cloud computing koristi uključuju grid computing, utility computing i tehnologije virtuelizacije. Grid computing je oblik distribuiranog, paralelnog procesiranja pri čemu su procesi podeljeni tako da se iskorišćava dostupna procesorska snaga više međusobno povezanih centralnih procesorskih jedinica (CPU) [14]. Utility computing omogućava korisnicima da iznajme računarske kapacitete (CPU, skladišni prostor, mrežni propusni opseg) i da na kraju plate račun isključivo na osnovu korišćenih resursa. Virtualizacione tehnologije predstavljaju virtuelni serveri i virtuelne privatne mreže i one pružaju mogućnost brze rekonfiguracije dostupnih resursa na zahtev korisnika uz obezbeđivanje neophodne i zagarantovane sigurnosti, sa ciljem zaštite od pretnji iz clouda, kao i podataka koji se prenose putem clouda.

Među značajnijim izazovima koji otežavaju šire usvajanje cloud computinga su svakako sigurnost i privatnost podataka u oblaku. Bezbednost podataka je verovatno najznačajnija prepreka bržem usvajanju cloud computinga [5]. Kako cloud computing nudi mogućnost premeštanja računarskih resursa u okruženje cloud computinga uz povećanje fleksibilnosti i istovremeno smanjenje troškova, neophodno je primeniti mehanizme zaštite poverljivosti i integriteta podataka sa ciljem sprečavanja njihovog izlaganja neovlašćenim korisnicima. Premeštanje podataka u cloud computing okruženje može da smanji troškove skladištenja i upravljanja informacijama, ali istovremeno predstavlja otvorene pretnje koje direktno utiču bezbednost podataka [37]. Primena i arhitektura izabranih servisa (npr. privatni, društveni, javni ili hibridni), mora da zadovolji sve zahteve vezane za sigurnost i privatnost organizacije koja će ih koristiti [7, 20, 26].

4. BEŽIČNI GRID

Bežični grid se može definisati kao ad-hoc dinamička razmena fizičkih i virtuelnih resursa između heterogenih uređaja, sadržaja i korisnika [39]. Kao budućnost distribuiranog computinga, bežični grid (slika 2) će omogućiti razmenu resursa između dinamičkih grupa ili društvenih mreža sa individualnim profilima kojima je dodeljen poseban status u odnosu na slične objekte i resurse koje koriste, bez posebnog servera potrebnog za upravljanje mrežom [25]. Grid computing podrazumeva agregaciju mrežno povezanih računara u cilju formiranja distribuiranog sistema za koordinaciju rešavanja problema i deljenja resursa [8, 9, 32]. Bežične grid infrastrukture mogu se sagledati kroz tri dimenzije: fizički sloj, mrežnu infrastrukturu i srednji sloj (*middleware*).



Slika 2: Wireless grid

U novijoj literaturi bežični grid se može identifikovati kao tri različite arhitekture:

- bežični senzorski grid,
- mobilni bežični
- fiksni bežični.

McKnight [24] daje klasifikaciju bežične mreže koje se razlikuje od tipične žičane mreže, i to:

- aplikacije koje sakupljaju informacije iz niza ulaznih / izlaznih interfejsa nomadskih (prenosnih) uređaja,
- aplikacije koje usklađuju lokacije i okolnosti u kojima se uređaji nalaze i
- aplikacije koje se zasnivaju na Mesh mrežnim mogućnostima grupe nomadskih (prenosnih) uređaja.

Bežični grid proširuje resurse grid mreže na bežične uređaje različitih veličina i kapaciteta, kao što su senzori, mobilni telefon, laptop računari, razni specijalni instrumenati i savremeni uređaji. Ovi uređaji mogu biti statički, mobilni, ili nomadski (prenosni), povezani na grid mrežu preko obližnjih desktop računara. Resursi mogu da se pretražuju, nalaze, pregledaju, i da se sa njima manipuliše putem bilo kog drugog servisa ili udaljenog uređaja povezanog na grid, a istovremeno, uređaji uvezani u bežični grid mogu vršiti funkciju i servera i klijenata. Agarwal [1] identifikuje bežične grid mreže kao proširenje žične grid mreže, koja olakšava razmenu informacija i interakciju između heterogenih bežičnih uređaja. Bežični grid može da podigne primenu računarske tehnike na viši nivo obezbeđivanjem bežičnog proširenja žičnog grida. Arhitektura ove vrste mreža je od velikog značaja, jer one mogu biti raspoređene tako da obezbede autonomne čvorove koji komuniciraju jedni sa drugima na decentralizovan način, tako da se svaki čvor mreže povezuje sa drugim bežičnom vezom, a deluje i kao host i kao ruter u slanju i primanju podataka.

Jedan od glavnih problema vezanih za bežične grid mreže je zaštita informacija. Integrisanje bežičnog grid rešenja sa postojećim informacionim sistemom (npr. cloud computing) ili tradicionalnom žičnom mrežom postavlja nove izazove u smislu rutiranja, agregiranja i vršenja upita nad podacima sa više bežično povezanih heterogenih uređaja. Kao i kod svih bežičnih komunikacija, komunikacioni uređaji u wireless grid komuniciraju i prenose informacije preko standardnih radio-frekvencija koje se mogu lako nadzirati [23]. Čak i ako bežična mreža koristi firewall i proxy sisteme koji filtriraju sve potencijalno zlonamerne mrežne pakete ili web sadržaje, podaci i dalje mogu da otiču sa mreže. Bežični grid je generalno ranjiviji na maliciozne i slučajne pretnje od svog žičnog pandama. Definisana bezbednosna arhitektura mora da bude obavezna komponenta bežične mreže da bi ta ranjivost bila rešena.

Moraju se takođe uzeti u obzir i bezbednosna arhitektura i analiza bezbednosti komunikacionih protokola mobilnih bežičnih mreža [27, 35]. Bezbednost predstavlja veliki problem kod mobilnih bežičnih uređaja, jer su osetljivi na širok spektar napada. Zbog urođene prirode bežične veze, zaštita podataka je veoma teška. Uticaj kvaliteta

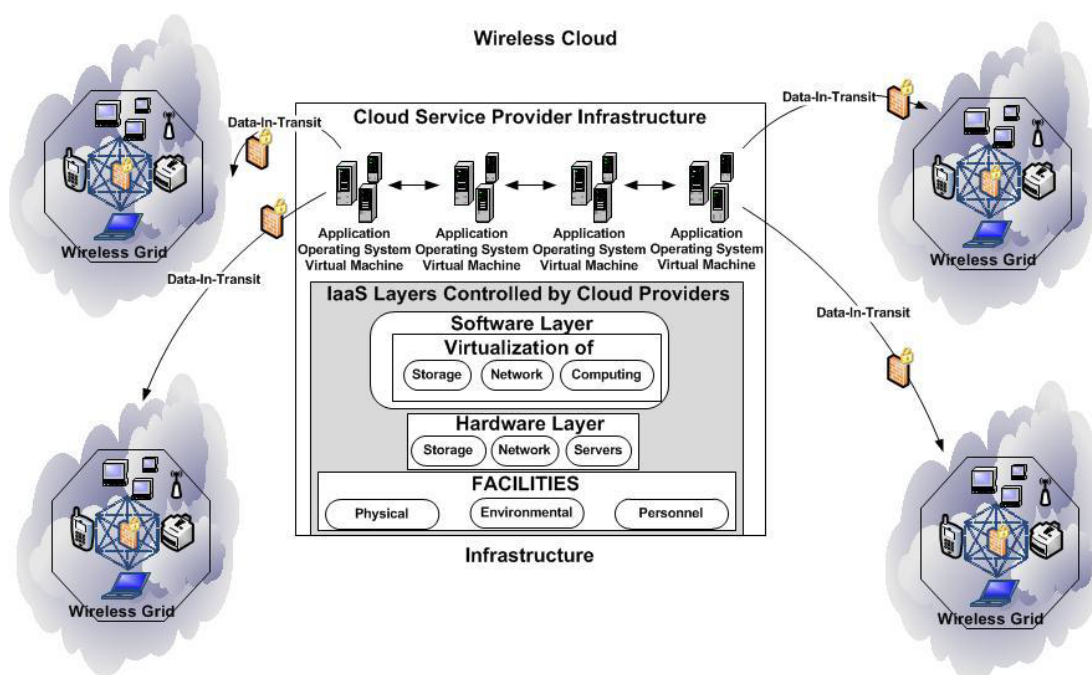
linka, potencijalna nepouzdanost uređaja na drugoj strani komunikacionog kanala, ograničenja u napajanju mobilnih uređaja i sprovođenje bezbednosne politike, predstavljaju najveće izazove u bežičnom mrežnom okruženju.

Većina postojećih zaštita koje se koriste u bežičnim sistemima obično sadrže neku formu bezbednosnih mehanizama koji pružaju zaštitu na bazi pristupa na za to isključivo definisanim pristupnim tačkama. Kako bežična mrežna tehnologija stalno napreduje, grid će postajati sve heterogeniji, što će zahtevati prenos podataka preko mnogobrojnih pouzdanih bežičnih mreža. Zbog toga će korisnici morati da traže snažnije mehanizme end-to-end zaštite. U cilju što bolje integracije bežičnih grid mreža i usluga cloud computinga, grid usluge će morati biti dopunjene dodavanjem novih sigurnosnih servisa, a to bi moglo dovesti do razvoja nove bežične cloud arhitekture.

5. WIRELESS CLOUD

U okviru ove bežične mrežne arhitekture, postojeći mrežno orijentisani modeli zaštite još uvek su daleko od adekvatnih. Ovi novi sistemi će raspoložu raznim mehanizmima razmene informacija koje su preko ugrađenih servisa izložene spoljnim bežičnim korisnicima putem standardnih web servisa. Bežični klijenti, koji i sami mogu biti aplikacije, dinamički otkrivaju njihove servise i u realnom vremenu koriste njihov kod i podatke. Njihovi servisi su lokacijski nezavisni i nije nužno da budu vezani za fizičku lokaciju, koja se vremenom može promeniti iz različitih razloga. Kako bežični mrežni klijenti i pružaoci usluga mogu pripadati različitim fizičkim mrežama ili čak različitim pružaocima usluga, te mreže i / ili organizacije mogu imati potpuno različite bezbednosne politike.

Zbog toga će, u bežičnim cloud okruženjima, organizacije morati da pomere težište zaštite sa perimetarski zasnovanog modela zaštite na zaštitu na nivou servisa. Akcenat bi trebao da bude na mrežnom identitetu, poverenju, kao i autorizaciji i korisnika i aplikacija, a ne na vlasništvu i upravljanju. Model bežičnog cloud computing okruženja prikazan je na slici 3. Ono obezbeđuje direktan pristup internetu, mrežnim uređajima i računskim mogućnostima (computing capabilities).



Slika 3 – Bežični cloud

Kombinovanje cloud computinga i bežičnog grida stvoriće novi oblik distribuiranog računarstva. Bežično spojeni računari koji zajedno rade na velikim projektima i objedinjuju ogromne računarske resurse, obezbediće buduću arhitekturu sposobnu da radi po principima žičnog grid modela. Uređaji bežičnih oblaka i lokacijska nezavisnost

omogućavaju bežičnom gridu pristup cloud sistemima, bez obzira na lokaciju uređaja ili tip uređaja koji se koristi. Performanse ovakvog sistema mogu biti narušene usled nedovoljnog protoka ili prevelikog opterećenja mreže.

Ovakav konceptualni model takođe naglašava značaj projektovanja oblaka kako bi se osiguralo da budu ispunjeni svi zahtevi savremenog poslovanja. Tipičan softver i sistemi koji nisu dizajnirani da iskoriste skalabilnosti i paralelizam oblaka verovatno neće imati potpunu korist od svega što nudi cloud computing okruženje. Bezbednost u bežičnom oblaku može se poboljšati dodavanjem novih sigurnosnih modela, ali uvek postoji veliki rizik od mogućeg gubitka kontrole nad osetljivim podacima. Sprovođenje bezbednosne politike mora da se odvija neprekidno kako bi mreža uvek imala najažurniju zaštitu od pretnji.

Kako se oblak i bežične tehnologije i dalje razvijaju, arhitektura bežičnog oblaka može napredovati od distribuirane, decentralizovane arhitekture sa dosta podataka u "tankim" pristupnim tačkama (AP) do centralizovane arhitekture sa "debelim" AP sa podacima koji se nalaze u bežičnim svičevima. Kada se razmatraju rizici povezani sa bežičnom cloud arhitekturom, najosnovniji element koji treba uzeti u obzir je kako okruženje bežičnog oblaka utiče na model poverenja (trust model). U tradicionalnom računarskom modelu aplikacija se nalazi na klijentskim mašinama, serverima ili mainframe računarima koji su u vlasništvu i pod kontrolom preduzeća. U takvom okruženju moguće je nametnuti mnoštvo bezbednosnih mehanizama sa ciljem ublažavanja rizika koji postoje u IT svetu. Ti mehanizmi uključuju zaštitne zidove (firewall), enkripciju podataka, antivirus rešenja, restriktivne dozvole za pristup, virtuelno ili fizičko razdvajanje mreža i još mnogo toga. Kada se te iste aplikacije presele u cloud arhitekturu, gde je osnovni poslovni model pružanje usluga širokom spektru klijenata, sigurnost tih aplikacija i njihovih podataka zavise od veštine, spremnosti i sposobnosti pružaoca usluge da zaštiti podatke i pruži pouzdan servis. Zbog činjenice da se model poverenja pomera sa korisnika na pružaoca usluga, bežični oblak predstavlja značajan izazov iz perspektive sigurnosti informacija. U takvom okruženju, gde bezbednost mora biti zajednička odgovornost, konačna instalacija i spoj elemenata mreže, rad sistema i alata moraće da obezbede operativno rešenje.

6. RANJIVOSTI I PRETNJE U WIRELESS CLOUD OKRUŽENJU

Imajući u vidu protok podataka kroz wireless cloud, neophodno je primeniti mehanizme za zaštitu integriteta i poverljivosti podataka kako bi se onemogućila njihova dostupnost neovlašćenim korisnicima. Svaka pretnja ima za cilj da iskoristi određene sigurnosne propuste u informacionom sistemu. Prilikom bilo koje procene rizika, upravo pretnje su te koje moraju najpre biti identifikovane. Uputstvo CNSS 4009 [41] kao pretnju definiše "bilo koju okolnost ili događaj sa potencijalom da negativno utiče na organizacione operacije (uključujući misiju, funkciju ili ugled), organizaciona sredstva, pojedince, druge organizacije ili nacije kroz informacioni sistem a preko neovlašćenog pristupa, razaranja, otkrivanja, modifikaciju informacija i / ili Denial-of-Service (DoS) napad".

Za razliku od žične mreže, bežični oblak nije ograničen fizičkim prostorom. Ovo potencijalno otvara mrežu za napad od strane lažnih korisnika koji nadziru bežične komunikacije ili neovlašćen pristup mreži iznutra ili spolja [16]. Tradicionalni lopovi, hakeri, high-tech kriminalci, virusi i druge vrste zlonamernog koda, tipični su uzroci bezbednosnih problema u bežičnim mrežama. Ciljevi napada su datoteke uskladištene na hard diskovima i drugim medijima, podaci i govorne komunikacije koje se prenose između udaljenih klijenata i interne mreže, ili udaljeni sistem jer se može iskoristiti za pristup glavnoj mreži.

Ranjivosti postoje i u bežičnim mrežama koje su međusobno povezane sa bilo kojim drugim sistemom. U takvim situacijama cela mreža postaje ranjiva, jer kada je jedan deo sistema ugrožen to utiče i na ostatak mreže. Nezaštićena bežična komunikaciona oprema je takođe podložna vandalizmu i terorističkim napadima koji mogu da izazovu prekid u komunikacijama i prestanak funkcionisanja mreže. Uspeh napada na bežičnu mrežu zavisi od tipa mreže, bezbednosnih mera preduzetih u mreži, lokacije mreže i sposobnosti protivnika koji želi doći do određene informacije.

Sve ranjivosti koje postoje u konvencionalnim žičnim mrežama, prenose se i u bežični cloud. Zlonamerni subjekti mogu preko bežične konekcije neovlašćeno pristupiti određenom računaru u mreži, zaobilazeći sve firewall zaštite i ukrasti identitet legitimnog korisnika koji će kasnije iskoristiti za pristup internoj mreži. Ovi subjekti mogu i da ugroze privatnost legitimnog korisnika prateći njegovo kretanje kroz mrežu. Zlonamerni kod ili virusi mogu oštetiti podatke na bežičnom uređaju, a potom se prebaciti i na žičnu konekciju. Iako je mnogo teže i potencijalno još važnije obezbediti bežičnu komunikaciju, problemi, pretnje i odgovarajuće potrebne mere da bi se adekvatno odgovorilo na njih su uglavnom iste za žične i bežične tehnologije.

Dva osnovna organizaciona izazova u informacionim sistemima su upravljanje bezbednosnim pretnjama i ranjivostima [42]. Administratori bezbednosti mogu da smanje rizike vezane za sistem kvalitetnom identifikacijom pretnji, na osnovu kojih će čineći promene u dizajnu ili proceduralne promene u sistemu da smanje ranjivost. U ovom radu identifikovaćemo neke od potencijalnih pretnji bežičnom cloud okruženju koje se mogu iskoristiti kao polazna tačka prilikom kreiranja sigurne cloud arhitekture. Ova lista

nije potpuna i verovatno će biti proširena novim iskustvima sa porastom upotrebe bežičnih cloud mreža, razvojem tehnologije i upornošću napadača koji stalno traže nove načine da ostvare svoje ciljeve.

Do sada postoji nekoliko identifikovanih pretnji od kojih je veći deo proistekao iz iskustava sa korišćenjem kompromitovanog WEP protokola za zaštitu bežičnih mreža. Navešćemo sledeće:

- Analiza saobraćaja – jednostavna tehnika u kojoj napadač određuje opterećenje komunikacionog kanala na osnovu broja i veličine paketa koji se šalju, izvor i odredište paketa i tip paketa.
- Pasivni nadzor – napadač pasivno nadzire bežičnu sesiju i njen sadržaj. Ako je sadržaj kriptovan, primenjuje tehnike za njegovo dekriptovanje da bi došao do otvorenog teksta.
- Aktivni nadzor – podrazumeva da napadač ubacuje podatke u nadziranu mrežu da bi na osnovu njih kasnije lakše dekriptovao sadržaj komunikacije i došao do željenih informacija.
- Neovlašćen pristup – najčešće nije usmeren ka korisniku ili grupi korisnika. Dobijanjem pristupa mreži, napadač ima priliku da planira druge vrste napada. Uglavnom napadači neovlašćeno pristupaju mrežama sa ciljem njihovog besplatnog korišćenja.
- Man in the middle – koristi se sa ciljem pristupanja privatnim podacima iz sesije, ili sa ciljem modifikovanja paketa u sesiji što narušava njen integritet.
- Otimanje sesije – napad na integritet sesije; napadač otima autorizovanu i autentifikovanu sesiju od svog pravog vlasnika.
- Ponavljanje (Replay) – koristi se za dobijanje pristupa mreži sa tuđim ovlašćenjima. Aktuelna sesija koja je napadnuta se ni na koji način ne menja niti se na nju utiče.

Iako su mnogi od gore spomenutih napada uobičajeni za bežična okruženja, visoko distribuirana i kolaborativna priroda bežičnog oblaka moraće da podigne nivo sigurnosnih protokola za zaštitu od pretnji bežičnom grid okruženju, okruženju oblaka i podacima koji se prenose iz oblaka u grid (slika 4, model pretnji bežičnom cloud). Dok se pretnje fokusiraju na specifične napade na računarska okruženja, model pretnji bežičnom oblaku uzima u obzir da treba sagledati veštinu napadača, njegovu sposobnost da zaista pokrene napad, procenu rizika da budu otkriveni i verovatnoću uspeha. Pretpostavka je da bi organizacije koje implementiraju bežični oblak u svoje okruženje najviše napadali visoko obučeni i motivisani hakeri.

