Madonreiät langattomissa ad hoc -verkoissa

Jan Wikholm

Kandidaatintutkielman aineversio
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Helsinki, 24. helmikuuta 2014

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Tietojenkäsittelytieteen laitos

Tekijä — Författare — Author
Jan Wikholm

Työn nimi — Arbetets titel — Title

Madonreiät langattomissa ad hoc -verkoissa

Oppiaine — Läroämne — Subject
Tietojenkäsittelytiede

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Kandidaatintutkielman aineversio	24. helmikuuta 2014	8

Tiivistelmä — Referat — Abstract

Madonreikä-hyökkäysten ja niiden vastatoimien tyypitys.

Avainsanat — Nyckelord — Keywords
ad hoc -verkot, wlan, hyökkäys, puolustus, havainnointi

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — Övriga uppgifter — Additional information

Sisältö

1 Johdanto

Langattomat päätelaitteet – kuten matkapuhelimet, PDA:t ja kannettavat tietokoneet – voivat muodostaa langattoman ad hoc -verkon, jonka avulla ne voivat kommunikoida ilman erillistä verkkoinfrastruktuuria. [CL06]. Sensori- ja ad hoc -verkot voivat toimia viestintäalustana monissa erilaisissa käyttötarkoituksissa kuten pelastus-, armeija- [HPJ03] sekä myös siviilikäytössä [KBS05]. Esimerkiksi luonnonkatastrofin jäljiltä perinteiset langattomat tukiasemat voivat olla tuhoutuneet ja pelastuslaitosten työntekijät voivat olla viestinnässään ad hoc -verkkojen varassa [HPJ03].

Näiden verkkojen suurimpia etuja ovat käyttöönoton nopeus ja kustannustehokkuus [CL06, HPJ03], sillä laitteisto on usein edullista ja päätelaitteet osaavat itsenäisesti luoda verkon. Vaikka ad hoc -verkkoja voi muodostaa myös langallisesti, on useimmiten käytössä langattomat teknologiat [HPJ03] ja siksi keskitymme niihin.

Pääosa teknologian alkuvaiheen tutkimuksesta on keskittynyt näiden lupausten toteuttamiseen luoden reititysprotokollia ja muita välttämättömiä viestinnän osia [KBS05]. Ad hoc -verkkojen avoimuuden ja autonomisuuden seurauksena ne ovat erityisen haavoittuvia monille erilaisille hyökkäyksille: *salakuuntelu* (eavesdropping), *väärennys* (spoofing) ja *toistaminen* (replay) [HPJ03]. Näiden lisäksi hyökkääjä voi tahallisesti olla välittämättä paketteja, *musta aukko -hyökkäys* (blackhole attack), tai syöttää niitä verkkoon paljon tukehduttaakseen sen järkevän käytön, *valkoinen aukko -hyökkäys* (white hole attack) [CL06]. *Madonreikähyökkäys* (wormhole attack) on erityisen vakava hyökkäys ad hoc -verkoissa [KBS05].

Madonreikähyökkäyksessä kaksi tai useampi paha-aikeista tahoa toimivat yhteistyössä saadakseen liikenteen ohjautumaan niiden välillä kulkevaa reittiä pitkin, jotta voivat toteuttaa edellä mainittuja hyökkäyksiä. Nämä tahot välittävät kaikki kuulemansa paketit toiselle osapuolelle, joka toistaa ne omassa päässään. Tämä pakettien välitys voidaan toteuttaa dedikoidulla suurinopeuksisella linkillä, pakettien kapseloinnilla normaalia verkkoa pitkin tai vaikka suuritehoisella lähettimellä. [KBS05]. Tunnelin ollessa toiminnassa se häiritsee reititysprotokollia tarjoten lyhimmän ja yleensä nopeimman reitin, joten muut verkon laitteet päätyvät lähettämään suuren osan paketeista sen läpi. Erityisen salakavalan hyökkäyksestä tekee se, että hyökkääjien ei tarvitse murtaa mitään salausta koska koko hyökkäys perustuu pakettien kopiointiin (salakuunteluun ja sen jälkeiseen toistoon) verkon osasta toiseen.

