Hermanni Hyytiälä

JXTA-arkkitehtuuri

Tietotekniikan (Ohjelmistotekniikka)
LuK-tutkielma
22.10.2002

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Hermanni Hyytiälä
Yhteystiedot: Hermanni Hyytiälä
Huhtalammentie 5 as. 17
40640 JYVÄSKYLÄ
sähköposti: hemppah@cc.jyu.fi
Työn nimi: gradu@title
Title in English: JXTA architecture
Työ: Tietotekniikan (Ohjelmistotekniikka) LuK-tutkielma
Sivumäärä: 24
Tiivistelmä: Tämä LuK-tutkielma käsittelee JXTA-arkkitehtuuria. JXTA on avoin teknologiaympäristö, jonka avulla voidaan kommunikoida, tehdä yhteistyötä ja jakaa tietoa vertaisverkkoympäristössä. Tutkielman tavoitteena on antaa lukijalle yleiskuva JXTA-arkkitehtuurista.
English abstract: This Bacheler's thesis gives a overview of project JXTA. Project JXTA is an open-source project that provides a set of methods for ad hoc, peer-to-peer distributed computing.
Avainsanat: Vertaisverkot, P2P, tietoverkot, tietoturva, hajautetut järjestelmät
Keywords: Peer-to-Peer, P2P, networking, secure computing, distributed computing

Sisältö

1 Johdanto

Tämä tutkielma käsittelee JXTA-vertaisverkkoarkkitehtuuria. Se on järjestelmäkokonaisuus, jonka avulla vertaisverkoissa voidaan siirtää tiedostoja, keskustella, jakaa työpöytiä ja hakea tietoa. JXTA poikkeaa useista muista vertaisverkkoarkkitehtuureista siten, että se on täysin avoin järjestelmä. Tämä tarkoittaa sitä, että JXTA kehittyy jatkuvasti useiden vapaaehtoisten sovelluskehittäjien toimesta. Lisäksi JXTA on tarkoitettu käytettävän yrityksissä, jonka seurauksena JXTA sisältää omaisuuksia, joita muista vertaisverkkoarkkitehtuureista ei löydy.

Tutkielma jakaantuu kolmeen osaan. Luvuissa 2 ja 3 käsitellään vertaisverkkoja ja JXTAa yleisellä tasolla, luvuissa 4, 5, 6 ja 7 keskitytään JXTA-järjestelmän ominaisuuksiin. Luku 8 käsittelee tiedonhakua vertaisverkossa.

2 Vertaisverkot ja JXTA

Viimeisen kymmenen vuoden aikana tiedon määrä tietoverkoissa on kasvanut niin suureksi, että kukaan ei pysty enää hallitsemaan kaikkea tietoa. On arvioitu, että uusien langattomien laitteiden markkinoille tulo kasvattaa tietoverkoissa käytettävien laitteiden määrää miljardeilla uusilla laitteilla [4].

Tiedon määrän kasvusta johtuen nykyisten tietoverkkojen rakenteiden heikkoudet ovat tulleet esille. Esimerkiksi laaja- alaisen ja paljon tietoa sisältävän tietokonejärjestelmän kuormittaminen keskitetysti (eng. Denial of service attack) voi aiheuttaa järjestelmän jumiutumisen, jolloin kaikki tietojärjestelmän tarjoavat palvelut lakkaavat toimimasta.

Keskitettyjen palveluiden haavoittuvuudesta johtuen on alettu kehittämään vaihtoehtoisia tapoja viestiä tietoverkoissa. Vertaisverkot ovat tietoverkkoja, joissa kaikki verkkoon kuuluvat laitteet ovat tasavertaisia. Tiedon siirtoon ei tarvita keskuskoneita, vaan verkon laitteet keskustelevat ainoastaan keskenään. IEEE 802.11b-standardi [16] on esimerkki vertaisverkkoarkkitehtuurista, jossa verkon laitteet eivät tarvitse keskustietokoneiden palveluita verkkoon liityttäessä.

Tiedotusvälineissä paljon julkisuutta saanut Napster-tiedostonjakoarkkitehtuuri [14] ei perustu vertaisverkkoteknologiaan, koska Napsterissa käytetään keskustietokoneita tiedon tallentamiseen (eng. Indexing). Itse tiedonsiirto tapahtuu kuitenkin ilman keskustietokoneita. Napsterin syntymän jälkeen on tehty lukuisia muita tiedostonjako-ohjelmistoja, jotka pohjautuvat enemmän vertaisverkkoideologiaan [6], [15].

