Aalto-yliopisto
Teknillinen korkeakoulu

Informaatio- ja luonnontieteiden tiedekunta
http://information.tkk.fi/
puhelin 09-470 23245

Väitöstiedote **2.11.2010**

Uusi hajautettu mobiiliverkkojen avaintenhallinta ja AAA mahdollistaa tukiasemapilviverkon

Väitöskirjan nimi	Improving and Distributing Key Management on Mobile Networks Avaintenhallinnan kehittäminen ja hajauttaminen mobiiliverkoissa
Väitöskirjan sisältö	Väitöskirja käsittelee mobiiliverkkojen avaintenhallinnan ja käyttäjän autentikoinnin ongelmaa, joka negatiivisesti vaikuttaa handoverin tehokkuuteen, lisää systeemin kuormaa mm. avainten neuvottelun. jakelun ja autentikoinnin ansiosta. Väitöskirjan tuloksena parannetaan avaintenhallinnan tehokkuutta ja samalla vähennetään kasvavia sijoituspaineita telekommunikaatioverkkojen ydinverkkoelementteihin, tarjotaan kriittisiä rakennusaineita tukiasemapilviverkkojen kehittämiselle. Uusi SKC (Session Keys Context) –avaintenhallintamenetelmä on merkittävä kontribuutio mobiiliverkkojen avaintenhallintaan nopean liikkuvuudenhallinnan kanssa verkoissa, joissa vaaditaan erilliset avaimet jokaiselle tukiasemalle. Se on paras löydettyjen joukossa vähentämään signalointikuormaa ja tekemään verkon liikkuvuudenhallinta riippumattomaksi tukiaseman ja avaintenjakelijan välisestä reitin viiveestä. Uusi lähettäjän ja vastaanottajan identiteettiin sidottu avaintenneuvotteluprotokolla symmetristen avainten kanssa on yleistys SKC:n käyttämästä identiteetin sitomisesta. Lisäksi uusi hajautettu AAA arkkitehtuuri SKC:n, sertifikaattien ja laitteistopohjaisen tietoturvan kanssa on disruptiivinen ehdotus ja näyttää miten äärimmillään mobiiliverkkojen avaintenjakelija voidaan hajauttaa verkon reunaelementteihin. Analyysi ja vertailu SKC:n ja LTE:n avaintenhallinnan välillä on uutta, eikä sitä ole nähty aikaisemmin. Väitöskirjan tutkimustulokset vaikuttivat LTE tietoturvan standardointiin 3GPP:ssä ja kontribuoi tukiasemien kehitykseen ja tutkimukseen.
Väitöskirjan ala	Tietotekniikka, Tietoliikenneturvallisuus
Väittelijä	Dan Forsberg, DI Syntynyt Kokkolassa 1976
Väitöksen ajankohta	3.12.2010 klo 12
Paikka	Aalto-yliopiston teknillinen korkeakoulu, T-talo, T2-sali, Konemiehentie 2, Espoo
Vastaväittäjä	Professor Gene Tsudik, Department of Computer Science, University of California
Valvoja	Professori Antti Ylä-Jääski, Aalto-yliopiston teknillinen korkeakoulu, Tietotekniikan laitos
Väitöskirjan verkko-osoite	*http://lib.tkk.fi/Diss/2010/isbn9789526034218/*
Väittelijän yhteystiedot	Dan Forsberg, p. +358 40 483 5507, dan@forsberg.fi

Väitöskirja on julkisesti nähtävillä Aalto-yliopiston teknillisen korkeakoulun ylivirastomestarin ilmoitustaululla sekä tiedekunnan kanslian ilmoitustaululla (Konemiehentie 2).