Pretnje iz wireless grid okruženja

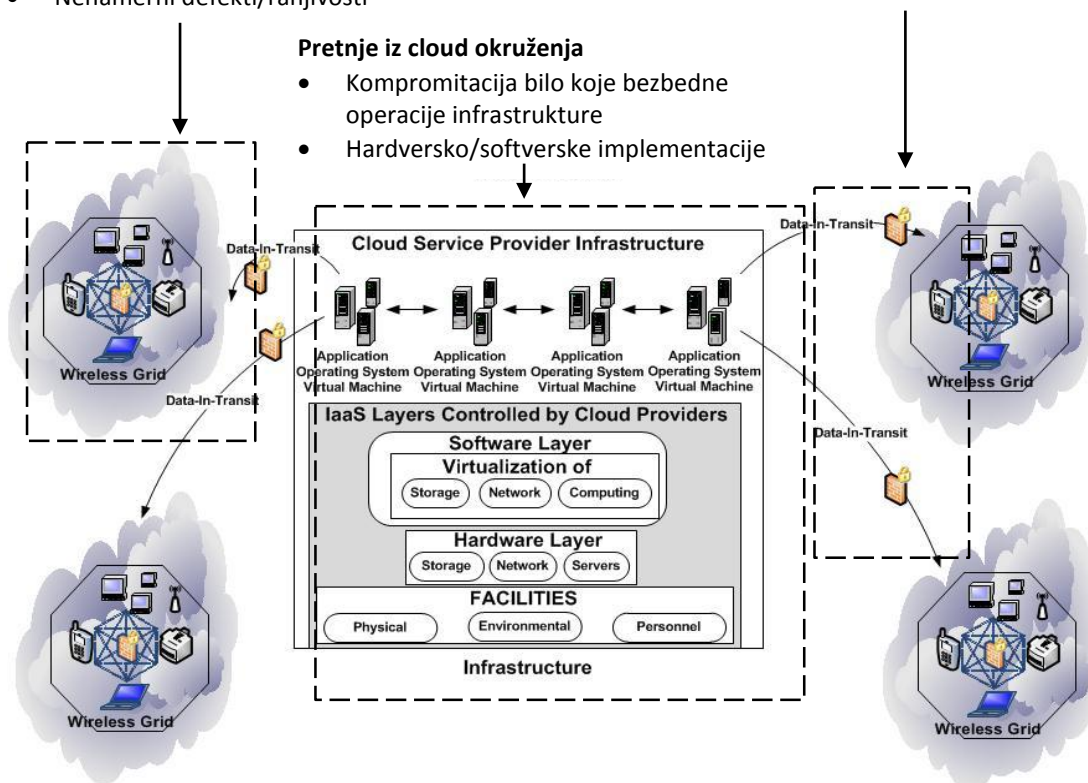
- Namerna/nenamerna rekonfiguracija bezbednosnih komponenti
- Nenamerni defekti/ranjivosti

Pretnje sa prenosnog puta

- Odbijanje servisa (DoS)
- Udaljeni upad u mrežu

Pretnje iz cloud okruženja

- Kompromitacija bilo koje bezbedne operacije infrastrukture
- Hardversko/softverske implementacije



Slika 4 – Model pretnji u bežičnim oblacima

Pretnje iz bežične grid sredine obuhvataju ona stanja koja se javljaju u operativnoj upotrebi bežičnih grid uređaja. Pošto svaka bežična grid lokacija koja je povezana sa cloud okruženjem može biti sa različitim stepenima zaštite, sa stanovišta procene rizika je potrebno razmotriti onu sa najgorim bezbednosnim uslovima. Ovi uslovi korišćenja uvode i pretnje od strane ljudi koji imaju ovlašćeni pristup i koji mogu namerno ili nenamerno da zloupotrebe, pogrešno konfigurišu ili zaobiđu bezbednosne postavke u okviru bežične grid mreže. To uključuje i one pretnje koji se odnose na mogućnost da neko ukrade ili zameni hardver ili softver uređaja koji vrši funkciju zaštite bežičnog grida.

Pretnje koje potiču od proizvođača bežičnih mrežnih uređaja mogu takođe izazvati zabrinutost u pogledu bezbednosti bežične cloud arhitekture. Celokupan proces implementacije, održavanja i nadogradnje hardvera i softvera bežičnih mrežnih uređaja može dovesti do pojave novih pretnji. Pretnje iz lanca snabdevanja bežičnih mreža hardverom i softverom odnose se na ono što proizvođač namerno izmeni u cilju zaobilaženja ili slabljenja bezbednosnih funkcija tokom razvoja, proizvodnje, distribucije, transporta, održavanja i skladištenja. Opasnost predstavljaju i nenamerni propusti u projektovanju i izradi bezbednosnih modula što takođe utiče na ukupnu bezbednost bežične mrežne arhitekture.

Pretnje u cloud computing okruženju su takođe od ogromnog značaja. Postoji više ciljeva napada u okviru softverske arhitekture clouda uključujući i softver za virtualizaciju, web browser-e, bezbednosni softver, i klijent / server operativne sisteme [21]. Napadi mogu biti pokrenuti i protiv većih cloud servisa, kao što su Amazon Web Servisi (AWS) i Google Apps i da potencijalno utiču na hiljade korisnika. Web servisi mogu biti napadani kroz eksploataciju ranjivosti svojstvenih XML-u (Extensible Markup Language), SOAP-u (Simple Object Access Protocol), i WSDL-u (Web Services Description Language). Napadi na web browser-e mogu ugroziti komunikaciju između korisnika i cloud provajdera i omogućiti napadačima da presretnu podatke (npr. lozinke, ključeve za šifrovanje, datoteke), preusmeriti web browser ka kompromitujućim sajtovima, sprečiti ga da ispravno funkcioniše, čime se onemogućuje internet komunikacija.

Jedan od najkritičnijih i najvećih izazova je obezbeđivanje kontinuirane dostupnosti bežičnih cloud resursa. Zaštita kritičnih infrastrukturnih komponenti, kao što su ruteri, mrežni prolazi (gateway), i DNS serveri, i komunikacionih puteva između cloud provajdera i korisnika, ključ je za održavanje raspoloživosti resursa i očuvanje integriteta i poverljivosti podataka koji se prenose preko ovih kanala. Pretnje koje mogu da utiču na komunikacije mogu biti ili zlonamerne, kao što su DoS napadi, usmereni ka bežičnim vezama ili uređajima, provajderima, korisnicima ili mrežnim resursima, ili nenamerne, uzrokovne kvarovima na opremi, nestancima struje, zagušenjem interneta ili prirodnim nepogodama. Stavljanje na crnu listu IP adresa koju koriste cloud servisi ili korisnici takođe može da bude ozbiljan problem. Usled neprimerenog ponašanja cloud korisnika iniciranog iz sredine clouda, može se desiti da IP adrese koje koristi cloud dospeju na crnu listu Internet provajdera (ISP) i ostalih cloud provajdera. Bez obzira da li su postupci bili nenamerni ili zlonamerni, stavljanje na crnu listu bi uticalo ne samo na pristup korisnika cloud servisima, već bi moglo biti finansijski pogubno i po cloud provajdera.

Fizička sigurnost bavi se pristupom računarskim objektima, infrastrukturom i kadrovima koji održavaju servise cloud provajdera, korisnicima i komunikacionim putevima između njih. Iako fizička bezbednost nije svojstvena samo za cloud computing, okruženje zajedničkih resursa bežične cloud arhitekture povećava potencijal za pristup podacima i računarskim resursima drugih organizacija. Fizičke povrede bezbednosti u okviru cloud data centra provajdera, dozvoljavaju napadačima mogućnost neovlašćenog pristupa podacima mnogobrojnih korisnika različitih organizacija [3]. Neovlašćen pristup računarskim sredstvima na strani korisnika može da omogući upad u okruženje cloud provajdera, što omogućava napadaču da ugradi maliciozne aplikacije u infrastrukturu provajdera.

U obzir se moraju uzeti i pretnje koje se tiču transfera podataka od oblaka ka bežičnom grid okruženju. Poverljivost i integritet podataka mora biti zaštićena u svakom trenutku [33], bez obzira na to gde se podaci nalaze. Bežični oblak mora da obezbedi i zaštitu od neovlašćenog menjanja poruka i dokumenata tokom prenosa podataka. Ovo je posebno važno u bežičnom cloud okruženju gde korisnici pristupaju podacima, aplikacijama i uslugama preko interneta, povećavajući izlaganje osetljivih podataka prisluškivanju, modifikaciji i ubacivanju malicioznog koda. Zaštita podataka u granicama bežičnog cloud

okruženja jednako je važna jer su javni oblaci sredine u kojima se računarski resursi potencijalno dele između mnoštva različitih korisnika i moraju biti zaštićeni od radoznalih očiju ostalih cloud korisnika. Takođe je važno zaštititi komunikacione kanale na kojima oblak počiva, kao i poruke i dokumente koji se njime prenose, tako da ne mogu biti dostupni neovlašćenim licima.

Tipične pretnje ka podacima smeštenim unutar bežičnog clouda mogle bi uključiti nenamernu ili zlonamernu izmenu ili brisanje podataka i datoteka, krađu podataka i DoS napade koji sprečavaju pristup podacima, aplikacijama i uslugama. Nepažljiva izmena ili brisanje podataka i datoteka, češće se dešava zbog loše konfigurisane kontrole pristupa nego zbog zlonamernih napada koje su počinili hakeri. Podaci u tranzitu su podložni presretanju (npr. MITM napadi) i modifikaciji, što predstavlja ozbiljan rizik za ugrožavanje poverljivosti i integriteta podataka. Podaci se takođe mogu neprimetno izvući iz nepravilno podešenih uređaja. Nepravilno zaštićen krajnji korisnik (na poslu ili kod kuće) može da proširi malware na virtuelnoj mašini (VM), koji bi se kasnije proširio i na druge korisnike koji koriste istu VM. Kako se bežični cloud korisnici povezuju sa resursima distribuiranim na više VM, malware može da se proširi i po njima. Radi smanjenja mogućnosti širenja zlonamernih programa od strane neovlašćenih ili ličnih uređaja, bezbednosna politika mora da reši da li će bezbednosni servisi, kao što su anti-virus i lične firewall aplikacije, biti prošireni na zaštitu kućnih personalnih računara (PC), telefona sa Internet mogućnostima ili samo omogućiti korisnicima da se povežu na resurse oblaka sa računarskim resursima koje im obezbeđuje kompanija.

Slično kao i haker koji napada od spolja, insajder sa ovlašćenim pristupom bežičnom cloud sistemu mogao bi da izvrši razne napade neovlašćenog pristupa drugim sistemima ili uskratiti uslugu korisnicima ovih drugih sistema. Zloupotreba od strane insajdera, zlonamerna ili slučajna, predstavlja najozbiljniju pretnju za bežične cloud sisteme. Iako se organizacije bave insajderskim pretnjama i danas, koncentracija informacija i njihova obrada u bežičnim oblacima uveličaće potencijalni uticaj ove pretnje. Bežični oblaci će biti posebno ugroženi od strane zlonamernih programa iz dva razloga:

- homogena struktura, mnogostruke interkonekcije i veličina oblaka povećava mogućnost inicijalne malware injekcije i omogućava joj mnogo puteva za umnožavanje, i
- koncentracija vrednih podataka u oblaku nudi potencijalnim napadačima, kako insajderima tako i spoljnim napadačima, vredne ciljeve zbog kojih je isplativo napisati specijalizovane malware samo za tu priliku.

Vlasnici podataka u bežičnom cloud-u će morati da brinu o dve potencijalne pretnje: slučajnom curenju informacija van bezbednosne enklave, kao i negativnom uticaju na integritet ili dostupnost njihovih informacija zbog izvršavanja zlonamernog koda ili DoS napada. Bežični oblaci će čuvati i obrađivati podatke iz različitih izvora, nuditi pristup različitim korisnicima, i povezivati se na razne spoljne sisteme. To povećava opasnost od curenja informacija između različitih domena. Bežični oblaci neće imati luksuz da čuvaju klijenta potpuno izolovanog već će morati da obezbede kontrolisanu razmenu njihovih

informacija. Ovi mehanizmi za razmenu predstavljaju najveću pretnju za curenje podataka. Zbog svega navedenog, moraju se obezbediti mehanizmi za rešavanje navedenih pretnji i stvaranje bezbednog bežičnog cloud okruženja.

7. ZAŠTITA BEŽIČNIH OBLAKA

Svaka komunikaciona mreža podložna je eksploataciji od strane pojedinaca ili grupa van ovlašćene grupe korisnika. Vladine komunikacije i komunikacije velikih korporacija su tradicionalno predmet takvih napada. Vojne i diplomatske komunikacije vlada su meta za dolaženje do nacionalnih tajni, dok su korporativne komunikacije meta industrijske špijunaže. Iskorišćavanje vladinih i korporativnih komunikacija zahteva veliku potrošnju resursa. Napadi na komunikacije se vrše sa ciljem omogućavanja pristupa podacima koji se prenose preko mreže, ometanja protoka podataka kroz mrežu i zauzimanja mrežnih resursa. Postoji i dodatni razlog za iskorišćavanje komunikacione mreže, a to je dezinformacija, ali se ona koristi u mnogo manjoj meri. Dezinformacija se ubacuje u komunikacione mreže sa ciljem da zavara, izazove konfuziju i sumnje i može obezbediti političku, vojnu ili ekonomsku prednost napadaču.

Prvi i najvažniji cilj bežične bezbednosne arhitekture cloud-a je da obezbedi da se servisi mogu pozivati i sa njima upravljati na bezbedan način. Kao sa skoro svakim kritičnim distribuiranim sistemom, postoji skup ključnih bezbednosnih uslova koji će morati biti ispunjeni a koji uključuju autentifikaciju i autorizaciju, poverljivost, integritet podataka, raspoloživost, neporecivost, bezbednosnu politiku razmene, detekciju upada, zaštitu i sigurno evidentiranje događaja, upravljivost i odgovornost [4, 8, 10, 22]. Zbog prirode i arhitekture bežičnih oblaka, moraće se sprovesti dodatne bezbednosne mere kako bi se obezbedilo kriptovanje (npr. poverljivost, integritet podataka, autentifikaciju entiteta, autentifikaciju porekla i dostupnost) svih informacija koje se preuzimaju, obrađuju i prenose. Integracija mora da obezbedi da bezbednosni okviri i bezbednosni alati budu dizajnirani i pozicionirani tako da se međusobno dopunjuju i budu interoperabilni na odgovarajući način.

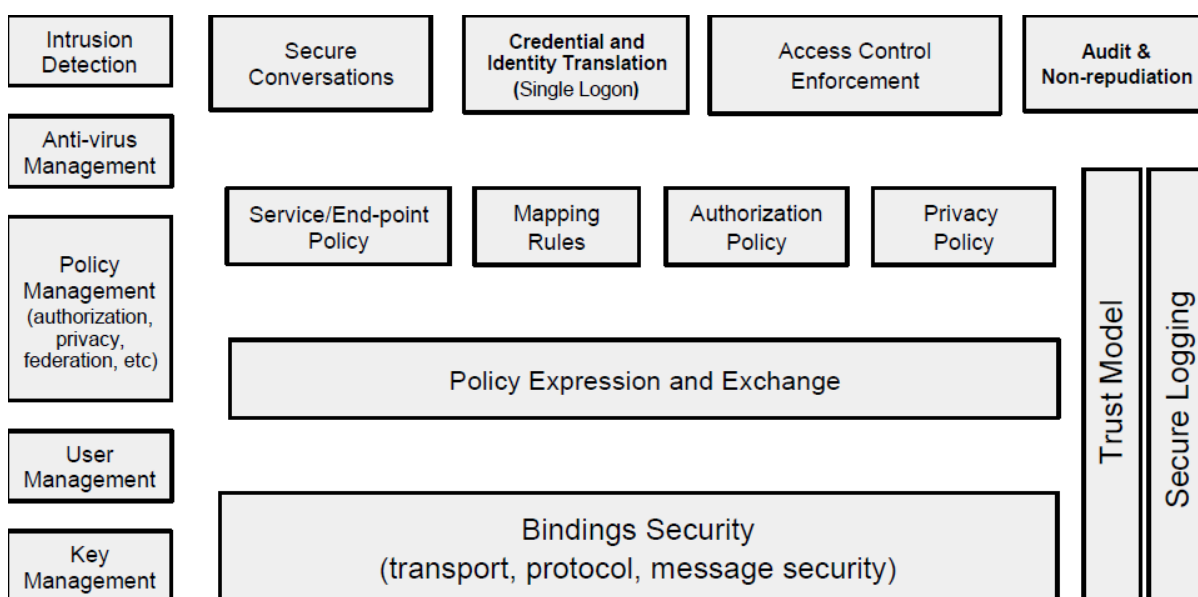
Sve gore navedeno uključuje:

- Interoperabilnost: kamen temeljac bežične cloud arhitekture koji mora biti očuvan u najvećoj meri kroz bezbednosnu arhitekturu. Glavne bezbednosne tačke integracije u arhitekturi - kao što su one između cloud computing provajdera usluga i bežične mreže klijenata, između pružaoca usluga i bezbednosne infrastrukture, kao i između bezbednosnih infrastrukture u različitim domenima poverenja (trust domain) - moraju imati stabilne i konzistentne interfejse zasnovane na široko prihvaćenim standardima, što omogućava svakom domenu ili organizaciji da implementira sopstvena rešenja.
- Ograničenja prilagođavanja bezbednosne politike: u tradicionalnom domenu bezbednosti, resursi i usluge su često zaštićeni jedinstvenim skupom bezbednosnih pravila koja nisu dovoljno detaljna da zadovolje specifične potrebe primene. Pošto korisnik koji pristupa resursu može ali i ne mora biti u lokalnom domenu organizacije, potrebni su različiti nivoi mehanizama za autentifikaciju i kontrolu pristupa. Shodno tome, bezbednosna politika treba da bude dovoljno

opširna i fleksibilna da bi se mogla prilagoditi i politici servis provajdera i politici bežičnog grida.

- Bezbednost uskladištenih podataka: fokusirajući se primarno na zaštitu poruka koje se prenose, sigurnosne mere moraju da zadovolje i zahteve za zaštitom pohranjenih podataka, koji nisu ograničeni samo na zaštitu čuvanja kredencijala (privatnih ključeva, itd.), ili zaštitu komponenata bezbednosne infrastrukture (bezbednosni izveštaji, itd.).

Zbog opasnosti od eksploatacije, bežični oblak će morati da bude zaštićen dobro definisanom bezbednosnom arhitekturom. Bezbednosna arhitektura obuhvata IT bezbednost i zahteve za zaštitom privatnosti podataka, kao i rešenja u kontekstu poslovne arhitekture. U bežičnom cloud modelu organizacije će imati manje kontrole nad svojom bezbednosnom arhitekturom nego u tradicionalnim mrežama, a istovremeno će se od njih zahtevati da dele IT infrastrukturu sa drugim entitetima. Jedan takav framework koji bi potencijalno mogao da prikaže pristup bezbednosti bežičnog oblaka u kreiranju bezbedne, integrisane i interoperabilne usluge je Grid security model [10, 28] prikazan na slici 5.



Slika 5 – Grid security model

Sigurnosni okvir omogućava da se osnovne bezbednosne prakse sprovede kroz organizaciju integrisanjem najboljih industrijskih bezbednosnih praksi na više nivoa u preduzeću: dizajn informacione infrastrukture, nabavku softvera, hardvera i usluga, razvoj aplikacija i obuku. Ovaj model može biti praktičan okvir na kome će se graditi i upravljati bežičnim Cloud sistemom da bi se ispoštovali zahtevi bezbednosti [11].

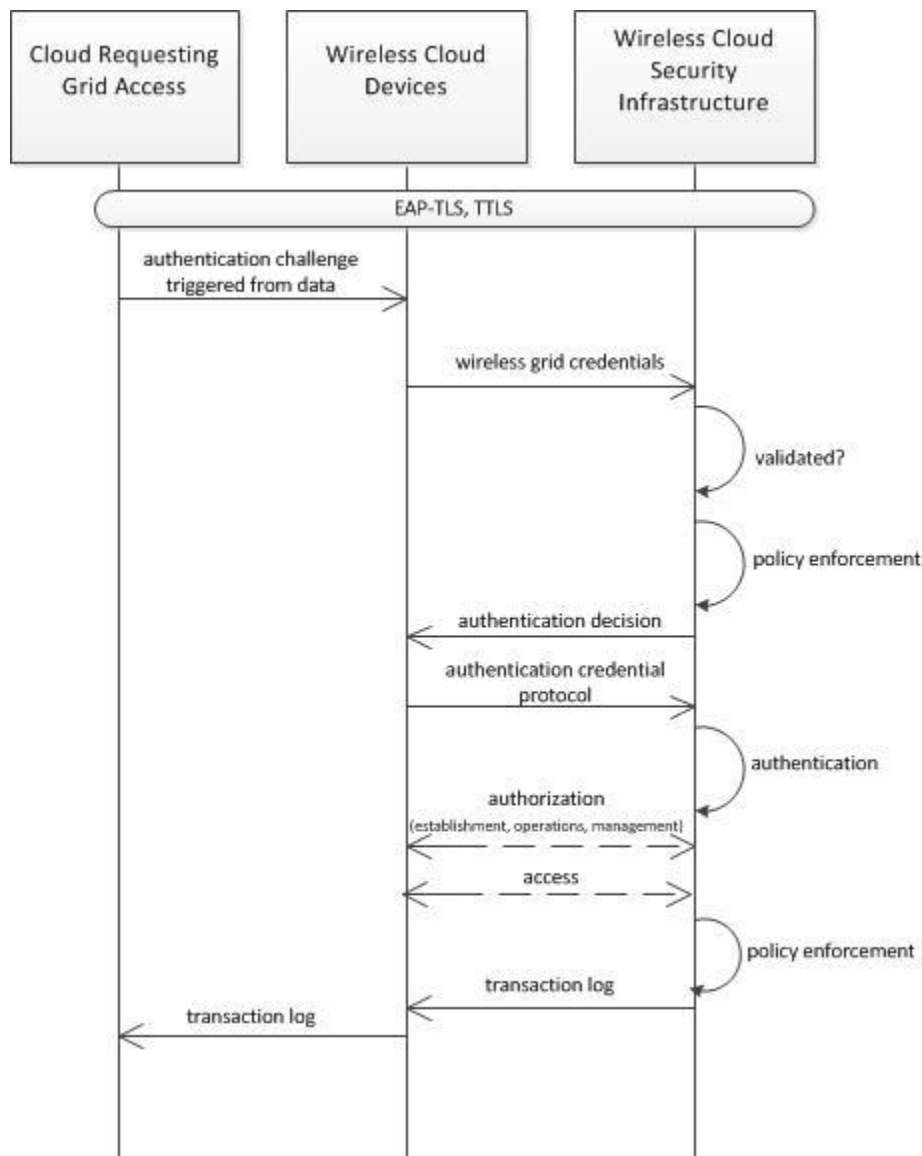
8. AUTENTIFIKACIJA

Neke od najvažnijih bezbednosnih kontrola svakog informacionog sistema vezane su za autorizaciju, autentifikaciju i pristup sistemu. Politike su jedan od aspekata informacija koje utiču na ponašanje objekata unutar sistema. Da bi se postigla i razmena podataka i zaštita podataka u bežičnom cloud okruženju, neophodno je da se koriste zajednički mehanizmi politike autentifikacije i autorizacije. Dok je autorizacija proces davanja korisničkih prava pristupa računarskim resursima na osnovu njihovih dozvola i privilegija, autentifikacija je potvrda identiteta ili drugih atributa na koje entitet polaže pravo (korisnik, proces ili uređaj) ili provera izvora i integriteta podataka. Autorizaciona politika bežičnog oblaka mora da se obrati procesima utvrđivanja ovlašćenja pre omogućavanja obavljanja radnje kao što su gledanje informacija ili pristupanje putem autentifikacije. U idealnom slučaju, mehanizam autorizacione politike će morati da obezbedi interoperabilne autorizacione mogućnosti među cloud provajderima.