Esittelemme luvussa 2 madonreikähyökkäysten hyökkääjä- [CL06] sekä hyökkäystyypit [KBS05] minkä jälkeen kerron laitteistoriippuvaisista puolustuskeinoista luvussa 3 ja protokollapohjaisista puolustusmekanismeista luvussa

4. Yhteenvedon näistä esitämme luvussa 5.

2 Hyökkääjä- ja hyökkäystyypit

Madonreikähyökkääjiä on kahta eri tyyppiä: *piilotettu* ja *avoin* [CL06] ja hyökkäyksiä on viittä eri tyyppiä. [KBS05]. Kaikkia hyökkäystyyppejä ei ole käsitelty kaikissa puolustuskeinoissa, joten käsittelemättömien hyökkäystyyppien torjumisen toimivuus on erinomainen kohde jatkotutkimukselle.

2.1 Piilotettu hyökkääjä

Piilotetut hyökkääjät toimivat verkossa kertomatta muille verkon laitteille omasta olemassaolostaan. Ne kuuntelevat liikennettä ja siirtävät paketteja madonreiän läpi täysin muokkaamatta. Tällöin kaukanakin olevat laitteet voivat luulla madonreiän läpi tulevia paketteja naapureilta tuleviksi, koska eivät tiedä välissä olevan toistimena toimiva madonreikä.

Esimerkiksi pakettihihnat toimivat piilotettuja hyökkääjiä vastaan.

2.2 Avoin hyökkääjä

Avoimet hyökkääjät rekisteröityvät verkkoon kuten muutkin laitteet. Muille verkon laitteille näyttää siltä, että nämä laitteet ovat ensimmäisen asteen naapureita ja siten niiden kautta löytyvä lyhyt polku on täysin käypä vaihtoehto. Tapa, jolla madonreikä on muodostettu, on jokin alla kuvailluista viidestä hyökkäystavasta.

2.3 Pakettikapselointi

Pakettikapseloinnissa hyökkääjät H1 ja H2 voivat käyttää jo olemassa olevaa verkkoa: H1 kuulee paketin ja luo uuden H2:lle suunnatun paketin, jonka sisältönä on sellaisenaan H1:n kaappaama paketti. Kun tämä kapseloitu paketti saavuttaa H2:n se toistaa alkuperäisen sisällön sellaisenaan verkkoon, joten sen naapurit luulevat H1:n naapureiden olevan lähellä.

2.4 Erilliskaistahyökkäys

Mikäli hyökkääjillä on normaalin lähetyskaistan - esim. wlan-verkko - lisäksi käytössä vaikkapa yksinkertaisesti kytketty ethernetverkko, voivat ne kommunikoida yleistä verkkoa nopeammin ja sen kantamaa pidemmälle. Tätä kutsutaan erilliskaistahyökkäykseksi ja tämä on nimenomaan se hyökkäys, johon suurin osa puolustuskeinoista viittaa itse madonreikähyökkäyksenä.

2.5 Suurteholähetys

Yksi oletus, mikä puolustuskeinoja laatiessa täytyy pitää mielessä on, että hyökkääjille voi olettaa loputtomat resurssit toisin kuin muille verkon laitteille, joita nimenomaan yleensä yhdistää resurssien vähyys. Tästä oletuksesta yhtenä esimerkkinä on suurteholähetys: hyökkääjälaite lähettää kaappaamansa reitityspaketit huomattavan suurella lähetysteholla ja täten saa aikaan sen itsensä lävitse kulkevan lyhimmän reitin. Tämä hyökkäys ei siis vaadi kahta osapuolta.

2.6 Pakettivälitys

Kuten suurteholähetys pakettivälityshyökkäys ei vaadi hyökkääjäparia vaan sen voi suorittaa yksikin vihamielinen laite. Tässä hyökkääjä on kahden laitteen välissä välittäen paketteja jolloin nämä laitteet luulevat olevansa naapureita ja hyökkääjä niiden välissä voi suorittaa esimerkiksi salakuuntelua tai palvelunestohyökkäystä.