3 JXTA-projekti

3.1 Yleistä

JXTA [12] on alunperin Sun Microsystemsin aloittama projekti. Projektin tavoitteena on luoda avoin arkkitehtuuri, joka mahdollistaa tehokkaan ja turvallisen tiedonsiirron vertaisverkoissa. JXTA-arkkitehtuuri perustuu vertaisverkko- ideologiaan. JXTAn avulla voidaan tietoverkoissa viestiä, tehdä yhteystyötä, jakaa resursseja ja hakea tietoa. JXTA on laitteisto- tai kieliriippumaton, joten se mahdollistaa erilaisten digitaalisten laitteiden- ja viestimien yhtäaikaisen käytön samassa vertaisverkossaa.

3.2 Tavoiteet

JXTA-projektin päämääränä on luoda vertaisverkkoarkkitehtuuri, josta hyötyisivät sekä yksityishenkilöt että yritykset. Kun projekti alkoi, luotiin kolme tavoitetta [4]:

Yhteensopivuus Lähes kaikki saatavilla olevat vertaisverkkoarkkitehtuurit ovat keskenään yhteensopimattomia. Projektin tavoitteena on luoda universaalinen vertaisverkkoarkkitehtuuri, jolloin kaikki tätä arkkitehtuuria käyttävät sovellukset ja olisivat keskenään yhteensopivia ja voisivat käyttää hyväksi toistensa palveluita.

Alusta riippumattomuus Useat vertaisverkko-arkkitehtuurit ovat sidottuja tiettyyn alustaan, koska ne ovat suunniteltu ja toteutettu tietyillä kielityökaluilla. Esimerkiksi jos vertaisverkko-ohjelma on toteutettu C++-ohjelmointikielellä, voi ohjelman siirrettävyys eri järjestelmien välillä olla vaikeaa tai jopa mahdotonta. JXTA on kielityökalu-, laitteisto- ja verkkoriippumaton vertaisverkkoarkkitehtuuri.

Kaikkialla läsnäoleva JXTA-teknologia on suunniteltu toimivan erilaisissa digitaalisissa laitteissa. Esimerkiksi erilaiset taskutietokoneet, kulutuselektroniikka- ja verkkolaitteistot ja tavalliset tietokoneet voivat keskustella keskenään JXTA-teknologian ansiosta.

4 JXTA-arkkitehtuuri

JXTA-arkkitehtuurin protokollat [4] luovat virtuaalisen verkon fyysisen verkon päälle. Virtuaaliverkon tarkoituksena on piilottaa alla olevan fyysisen verkon monimutkaisuus, esimerkiksi palomuurit, ja luoda yhtenäinen kokonaisuus verkon laitteiden kesken. Kuvassa 4.1 on esitetty JXTA-verkon virtuaalisen verkon rakenne.

Seuraavissa kappaleissa esitellään JXTAn verkkoarkkitehtuurin tärkeimmät ominaisuudet.

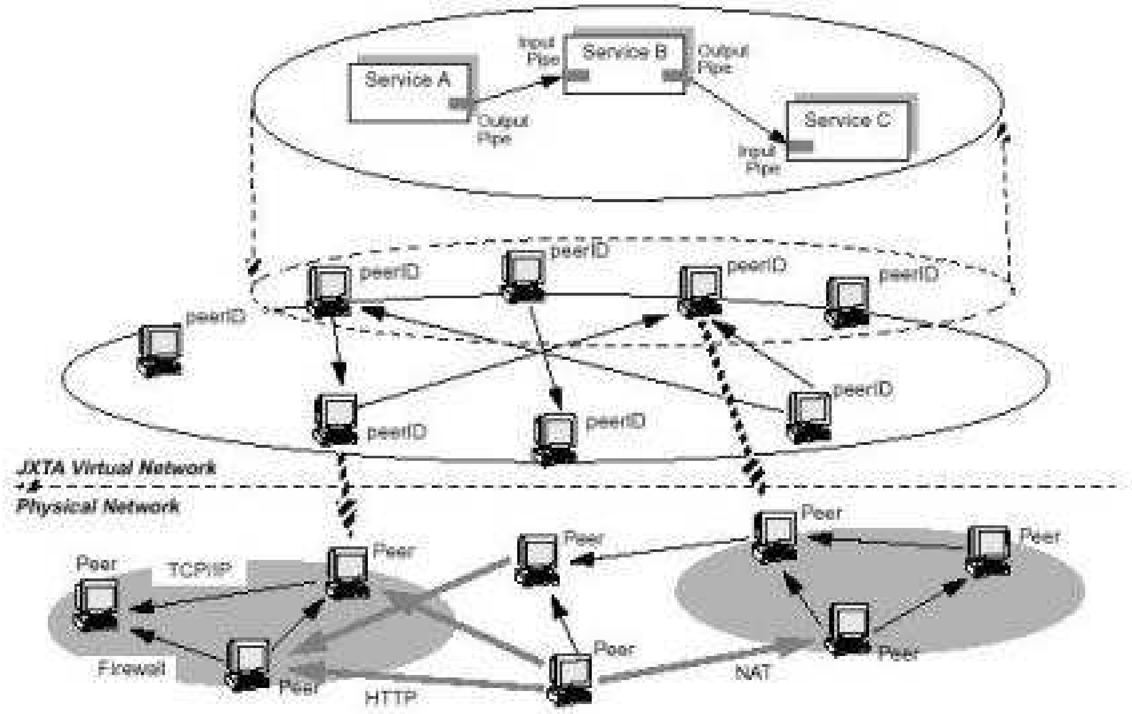
4.1 Verkkolaitteiden tunnistus (eng. Uniform Peer Addressing)