Cloud servis provajderi će zahtevati da bežične grid organizacije imaju autorizacione i autentifikacione politike i sklopljen ugovor pre nego što im dozvole pristup određenim podacima. Različiti standardi autentifikacionih mehanizama moraju biti usklađeni, podržani, konfigurabilni i proširivi u zavisnosti od zahteva za specifičnim servisima (npr. - eXtensible Access Control Markup Language [XACML] Authorization Model, Security Assertion Markup Language [SAML], Globus Toolkit [GT] 5.03 [19, 29]). Kontrola pristupa cloud servisima na osnovu autorizacione politike (tj. ko može da pristupi servisu i pod kojim uslovima) može da se pridruži svakom servisu. Mogu se primenjivati različiti modeli kontrole pristupa, kao što su obavezna kontrola pristupa [31], diskrecioni [36], ili model kontrole zasnovan na ulozi [43]. Implementacija autorizacije mora biti proširiva da bi mogla da se prilagodi specifičnim servisima (npr. specifične finansijske informacije za finansijske institucije). U idealnom slučaju, autorizacionu politiku bi trebali da kreiraju provajderi cloud computing usluga i organizacije koje koriste bežični grid. Ovaj nivo je neophodan kako bi se obezbedile interoperabilne autorizacione mogućnosti između mnogobrojnih entiteta. Bez definisanih postupaka i metoda koje sprečavaju deljenje podataka bez zaštite, saradnja između tih entiteta nije moguća.

Potpuno realizovana sigurnosna arhitektura bežičnih cloud sistema dosta će zavisiti od decentralizovanog upravljanja identitetima i arhitekture autentifikacije sposobne da rastereti sam proces autentifikacije. Sistemi za autentifikaciju ne samo da treba da upravljaju sertifikatima identiteta korisnika, već i sertifikatima koje uređaji razmenjuju međusobno. Korisnici koriste ove sertifikate za autentifikaciju na pristupnoj tački sistema, dok ih uređaji koriste za međusobnu autentifikaciju i kreiranje kriptovanih tunela. Zbog nedovoljne izgrađenosti politike zaštite krajnjih pristupnih tačaka sistema koje imaju mogućnost samostalnog skeniranja i automatskog odobravanja pristupa u sklopu procesa provere identiteta, obezbeđivanje sigurnih krajnjih tačaka predstavlja mukotrpan proces njihovog međusobnog usklađivanja i konfigurisanja.

Autentifikacija / autorizacija stvaraju, dodeljuju i upravljaju identitetima i smeštaju ih u akreditivne (tj. X.509 sertifikate). Autentifikacioni mehanizmi su potrebni za uspostavljanje identiteta pojedinaca i usluga, a pružaoci usluga moraju implementirati autorizacione mehanizme za primenu smernica o tome kako se svaka usluga koristi [28]. Autentifikacija koristi identitete u sistemu i upravlja bezbednosnim atributima kao što su uloge (role) u sistemu. Slika 6. prikazuje generičku Wireless Cloud autentifikaciju, autorizaciju i proces kontrole pristupa.



Slika 6 – Proces Wireless Cloud autentifikacije, autorizacije i kontrole pristupa

Autentifikacija zahteva da korisnik (npr. cloud computing sistem) dokaže svoj identitet. Čim se podaci proslede iz oblaka u bežičnu mrežu, kao metod identifikacije se koristi mehanizam izazov / odgovor (challenge/response). Autentifikacija treba da bude dvosmerna, tako da kad bežični mrežni akreditivi budu prihvaćeni i potvrđeni, sprovođenje politike zaštite mora da obezbedi donešnje odluke o autentičnosti. Ovo sistemu omogućava da spozna da komunicira sa pravim korisnikom. Potvrđivanjem identiteta korisnika od strane sistema, smanjuje se mogućnost da će neovlašćeno treće

lice moći da se predstavi kao sistem ubacivanjem u vezu između korisnika i stvarnog sistema (tj. MITM - man-in-the-middle).

Autentifikacija u bežičnim grid mrežama treba da se zasniva na mehanizmima autentifikacije u bežičnim mrežama [13]. Autentifikacija u bežičnim grid mrežama mora da koristi snažnu enkripciju u cilju sprečavanja upada i mora da uključi uzajamnu autentifikaciju kako bi se obezbedilo da osetljive informacije budu prenošene samo preko legitimnih mreža. Bežična grid mreža mora imati jake standarde da bi ispunila stroge zahteve enkripcije i autentifikacije. Strogi zahtevi enkripcije i autentifikacije ispunjeni su od strane bežičnih lokalnih mreža zasnovanih na IEEE 802.11 kroz implementaciju standarda IEEE 802.1x. Ovaj standard utvrđuje korišćenje Extensible Authentication Protocol (EAP) direktno preko protokola linka.

EAP je u suštini protokol za prenos koji se može koristiti od strane različitih vrsta provere identiteta, poznatih kao EAP metode. Među EAP metodama razvijenim specijalno za bežične mreže je i skup metoda baziranih na sertifikaciji javnim ključem i TLS protokolu (Transport Layer Security protocol). To su EAP-TLS (Extensible Authentication Protocol Transport Layer Security) i EAP-TTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) metode.

EAP-TLS koristi mehanizam autentifikacije sertifikata TLS javnim ključem u okviru EAP u cilju obezbeđivanja međusobne autentifikacije klijenta serveru i servera klijentu [12]. Sa EAP-TLS, i klijentu i serveru moraju biti dodeljeni digitalni sertifikati potpisani od strane autoriteta za izdavanje sertifikata (CA) kojem oboje veruju. EAP-TLS sistem ključeva koristi dinamičke WEP (Wired Equivalent Privacy) ili TKIP (Temporal Key Integrity Protocol) ključeve. EAP-TLS koristi TLS rukovanje (handshake) kao osnovu za međusobnu potvrdu identiteta [12]. EAP-TTLS je realizovan u pojedinim RADIUS (Remote Authentication Dial-In User Service) serverima i softveru dizajniranom za upotrebu u 802.11 WLAN mrežama. U EAP-TLS, TLS handshake se koristi za međusobnu potvrdu identiteta klijenta i servera. EAP-TTLS proširuje ovaj proces autentifikacije pomoću bezbedne veze uspostavljene sa TLS handshake za razmenu dodatnih informacija između klijenta i servera. U EAP-TTLS, TLS handshake može biti obostran ili jednosmeran, u kom slučaju se samo server autentifikuje klijentu. Bezbedna veza uspostavljena rukovanjem se onda može iskoristiti da omogući serveru da autentifikuje identitet klijenta koristeći postojeće, široko rasprostranjene autentifikacijske infrastrukture kao što su RADIUS serveri.

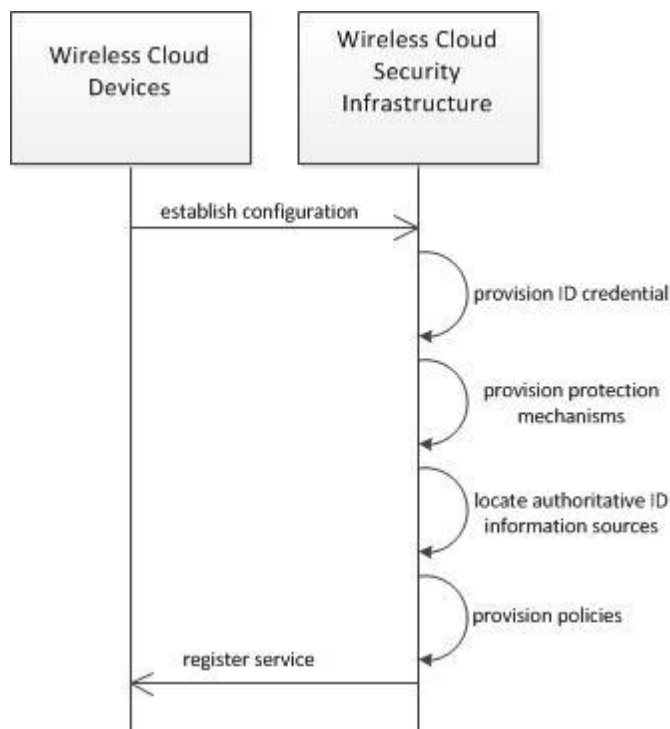
9. AUTORIZACIJA

Nakon što je korisnik dokazao da je onaj za koga se predstavlja, sledeći korak je da se obezbedi ovlašćenje. Ovlašćenje je davanje pristupa mrežnim resursima i uslugama i podrazumeva ograničavanje pristupa unutrašnjim resursima od strane korisnika. U cilju obezbeđivanja potpune autentifikacije u bežičnim cloud sistemima, moraju se implementirati tri kategorije podfunkcija autorizacije: uspostavljanje, izvršavanje i upravljanje. Prvi proces je funkcija uspostavljanja i zadužen je za uspešno pokretanje funkcije i obezbeđivanje njenog pravilnog izvršavanja. Druga je funkcija izvršavanja, koju funkcija autorizacije obavlja sa ciljem ispunjavanja svoje uloge. Treća kategorija je funkcija održavanja, koja se bavi pravilnim izvršavanjem funkcije autorizacije.

9.1 Funkcija uspostavljanja

Proces autorizacije u bežičnim oblacima mora da bude unapred snabdeven sa potrebnim informacijama, kako bi se mogao izvršavati i dati očekivane rezultate. Slika 7 prikazuje funkciju uspostavljanja bežične cloud autorizacije.

Prvi korak u procesu autorizacije je definisanje obrazaca podataka koji se primaju. Jednom primljen, proces obezbeđivanja identifikacionih kredencijala (ID) identifikuje akreditive za sopstvenu upotrebu (npr. PKI sertifikat), tako da se može identifikovati i biti autentifikovan u sistemu. Mehanizam zaštite mora da zaštiti informacije sa kojima rukuje, kako onih u tranzitu tako i uskladištenih, što nameće i upotrebu kriptografskih mehanizama za šifrovanje i dešifrovanje podataka. Trust anchor, sa kojim se verifikuju poruke i potpisi, poseduje sopstvene algoritme i ključeve za potpisivanje u cilju obezbeđivanja integriteta.



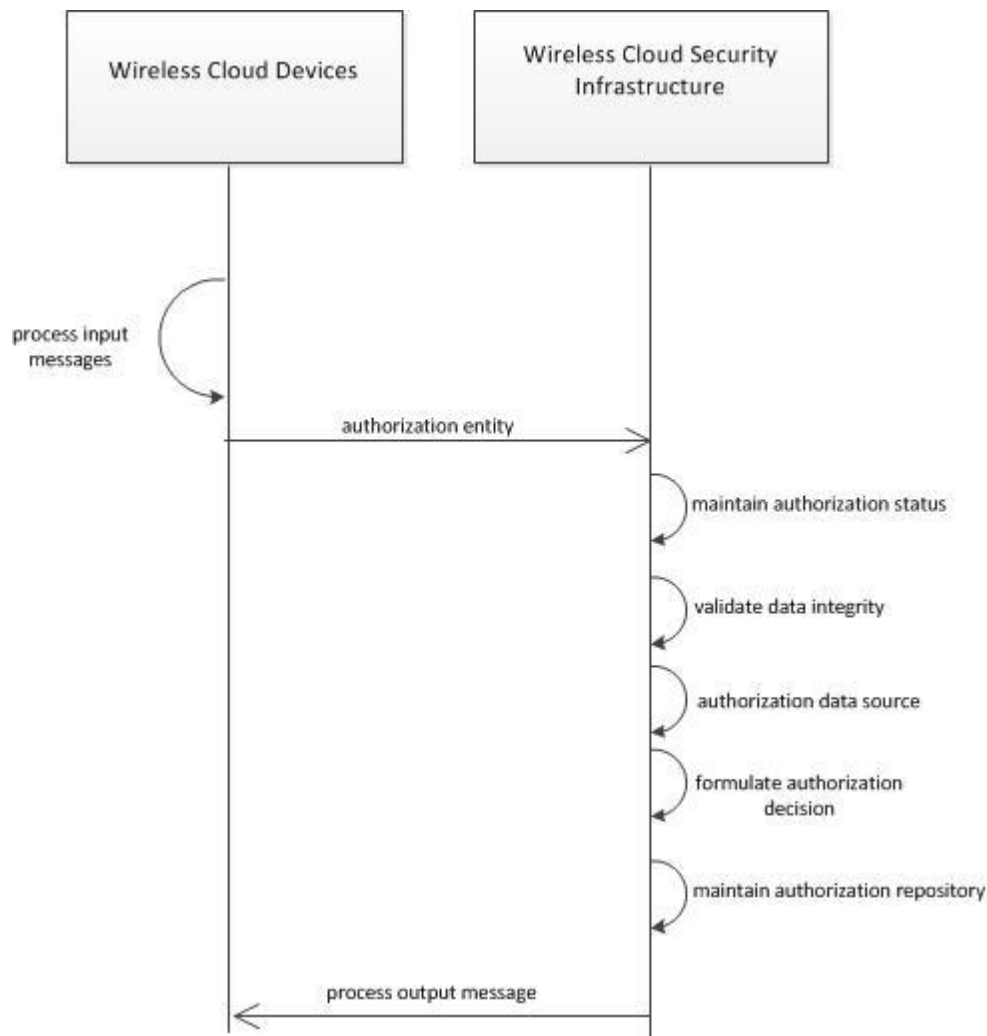
Slika 7 – Proces uspostavljanja

Lokator ID autoritativnih izvora u okviru sistema otkriva lokaciju servisa sa kojim se treba stupiti u interakciju. Pored toga, ova pod - funkcija otkriva lokacije svih autoritativnih izvora sa kojima funkcija autentifikacije mora da komunicira, uključujući i identifikaciju specifičnih vrsta sadržaja za svaki izvor i mehanizme potrebne za potvrđivanje da izvor transakcija sa svakim od ovih autoritativnih izvora može biti proveren. Podfunkcija obezbeđivanja politika preuzima sva unapređenja digitalne politike i instalira ispravke i dopunjuje ih. Funkcija registracije čini funkciju autorizacije vidljivom kroz ceo sistem. To bi trebala da bude poslednja podfunkcija uspostavljanja koja se izvršava.

9.2 Operativne funkcije

Slika 8. prikazuje operativne funkcije procesa bežične Cloud autentifikacije. Kada se prime podaci, obrada ulazne poruke dolazi do funkcije autorizacije tražeći određenu uslugu (npr. autorizaciju entiteta, autorizaciju izvora poruke, itd). Prvi korak je da se dolazna poruka obradi kako bi se potvrdio integritet poruke, da se poruka može ispravno dešifrovati ako je kriptovana, da se pošiljalac poruke može autorizovati i ako je potrebno da se proverí da li je pošiljalac ovlašćen da pošalje takvu poruku. Ako su svi uslovi ispunjeni, poruka se prosleđuje glavnoj autorizacionoj funkciji. Zahtev za autorizovanje entiteta u sistemu će sadržati tvrdeni identitet (claimed identity) i autorizacionu vrednost koja pokazuje da je entitet potvrdio svoj identitet. U zavisnosti od sistema koji se koristi, autorizaciona vrednost će biti niz znakova potpisan ili šifrovani privatnim ključem, u cilju dokazivanja posedovanja privatnog ključa.

Održavanjem autorizacionog statusa ažurnim pratiti se da li su entiteti trenutno autorizovani u navedenom sistemu. Kada je entitet autorizovan ova podfunkcija upisuje podatak u autorizacioni registar. Politika diktira parametre autorizacije (npr. važi za 24 sata pre nego što je potrebna ponovna autorizacija, ili automatski ističe nakon 10 minuta, itd) . Ova podfunkcija vodi registar svih trenutnih i nedavno isteklih ovlašćenja i može da signalizira drugim funkcijama kada je potrebno tražiti novo ovlašćenje. Provera integriteta podataka određuje da li je neki od podataka sadržanih u poruci promenjen. Mogući mehanizmi koji se mogu koristiti uključuju CRC proveru, proveru hash vrednosti poruke i digitalne potpise .



Slika 8 - Operativne funkcije

Autorizacija izvora podataka sprovodi se kroz dva koraka :

- potvrđivanje integriteta podataka i
- autorizovanje entiteta koji je navodni izvor podataka .

Odluka o autorizaciji može biti jača ili slabija na osnovu brojnih faktora, uključujući tip ovlašćenja (npr. autorizacija sa dva faktora bi trebala da bude jača nego autorizacija sa jednim faktorom), zaštitu autorizacionog kanala (npr. da li je moguće da je napadač kopirao višekratnu autorizacionu vrednost, ili ubacuje lažnu vrednost u kanal) i zaštitu kojom se obezbeđuje autorizaciona baza podataka (na primer, da li je moguće da je napadač uklonio pravu autorizacionu vrednosti iz baze podataka , a zamenio je lažnom) .

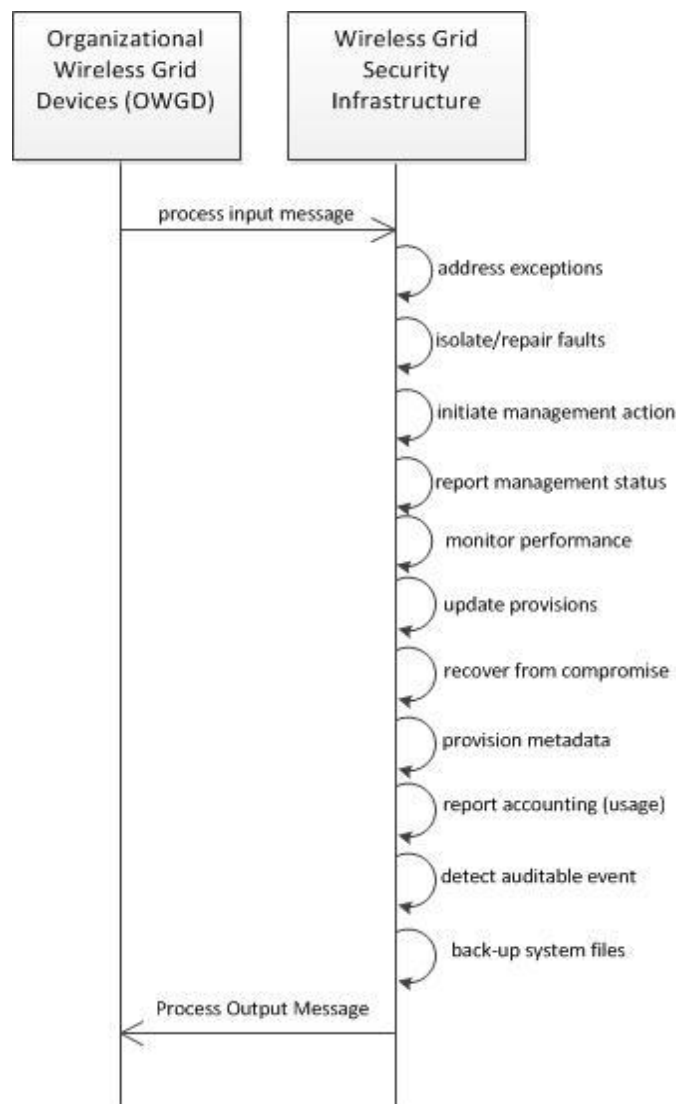
Konačno, podfunkcija formulisanja autorizacione odluke preuzima odgovore od drugih podfunkcija i stvara poruku odgovora koja može biti poslata zahtevaocu. Za održavanje autorizacionog repozitorijuma potreban je lokalni repozitorijum koji se koristi za sopstvenu upotrebu, za čuvanje svoje politike, autorizacionih odluka i trenutnih

autorizacionih vrednosti. Proces koji kreira izlaznu poruku odgovoran je za određivanje odredišta poruke i njenu zaštitu u skladu sa politikom (enkripcija, zaštita integriteta , digitalni potpis) .

