Madonreiät langattomissa ad hoc -verkoissa

Jan Wikholm

Kandidaatintutkielman aineversio
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Helsinki, 22. 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	22. helmikuuta 2014	6

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 pitää pitää mielessä on, että hyökkääjille pitää 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 lyhyimmän 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 ei 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 Aika- ja geohihnat

Yih-Chun Hu et al kertovat aika- ja geohihnoista [HPJ03]

- Vahva aikasynkronointivaativuus tai
- lokaatiotiedon tarkkuus (esim. GPS)
- muisti- ja laskentavaativuudet - merkle-puut, tiivisteet, symm. krypto
- ei sovi sensoriverkkoihin (resurssivähyys)

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.