2.7 Protokollapoikkeamat

Protokollapoikkeamilla tarkoitetaan paha-aikeisten laitteiden tahallista verkkoprotokollan rikkomista: esimerkiksi pakettitörmäysten estämiseksi tietyt protokollat vaativat reitityspakettien lähetyksessä pientä viivettä - paha-aikeinen laite voi täten lähettää paketit heti ja aiheuttaa tavallisille laitteille haittaa törmäyksillä. Toinen vaihtoehto on reitityspakettien lähettämättä jättäminen jolloin verkon reititys ja polunetsintä eivät toimi oikein. Kummassakin tapauksessa hyökkääjä voi junailla toimensa siten, että suuri osa verkon liikenteestä päätyy reitittymään sen läpi.

3 Laitteistoriippuvaiset puolustusmekanismit

Nämä puolustusmekanismit eivät vaadi reititysprotokolliin muutoksia, mutta niillä on laitteistovaatimuksia.

3.1 Pakettihihnat ja TIK-protokolla

Yih-Chun Hu et al [HPJ03] kuvailevat uuden mekanismin - *pakettihihnat* (packet leashes) - ja sen kaksi eri varianttia: *aikahihnan* (temporal leash) ja *geohihnan* (geographic leash). Tässä hihnalla tarkoitetaan sellaista dataa, jolla paketin enimmäiskantamaa voidaan rajoittaa.

Pakettihihnojen lisäksi he luovat uuden TIK-verkkoprotokollan, joka käyttää aikahihnoja madonreikiä vastaan.

Aikahihnat
Aikahihnojen edellytyksenä on tarkka kellojen synkronointitarkkuus: muutaman mikrosekunnin tai jopa satojen nanosekuntien tarkkuus. Kaikkien laitteiden pitää myöskin olla tietoisia virhemarginaalin suuruusluokasta kahden laitteen välillä. Tällainen synkronointitarkkuus onnistuu esimerkiksi GPS:n avulla. Vaikka tarkkuusvaatimus on erittäin tiukka, on se kirjoittajien mukaan täysin hyväksyttävä ottaen huomioon madonreikähyökkäyksen vakavuuden.

Aikahihnaa muodostaessa lähettäjä päättää enimmäispituuden lähetykselle ja laskee kauanko valonnopeudella kulkevalla radiosignaalilla kestää sinne päätyä – tässä tietenkin otetaan huomioon synkronoinnin virhemarginaali – ja tämän avulla lähettäjä laskee paketille vanhenemisajan, jonka jälkeen paketti on hylättävä. Tunnelointi aiheuttaa pakosti viivettä, koska se kulkee kauemmaksi, joten madonreiän toisella puolella olevat laitteet pudottavat vanhentuneet paketit.

Vaikka aikahihna on hihnatyypeistä tarkempi on sen haasteena se, ettei lähettäjä tiedä aina tarkalleen omaa lähetysaikaansa, koska fyysisen kerroksen lähetysmekanismi voi joutua odottamaan; täten on vaikeaa etukäteen luoda lähetysajankohtaan perustuvaa digitaalista allekirjoitusta.

Geohihnat
Geohihnoja käytettäessä kaikkien verkon laitteiden pitää tietää oma sijaintitietonsa sekä niiden pitää pystyä synkronoimaan kellonsa muiden kanssa; joskin kellojen synkronointitarkkuus ei ole niin tärkeä seikka, koska laitteiden liikkumisvauhti suhteessa valonnopeuteen on marginaalinen.

Geohihnan toiminta on hyvin yksinkertainen: laite tarkistaa onko sen oma sijainti alkuperäisessä paketissa määritellyn sallitun matkan päässä. Koska paketit allekirjoitetaan digitaalisesti, voi laite luottaa paikannustiedon olevan alkuperäiseltä lähteeltä. Toisin kuin pelkkä matkan pituuteen perustuva tarkistus geohihnat toimivat myös siinä tilanteessa, että madonreikä kuljettaa paketin jonkin esteen ohi.