9.3 Funkcije upravljanja

Funkcije upravljanja se izvršavaju istovremeno sa operativnim funkcijama i staraju se o pravilnom funkcionisanju autorizacione funkcije (Slika 9). Kao i sa proceduralnim porukama, sve poruke upravljanja moraju biti obrađene i dekrptovane, ako je potrebno, da bi se utvrdio integritet njihovog izvora i da li je on autorizovan da pošalje navedenu poruku. Kada se otkrije stanje koje se ne smatra normalnim, smatra se da se dogodio izuzetak.

U ovom slučaju funkcija upravljanja mora prijaviti stanje izuzetka (npr. Administratoru sistema), odrediti odgovarajuće opcije (npr. restart sistema , restartovanje procesa) i preduzeti mere da se autorizaciona funkcija ponovo osposobi za normalan rad.



Slika 9 – Funkcije upravljanja

Proces otkrivanja grešaka u autorizaciji mora da identifikuje neispravnosti i greške mehanizama funkcija i resursa na kojima funkcija počiva, i pokrene odgovarajuće mehanizme otklanjanja problema uz istovremeno obezbeđivanje nesmetanog izvršavanja tekuće operacije. Mere koje se preduzimaju mogu biti pokretanje akcija oporavka, aktiviranje narušenih funkcija na nekoj drugoj lokaciji, ili neka druga kombinacija postupaka. Kada je došlo do greške ili do degradiranja performansi ispod nekog prihvatljivog nivoa, akcija upravljanja, bez obzira da li automatizovano ili od strane čoveka, mora razrešiti navedeni problem.

U odgovoru na zahteve, izveštaj o stanju može da sadrži podatke o upotrebi, otkrivenim greškama, degradacijama performansi, statusu akcija upravljanja, statusu dozvola, statusu incidenata, statusu odziva sistema i druge vrednosti. Funkcija praćenja performansi sagledava ključne indikatore performansi kao što je navedeno u politici i izveštajima ili preduzima neku drugu radnju kada dođe do opadanja performansi, bez obzira na uzrok. Proces ažuriranja je odgovoran za izveštavanje o statusu i ažuriranje kada je to potrebno bilo kom od brojnih ključnih delova sistema, uključujući i politike, konfiguracijske parametre, podatke o ključevima, itd.

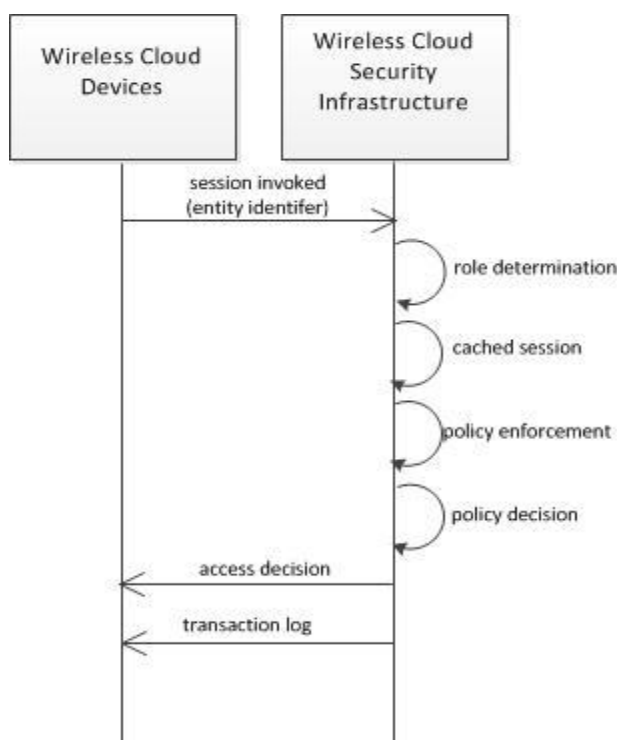
Podfunkcija oporavka od kompromitacije aktivira se kada se utvrdi da je došlo do kompromitovanja sistema ili za to postoji i najmanja sumnja. Navedena podfunkcija poseduje i mogućnost da utvrdi uticaj kompromitacije, identifikuje opcije za ublažavanje efekta kompromitacije i izabere adekvatan odgovor u cilju ublažavanja posledica.

Podfunkcija izveštavanja o iskorišćenosti održava log fajlove o korišćenju u kojima se beleži kada je funkcija autorizacije bila on-line i dostupna, kao i parametre i statistike o transakcijama. Primeri ovih parametara uključuju broj zahtevanih transakcija, specifične zahteve korisnika i specifične zahteve transakcija, vreme nastanka transakcije, kao i vreme proteklo do odgovora. Podfunkcija detektovanja događaja identifikuje pojavu događaja koji je specifikovan audit politikom. Nakon otkrivanja, ova funkcija će generisati zapis audit log događaja, koji će se interno štititi i arhivirati. Poslednja podfunkcija kreira back-up sistemskih fajlova i arhivira sve informacije potrebne za rekonstruisanje i ponovnu inicijalizaciju autorizacione funkcije. Kao i za operative poruke, funkcija obrade izlaznih poruka je odgovorna za određivanjeredišta poruke i zaštitu u skladu sa politikom (enkripcija, zaštita integriteta, digitalno potpisivanje).

10. KONTROLA PRISTUPA

Kontrola pristupa bežičnog oblaka koristi procese i procedure kako bi proverila da li je autorizovan i ovlašćeni entitet cloud computing/bežičnog grid sistema dobio ulogu. Entitet sistema mora imati potrebna ovlašćenja za korišćenje i pristup sistemskim resursima i mogućnost odlučivanja da li da dozvoli pristup informacijama ili izvršenje neke operacije na osnovu bezbednosne politike bežičnog oblaka. Sistem bi trebalo da dozvoli samo unapred izabrane entitete kojima je pristup omogućen kroz listu kontrole bežičnog pristupa (WCACL⁵ - wireless cloud access control list). Ovom listom upravljaju i održavaju je aplikacije u cilju obezbeđivanja mogućnosti upravljanja bezbednošću bežične kontrole pristupa u oblacima.

Kritična karakteristika svakog mehanizma kontrole pristupa je beleženje uspešno obavljenih transakcija i događaja (neočekivanih događaja) za kasniju reviziju ili analizu od strane sistema ili funkcija za upravljanje bezbednošću [27 , 44]. Sistemi koji sprovode odluke u cilju kontrole pristupa moraju inkorporirati i evidentiranje transakcija i događaja. Ovi sistemi moraju da obezbede integritet svojih transakcija i logova događaja kako u bazama podataka tako i na prenosnom putu. U zavisnosti od sadržaja log fajla, za skladištenje i prenos može biti neophodna i zaštita poverljivosti. Slika 10 prikazuje proces kontrole pristupa u bežičnim grid mrežama.



Slika 10 – Kontrola pristupa

⁵ WCACL lista će verovatno sadržati spisak ovlašćenih entiteta , kao što su sistemska korisnička imena i lozinke, obezbediti zaštitu integriteta ovih informacija i može da obezbedi zaštitu poverljivosti ovih informacija u zavisnosti od funkcije sistema .

Kada autentifikovan i ovlašćeni sistemski entitet inicira sesiju⁶, vrši izbor servisne tačke bežičnog oblaka (npr. senzorske mreže) na osnovu zadatka koji želi da ostvari. Identifikacija entiteta (npr. PKI sertifikat , itd) se bezbedno prosleđuje servisnoj tački. Identifikator ukazuje gde se fizički nalazi entitet , pridruženi rizik za informacije i sva ograničenja koje nameće politika zaštite u vezi sa njegovom lokacijom. Da bi dobila ulogu sistemskog entiteta (i ovlašćenja u skladu sa ulogom) bežična cloud servisna tačka prosleđuje preko sigurne konekcije identitet entiteta bezbednosnoj infrastrukturi bežičnog cloud-a .

Koristeći prosleđen identitet entiteta, bezbednosna infrastruktura bežičnog oblaka pronalazi ulogu (kao i pridodeljena ovlašćenja) za koju se entitet prijavio za ovaj dati proces i vraća, po zaštićenom kanalu, uloge entiteta (kao i ovlašćenja) do servisne tačke. Bezbednosna infrastruktura bežičnog oblaka kešira parametre sesije (identitet entiteta, dodeljene uloge, itd) za vreme njenog trajanja.

Istovremeno, kroz sprovođenje politika bežičnog oblaka vrši se unakrsna provera identiteta entiteta kroz keširane ili druge aktivne sesije koje isti entitet izvršava u tom trenutku kako bi se osiguralo da entitet ne poziva međusobno isključive uloge. Ako bi dodatna uloga izazvala povredu bezbednosne politike, obaveštenje se šalje na bežični oblak point-of-service koji upravlja sa spornom ulogom. Zauzvrat, funkcionalni portal kešira uloge entiteta (uključujući i ovlašćenja) za vreme trajanja sesije i bezbedno prosleđuje sistemsku autorizaciju entiteta zasnovanu na ulogama svaki put kada inicira interakciju sa bilo kojim dodatnim elementima sistema (aplikacijama, upitima, data brokerima, itd.) Svi zahtevi prosleđeni tim elementima sistema su u okviru ovlašćenja entiteta zasnovanog na ulogama. Sistem obaveštava cloud bežičnu bezbednosnu infrastrukturu o završetku ili prekidu sesije entiteta s bežičnom cloud servisnom tačkom i loguje sve transakcije za potrebe naknadne analize.

U nekim slučajevima, autentifikacija, autorizacija i kontrola pristupa se mogu postići jedino preko interfejsa bežične servisne tačke, omogućavajući sistemskom entitetu pristup samo onim mogućnostima posebno autorizovanim ulogom entiteta.

Stvarajući bežični oblak moramo obezbediti adekvatnu zaštitu informacionih sistema i izvora podataka i obezbediti određenu fleksibilnost vezanu za lokaciju i prirodu odlučivanja u procesima autentikacije, autorizacije i kontrole pristupa u bežičnim oblacima.

⁶ Sesija se odnosi na niz interakcija između entiteta i point of service , kao i na sve akcije u okviru sistema koje proizilaze iz pozivanja određenih point - of -service od strane entiteta. Sesija se završava kada entitet dobije tražene usluge, a zatim prekine interakciju sa tim point - of -service .

11. PREPORUKE ZA BEŽIČNE CLOUD MREŽE

Sistem, aplikacije ili usluge bežičnog oblaka moraju da sadrže definisan skup opcija za autentifikaciju, autorizaciju i kontrolu pristupa koje odgovaraju svim mogućim slučajevima korišćenja i dovoljno su robusne da bi se obezbedilo poštovanje bezbednosne politike u kombinovanom cloud computing / bežičnom grid okruženju. Moraju se razmotriti i evaluirati alternativni pristupi tokom projektovanja sistema, a ne pre ili posle njegovog puštanja u rad. U nekim slučajevima je najbolja opcija da bežični cloud sistem sam za sebe donosi sve odluke o autentifikaciji, autorizaciji i kontroli pristupa. U drugim slučajevima, bežični oblak će morati da se osloni na druge sisteme ili informacione infrastrukture za neke ili sve procese autentifikacije, autorizacije i kontrole pristupa.

Što se tiče bezbednosnih aspekata koje obrađujemo u ovom radu razmotrićemo neke ključne preporuke za kreiranje bežične cloud arhitekture koje će pomoći da se podigne nivo poverenja platformi zasnovanih na bežičnim oblacima.

11.1 Politika upravljanja identitetima i pristupom

Mehanizmi politike upravljanja identitetima i pristupom (IAM- Identity and Access Management), moraju voditi proces u cilju utvrđivanja koji uređaji (i njihovi korisnici) u bežičnoj grid mreži imaju mogućnost pristupa aplikacijama i / ili podacima koji se nalaze u bežičnom oblaku. Rezervisanje identiteta omogućava provajderima oblaka da bezbedno i blagovremeno omoguće ili ukinu korisnicima pristup [38] . Podešavanje robusne platforme za rezervisanje identiteta će olakšati upravljanje i kontrolu pristupa i ujedno omogućiti brz odgovor na zahteve za pristup uslugama i prestanak korišćenja. Izabran model autentifikacije mora da funkcioniše između svih cloud servisa, zatim u kombinaciji sa korisničkim IAM šemama za ne - cloud servise, i na kraju da radi na svim uređajima koji su povezani na bežični oblak.

Korisnici cloud-a će imati odgovornost za kreiranje, doslednost u korišćenju i održavanju politika i procedura IAM. Činjenje ili nečinjenje bilo kog korisnika bežičnog oblaka u ovoj ključnoj oblasti ima implikacije na sve korisnike. Proširenje IAM na oblak uslovljava pažljivo planiranje i razmatranje trenutnog i budućeg unutrašnjeg IAM platforme korisnika. Davaoci cloud usluga i projektanti bežičnih cloud sistema moraju tesno da sarađuju u cilju uspostavljanja IAM politike i procedura koje će podržati interoperabilno korišćenje cloud servisa među celinama unutar bežične grid mreže. Pomaganje korisnicima u planiranju IAM poslaće im pozitivnu poruku o tome koji su provajderi fokusirani na zaštitu bezbednosti i privatnosti i spremni da uzmu ulogu u zaštiti usluga koje nude od neovlašćenog pristupa. Saradnja između projekatata bežičnih cloud sistema i cloud provajdera potencijalno može da dovede do uspostavljanja autoritativnih smernica o pitanjima kao što su IAM , jer se odnose i na bežični oblak i cloud computing uopšte što bi takođe dovelo do većeg poverenja u ovu računarsku oblast.

11.2 Enkripcija, upravljanje ključevima i uključivanje kriptografije

Neki od najvećih strahova potencijalnih kupaca koji se odnose na cloud computing su zlonamerne izmene podataka ili brisanje podataka i fajlova, krađa podataka i gubitak podataka i presretanje od strane neželjenih lica. U višekorisničkim virtuelnim cloud okruženjima, gde se podacima upravlja od strane trećeg lica, uvek postoji potreba da se zaštite poverljivi podaci. U bežičnom okruženju, informacija koja se saopštava i prolazi između mrežnih čvorova putuje preko standardnih radio frekvencija koje su osjetljive na prisluškivanje od strane trećih lica. Autentifikacija i enkripcija se moraju sprovesti istovremeno kako bi se sprečilo prisluškivanje u toku prenosa podataka preko bežičnih mreža i kako bi se garantovalo da su osjetljive informacije koje se prenose preko mreže legitimne. Pored zaštite podataka već u samom bežičnom oblaku, korisnicima treba garancija da će njihovi brojevi kreditnih kartica, lozinke i lični identiteti korisnika ostati bezbedni dok putuju preko Interneta i između mreže i oblaka, ili biti bezbedno čuvani na uređajima povezanim na mrežu. Enkripcija i upravljanje ključevima će biti implementirani od strane projekatanta bežičnih cloud sistema kroz korišćenje tehnologija i standarda opisanih ranije.

Primenom kriptografije u oblaku, provajderi mogu da zaštite bežičnu mrežu organizacije od zlonamernih korisnika i malicioznih procesa u oblaku šifrujući podatke, tako da ih učine nerazumljivim nepozvanim korisnicima. Provajderi bi trebalo da ponude alate za šifrovanje IaaS korisnicima što bi im omogućilo da šifruju podatke pre slanja u oblak i dešifruju podatke nakon što se preuzmu iz oblaka. PaaS treba da sadrži standardne alate za zaštitu podataka u bazama i / ili u memoriji. SaaS korisnicima bi unapred trebalo da se kaže da sam provajder ima mogućnost da šifrue podatke koji se čuvaju na serverima u oblaku [38].

Korisnicima bežičnih oblaka na SaaS nivou podrška i servis šifrovanja moraju biti ponuđeni čak i bez potrebe da to sami zahtevaju. Pored toga, cloud provajderi moraju da učine sve što je u njihovim mogućnostima da podrže robusne šeme upravljanja ključevima, gde se ključevi čuvaju na bezbednim mestima i ne mogu biti presretnuti ili ukradeni od strane neovlašćenih lica. Čuvanje ključeva unutar oblaka se treba organizovati na takav način da je pristup pojedinačnim ključevima omogućen samo licima kojima su legitimno potrebni. Takođe, uloge entiteta koji koriste ključeve moraju biti razdvojene od uloga entiteta koji ih čuvaju. Zajedno sa politikama za čuvanje ključeva, cloud provajderi bi trebalo da imaju jake politike kreiranja i uništavanja ključeva, kao i mogućnost za bezbedno pravljenje kopija i oporavak ključeva.

Neosporno je da se ranjivosti sistema u smislu bezbednosti podataka uvećavaju kada se cloud servisi baziraju na bežičnim grid mrežama pa je neophodno robusnije rešenje koje će se ovim ranjivostima baviti. Međutim, vodeći računa da se podaci što bolje zaštite od neželjenih korisnika, moraju se razmotriti i mogući uticaji curenja podataka u bežičnom oblaku, ako se kojim slučajem to desi. Sve dok industrija oblaka ne bude u mogućnosti da iznađe standarde i end-to-end tehnološka rešenja za zaštitu podataka koji se čuvaju, koji su u upotrebi i u tranzitu, projektanti bežičnih cloud sistema i cloud provajderi moraju

da rade zajedno da izgrade i održe jaku politiku i praksu enkripcije i upravljanja ključevima.

11.3 Poreklo

Povećana transparentnost podataka i usluga u oblaku je još jedna od prepreka za njegovo rasprostranjenije usvajanje. Mnogi potencijalni klijenti nerado koriste oblak zbog nekih od nedostataka brzog pružanja usluga: nemogućnost cloud provajdera da pruži detaljne informacije o podacima (npr. kretanje , geografska lokacija na kojoj se čuvaju podaci, itd) koje su neophodne administratorima bežičnih cloud sistema, kako bi se ispunili određeni bezbednosni uslovi. Podatak o poreklu je prvi korak u tom pravcu. Poreklo je meta podatak koji opisuje poreklo digitalnog objekta [17]. Pružaoci usluga mogu da koriste podatak o poreklu za otkrivanje obrazaca pristupa i neuobičajeno ponašanje, kao i da poboljšaju svoje usluge. Administratori i korisnici bežičnog cloud sistema mogu da koriste poreklo da prate podatke, u skladu sa standardima i zahtevima kontrole, i da pretražuju podatke čak i kada su šifrovani. Komercijalne cloud usluge, kao što je Amazon, daju neke mogućnosti klijentima da skladište i preuzimaju meta podatke o poreklu iz svojih ličnih uređaja, ali nisu u stanju da ih sami generišu. Odgovornost za to ostaje na korisniku cloud servisa. Da bi koristili podatke o poreklu, klijenti koji koriste bežični cloud moraju da se pretplate na servis koji pristupa bazi podataka provajdera i da pomoću njega u navedenu bazu upisuju podatke o povezanim uređajima. Tek nakon toga klijenti mogu koristiti ili klijentski softver ili softverske aplikacije izrađene za pristup bazi podataka u cilju pretraživanja podataka o poreklu.

Podaci o poreklu u oblacima su još uvek u fazi istraživanja i imaju neka ograničenja. Nerešena pitanja u vezi korišćenja podataka o poreklu obuhvataju i problem kako sprečiti korisnike da daju lažne podatke o poreklu, kako zaštititi navedene podatke od falsifikovanja ili uništavanja i kako osigurati konzistentnost podataka sa objektom koji se opisuje.

11.4 Problemi privatnosti u toku razvoja/izbora provajdera bežičnih cloud servisa

Za neke od glavnih komercijalnih provajdera usluga, kao što je Google, cloud computing je počeo sa ciljem ostvarivanja profita na račun iznajmljivanja viška kapaciteta u sopstvenim data centrima. Tada je nastala prva paradigma cloud computing, jer čineći to, manje pažnje su posvetili privatnosti i sigurnosti, a više proizvodnji tržišno prihvatljivijih ponuda usluga. Trenutna istraživanja ukazuju na zabludu u tom pristupu napominjući da privatnost treba uzeti u obzir još u fazi razvoja novih ponuda.

Cloud servis programeri su prilikom dizajniranja i razvoja odgovorni za sprovođenje takve prakse kojom se izbegavaju neki osnovni nedostaci u dizajnu i implementaciji, a koji kasnije mogu dovesti do narušavanja privatnosti. Ove prakse obuhvataju:

- restriktivno projektovanje usluga koje određene lične informacije šalju ili skladište u oblaku,

- davanje korisnicima maksimalne kontrole nad tim ko i pod kojim uslovima može da pristupi, upravlja i promeni njihove lične podatke u oblaku,
- obezbeđivanje načina provajderima da garantuju da se lični podaci obrađuju u skladu sa specifikacijama korisnika i
- pružanje povratne informacije korisnicima o tome kako se lični podaci koriste i štite.