Uniform Peer Addressing on tekniikka, jonka avulla verkon laitteet tunnistetaan JXTA-arkkitehtuurin mukaisessa vertaisverkossa. Jokaiselle verkon laitteelle luodaan verkkoon liittymisen yhteydessä 128-bittinen tunniste (eng. Universal User Identification). Tunnisteen avulla voidaan yksikäsitteisesti tunnistaa verkon laite, oli kyseessä sitten DHCP-tekniikkaa käyttävä laite tai erilaisia verkkoliityntöjä käyttävä laite (esimerkiksi Ethernet, Bluetooth). Jokainen JXTA-verkon laite omaa laiterajapinnan (eng. Peer Endpoint), joka kertoo muille verkon laitteille laitteen osaamat verkkotekniikat. Esimerkiksi kun JXTA-verkon laite A saa tietoonsa toisen JXTA-verkon laitteen B laiterajapinnan, laite A voi valita parhaan tiedonsiirtokäytännön laitteen B kanssa.

4.2 Viestit (eng. Messages)

Kuten muissa ei-suunnitelluissa (eng. Ad-Hoc) ja mukautuvissa (eng. Adaptive) vertaisverkoissa, myös JXTA-verkossa yhteydet verkon laitteiden välillä voivat olla ohimeneviä. Tiedon välitysreitit voivat vaihtua ja olla lisäksi asynkronisia. JXTA-verkossa siirtyvät viestit on suunniteltu tällaisia tarpeita ajatellen.

Jokainen JXTA-verkon viesti sisältää otsikon (eng. Header), ei-pakollisen tiivistelmän (eng. Digest), päällysen (eng. Envelope) ja pinon (eng. Stack) sisältäen eri h



Kuva 4.1: JXTA-arkkitehtuurin virtuaaliverkko (© Sun Microsystems).

```xml
<?xml version="1.0"?>
<!DOCTYPE jxta:PGA>
<jxta:PGA xmlns:jxta="http://jxta.org">
    <GID> urn:jxta:jxta-NetGroup</GID>
    <MSID>urn:jxta:uuid-DEADBEEFDEAFBABAFEEDBABE000000010206</MSID>
    <Name>NetPeerGroup</Name>
    <Desc>NetPeerGroup by default</Desc>
</jxta:PGA>
```

Kuva 4.2: XML-muotoinen mainos (© Sun Microsystems).

protokollien otsikot ja tiedot (eng. Body). Päällynen sisältää otsikon, ei-pakollisen viestin lyhennelmän, lähettäjän sekä vastaanottajan. Vastaanottaja on looginen kohde, joka on annettu URI-muotoisena tietona.

Viestin tieto sisältää muuttuvan määrän tietoa sekä tunnisteita, joiden avulla yksikäsitteisesti voidaan tunnistaa viestin lähettäjä ja vastaanottaja. Tunniste voi olla esimerkiksi digitaalinen allekirjoitus, joka määrittää viestin lähteen.

4.3 Mainokset (eng. Advertisements)

Mainos on JXTA-verkossa siirtyvä XML-muotoinen viesti, joka kuvaa verkossa olevan laitteen palveluita. Kaikki JXTA-verkon resurssit ja palvelut kuvataan mainoksilla. JXTA-arkkitehtuurissa on seitsemän valmista mainospohjaa, joita voidaan käyttää mainosten luomisessa: Vertaissolmu-mainos (eng. Peer advertisement), vertaissolmuryhmämainos (eng. Peer Group advertisement), piippu-mainos (eng. Pipe advertisement), moduuli-mainos (eng. Module advertisement), vertaissolmutieto-mainos (eng. Peer Info advertisement), sisällys-mainos (eng. Content advertisement) ja laiterajapintamainos (eng. Peer Endpoint advertisement).