Geohihnoissa laitteet tietävät toistensa oletetun maksimiliikenopeuden ja täten madonreikätunneloitu paketti voidaan tunnistaa ilkivaltaisen laitteen lähettämäksi, jos se lähettää verkkoon kaksi pakettia joiden lokaatiotiedoissa on tapahtunut maksimiliikenopeutta nopeampaa liikettä edellyttävä muutos.

TIK-protokolla
TIK-protokollan nimi tulee sanoista “TESLA with Instant Key disclosure“, eli se on TESLA-protokollan laajennus välittömällä avainten paljastuksella.

TIK-protokolla käyttää kirjoittajien aikahihnoja.

Tärkeimpänä ominaisuutena koko aikahihnafunktion toiminnassa on aikaleimojen luotettavuus; leimat pitää pystyä todentamaan. Jaetut avaimet hylätään suoraan todeten niiden hallinnan olevan liian raskas operaatio. Toisena ideana on digitaalisen allekirjoituksen liittäminen jokaiseen pakettiin, jolloin jokaiselle laitteelle riittää yksi julkinen-yksityinen–avainpari ja jokaisen laitteen tarvitsee tietää vain tämä kaikkien julkisten avainten joukko. Digitaaliset allekirjoitukset kuitenkin yleensä perustuvat raskaaseen asymmetriseen kryptografiaan, joka ei sovi ad hoc –verkkojen oletettuun resurssivähyyteen.

Symmetriseksi vaihtoehdoksi raportti tarjoaa tiivisteistä koostuvaa binääripuuta (Merkle-tiivistepuu). Tiivisteiden hyväksi puoleksi kerrotaan niiden erittäin tehokas laskeminen ja yksisuuntaisuus. Merkle-puussa jokainen tiiviste muodostuu kahden lapsensa tiivisteistä aina juureen saakka. Tämä juuritiiviste on laitteen julkinen avain ja alimman tason lapset ovat yksityinen avain.

Lähettäjän avainnippu koostuu satunnaisluvuista, jotka on tallennettu Merklepuun pohjalle siten että ne on indeksoitu juoksevaan järjestykseen. Tätä järjestyslukua vastaa ajanhetkien järjestysluku; ajanlasku alkaa laitteiden yhtenään sopimasta hetkestä ja etenee sovituin lisäyksin (esimerkiksi 11,5 mikrosekuntia).

Vastaanottaja tietää jo etukäteen lähettäjän julkisen avaimen, eli Merklepuun juuritiivisteen, ja jokaisen paketin yhteydessä se saa neljä uutta datapalaa:

1. tiivisteen viestistä ja avaimesta K_i,
2. viestin,
3. tiedot, joiden avulla avaimesta K_i saadaan laskettua juuritiiviste, sekä
4. avaimen K_i.

Nämä osat tulevat nimenomaan tarkasti tässä järjestyksessä. Koska avainta ei ole viestin tiivistelaskennan aikaan vielä lähetetty, vastaanottaja voi nyt olla varma, ettei kukaan ole voinut väärentää tiivistettä. Vastaanottajan tarkistettua viestin aitouden se tarkistaa vielä aikahihnan rajat ja katsoo, onko paketti voimassa.

Resurssivaativuus
Resurssien niukkuuteen kirjoittajat mainitsevat pääratkaisuna symmetrisen

kryptografian käyttö asymmetrisen sijaan – operaatioiden nopeuserot voivat olla kolmesta neljään suuruusluokkaa (100–1000-kertaisia) hitaampia jälkimmäisessä.

TIK-protokollaa arvioidessaan kirjoittajat tarkastelivat nykyisten (2001) mobiililaitteiden laskentatehoa ja muistimäärää. He toteavat protokollan laskenta- ja muistivaatimukset mahdollisiksi saatavilla olevilla laitteilla; joskin huomauttavat ettei TIK sovi resursseiltaan aivan kaikkein köyhimpiin laitteisiin kuten sensoriverkkoihin.