Mere zaštite privatnosti ugrađene u bežične oblake trebaju biti neprimetne i sveobuhvatne. Projektanti bežičnih cloud sistema moraju dizajnirati pouzdane interfejsse između davaoca usluga i mrežnog okruženja u cilju praćenja kretanja podataka od oblaka i ka oblaku, kako bi obezbedili neophodne informacije provajderima da u slučaju potrebe mogu dostaviti podatke o korišćenju i zaštiti ličnih / poverljivih podataka u oblaku. Takođe, prilikom izbora cloud usluge, korisnik mora sa provajderom da precizira koja su njegova očekivanja po pitanjima privatnosti. Umesto pretpostavke da je privatnost podataka zagarantovana od strane provajdera, korisnici moraju dobro da prouče i razumeju za šta je provajder odgovoran a za šta nije i šta može da uradi da bi se obezbedila privatnost podataka korisnika bežičnih cloud servisa.

12. BEŽIČNE MESH MREŽE

Bežična mesh mreža predstavlja bežičnu mrežu u kojoj svaki od čvorova može indirektno ili neposredno da komunicira sa jednim ili više čvorova. Termin mesh podrazumeva da su svi čvorovi uvezani po principu svaki sa svakim, a u današnjim mesh mrežama to uglavnom znači da su grupe čvorova povezane sa drugim grupama čvorova. U bežičnim mesh mrežama postoje dva tipa čvorova:

- Mesh ruteri
- Mesh klijenti

Oba tipa čvorova mogu da igraju ulogu i hosta i rutera. Paketi se prosleđuju u ime drugih čvorova koji ne moraju da budu u direktnoj bežičnoj vezi sa odredišnim čvorovima [45].

12.1 Mesh ruteri

Mesh ruteri su u većini slučajeva stacionarni uređaji. Upotrebom multi-hop tehnologije mogu da ostvare istu pokrivenost kao i standardni ruteri, ali uz dosta manje predajne snage. Poseduju i dodatne funkcije koje omogućavaju mesh umrežavanje. Kroz gateway i bridge funkcionalnost, mogu se integrisati sa različitim postojećim bežičnim mrežama, kao što su mobilna i Wi-Fi.

12.2 Mesh klijenti

Mesh klijenti mogu biti pokretni ili stacionarni. Poseduju neophodne mesh funkcionalnosti koje im omogućavaju da se ponašaju kao ruteri, ali ne poseduju ni gateway ni bridge funkcionalnost. Različite vrste uređaja mogu da igraju ulogu mesh klijenata.



Slika 11: Primer mesh klijenata

12.3 Bežična mesh mrežna arhitektura

Bežična mesh mreža može biti predstavljena kroz tri različite mrežne arhitekture, u zavisnosti od mrežne topologije i funkcionalnosti čvorova. Ukratko ćemo prokomentarisati svaku od njih.

12.3.1 Infrastrukturna/backbone WMN

Ovaj tip mrežne arhitekture se formira povezivanjem različitih tipova čvorova koji mogu biti i klijenti i ruteri. Svi čvorovi su međusobno na istom nivou [46]. Sačinjavaju je mrežni ruteri koji formiraju infrastrukturu na koju se povezuju klijenti. Infrastruktura može biti izgrađena korišćenjem različitih vrsta radio tehnologija, koje mogu biti značajno različite. U upotrebi su najčešće dva tipa radio tehnologija koje se koriste u ruterima, jedna za komunikaciju između rutera (backbone komunikaciju) i druga za komunikaciju ka korisnicima. U zavisnosti od tipa komunikacije, razlikuju se i tipovi antena na uređajima. Za backbone komunikaciju koriste se usmerene antene, dok se za komunikaciju sa klijentima koriste omni direktivne antene. Backbone mreže se formiraju na taj način da se samostalno konfigurišu i leče, međusobno uspostavljajući linkove[47]. Takođe poseduju i mogućnost da se samostalno formiraju. Svaki čvor u mreži osluškuje okolinu i kada pronade novi čvor, šalje mu zahtev da se priključi mreži. Kada se ispune svi bezbednosni zahtevi, novi čvor se priključuje mreži. Sa njegovim priključivanjem mreži, formiraju se nove putanje, a podaci o tome šalju se svim čvorovima u mreži [50]. Ako se jedan ili više čvorova premeste sa jedne lokacije na drugu, funkcija samoizlečenja obezbeđuje reorganizaciju čvorova i obezbeđuje premeštenim čvorovima da nastavu da funkcionišu u mreži. Funkcija samoizlečenja obezbeđuje redundantnost u mesh mrežama slanjem poruka svim čvorovima u mreži o otkazivanjima pojedinih čvorova i novim mogućim putanjama. Funkcija samokonfigurisanja omogućava da se mesh mreža samostalno i automatski konfiguriše, bez potrebe za intervencijom od strane čoveka.

Kroz gateway funkcionalnost, mesh ruteri mogu biti povezani na Internet i obezbediti okosnicu konvencionalnim klijentima u mesh mreži [45]. Korisnici koji poseduju ethernet interfejsu mogu biti povezani na mesh ruter posredstvom ethernet linkova. Ruteri se međusobno povezuju i formiraju mesh mrežu i odgovorni su za rutiranje podataka koje razmenjuju klijenti. Podaci mogu putovati preko više mesh rutera dok dođu do svog cilja [48]. U slučaju da konvencionalni klijent koristi istu radio tehnologiju kao mesh ruter, može se sa njim povezati direktno. U suprotnom, ako koristi različitu radio tehnologiju, mora se povezati na mesh ruter koristeći ethernet konekciju. U praksi se može desiti da postoji nekoliko različitih mreža, koje su preko bežičnih mesh rutera, postavljenih na krovovima zgrada, međusobno povezane. Mesh rutere kao pristupne tačke mogu koristiti

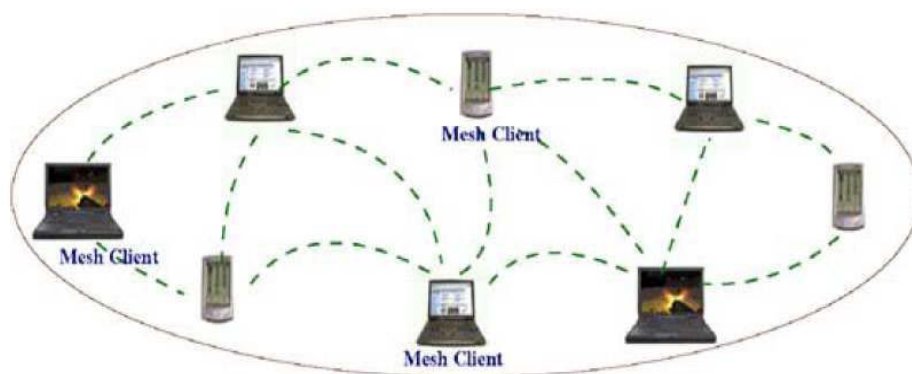
i klijenti iz lokalnih mreža i korisnici koji prolaze kroz zonu koju pokriva mesh ruter, pod uslovom da imaju sva potrebna odobrenja (slika 12).



Slika 12 – Infrastrukturna/backbone WMN

12.3.2 Klijentska WMN

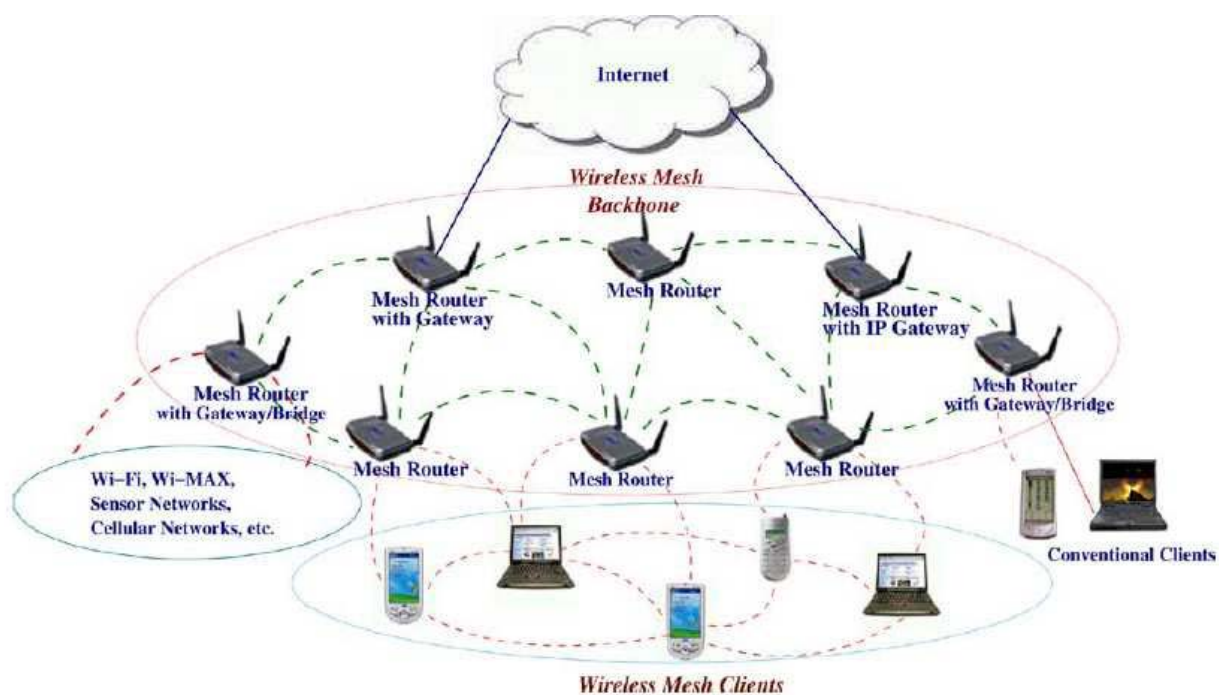
U ovoj vrsti WMN, pored uspostavljanja međusobne peer to peer mreže, klijentski čvorovi izvršavaju rutiranje podataka a i obezbeđivanje end user aplikacija korisnicima. Ovde krajnji uređaji imaju mnogo manje mogućnosti nego u infrastrukturnim WMN. Višestruki čvorovi se i ovde koriste za prenos podataka od izvora do odredišta. Klijentske WMN se formiraju korišćenjem jednog radio standarda na svim čvorovima. Kako u ovoj mreži ne postoje mesh ruteri, krajnji korisnici moraju imati mogućnost da se sami konfigurišu i rutiraju podatke, pa su stoga i zahtevi koje moraju ispuniti mnogo veći nego što je to u infrastrukturnim mesh mrežama.



Slika 13 – Klijentska WMN

12.3.3 Hibridna WMN

Ova vrsta mesh mreže je kombinacija obe navedene mesh arhitekture (infrastrukturne i klijentske). U hibridnim mesh mrežama korisnici mogu pristupiti mreži preko mesh rutera ili preko mesh klijenata. Kombinacijom infrastrukturne i klijentske WMN postiže se da je istovremeno preko mesh rutera obezbeđena konekcija ka drugim vrstama mreža (Internet, Wi-Fi, WiMAX, mobilna mreža, senzorska mreža...), dok mesh klijenti obezbeđuju veću pokrivenost i broj pristupnih tačaka u okviru WMN. Ova arhitektura je posebno značajna ako se uzme u obzir činjenica da je za razvoj WMN veoma bitan način i mogućnost integrisanja sa postojećim vrstama mreža.



Slika 14 – Hibridna WMN

13. KARAKTERISTIKE WMN

Bežične mesh mreže su multi hop mreže i obezbeđuju mnogo veću pokrivenost u odnosu na standardne bežične mreže. U slučajevima da jedan od čvorova prestane da funkcioniše, poruka se može preusmeriti preko drugih susednih čvorova, čime se postiže redundantnost mesh mreže. Pored njenih moćnosti da se sama izleči i sama konfiguriše, poseduje i dobru podršku za Ad Hoc umrežavanje. Kroz multi hoping tehnologiju, postiže se veća propusna moć i efikasnije korišćenje radio spektra. Zbog redukcije broja neophodnih pristupnih tačaka internetu značajno se smanjuje cena i pojednostavljuje procedura osnovne instalacije, što predstavlja jednu od najvećih prednosti ove mreže. Fleksibilna mrežna arhitektura i mogućnost povezivanja za postojećim mrežama kao što su WiMax, Wi-Fi i mreže mobilne telefonije, čine je veoma konkurentnom u procesu odlučivanja o izboru mreže u fazi projektovanja mrežnih okruženja.

13.1 Razlike između WMN i AdHoc mreža

Poređenje je izvršeno po sledećim karakteristikama:

13.1.1 Bežična infrastruktura/backbone

13.1.2 Integracija

13.1.3 Specifičnosti rutiranja i konfiguracije

13.1.4 Višestruki radio standardi

13.1.5 Mobilnost

13.1.6 Oblasti primene

13.1.1 Bežična infrastruktura/backbone

Bežične mesh mreže formiraju bežični backbone zasnovan na upotrebi mesh rutera i na taj način obezbeđuju veliku pokrivenost, mogućnost povezivanja i robusnost. Nasuprot njima, pokrivenost ad hoc mreža zavisi od broja i volje krajnjih korisnika, što ne garantuje zahtevanu pouzdanost.

13.1.2 Integracija

Kroz svoje gateway i bridge mogućnosti, WMN omogućavaju integraciju sa mnogobrojnim postojećim mrežama (Wi-Fi 802.11a,b,g,n, Internet, mobilne telefonske mreže, senzorske mreže..), što sa standardnim ad hoc mrežama nije slučaj.

13.1.3 Specifičnosti rutiranja i konfiguracije

U WMN mrežama funkcije rutiranja i konfigurisanja obavljaju mesh ruteri, dok u ad hoc mrežama to obavljaju uređaji krajnjih korisnika što ih čini mnogo više opterećenijim u poređenju sa korisnicima bežičnih mesh mreža.

13.1.4 Višestruki radio standardi

U WMN u mesh ruterima može biti ugrađeno više tipova radio primopredajnika baziranih na različitim tehnologijama, u cilju pokrivanja šireg spektra korisnika. Specifična konfiguracija i sposobnost rutiranja uvećavaju propusnu moć mesh mreže, što je kod ad hoc mreža nemoguće postići sa upotrebom samo jednog radio uređaja [47].

13.1.5 Mobilnost

Kod ad hoc mreža, mrežna topologija se menja u zavisnosti od kretanja korisnika. Sa druge strane, WMN imaju fiksne čvorove i dosta su statičnije, pa im je u poređenju sa ad hoc mrežama i mobilnost relativno manja.

13.1.6 Oblasti primene

Zbog svojih dobrih osobina, WMN se koriste i u vojnim i u civilnim aplikacijama. Za razliku od njih, ad-hoc mreže su uglavnom privremene, pa se ne mogu koristiti na obe strane. Mesh mreže se koriste i za širokopojasne kućne mreže, društvene mreže, korporacijske mreže, transportne sisteme, zdravstvene sisteme i u bezbednosnim i sistemima nadzora.

13.2 Tehnologija WMN

Bežične mesh mreže funkcionišu na isti način na koji funkcionišu i žične internet komunikacije, gde u svakom trenutku postoji više od jedne moguće putanje između svakog od komunikacionih čvorova. U mesh mrežama point to point i point to multipoint komunikacija višestruko povećava stabilnost i pouzdanost komunikacija.

13.2.1 Mesh rutiranje

Kod bežičnog mesh rutiranja koristi se više tehnologija koje proaktivno i reaktivno određuju putanju i kretanje podataka u okviru mreže. Na zahtev, putanja se do cilja kreira bazirana na reaktivnom protokolu, dok se proaktivno rutiranje koristi za pronalaženje najbolje putanje u zavisnosti od stanja linkova. Kombinacija reaktivnog i proaktivnog rutiranja se koristi u najvećem broju protokola. Najčešće implementacije ad-hoc mreža zasnovane su na hibridnim on-demand i link-state rutiranjima.

On-demand osnovne operacije

Najpopularniji primer on-demand ad—hoc rutinog protokola je svakako Ad-Hoc On-Demand Distance Vector (AODV) rutiranje. U ovom protokolu putanja se dobija slanjem poruke sa zahtevom (RREQ) kroz mrežu. Odgovor sadrži putanju do cilja (RREP). Svaki čvor za sebe čuva listu svih dostupnih susednih čvorova i putanja do njih. U slučaju prekida linka, kroz mrežu se šalje izveštaj koristeći poruku o grešci na ruti (RERR) [58].

Link-state osnovne operacije

Primer proaktivnog rutinog protokola je Optimized Link State Routing Protocol (OLSR). Ovde se susedne rute otkrivaju slanjem periodičnih poruka. U slučaju da se ruta do ciljanog čvora ne može pronaći, šalje se RREQ poruka susednim čvorovima. Ako neki od susednih čvorova zna put do cilja, šalje RREP poruku zahtevaocu, a ako nema podatke o ruti do cilja, ponavlja zahtev dalje, ka svojim susedima. Na kraju se dobijena ruta kroz RREP poruku sa rednim brojem šalje zahtevacu.

13.2.2 Mrežna topologija

U cilju obezbeđivanja funkcija samoizlečenja i optimizacije procesa u mesh mrežama koriste se sledeće topologije čvorova:

- Point to Point
- Point to Multipoint
- Multipoint to Multipoint

Point to Point

Point to Point topologija obezbeđuje odlične performanse, brze interkonekcije i stabilne veze između čvorova. To je ujedno i najjednostavniji oblik bežične komunikacije koji obezbeđuje vezu između dva čvora. Nije previše skalabilna i može se primeniti veoma lako.

Point to Multipoint

U ovoj topologiji postoji više konekcija po čvoru. Veza bazne stanice i ostalih čvorova ostvaruje se korišćenjem više čvorova. Kada novi korisnik želi da pristupi mreži, mora biti u dometu bazne stanice i mora posedovati samo opremu koju koriste krajnji korisnici. Ova vrsta konekcije je dobra za backhaul operacije kao što je konekcija na centralnu mrežu. Podaci se prenose sa udaljenog mesta do centralne mreže/backbone. Veza se ostvaruje sa centralnog radio predajnika ka ostatku mreže. Na svakom udaljenom mestu u mreži mora postojati odgovarajuća bežična arhitektura.

Multipoint to Multipoint

Podaci se rutiraju između različitih čvorova do cilja, pa se u tu svrhu formira mesh topologija. U cilju obezbeđivanja maksimalne pokrivenosti i gustine mreže postavlja se veći broj pristupnih rutera, koji obezbeđuju prenos podataka kroz mrežu putem višestrukih skokova [49]. Korisnici mogu pristupiti mreži bilo kad i bilo gde u celoj mesh mreži, bez obzira na to da li će se povezati žično ili bežično.

14. MREŽNO UPRAVLJANJE U WMN

Nadzor i upravljanje mrežom predstavljaju veliki problem za sve vrste mreža. Prilikom razmatranja vezanih za upravljanje mrežom, postavlja se dosta pitanja o načinima na koje možemo zaštititi mrežu od različitih tipova grešaka. Ako želimo da mrežu učinimo operativnijom u smislu performansi i kvaliteta servisa, moramo da razmotrimo sve aspekte upravljanja mrežom još u trenutku njenog projektovanja. U okviru upravljanja mrežom razmotrićemo neke oblasti koje se tiču upravljanja greškama, upravljanja konfiguracijama, upravljanja naložima, upravljanja performansama i upravljanja bezbednošću.

14.1 Upravljanje greškama

Tipični cilj upravljanja greškama je njihova detekcija i odgovor administratora mreže na grešku u mreži. Otklanjanje grešaka može biti izvršeno ručno, od strane administratora, ili procesom za automatsko otklanjanje grešaka. U slučaju ručnog otklanjanja grešaka, potrebno je mnogo više vremena nego u varijanti da to radi proces za automatsko otklanjanje grešaka. Za ručno upravljanje greškama, neophodno je angažovati eksperta za mreže. Kada se radi o velikim mrežama, poželjnije je i efikasnije koristiti automatsko upravljanje greškama. U takvom slučaju, mreža se neprekidno kontroliše, a svaka greška izaziva automatsko pokretanje procedura za njeno otklanjanje. Na taj način se smanjuje vreme reakcije, a mogućnost ljudske greške u potpunosti eliminiše.

U WMN se mogu dogoditi različiti tipovi grešaka. Može se desiti greška u prenosu prouzrokovana velikim kašnjenjem paketa zbog lošeg funkcionisanja klijenata u mreži. Može doći i do prekida napajanja ili do hardverskih kvarova na mesh uređajima u mreži. Zagušenja u protoku mogu prouzrokovati pad mrežnih performansi, a do njih može doći u slučaju da se od linka traži veća propusna moć od one koja se može obezbediti, a sistem to ne prepozna na vreme i ne preduzme odgovarajuće mere da do toga ne dođe. Ovakva greška se najčešće javlja na čvorovima u blizini gateway-a jer kroz njih prolazi većina mrežnih paketa drugih čvorova. Kako je sve ovo teško kontrolisati ljudskim resursima, poželjno je primeniti automatske mehanizme upravljanja greškama.