Mainoksia analysoimalla verkon laitteet pystyvät löytämään halumansa palvelut JXTA-verkosta. Kaikki vertaissolmut tallentavat, julkaisevat ja siirtävät mainoksia JXTA-verkossa. Kaikkiin mainoksiin liittyy elämänpituus-arvo (eng. Lifetime), joka määrittelee mainoksessa eliniän JXTA-verkossa. Mainos voidaan uudelleen julkaista, jolloin elämänpituus-arvoa voidaan tarvittaessa kasvattaa. Kuvassa 4.2 on esitetty eräs JXTA-arkkitehtuurin mukainen mainos.

4.4 Vertaissolmu (eng. Peer)

JXTA-verkko koostuu vertaissolmuista. Vertaissolmu voi olla tietokone, kämmentietokone tai langaton puhelin. Vertaissolmun pitää osata keskustella muiden vertaissolmujen kanssa JXTA-arkkitehtuurin mukaisten protokollien avulla.

4.5 Vertaissolmuryhmät (eng. Peer Groups)

JXTA-verkossa voi muodostua vertaissolmuryhmiä. Vertaissolmuryhmät ovat virtuaalisia konaisuuksia, jotka koostuvat yksittäisistä vertaissolmuista, joilla on samat kiinnostuksen kohteet. Yleensä samaan vertaissolmuryhmään kuuluvat vertaissolmut ovat sopineet erilaisista käytännöistä (eng. Policies), joita noudatetaan vertaissolmuryhmän sisällä. Jokainen vertaissolmuryhmä tunnistetaan yksillöllisen tunnisteen avulla. Uusi vertaissolmuryhmä voidaan luoda dynaamisesti JXTA-verkon käyttäjän, sovelluksen tai ylläpitäjän toimesta. Yksittäinen vertaissolmu voi kuulua samanaikaisesti useaan eri vertaissolmuryhmään.

Vertaissolmuryhmien olemassaoloon JXTA-arkkitehtuurin kehittäjät ovat löytäneet kolme motiivia: luottamuksellisen tiedon siirto rajoitetussa ympäristössä, samanlaisten intressien jakaminen rajoitetussa ympärisössä sekä rajoitetun ympäristön monitorointi ja analsyointi. JXTA-verkossa on implisiittinen, koko verkon laajuinen World Peer Group-vertaissolmuryhmä (WPG), joka kattaa kaikki verkon vertaissolmut. Tämä ei kuitenkaan tarkoita sitä, että kaikki WGP-ryhmän vertaissolmut voisivat löytää kaikki muut vertaissolmut.

4.6 Piiput (eng. Pipes)

Piiput ovat asynkronisia kanavia, joiden kautta viestejä lähetetään JXTA-verkossa. Piiput ovat myös virtuaalisia, piipun kohde voidaan yhdistää yhteen tai useaan vertaissolmuun. Piippuja käyttävät JXTA-verkon palvelut sekä sovellukset.

Piippu yhdistetään yleensä ajonaikaisesti vertaissolmuun käyttäen piipun yhdistys protokollaa (eng. Pipe Binding Protocol). Yksittäinen piippu voidaan yhdistää eri aikoina eri vertaissolmuihin. Tämä on hyöydyllinen omainaisuus silloin kun halutaan varmistaa järjestelmän toimivuus kriittisissä tilanteissa. Vioittunut vertaissolmu esimerkiksi verkossa voidaan korvata toisella toimivalla vertaissolmulla.

Pisteestä-pisteeseen-piipulla (eng. Point-to-point pipe) voidaan yhdistää tasan kaksi vertaissolmua keskenään. Tällöin piippu on ulosmeno-piippu lähettäjälle ja sisäänmeno-piippu vastaanottajalle. Liikenne on yksisuuntaista, lähettäjältä vastaanottajalle. Levittäytyvät-piiput (eng. Propagate pipe) pystyvät yhdistämään usean vertaissolmun laiterajapinnat keskenään.

4.7 Resurssien kartoitus (eng. Universal Resource Binding and Rendezvous)

JXTA-verkossa käytetään universaalia päättäjä-palvelua (eng. Resolver), joka hoitaa verkon palveluihin liittyviä perustehtäviä. Näitä ovat esimerkiksi vertaissolmun nimen liittäminen IP-osoitteeseen, IP-pistorasian (eng. Socket) liittäminen porttiin, palvelun löytäminen LDAP-hakemistopalvelun avulla ja tiedon etsintä hajautetussa tiedostojärjestelmässä (eng. Network Filesystem, NFS). Kaikki edellä mainitut operaatiot käyttävät JXTA-verkon mainoksia hyväkseen.