Allekirjoitusta varten muodostettavan tiivistepuun muodostusta ja tallennusta voi optimoida siten että vain osa puusta säilötään muistissa ja osa lasketaan tarvittaessa. Tällaisen optimoinnin takia yhden vuorokauden yksityiset avaimet sisältävä osittainen puu saadaan mahtumaan 2,5 megatavuun kokonaisen puun 170 gigatavun sijaan.

Kirjoittajien yhteenveto protokollastaan: TIK-protokolla suojaa laitteita tehokkaasti ilkivaltaiselta toistolta, väärennykseltä ja madonreikähyökkäyksiltä; sekä varmistaa tuoreuden. Protokolla on toteutettavissa nykylaitteistoilla vaikka se ei sovikaan kaikista rajoitetuimpiin sensoriverkkoihin.

3.2 Suunta-antenni

Lingxuan Hu ja David Evans kuvaavat suunta-antennin käyttöä madonreikien estämisessä [HE04].

- laitteiden sisäisen kompassin tarkka suuntima
- magneeteilla häiriötä
- vaatii 3. osapuolen todentamaan liikenteen suuntaa
- olettaa linkkien väliset salaukset
- naapurilistat
- Worawannotai-hyökkäys (erikoistapaus todentaja-aseman väärinkäytöstä)

4 Puhtaasti protokollapohjaiset puolustusmekanismit

Seuraavilla ratkaisuilla on laajempi käyttöpotentiaali, koska ne eivät vaadi erityislaitteistoa.

4.1 DeWorm

Hayajneh et al kuvailevat DeWorm-protokollan [HKT09]

- Isossa verkossa raskas
- verkkoliikenne-kustannukset
- pala palalta polun tarkistus jokaiselle eri polulle

4.2 DelPHI

Hon Sun Chiu ja King-Shan Lui kertovat viiveeseen perustuvasta DelPHI-protokollastaan [CL06]

- Kokonaiskesto RTT / hyppyjen määrällä
- Normaali verkko: A->B->C->D->E (4 hyppyä)
- Rei'itetty salattu verkko: A->(M1->M2)->E (1 hyppy)
- rei'itetty on nopeampi, mutta RTT / hyppyjen määrällä on sillä selvästi isompi kuin pienin hypyin etenevä rehti verkko => madonreikä.

4.3 LiteWorp

Khalil et al esittelevät naapurilistoihin ja vartiointiin perustuvan LiteWorp-protokollan [KBS05]

- vartijat
- väärät syytökset vs verkkopakettien törmäilyt
- vahtilistojen ja -puskurien tilavaativuudet
- protokollan heikkeneminen tiheissä verkoissa (naapuri-lkm >20)

Lähteet

[CL06] Hon Sun Chiu ja King Shan Lui: *DelPHI: wormhole detection mechanism for ad hoc wireless networks.* Teoksessa *Wireless Pervasive Computing, 2006 1st International Symposium on*, sivut 6 pp.–, Jan 2006.

[HE04] Lingxuan Hu ja David Evans: *Using Directional Antennas to Prevent Wormhole Attacks.* Teoksessa *The 11th Annual Network and Distributed System Security Symposium, 2004. NDSS 2004. Proceedings.*, February 2004.

[HKT09] T. Hayajneh, P. Krishnamurthy ja D. Tipper: *DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad Hoc Networks.* Teoksessa *Network and System Security, 2009. NSS '09. Third International Conference on*, sivut 73–80, Oct 2009.

[HPJ03] Yih Chun Hu, A. Perrig ja D.B. Johnson: *Packet leashes: a defense against wormhole attacks in wireless networks.* Teoksessa *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, nide 3, sivut 1976–1986 vol.3, March 2003.

[KBS05] I. Khalil, S. Bagchi ja N.B. Shroff: *LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks.* Teoksessa *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on*, sivut 612–621, June 2005.