14.2 Upravljanje konfiguracijom

Glavna uloga upravljanja konfiguracijom je da omogući administratorima mreže da uspešno mogu da prate stanje u njoj. Mrežni menadžeri moraju imati neophodna prava da modifikuju softverske ili hardverske konfiguracije uređaja koji se koriste u mreži.

Upravljanje konfiguracijom se u mreži sprovodi kroz konfigurisanja na raznim nivoima, kao što su konfigurisanje bežičnih gateway-a ili bežičnih pristupnih tačaka.

14.3 Upravljanje nalogima

Administriranje autorizovanih korisnika vrši se uglavnom dodeljivanjem lozinki i odobrenja. Administriranje opreme je nešto osjetljivije i rešava se implementiranjem različitih politika.

14.4 Upravljanje performansama

Cilj upravljanja performansama u mreži je merenje, analiza izveštavanje i upravljanje performansama mrežnih komponenti u širem vremenskom okviru. U toku tog perioda, mrežne performanse se nadziru i analiziraju u skladu sa postavljenim QoS standardima i drugim faktorima kao što su bezbednost i skalabilnost mesh mreže.

14.5 Upravljanje bezbednošću

Glavni cilj upravljanja bezbednošću je upravljanje pristupom korisnika u mreži. Dosta je činilaca koji su uključeni u upravljanje bezbednošću i to će detaljnije biti opisano kasnije u ovom radu.

15. ANALIZA RADIO STANDARDA KOJI SE KORISTE U MESH MREŽAMA

15.1 802.11a

Standard 802.11a radi na frekvenciji od 5GHz. Obezbeđuje prosečni protok podataka od 23Mbit/sec i maksimalni od 54Mbit/sec. Domet mu je oko 40 metara, što je nešto manje nego domet 802.11b sistema. Za radio prenos koristi se OFDM (Orthogonal Frequency Division Multiplexing) standard. Koristi 8 nepreklapajućih kanala i podržava do 64 korisnika po AP [12,13].

15.1.1 802.11a prednosti

U odnosu na druge standarde kao 801.11b, poseduje neke prednosti:

- Brzina prenosa je do 54Mbit/sec, a u Turbo modu ide i do 108 Mbit/sec
- U poređenju sa 802.11b ima veću pokrivenost koja proizilazi iz većeg broja mogućih AP, pa samim tim podržava i veći broj korisnika.

15.1.2 Bezbednost i upotreba 802.11a

U 802.11a koristi se WEP algoritam za enkripciju. Zbog svoje slabosti ne koristi se za prenos kritičnih podataka. Najčešće se primenjuje na mestima gde se traži veća propusna moć npr. u konferencijskim halama. Nije direktno kompatibilan sa drugim standardima kao što su 802.11b ili 802.11g. Za njihovo međusobno povezivanje neophodno je koristiti rutere. Ima kraći domet i ima slabije penetracione mogućnosti u zatvorenim prostorima[52].

15.2 802.11b

Ovaj standard ja na tržištu široko rasprostranjen. Radi na frekvenciji od 2.4GHz i ima propusnu moć oko 4.5 Mbit/sec. Koristi se najčešće u situacijama kada je potrebno nešto brzo razmeniti (npr. neke kraće fajlove). U praksi, sa mnogo manje AP u odnosu na 802.11a, pokriva se isti prostor. Koristi se na aerodromima, ugostiteljskim objektima i hotelima. Modulaciona tehnika koja se koristi je Direct Sequence Spread Spectrum (DSSS). Koristi 3 nepreklapajuća kanala sa čime se može opslužiti do 32 korisnika po AP [52].

15.2.1 802.11b prednosti

Ima dosta prednosti u odnosu na ostale protokole. Neke od njih su:

- Cenovno je najprihvatljiviji u odnosu na druge (cene AP i rutera),
- Može da radi u dual-band režimu kao 802.11g. Oprema različitih proizvođača međusobno je kompatibilna.
- Domet je od 40 do 500 metara na otvorenom prostoru. Zbog manje potrošnje energije, klijentski uređaji mogu duže da rade.

15.2.2 Bezbednost i upotreba 802.11b

I ovaj standard koristi WEP algoritam. Omogućava korišćenje 48, 64 i 128-bitne enkripcije. Obezbeđuje veći domet na otvorenom i u zatvorenom prostoru u odnosu na 802.11a protokol. Idealan je za korišćenje u kancelarijskim uslovima, za prenos fajlova, povezivanje na bežične štampače i razmenu e-mail-a. Zbog slabe enkripcije nije preporučljivo koristiti ga u sredinama gde je privatnost podataka bitan faktor. U tim slučajevima, neophodno je koristiti 802.11b uređaje koji podržavaju 802.1x autentifikaciju [52].

15.3 802.11g

Ovaj standard predstavlja proširenje 802.11b standarda. Radi na 2.4GHz i tipičan protok mu je 19Mbit/sec dok je maksimalan protok 54Mbit/sec. Modulaciona tehnika koja se koristi u ovom standardu je OFDM. 802.11g uređaji su kompatibilni sa 802.11b uređajima pa se međusobno mogu povezati (ali samo u „b“ modu). Posедуje nepreklapajuće kanale [51].

15.3.1 802.11b prednosti

Standard 802.11g ima nekoliko prednosti:

- Maksimalnu propusnu moć do 54 Mbit/sec
- Kompatibilan je sa 802.11b uređajima
- Ima redukovanu potrošnju električne energije
- Efikasniji je za upotrebu i pokriva veću zonu u odnosu na uređaje koji rade na 5GHz
- Može se koristiti i na otvorenom i u zatvorenom prostoru

15.3.2 Bezbednost i upotreba 802.11g

Kao i 802.11b i ovaj standard poseduje mogućnost WEP enkripcije, ali se ona u nekim ozbiljnijim primenama ne koristi. Pored nje, standard 802.11g uvodi i WPA (Wi-Fi Protected Access) i WPA2 enkripcije koje koriste 256-bitne AES algoritme za enkripciju. Brži je od 802.11b standarda pa se više koristi tamo gde je neophodan veći propusni opseg. Manje je cene koštanja od 802.11a standarda i sa njim nije kompatibilan. Oba standarda se mogu koristiti u istoj mreži i pristupati jedan drugome posredstvom rutera [52].

15.4 802.11n

Glavni cilj uvođenja standarda 802.11n je je obezbeđivanje većeg kvaliteta servisa. On predstavlja prvi standard koji podržava frekventne opsege od 5GHz i od 2.4GHz. Tipičan protok koji obezbeđuje ovaj standard je 74Mbit/sec, a maksimalan do 600 Mbit/sec. Domet ovog standarda je oko 80 metara. U svojoj osnovi koristi MIMO tehnologiju, što znači da se za vreme prenosa koriste višestruki strimovi. Povećavanje propusnog opsega realizovano je kroz povećanje stope modulacije, redukovanje nepotrebnih podataka i povećanje veličine komunikacionog kanala, što je jedna od najvećih promena u mreži. Standard 802.11n je unazad kompatibilan sa 802.11a,b,g [56].

15.4.1 802.11n prednosti

Prednosti standarda 802.11n ogledaju se u sledećem:

- Brzina prenosa do 600Mbit/s
- Povećana otpornost na smetnje
- Povećana bezbednost zbog upotrebe WPA2 standarda i AES enkripcije

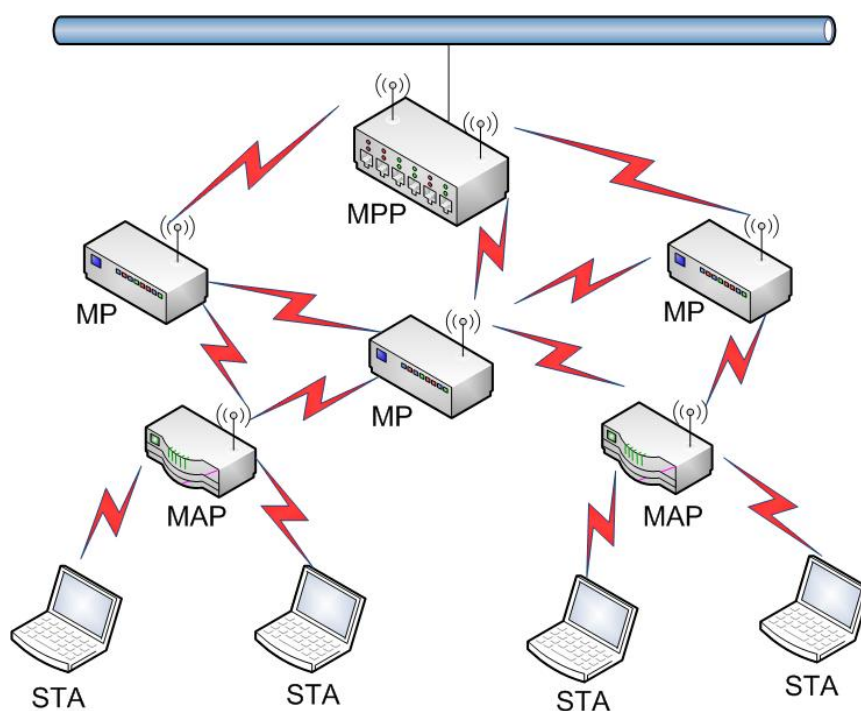
15.4.2 Bezbednost i upotreba 802.11n

Upotreba WPA2 standarda i AES enkripcije povećava bezbednost podataka koji se prenose. Upotreba enkripcije se nameće sama po sebi, jer je jedino tada moguće koristiti uređaje sa maksimalnih 600Mbit/s. Bez upotrebe enkripcije, uređaji rade na brzinama do 54Mbit/s. Koristi se u svim aplikacijama koje zahtevaju prenos velike količine podataka. Kompatibilnost sa prethodnim generacijama omogućava postepeno znavljanje opreme. Prilikom korišćenja radnih frekvencija od 5GHz, smanjene su penetracione mogućnosti radio signala.

16. ANALIZA STANDARDA 802.11s

16.1 802.11s Topologija

Standard 802.11s razvijen je sa ciljem kreiranja bežičnog distributivnog sistema sa automatskim učenjem topologije i konfiguracijom putanja. Navedeni standard definiše načine na koje se bežični uređaji međusobno povezuju u cilju formiranja ad-hoc mreže. U okviru njega, moguće je izgraditi male, srednje i velike mesh mreže. 802.11s omogućava dinamičku selekciju najboljeg komunikacionog radio kanala u mesh mreži koji obezbeđuje kvalitetan prenos signala preko jedne ili više povezanih putanja. Ovaj standard je lako proširiv u cilju prilagođavanja i podrške različitim aplikacijama i budućim inovacijama. U cilju zaštite podataka koji se prenose, koristi 802.11 i mehanizme zaštite.



Slika 15: 802.11s frameworks

16.1.1 Mesh portal (MPP)

Mesh portal je tačka na kojoj se nalaze jedinice MAC data servisa (MSDUs – MAC Service Data Unit).

16.1.2 Mesh Point (MP)

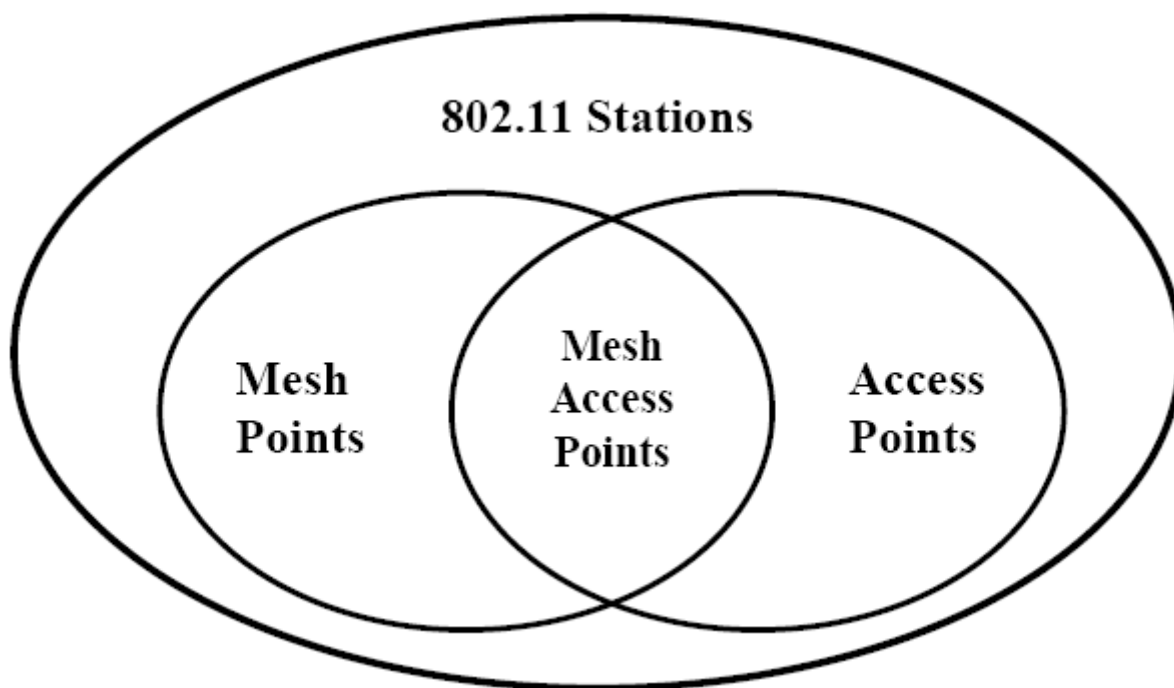
Mesh point uspostavlja vezu sa susednim MP i na taj način obezbeđuju Mesh servise u mreži.

16.1.3 Mesh AP (MAP)

Funkcionalnost MP se obezbeđuje preko MAP. Mesh AP imaju ulogu da omoguće povezivanje klijenata (Station – STA) na mesh mrežu.

16.1.4 Station (STA)

Stanice su tačke izvan bežične Mesh mreže i na nju se povezuju preko Mesh AP.



Slika 16 802.11s topologija

U bežičnim meš mrežama MP samostalno otkrivaju susedne tačke sa kojima mogu ostvariti konekciju. U cilju podrške za jednokanalni odnosno višekanalni mesh, svaki MP može imati jedan ili više logičkih radio interfejsa. Mesh mreže imaju širok spektar protokola za izbor putanje koje proizvođači mogu koristiti po svom izboru. Pojedinačni

mesh može imati samo jedan aktivan protokol u jednom trenutku i samo jedan protokol može biti aktivan u pojedinačnom linku istovremeno. Mesh Points međusobno razmenjuju podatke o protokolima koje koriste. U slučaju kada se u mrežu uključuju novi MP, postojeći MP ne moraju menjati protokole koje već koriste.

16.2 Bezbednost u 802.11s

Kako MP nisu striktno vezani jedni za druge, među njima ne postoji jasno definisana unutrašnja hijerarhija. Da bi sa obezbedila bezbedna komunikacija, MP moraju da održavaju zaštićene linkove sa ostalim MP.

17. BEZBEDNOST U BEŽIČNIM MESH MREŽAMA

Kada govorimo o bežičnim mesh mrežama, ne smemo ignorisati njihove potencijale kao ni bezbednosne rizike. Zbog dinamičke promene mrežne topologije, distribuirane mrežne arhitekture i deljenja bežičnog spojnog puta, korišćenje WMN nosi sa sobom i određene bezbednosne rizike. Napadi se mogu javiti na različitim slojevima protokola što može ugroziti saobraćaj i podatke koji se prenose kroz mrežu. U WMN se koriste različiti tipovi arhitektura sa različitim pristupima bežičnoj mesh bezbednosti [53].

17.1 Osnovna prevencija

Primarni faktori koji utiču na zaštitu privatnosti su poverljivost podataka i poverljivost saobraćaja.

17.1.1 Poverljivost podataka

Glavna uloga mu je da zaštititi podatke od presretanja i napada. Kontrolisana je od strane mesh rutera. Način na koji se štite podaci je kriptovanjem poruka.

17.1.2 Poverljivost saobraćaja

Poverljivost saobraćaja je, uzimajući u obzir moguće napade, veoma teško obezbediti. Da bi se obezbedila, korisnici moraju znati sa kime komuniciraju. Napadi se najčešće dešavaju na samim mesh ruterima, u toku prenosa podataka. Upotrebom različitih mehanizama za distribuciju ključeva WMN mogu prevazići ovu vrstu napada [54].

17.2 Mesh bezbednost

Standard 802.11s će se u budućnosti koristiti u svim vrstama komercijalnih mesh proizvoda. Mesh proizvodi trenutno imaju različite pristupe bezbednosti a mnogi od njih su izvedeni iz postojećih ad-hoc mehanizama zaštite. 802.11s je standard koji će se primarno bazirati na 802.11i bezbednosnim mehanizmima.

U bilo kojoj primeni, bezbednosni ciljevi su osnovni ciljevi koji se moraju razmotriti da bi se prevazišao problem zaštite. Ovi ciljevi nisu specifični za svaku posebnu aplikaciju. U WMN primeni postoje iste pretnje koje se sreću i u klasičnim žičnim i bežičnim

mrežama. Napadač može presresti, izmeniti, odložiti, ili ponoviti poruku. Napadač može čak i ubaciti novu poruku u mrežu.

17.2.1 Poverljivost

U toku komunikacije, kompletan prenosni put mora biti zaštićen da bi se onemogućilo namerno menjanje poruke u toku prenosa. Da bi sigurna komunikacija bila moguća korisnici se moraju međusobno poznavati. Poruka se ni na koji način ne sme učiniti dostupnom trećim licima. Pravi podaci će biti dostupni jedino ciljanim korisnicima.

17.2.2 Dostupnost

Neophodno je osigurati da autorizovani korisnici mogu da obavljaju bezbednu komunikaciju uz pouzdanu isporuku poruka do krajnjeg odredišta, kao i zaštititi poruke i podatke od DoS (Denial of Service).

17.2.3 Autentikacija

Zbog promena spojnih puteva koji se u WMN često dešavaju, autentifikacija je veoma važna. Za slanje i prijem podataka se zbog toga moraju koristiti adekvatni mehanizmi. Ako se korisnici toga ne budu pridržavali, lako može doći do narušavanja pouzdanog prenosa podataka inficiranjem poruka ili fabrikovanjem novih od strane trećih lica, što može izazvati probleme u mrežnom prenosu.

17.2.4 Autorizacija

Korisnici imaju pravo da menjaju podatke. Ako neko želi da izvrši određeni zadatak, mora postojati odgovarajući mehanizam koji će garantovati da taj korisnik ima pravo da isti zadatak i izvrši.

17.2.5 Merenje

U slučaju da korisnik koristi bilo koji servis, mora postojati i određeni mehanizam koji će izvršiti merenje iskorišćenih resursa u cilju kasnije naplate.

17.2.6 Integritet

Korisnik ne može menjati podatke ako nema odgovarajuća prava da to izvrši. Ako korisnik ne poseduje prava da obavi bilo koji zadatak, onda i ne može modifikovati poruku.

17.2.7 Kontrola pristupa

Korisnicima se mora obezbediti da mogu da izvršavaju samo one zadatke za koje imaju odobrenje. Ako određeni korisnik hoće da promeni poruku a nema ovlašćenje za to, mora da traži odobrenje od administratora.

17.3 Bezbednosni izazovi

Zbog svojih dinamičkih promena WMN obiluju raznim bezbednosnim izazovima. Fizičko obezbeđenje pristupnih tačaka samo po sebi predstavlja problem koji se mora razmatrati jer može prouzrokovati probleme u funkcionisanju same mreže. Veliki izazov predstavlja i multi-hop mrežna komunikacija, na koju administrator ne može primeniti statičku zaštitu zbog velikog broja korisnika koji se često pridružuju mesh mreži i napuštaju je. Čak se ista konfiguracija ne može primeniti ni na mesh ruterima i mesh klijentima zbog dosta njihovh različitih karakteristika (mobilnost, napajanje,...) [57].

17.4 Pregled potencijalnih napada

U WMN su karkteristične dve vrste napada:

- Spoljašnji napadi
- Napadi iz mreže

Spoljašnji napadi

Napadač može da ometa komunikaciju u mreži. Napadač koji ne pripada mesh mreži može da ubaci određene informacije u mrežu. Aktivni napadi mogu da omoguće napadaču da modifikuje i ubaci poruku u mesh mrežu.

Napadi iz mreže

Napadi iz mreže su najteže vrste ugrožavanja bezbednosti mreže. Uglavnom potiču od kompromitovanih pristupnih tačaka u okviru same mesh mreže. Zaštita od ove vrste napada ni blizu nije tako laka ako se poredi sa spoljašnjim napadima jer napadač može presresti komunikaciju i ubaciti svoju poruku u mrežu.

U različitim slojevima mreže se mogu sresti različite vrste napada. Na fizičkom nivou napadač može oštetiti hardver mreže, ili može ometati prenos i na taj način preuzeti pristupnu tačku. Ovakva vrsta napada se najlakše otkriva i locira. Na MAC nivou, napadač može izmeniti protokole za komunikaciju. Na nivou rutiranja, napadač može izmeniti tabele rutiranja što će onemogućiti pravilno funkcionisanje mreže. Ako pristupi ovom nivou, napadač može i da izbegne protokole za rutiranje i da pristupi čvorovima do kojih inače ne bi smeo da dođe. U aplikativnom sloju napadač može ubacivati lažne podatke [57].