Kohtauspaikka-vertaisolmu (eng. Rendezvous Peer) on erityinen vertaissolmu, jotka ovat tunnettuja muiden vertaissolmujen keskuudessa ryhmän sisällä. Kohtauspaikka-vertaissolmu tallentaa muistiinsa suuren määrän mainoksia, tarjoten palveluita muille ryhmän jäsenille. Ryhmä voi sisältää mielivaltaisen monta kohtauspaikka- vertaissolmua.

Yleisesti vertaisverkoissa ylemmän tason (eng. High level) hakupalvelut tarjoavat tehokkaammat hakumenetelmät, koska palveluilla on parempi tietous tiedon levinneisyydestä vertaissolmujen keskuudessa (esimerkkeinä Chord [2], Content Addressable Network (CAN) [7]). Kohtauspaikka-arkkitehtuuri tarjoaa sekä alemman tason hakupalvelut mainosten löytämiseen sekä koukkuja (eng. Hooks), joita voidaan käyttää hyväksi ylemmän tason mainosten etsintään.

5 Protokollat

Tässä kappaleessa on esitelty JXTA-verkon pääprotokollat.

5.1 Peer Discovery Protocol

Auttaa yksittäistä vertaissolmua löytämään mainoksia, toisia vertaissolmuja ja vertaissolmuryhmiä JXTA-verkossa. Jos vertaissolmun tai vertaissolmuryhmän nimeä ei ole määritelty, protokolla palauttaa kaikkia saatavilla olevat mainokset haun tuloksena.

5.2 Peer Resolver Protocol

Mahdollistaa vertaissolmun lähettää ja vastaanottaa yleisiä kyselyitä vertaissolmuun, vertaissolmuryhmään, piippuihin tai tietoon liittyen. Yleensä tämä protokolla on ainoastaan käytössä kohtauspaikka-vertaissolmuissa.

5.3 Peer Information Protocol

Auttaa vertaissolmua ymmärtämään muiden vertaissolmujen palveluita sekä tiloja. Esimerkiksi vertaissolmu voi lähettää testi-viestin (eng. Ping message) toiselle vertaissolmulle varmistaakseen, että onko kohteena ollut vertaissolmu saatavilla.

5.4 Peer Membership Protocol

Mahdollistaa yksittäisen vertaissolmun tulla vertaissolmuryhmän jäseneksi, luoda hakemus vertaissolmuryhmään liittymiseksi tai ryhmästä poistumiseksi, ottaa ryhmän mainoksia vastaan ja päivittää ryhmän jäsenyyteen liittyviä tietoja.

5.5 Pipe Binding Protocol

Mahdollistaa vertaissolmun liittää piipun mainos piipun kohteeseen.

5.6 Peer Endpoint Protocol

Auttaa vertaissolmua kysymään reititin-vertaissolmulta (eng. Peer Router) polkuja kohde vertaissolmuun. Tämä on hyödyllistä silloin, kun vertaissolmut ovat fyysisesti eri verkoissa tai kun palomuuri on vertaissolmujen välissä. Vertaissolmu voi luoda itsestään reititin-vertaissolmun hyödyntämällä Peer Endpoint-tekniikkaa.

6 Ohjelmistoarkkitehtuuri

JXTA-teknologian ohjelmistoarkkitehtuuri jakaantuu kolmeen päällekkäiseen kerrokseen, ytimeen, palveluihin ja sovelluksiin. Kuvassa 6.1 on esitetty JXTAn ohjelmistoarkkitehtuuri.

Seuraavissa kappaleissa käsitellään JXTAn ohjelmistoarkkitehtuurin eri kerroksia.

6.1 Ydin (eng. Core)

JXTAn ydin tarjoaa peruspavelut vertaissolmu-palveluille sekä -sovelluksille. Turvallinen suoritusympäristö, vertaissolmuryhmät, piiput sekä JXTA-verkon monitorointi on sisään rakennettu ytimeen.

Ytimessä on tuki myös anonyymeille tai rekisteröityneille käyttäjille sekä salatulle tai ei-salatulle tiedolle.

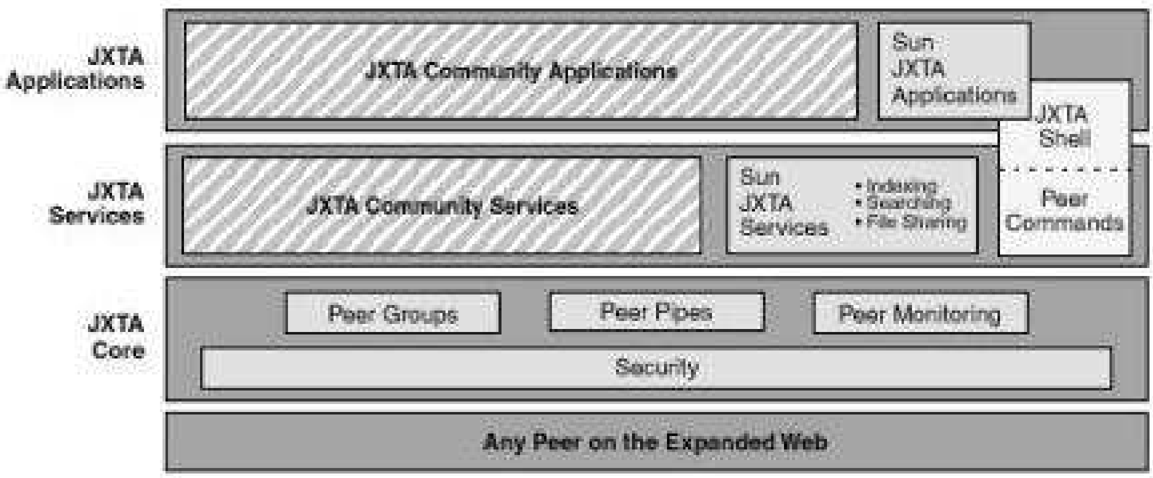
6.2 Palvelut (eng. Services)

Palvelut-kerros laajentaa ydin-kerroksen palveluita. Palvelu-kerros tarjoaa palvelut tiedon hakemiseen, tiedon jakamiseen, tiedon indeksointiin ja tiedon tallentamiseen.

Palvelu-kerros sisältää lisäksi tietoturvapalveluita, joiden avulla voidaan rakentaa turvallisia vertaisverkko- sovelluksia.

6.3 Sovellukset (eng. Applications)

JXTA-sovellukset on rakenettu käyttäen ydin- ja palvelu-kerroksen palveluita hyväksi. JXTA-sovelluksia voivat olla esimerkiksi pikaviestimet, sähköposti- ja kalenteripavelut sekä resurssien hakuun tai siirtoon erikoistuneet sovellukset.



Kuva 6.1: JXTAn ohjelmistoarkkitehtuuri (© Sun Microsystems).

6.4 Esimerkki sovellus: Kuori (eng. JXTA Shell)

Kuori on hyvä esimerkki JXTA-arkkitehtuurin päälle rakennetusta sovelluksesta. Kuori on interaktiivinen komentorivipohjainen sovellus, samanlainen mitä yleimmät kuoret ovat Unix-järjestelmissä. Suurin ero Unix-kuoren ja JXTA-kuoren välillä on se, että Unix-kuoren komennot on tarkoitettu suoritettavaksi paikallisessa ympäristössä, kun taas JXTA-kuoren komennot suoritetaan hajautetussa verkkoympäristössä.

Kuori JXTA-ympäristössä on yksinkertainen komentotulkki, joka hyväksyy komennon, tulkitsee komennon, suorittaa komennon ja odottaa komentoon vastausta. Komentoja ovat esimerkiksi "ls", "cat"ja "grep", aivan kuten perinteisissä Unix-järjestelmissä. Kuoren omainaisuuksiin kuuluu "piiputus", (vertaa edelleen perinteiset Unix-järjestelmät), jonka avulla tietyn komennon vaste voidaan antaa toisen komennon syötteeksi.