17.4.1 Flooding napad

Kao što je već rečeno, napadač može slati MAC kontrolne poruke susednom čvoru i učiniti ga nedostupnim za ostale (DoS napad). Na ovaj način pored propusne moći kanala utiče i na pražnjenje baterije ako se radi o mobilnom klijentu.

17.4.2 Ometanje

Ova vrsta napada direktno utiče na performanse bežične mreže. Poznata je i kao DoS napad na čvorovima, jer ometa njihovu međusobnu komunikaciju.

17.4.3 Napadi usmereni ka onemogućavanju uštede energije i ispuštanju paketa (Sleep Deprivation and Packet Dropping Attacks)

Ovim napadima se degradira baterija napadnutog čvora čime se on nakon nekog vremena izbacuje iz funkcije. Ako se saobraćaj obavlja preko ovog čvora, njegovo ispadanje iz mreže će usloviti i gubljenje pojedinih paketa.

17.4.4 Napadi na rutiranje

Postoje mnogobrojni napadi koji utiču na rutiranje paketa. Neki koji su specifični za mesh mreže su:

17.4.4.1 *Napad „Crna rupa“*

Napadač kreira lažne pakete koji koriste lažne rute. Ove lažne rute se korisnicima predstavljaju kao kvalitetne rute sa najmanjim brojem koraka pa ih klijentski čvorovi koriste za prenos paketa. Paketi koji se šalju na ovaj način ne stižu do ciljanog čvora.

17.4.4.2 *Napad „Siva rupa“*

Ovaj napad je sličan kao i prethodni s tom razlikom što je usmeren na konkretan čvor čije rute i saobraćaj uništava.

17.4.4.3 *Ubacivanje greške u rutama*

Mesh linkovi se mogu prekinuti ubacivanjem lažnih ruta. Ovo je vrlo ozbiljan napad koji direktno narušava funkcionisanje mesh mreže.

17.5 Zaštita od pretnji i napada

Zaštita WMN od pretnji i napada može se obezbediti po centralizovanom i decentralizovanom modelu.

17.5.1 Centralizovani modeli

Prednost centralizovanog modela zaštite u odnosu na korisnike je da im omogućava lako korišćenje WMN, ali se sa druge strane veoma oslanja na servere. Ovo ceo sistem čini ranjivim na DoS ili slične napade koji kompromitacijom servera mogu celu mrežu izbaciti iz upotrebe.

17.5.1.1 *Kerberos*

Kerberos je centralizovani autentifikacioni servis koji korisnicima odobrava pristup resursima po tzv. "ticket-based" algoritmu. Transparentnost ovog servisa zagarantovana je obaveznom autentifikacijom i korisnika i servera prilikom svakog zahteva. Jednostavnost autentifikacije ga čini veoma efikasnim mehanizmom zaštite.

17.5.1.2 *Standard X.509*

Standard X.509 dozvoljava kreiranje sertifikata sa propisanim parametrima koji korisnika povezuju sa javnim ključem. Ovim standardom je takođe obezbeđen i opoziv sertifikata kojim se onemogućava povezivanje korisnika sa javnim ključem. Princip na kome se bazira sertifikacija je postojanje višeg autoriteta koji garantuje ispravnost javnog ključa korisnika. Sam sertifikat se potpisuje od strane autorizacionog tela što može kasnije biti autentifikovano od strane svih korisnika. Ovaj mehanizam se već pokazao kao vrlo pouzdan u WWW okruženju.

17.5.2 Decentralizovani modeli

U decentralizovanim modelima najveći nedostaci su nepostojanje autoriteta za autentifikaciju / sertifikaciju koji bi procenili kredibilitet korisnika i koji bi po potrebi mogli da oduzmu sertifikat ili stave korisnika na crnu listu.

PGP je besplatan mehanizam zaštite koji se najčešće koristi u aplikacijama za e-mail razmenu i skladištenje datoteka. Kombinacija algoritama i kriptografskih funkcija, čini ga jednim od najboljih izbora zbog sopstvene otpornosti, jednostavnosti korišćenja i široke rasprostranjenosti. PGP je decentralizovani sistem u kome korisnici imaju više parova tajnih i javnih ključeva. Informacije se šalju kriptovane sesijskim ključem koji se koristi samo jednom. Sesijski ključ se šalje kriptovan javnim ključem primaoca. PGP takođe omogućava i proveru integriteta i autentičnosti poruke. Uklanjanje javnog ključa obično vrši vlasnik ključa u slučaju kada je isti kompromitovan. Korisnik zahteva uklanjanje ključa sertifikatom potpisanim sa sopstvenim tajnim ključem.

Zbog potpuno decentralizovane strukture WMN i njihove sposobnosti samoorganizovanja gde svaki čvor ima jednaku ulogu, potrebno je obezbediti i mehanizme zaštite prilagođene ovom okruženju. Po ugledu na PGP, svaki čvor u WMN emituje sopstvene sertifikate i poseduje listu proverenih javnih ključeva ostalih čvorova.

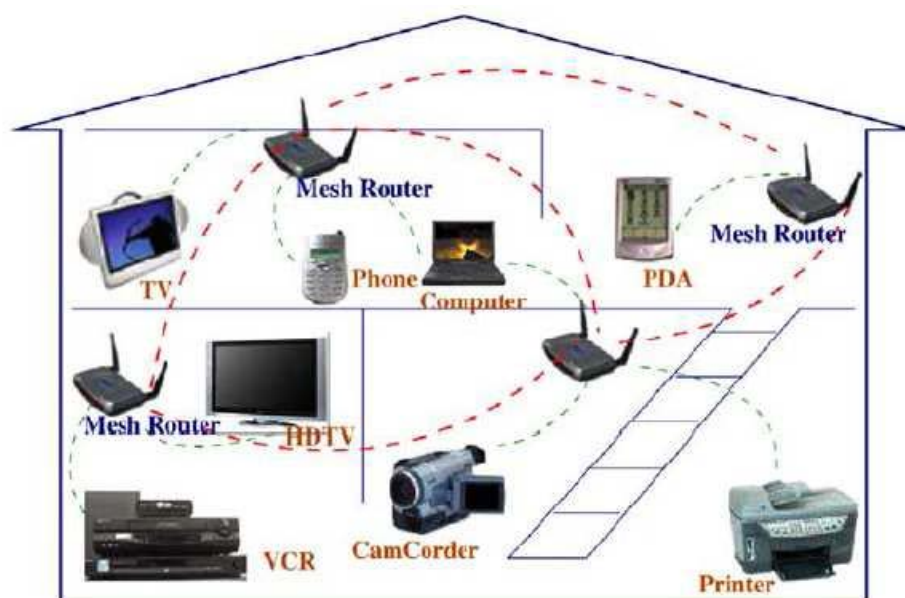
Svojstva PGP mehanizma obezbeđuju izbalansiran set kriptografskih funkcija i omogućavaju odličnu zaštitu uz očuvanje efikasnosti i efektivnosti mesh mreža. Navedeni protokol poseduje sve karakteristike dobrog mehanizma zaštite koji može rešiti problem decentralizovanog deljenja ključeva.

U odnosu na centralizovani model, upotreba decentralizovanog modela iziskuje više napora u samoj implementaciji, ali garantuje redundantnost zaštite, koja je u WMN od velikog značaja.

18. PRIMENA BEŽIČNIH MESH MREŽA

18.1 Širokopojasna kućna mreža

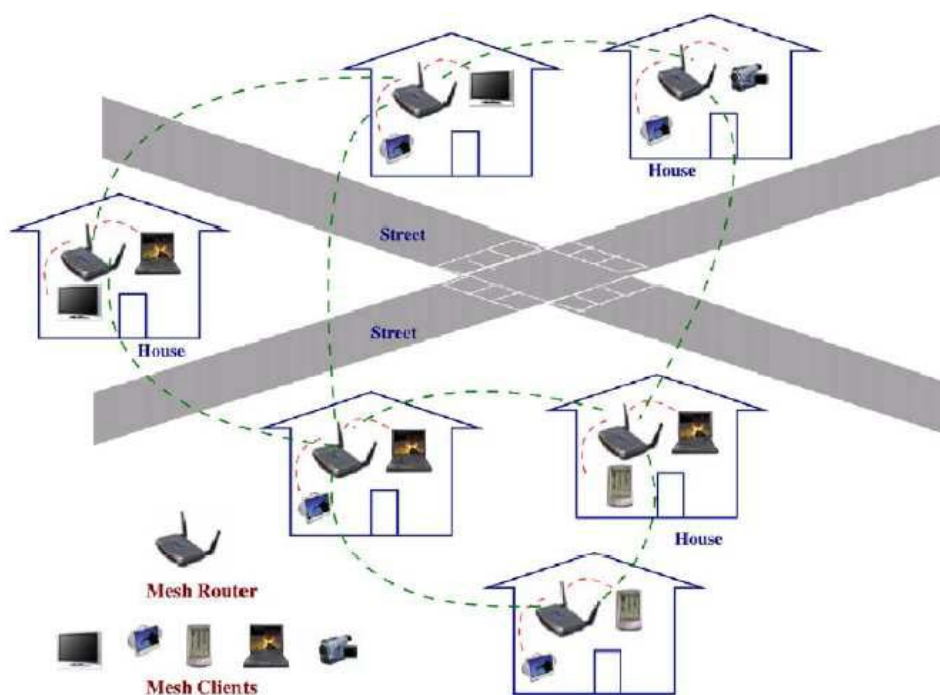
Kućno mrežavanje je najčešće izvedeno primenom IEEE802.11 WLAN standarda. Instaliranje više AP kako bi se pokrio ceo objekat je skupo i nepraktično, jer se svaki AP mora žičano povezati na backhaul uređaje. I tada se može desiti da u objektu postoje mrtve zone u kojima nema signala. U slučaju kada postoje dva AP, komunikacija između njihovih krajnjih čvorova mora proći preko oba AP i sviča sa kojim su povezani, što nije efikasno, naročito za širokopojasni internet. Mesh umrežavanje efikasno rešava navedeni problem jer krajnji čvorovi komuniciraju međusobno koristeći najkraći spojni put i nije potrebno uvoditi dodatnu kablaju [55].



Slika 17: Širokopojasna kućna mreža

18.2 Umrežavanje zajednice

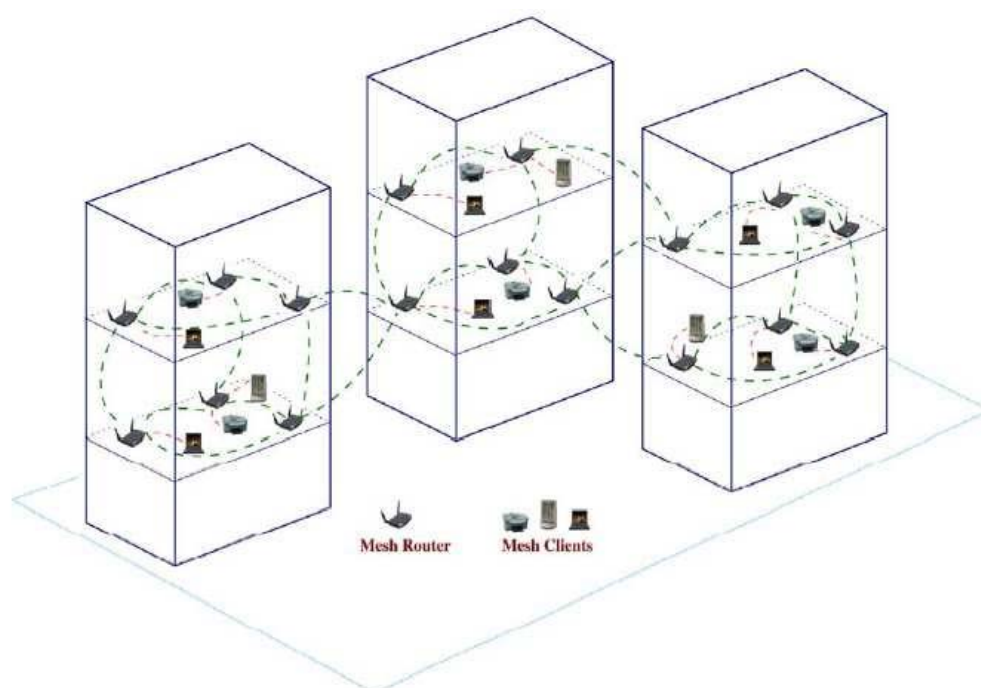
Umrežavanje susednih objekata u jednoj zajednici prilično je teško na konvencionalan način zbog njihove uobičajene mrežne arhitekture koja je povezana na internet kablovskim ili DSL modemom. Krajnja tačka u ovoj mreži je bežični ruter koji je povezan sa navedenim modemima. Ovakav način povezivanja ima nekoliko nedostataka. Nepotrebno se koriste resursi za deljenje informacija između članova zajednice jer je jedini način da se to učini preko interneta. U takvom okruženju veoma je teško podesiti deljenje resursa. Za komunikaciju sa susednim objektom postoji samo jedna putanja, preko interneta. WMN mogu prevazići ove probleme i obezbediti servise kao što su distribuirano čuvanje podataka, distribuirani pristup podacima i video streaming [21,22].



Slika 18: Umrežavanje u zajednici

18.3 Poslovno umrežavanje

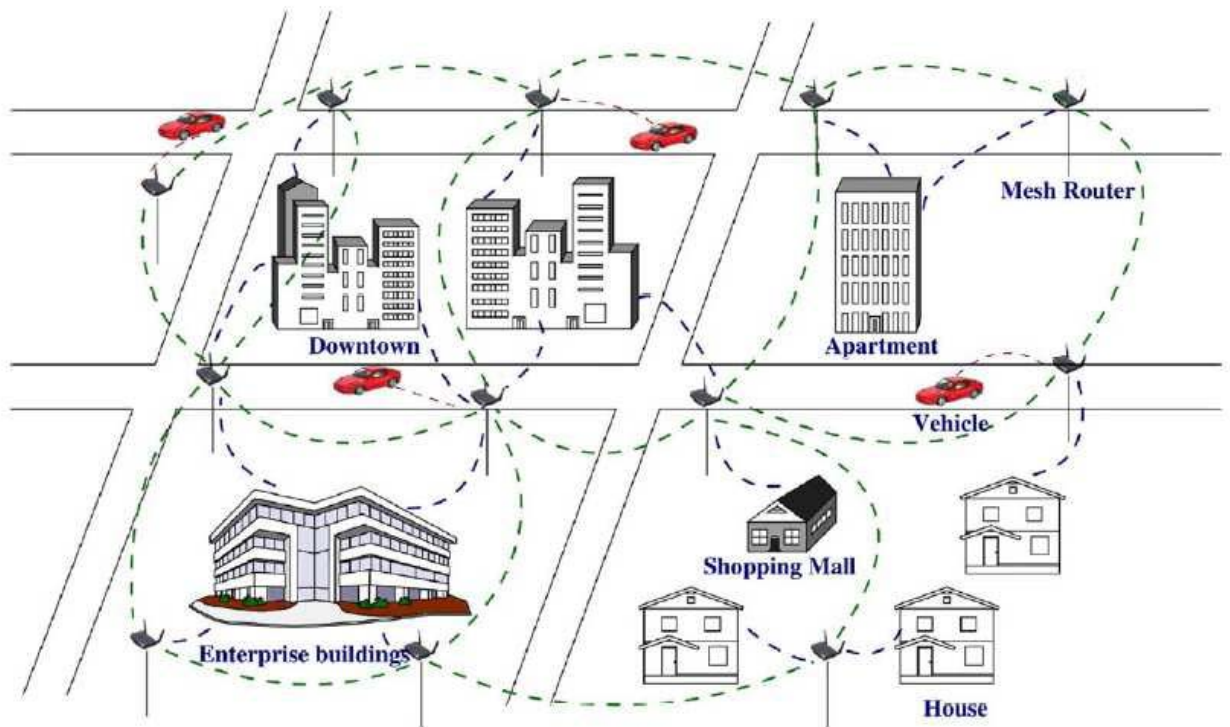
Trenutno se na mnogim mestima kao što su kancelarije ili poslovne zgrade, koristi IEEE802.11 WLAN. U kancelarijama se uređaji najčešće umrežavaju žično, što često može biti vrlo skupo. Da bi se povećao propusni opseg, lokalno se moraju dodavati backhaul modemima. U slučaju gubitka linka, ne postoji rezervno rešenje. Često u ovakvim okruženjima može doći do zagušenja mreže. Bežične mesh mreže pružaju pristup mnogobrojnim backhaul modemima koje mogu koristiti svi čvorovi u mreži [56]. Prednost korišćenja WMN je i skalabilnost jer se one mogu i proširivati i prilagođavati potrebama preduzeća.



Slika 19 Poslovno umrežavanje

18.4 Gradske mreže (Metropolitan Area Networks – MAN)

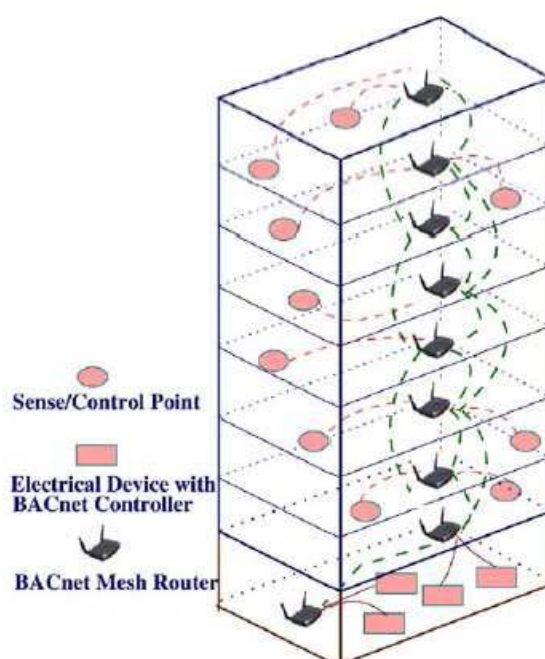
Obezbeđuje veće brzine prenosa kada se poredi sa drugim mrežama kao što je mreža mobilne telefonije. Komunikacija između čvorova u WMN se ne zasniva na žičnoj okosnici. Ekonomski gledano, nerazvijenim regionima predstavlja najbolju alternativu za širokopojasno umrežavanje. Sa bežičnim mesh MAN može se pokriti široko područje.



Slika 20: Gradska mreža

18.5 Automatizacija zgrada

Upravljanje i nadzor su kritična pitanja u svim oblastima. Kako administrator zgrade želi da nadzire i kontroliše rad liftova, klima uređaja i sl., potreban mu je bolji sistem upravljanja. Bežične mesh mreže mu prožaju tu mogućnost po mnogo manjoj ceni nego što bi to bilo primenom žičnih mreža i WIFI sistema. U mnogim zgradama je i dalje u upotrebi žični sistem mreža. Wi-Fi mreže su ekonomski isplativije od žičnih ali im performanse i cena nisu zadovoljavajuće u poređenju sa mesh mrežama. Lakoća uspostavljanja konekcija između čvorova čini ih mnogo jednostavnijim za primenu od ostalih tipova mreža [58].



Slika 21: Automatizacija zgrade

18.6 Medicinski sistemi

Bežične mesh mreže predstavljaju dobro rešenje za nadzor i upravljanje aktivnostima u medicinskim centrima i bolnicama. Prosleđivanje informacija od sobe do sobe mora stalno biti nadgledano i kontrolisano. U većini zdravstvenih centara još uvek se koristi žična mreža što umnogome ograničava pristup mreži i povećava cenu koštanja sistema [57].

18.7 Mreže za obezbeđivanje komunikacija u zonama pogođenim elementarnim nepogodama

Glavni izazov koji se javlja u situacijama nastalim razaranjima usled elementarnih nepogoda svakako je obezbeđivanje uslova za međusobne komunikacije ljudi na toj teritoriji kao i njihovu vezu prema spoljnom svetu. U takvim situacijama, oslanjanje na infrastrukturu telekomunikacionih provajdera najčešće je nemoguće. Mesh mreže se ovde same nameću kao jedno od rešenja prihvatljivog za širu populaciju ljudi, jer se mogu osloniti na već postojeću tehnologiju. Široka rasprostranjenost smart uređaja zasnovanih na android operativnom sistemu, njihova sve veća procesorska snaga kao i prodor na tržišta sa niskim nivoom primanja, uticali su na razvoj aplikacija koje su oslobođene zavisnosti od telekomunikacione infrastrukture i troškova a omogućavaju međusobnu komunikaciju njihovim korisnicima. Značajna je i činjenica da su korisnici već upoznati sa radom na svojim smart uređajima što im u kriznim situacijama mnogostruko olakšava rukovanje sa navedenim aplikacijama. Jedan od projekata koji se svojom ozbiljnošću izdvojio od ostalih je Serval Mesh Project [59].