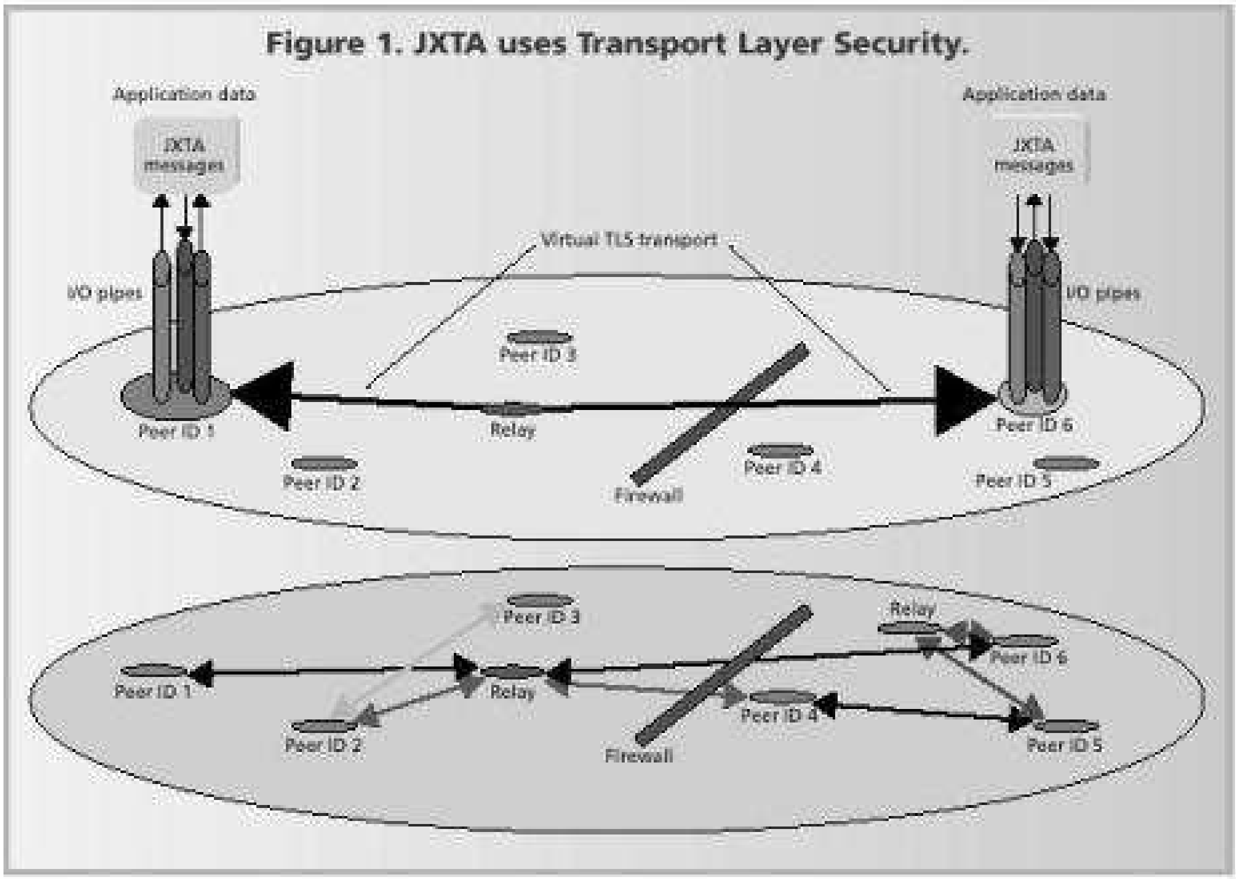
7 Tietoturva JXTA-arkkitehtuurissa

Kuten muissakin tietojärjestelmissä, myös vertaisverkoissa tarvitaan tiedon salaamista. Luottamus, koskemattomuus ja saatavuus ovat avainsanoja puhuttaessa tietoturvasta. Käytännössä edellä esitetyt vaatimukset tarkoittavat käyttäjän tunnistusta, valvontaa, tiedon sekä liikenteen salausta.

Jos JXTA-verkossa halutaan käyttää tiedonsiirron yhteydessä salausta, on käytettävä Transport Secutiry Layer 1.0- protokollaa (TSL 1.0) [3] . TSL-protokollan käyttö jakaa JXTA-verkon kahteen päällekkäiseen kerrokseen. Alempi kerros koostuu JXTA-verkon pohjalla olevasta virtuaaliverkosta, joka mahdollistaa tiedon siirron kahden vertaissolmun välillä, vaikka fyysisessä verkossa tämä olisi huomattavan vaikeaa. Ylempi kerros koostuu TLS 1.0-protokollaa käyttävästä, edelleen virtuaalisesta verkosta. Ero alemman kerroksen virtuaaliseen verkkoon on se, että TLS-protokolla luo turvallisen siirtoyhteyden niiden vertaissolmujen välille, joiden keskuudessa tiedosiirto tapahtuu. Kuvassa 7.1 on esitetty arkkitehtuurin perusrakenne.