Smart uređaji uglavnom nude tri tipa radio tehnologija za međusobnu direktnu komunikaciju. To su multi-band cellular, Bluetooth i Wi-Fi. Celularni radio je praktično nemoguće reprogramirati zbog toga što proizvođači čip setova takve informacije najstrožije čuvaju. Bluetooth je veoma ograničenog dometa pa stoga nije pogodan za ovaj vid komunikacija. Zbog svega navedenog, Wi-Fi se nameće kao najpogodnija opcija za rešenje problema. Ovome naočito ide u prilog i činjenica da danas većina smart uređaja ima opciju da funkcioniše i kao Wi-Fi Access Point (AP), što im omogućava da međusobno komuniciraju bez oslanjanja na bilo koju drugu infrastrukturu.

Smenjivanjem Wi-Fi modova rada između AP i klijentskog, uz korišćenje odgovarajućih protokola, moguće je dozvoliti smart uređajima da međusobno dele podatke, čak iako nisu u direktnoj vezi i čak iako su samo povremeno u vezi sa bilo kojim drugim smart uređajem [60]. Spomenuti softverski projekat se fokusira upravo na formiranje mesh mreže korišćenjem Wi-Fi u AP i klijentskom modu, pod uslovom da ne postoji bolja alternativa.

Wi-Fi takođe nudi i treći mod rada, ad-hoc mod, koji omogućava direktnu komunikaciju između smart uređaja koji ga podržavaju. Veoma mali broj uređaja podržava ovaj mod rada, dok je na određenom broju drugih neophodan „rooting“, „jailbreaking“ ili instaliranje prepravljenog operativnog sistema.

Projekat Serval je open-source mesh komunikaciona platforma nastala posle zemljotresa na Haitiu 2010. godine. Sa misijom „komunikacija bilo gde i bilo kada“, nastao je na pretpostavci nepostojanja bilo kakve komunikacione infrastrukture.

Serval Mesh softver omogućava smart telefonima da izgrade samoorganizovanu mesh mrežu koristeći Wi-Fi u AP i klijent modu, uz odgovarajuće protokole. Napravljen je da bude jednostavan za korišćenje svim korisnicima. Kompleksan proces alociranja mrežnih

adresa rešen je potpuno transparentno, tako da ni na koji način ne opterećuje korisnike, što ga čini upotrebljivim i korisnicima sa niskim nivoom tehničkog znanja. Kada se aplikacija jednom instalira na telefon, ona sama nudi i drugim telefonima u bliskom okruženju da je preuzmu i instaliraju, što je veoma bitno u kriznim situacijama kada je pristup internetu praktično nemoguć.

Aplikacija poseduje mogućnosti da ostvaruje glasovne komunikacije sa drugim korisnicima u mesh mreži, šalje i prima SMS poruke, distribuira, deli i razmenjuje fajlove, uključujući i unapređenja sopstvenog koda. U sebi integriše i GIS aplikaciju koja razmenjuje mape i tačke interesa sa ostalim korisnicima. Svaka od navedenih komponenti podržana je robusnim sigurnosnim mehanizmima koji nude jaku zaštitu privatnih komunikacija.

Serval Project koristi Diffie-Hellman protokole za razmenu ključeva između učesnika u komunikaciji, što je u osnovi mnogo bolja zaštita od one koju koriste celularne mreže. Komunikacija se dalje isključivo enkriptuje 256 bitnim Elliptic Curve Cryptography (ECC) Curve25519 kriptografskim sistemom, što im omogućava da budu propisno zaštićene, autentifikovane i potpisane.

Problem koji je evidentan u ovakvim mrežama, a koji je direktna posledica tehničkih mogućnosti Wi-Fi mreža je domet koji je u urbanim sredinama ograničen na oko 60m. U kriznim situacijama to može predstavljati problem. Rešenje problema je upotreba Serval Mesh ekstendera sa sopstvenim baterijskim napajanjem koji poseduju i Wi-Fi i UHF paketski radio u ISM opsegu. Navedene uređaje moguće je na krizna područja ubacivati iz vazduha. Wi-Fi mreža im omogućava uvezivanje sa korisnicima u zoni dometa, dok preko UHF radija ostvaruju konekciju sa drugim mesh ekstenderima. Uz optičku vidljivost između dva ekstendera, domet je 3 i više kilometara, dok je u gusto naseljenim mestima preko 300 metara. Dometi su postignuti uz upotrebu omnidirekcionih antena. Mala cena koštanja ovih ekstendera i sposobnost samoorganizovanja mreže omogućavaju njihovu brzu i masovnu upotrebu. Krajnji ekstenderi se mogu uvezati na druge vrste mreža (Internet, lokalne mreže kriznih službi,...) što korisnicima omogućava komunikaciju i van sopstvene mesh mreže.

19. ZAKLJUČAK

U ovom radu razmotrili smo implikacije razvoja bežičnih oblaka i potencijalne bezbednosne pretnje koje iz njega proističu kroz konceptualni model bežične cloud arhitekture, identifikaciju potencijalnih ranjivosti u bežičnom oblaku, prepoznavanje bezbednosnih rešenja za bežični oblak i razmatranje pitanja politike ovlašćenja.

Prelaz na bežičnu cloud arhitekturu potencijalno bi mogao da zadovolji potrebe i očekivanja poslovnih korisnika. Kao deo tranzicije organizacija na bežičnu cloud strukturu, biće važno da mogu da procene potencijalnu isplativost i da budu sigurni da se njihova IT sredstva mudro koriste. Pozitivan povraćaj uložениh investicija će verovatno biti izveden iz smanjenja operativnih troškova koji proističu iz deljenja infrastrukture i resursa (npr. hardverskih i softverskih troškova, ljudskih resursa, itd.). Kritičan uslov za uspeh tranzicije na bežičnu cloud arhitekturu je sposobnost cloud provajdera da obezbede kontinuitet zaštite podataka svojim klijentima. Cloud provajderi moraju istražiti nove mehanizme zaštite podataka u cilju obezbeđivanja privatnosti podataka, bezbednosti resursa i autorskih prava sadržaja. Korisnici bežičnih oblaka suočiće se sa jedinstvenim izazovima, ne samo u zadovoljavanju bezbednosnih imperativa već i imperativa privatnosti. Privatnost u bežičnom oblaku podrazumeva ugovorna i zakonska prava pojedinaca da kontrolišu sopstvene informacije, uključujući i odluke o podnošenju, korišćenju, objavljivanju i zaštiti podataka.

Korisnici bežičnih oblaka moraju da shvate da će njihovo korišćenje promeniti način na koji oni definišu bezbednosne granice svog sistema. Njihove potrebe za zaštitom moraju da se rešavaju na nivou zaštite informacija da bi obezbedili da njihova obrada, skladištenje, prenosni sistemi i aplikacije u cloudu rade isto tako efektivno i efikasno kao i njihovi pandami u tradicionalnim mrežnim okruženjima. Ovo posebno važi za obezbeđivanje kontinuiteta kritičnih procesa i operacija.

Uprkos izazovima koje bežični oblak nosi sa sobom, nijedan od bezbednosnih uslova prikazanih u ovom tekstu nije potpuno nov. Dalja istraživanja u sferi bezbednosti bežičnog oblaka moraju biti usklađena sa bezbednosnom arhitekturom, politikom, upravljanjem, upravljanjem rizikom i ublažavanjem rizika. Uspešna i sigurna migracija na bežični oblak zahtevaće razumevanje tehnologija oblaka i bežičnih mreža i kreiranje zvaničnih politika u cilju usvajanja sveobuhvatne metodologije tranzicije i unapređenja saradnje između cloud provajdera, stručnjaka za bežične mreže, zajednice i bezbednosnih stručnjaka za bežično umrežavanje.

Kritična stvar za uspeh bežičnih oblaka biće spoznaja mogućnosti koje pruža integracija cloud computing-a i bežičnih grid mreža. Buduća područja istraživanja vezana za usklađivanja ovog tipa arhitekture uključuju rešavanje sledećih problema :

- Koja svojstva bežičnog cloud-a mogu predstavljati najveće bezbednosne izazove?
- Kako podeliti bezbednosnu odgovornost između cloud provajdera i projekatnata bežičnih grid mreža?

- Kako se menja izloženost pretnjama prilikom korišćenja bežičnog cloud-a?
- Koja svojstva bežičnog cloud-a predstavljaju najveće bezbednosno unapređenje?
- Koji su to mehanizmi bezbednosne kontrole koje treba očekivati u bežičnom cloud-u?

Za stvaranje poverenja u implementaciji bežičnog cloud-a, neophodno je postojanje mogućnosti da se nadgledaju i kontrolišu svi aspekti arhitekture, kao i da se njima upravlja, uključujući i mogućnost praćenja bezbednosnih problema sve do mesta njihovog nastanka. Treba shvatiti da arhitektura bežičnog oblaka nosi sa sobom određene rizike koje treba otkloniti prilagođavanjem postojećih bezbednosnih arhitektura i kontrola, a ne njihovim ponovnim razvijanjem od samog početka. Uz promišljeno planiranje, sistemi zasnovani na bežičnoj cloud arhitekturi mogu biti podjednako bezbedni, ako ne i sigurniji od tradicionalnog žičnog sistema .

Gledajući bežične mesh mreže, dolazimo do zaključka da je ključan faktor u WMN koji umanjuje kompleksnost mreže i troškove održavanja njihova mogućnost samoizlečenja i samoorganizovanja. Zbog svojih atraktivnih ekonomskih faktora WMN će postepeno preuzimati deo tržišta telekomunikacija i postati okosnica kroz koju korisnici mogu da se povežu sa internetom bilo gde i bilo kada, čak i u kriznim situacijama kada ni jedna druga vrsta komunikacija ne funkcioniše, pa može postati osnova budućih bežičnih mreža. Sa tolikom snagom WMN dolazi i velika odgovornost da se zaštite svi podaci koji se generišu i prolaze kroz mrežu. Kao takve, značajno su uvećale mogućnost i pouzdanost ad hoc mreža. I pored toga, postoji još uvek dosta problema u WMN koji se moraju rešiti. Postojeći pristupi su efikasni za zaštitu pojedinačnih slojeva mreže, ali ne dovoljno da zaštite i kompletnu mrežu sa njenim protokolima pa je u cilju izgrađivanja robusne i bezbedne mesh mreže neophodno primeniti pravu kombinaciju mehanizama, servisa i politika zaštite.

20. LITERATURA

- [1] A. Agarwal, *et al.*, “Wireless Grids: Approaches, Architectures and Technical Challenges,” *Working Paper, Massachusetts Institute of Technology (MIT), Sloan School of Management*, 2004.
- [2] S. Ahuja and J. Myers, “A Survey on Wireless Grid Computing,” *Journal of Supercomputing*, vol.37(1), pp. 3-21, 2006.
- [3] M. Armbrust, *et al.*, “Above the Clouds: a Berkeley View of Cloud Computing,” *Technical Report No. UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley*, vol. 28, 2009.
- [4] M. Bishop, “Computer Security,” *Art and Science*, Addison-Wesley, Boston, 2003.
- [5] Y. Chen, *et al.*, “What’s New About Cloud Computing Security?” *Technical Report No. UCB/EECS-2010-5, Electrical Engineering and Computer Sciences, University of California at Berkeley*, vol. 20, 2010.
- [6] M. Dikaiakos, *et al.*, “Cloud Computing: Distributed Internet Computing for IT and Scientific Research,” *IEEE Internet Computing*, vol. 13(5), pp. 10–13, 2009.
- [7] J. Ekanayake, *et al.*, “High Performance Parallel Computing with Clouds and Cloud Technologies,” in *Cloud Computing and Software Services: Theory and Techniques*, CRC Press (Taylor and Francis). 2010.
- [8] I. Foster, “What is the Grid? A Three Point Checklist,” *GRIDToday*, vol. 1(6), 2002.
- [9] I. Foster, *et al.*, “The Anatomy of the Grid: Enabling Scalable Virtual Organizations,” *International Journal of Supercomputer Applications*, vol. 15(3), pp. 200-222, 2001.
- [10] I. Foster, *et al.*, “The Open Grid Services Architecture, Version 1.5,” *Global Grid Forum*, 2006, accessed June 15, 2014, from <http://www.ggf.org/documents/GFD.80.pdf>.
- [11] I. Foster, *et al.*, “The Physiology of the Grid,” in *Berman, F., Hey, A. and Fox, G. (eds.), Grid Computing - Making the Global Infrastructure a Reality*, John Wiley and Sons, pp. 217-249, 2003.
- [12] P. Funk and S. Blake-Wilson, “Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0),” RFC 5281, *Internet Engineering Task Force*, 2008.
- [13] M. Gaynor, *et al.*, “Integrating Wireless Sensor Networks with the Grid,” *IEEE Internet Computing*, vol. 8(4), pp. 32–39, 2004.
- [14] C. Hoffa, *et al.*, “On the Use of Cloud Computing for Scientific Workflows,” in *ESCIENCE '08: Proceedings of the 2008 Fourth IEEE International Conference on eScience, IEEE Computer Society*, 2008, pp. 640–645.
- [15] P. Jaeger, *et al.*, “Cloud Computing and Information Policy: Computing in a Policy Cloud?” *Journal of Information Technology & Politics*, vol. 5(3), pp. 269–283, 2008.
- [16] S. Jajodia, Steven Noel, Brian O’Berry, “Topological Analysis of Network Attack Vulnerability,”
- [17] K. Muniswamy-Reddy and M. Seltzer, “Provenance as First Class Cloud Data,” *ACM SIGOPS Operating Systems Review*, vol. 43(4), pp. 11-16, 2010.
- [18] M. Klems, *et al.*, “Do Clouds Compute? Framework for Estimating the Value of Cloud Computing,” in *Weinhardt, C., Luckner, S. & Stöber, J. (eds.) Lecture Notes in Business Information Processing*, vol. 22, 2009, pp. 110 – 123.
- [19] B. Lang, *et al.*, “A Multipolicy Authorization Framework for Grid Security,” in *Proceedings of the Fifth IEEE Symposium on Network Computing and*

- Application*, pp. 269-272, 2006.
- [20] H. Lim, *et al.*, “Automated Control in Cloud Computing: Challenges and Opportunities,” in *Proceedings of the First workshop on Automated Control for Datacenters and Clouds (ACDC '09)*, 2009, pp. 13-18.
 - [21] H. Lohr, *et al.*, “Enhancing Grid Security Using Trusted Virtualization,” in *Autonomic and Trusted Computing, Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 2007, pp. 372–384.
 - [22] Q. Ma and J. Pearson, “ISO 17799: Best Practices in Information Security Management” *Communications of the Association for Information Systems*, vol. 15(32), pp. 577-591, 2005.
 - [23] S. Manvi and M. Birje, “A Review on Wireless Grid Computing,” *International Journal of Computer and Electrical Engineering*, vol. 2(3), pp. 469-474, 2010.
 - [24] L. McKnight, *et al.*, “Wireless Grids: Distributed Resource Sharing by Mobile, Nomadic, and Fixed Devices,” *IEEE Internet Computing*, vol. 8(4), pp. 24–31, 2004.
 - [25] L. McKnight, *et al.*, “Wireless Grids: Assessing a New Technology for a User Perspective,” in *Designing Ubiquitous Information Environments: Socio-Technical Issues and Challenges*, 2005, pp. 169–181.
 - [26] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” *National Institute of Standards and Technology, Information Technology Laboratory*, Version 15, 2009.
 - [27] S. Nanz and C. Hankin, “A Framework for Security Analysis of Mobile Wireless Networks,” *Theoretical Computer Science*, vol. 367 (1-2), pp. 203-227, 2006.
 - [28] N. Nagaratnam, *et al.*, “The Security Architecture for Open Grid Services,” Open Grid Service Architecture Security Working Group (OGSA-SEC-WG), 2002, accessed June 15, 2013, from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.5693&rep=rep1&type=pdf>.
 - [29] M. Naedele, “Standards for XML and Web Services Security,” *Computer*, vol. 36 (4), pp. 96-98, 2003.
 - [30] S. Ostermann, *et al.*, “A Performance Analysis of EC2 Cloud Computing Services for Scientific Computing,” in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 34 (4), 2010, pp. 115-131.
 - [31] J. Park and R. Sandhu, *et al.*, “Towards Usage Control Models: Beyond Traditional Access Control,” in *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies (SACMAT'02)*, 2002, pp. 57–64.
 - [32] T. Phan, *et al.*, “Integrating Wireless Devices into the Computational Grid,” in *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MOBICOM 2002)*, 2002, pp. 271–278.
 - [33] A. Raghunathan, *et al.* “Securing Wireless Data: System Architecture Challenges,” In *Proceedings of the 15th International Symposium on System Synthesis (ISSS 2002)*, 2002, pp. 195-200.
 - [34] B. Rimal, *et al.*, “A Taxonomy and Survey of Cloud Computing Systems,” in *Proceedings of the Fifth International Joint Conference on INC, IMS and IDC*, 2009, pp. 44–51.
 - [35] D. Rosado, *et al.*, “Analysis of Secure Mobile Grid Systems: A Systematic Approach,” *Information and Software Technology*, vol. 52, pp. 517– 536, 2010.
 - [36] R. Sandhu and Q. Munawer, “How to do Discretionary Access Control Using Roles,” in *Proceedings of the Third ACM Workshop on Role-Based Access Control (RBAC '98)*, 1998, pp. 47–54.
 - [37] N. Santos, *et al.*, “Towards Trusted Cloud Computing,” in *Proceedings of the*

- 2009 conference on Hot Topics in Cloud Computing (HotCloud 2009), vol. 3, 2009.
- [38] G. Brunette and R. Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," *Cloud Security Alliance*, pp. 1-76, 2009.
 - [39] J. Treglia, *et al.*, "Collaboration in a Wireless Grid Innovation Testbed by Virtual Consortium," in *Networks for Grid Applications. Lecture Notes of the Institute for Computer Sciences, Social- Informatics and Telecommunications Engineering*, vol. 25, 2010, pp. 139 – 146.
 - [40] L. Vaquero, *et al.*, "A Break in the Clouds: Towards a Cloud Definition," *SIGCOMM Computer Communications Review*, vol. 39(1), pp. 50-55, 2008.
 - [41] CNSS Instruction 4009, "National Information Assurance Glossary," Committee on National Security Systems, 2003, accessed June 15, 2014, from http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.
 - [42] C. Onwubiko and A. Lenaghan, "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises," in *Proceedings of the 2007 IEEE International Conference on Intelligence and Security Informatics*, 2007, pp. 244-249.
 - [43] R. Sandhu, *et al.*, "Role-Based Access Control Models," *IEEE Computer*, vol. 29(2), pp. 38–47, 1996.
 - [44] A. Perrig, *et al.*, "Security in Wireless Sensor Networks," *Communication of the ACM*, vol. 47(6), pp. 53–57, 2004.
 - [45] Omar Villavicencio-Calderon. "wireless mesh networks: performance analysis and enhancements." university of puerto rico mayaguez campus, 2008.
 - [46] Hamid, Zara; Khan, Shoab A., "An Augmented Security Protocol for WirelessMAN Mesh Networks," *Communications and Information Technologies*, 2006. ISCIT '06. International Symposium on , vol., no., pp.861-865, Oct. 18 2006-Sept. 20 2006
 - [47] Carlo Alberto Boano and Md. Sakhawat Hossen. "VoIP over Wireless Mesh Networks: Implications and Challenges," May 1, 2008.
 - [48] S. Asherson, A. Hutchison. "Secure Routing in Wireless Mesh Networks". University of Cape Town.
 - [49] White Paper "Wireless Mesh Technology: Connecting the new millennium". An IJIS Institute Briefing Paper.
 - [50] Portmann, M. Amir, A, P. "Wireless Mesh Networks for Public Safety and Disaster Recovery Communications".
 - [51] S. Kapp, "802.11: Leaving the Wire Behind," *IEEE Internet Computing*, vol. 6, no.1, Jan./Feb. 2002, pp. 82-85.
 - [52] Netgear every body connecting "The ABGs of Wireless LAN" Technology Overview. February 2003.
 - [53] A.Gerkis "A Survey of Wireless Mesh Networking Security Technology and Threats". September 2006.
 - [54] Ian F. Akyildiz, Xudong Wang, "Security in Wireless Mesh Networks".December 19, 2006
 - [55] Akyildiz, I.F., Wang, X. and Wang, W., *Wireless Mesh Networks: A Survey*, *Computer Networks Journal (Elsevier)*, March 2005.
 - [56] I.F. Akyildiz, *Wireless Mesh Networks: Broadband and wireless networking laboratory*. <http://www.ece.gatech.edu/research/labs/bwn>. Access date: 15 April, 2014.

- [57] Yan Zhang, Jijun Luo, Honglin Hu, 'Wireless Mesh Networking architectures protocols and standards '.
- [58] Guangsong Li, An Identity-Based Security Architecture for Wireless MeshNetworks. 2007.
- [59] P. Gardner-Stephen et al. ,, Serval Project Developer Wiki [Online]"
<http://developer.servalproject.org/wiki>. Access date: 12 January, 2015.
- [60] P. Gardner-Stephen and S. Palaniswamy. "Serval mesh software – WiFi multi model management", in Proc. of the 1st International Conference on Wireless Technologies for Humanitarian Relief, India, 2011, pp. 71-77.