JXTA-verkossa käytetään Poblano-tietoturva-arkkitehtuuria [17]. Tiedon kuljettamiseen käytetään TSL 1.0-protokollaa ja tiedon salaamiseen RSA 1024-, 3DES- ja SHA-1-algoritmeja. TLS 1.0-protokollan on kehittänyt Internet Engineering Task Forde (IETF) ja se on jatkokehitysversio aiemmin luodulle Secure Sockey Layer 3.0-protokolalle. TSL 1.0-protokolla on kaksisuuntainen ja tieto siirtyy JXTA-verkossa 16 kilotavun osissa. Koska tiedonsiirtoväylä on kaksi suuntainen, pitää tiedonsiirron molemmat osapuolet pystyä tunnistamaan. Vertaissolmun pitää hankkia itselleen toisen vertaissolmun X509.V3-juuriserfifikaatti (eng. Root Certificate), jotta tiedonsiirto tapahtuisi turvallisesti. Sertifikaatti sisältää RSA 1024-algoritmin mukaisen julkisen avaimen, jonka avulla vertaissolmu voi tunnistaa X509.V3-palvelusertifikaatin yksityisen avaimen. TLS 1.0-protokolla käyttää palvelusertifikaatteja vertaissolmujen tunnistamiseen.

Vertaissolmut voivat hankkia toisen vertaissolmun juurisertifikaatin itselleen kahdella eri tavalla. Ensimmäinen tapa on levittää vertaissolmun juurisertifikaattia JXTA-verkon mainoksissa. Tämä ei kuitenkaan suositeltavaa, koska silloin "Mies keskellä-



Kuva 7.1: TSL-protokolla JXTA-arkkitehtuurissa (© IEEE).

hyökkäys (eng. Man In The Middle Attack, MITM) saattaa tapahtua. MITM-hyökkäys on käytännössä vaikea suorittaa, koska sertifikaatit on vahvasti salattuja. Toinen, turvallisempi tapa levittää juurisertifikaatteja on liitää juurisertifikaatti binäärisen tiedon sekaan, jolloin MITM-hyökkäykset eivät olet mahdollisia.

Tällä hetkellä JXTA-projektissa kehitetään menetelmää, joka mahdollistaa vertaissolmuryhmien tunnistamisen. Menetelmä pohjautuu X509.V3-sertifikaatteihin. Kun vertaissolmu liittyy vertaissolmuryhmään, saa uusi vertaissolmu ryhmän perustajan julkisen juurisertifikaatin itselleen tiedonsiirtokanavaa pitkin, jossa käytetään TLS 1.0-protokollaa. Tämän jälkeen uusi vertaissolmu käyttää Certificate Service Request-palvelua (CSR) ja juuri saatua julkista avainta hyväksi hankkiessaan ryhmänjäsenyys-sertifikaatin itselleen. Sertifikaatti on X509.V3-muotoinen ja se on allekirjoitettu ryhmän perustajan yksityisellä juurisertifikaatti-avaimella.

8 Tiedonhaku vertais- ja JXTA-verkoissa

8.1 Tiedonhaku vertaisverkoissa

Tiedon hakeminen hajautetussa vertaisverkossa voidaan jakaa kahteen eri osaan [?]. Ensimmäinen, ei-sisältöpohjainen haku (eng. Content-agnostic Search), pohjautuu menetelmään, jossa tarkoituksena on löytää verkosta muita solmuja, jotka sisältävät tarvittavat tiedot haun suorittamiseen. Yleensä nämä solmut ovat palvelimia, jotka pitävät yllä erilaisia hakemistoja verkossa liikkuvasta tiedosta ja tietoon liittyvistä solmuista. Ei-sisältöpohjaista hakutekniikkaa käyttävät esimerkiksi Napster- ja Gnutella-tiedostonjako-ohjelmat. Ei-sisältöpohjaisen haun etuina ovat haun nopeus sekä pieni verkon kuormitus. Heikkouksina voidaan pitää virheensietokykyä, laajennettavuutta sekä keskitettyä ylläpitoa.

Toinen tekniikka on nimeltään sisältöpohjainen haku (eng. Content-based Search). Sisältöpohjaisessa haussa haun kyselyä (eng. Search Query) ohjataan haun sisällön perusteella verkon solmujen välillä. Jossain vaiheessa kysely ohjautuu verkossa oikealle solmulle, joka pystyy vastaamaan kyselyyn ja palauttamaan haun tulokseen. Esimerkkejä tietopohjaisesta hausta ovat (CAN) sekä Chord. Kun uusi solmu liittyy tietoverkkoon, jossa käytetään tietopohjaista hakua, tulee solmun ensimmäiseksi luoda hakemisto (eng. Index) oman alueen (eng. Zone) mainoksista. Yksittäisten alueiden hakemisto-unioni muodostaa olemassa olevan verkon koko tietovaraston. Alue, joka uudellee solmulle varataan, on dynaaminen ja se rippuu verkon solmujen lukumäärästä sekä yksittäisten solmujen poistumisesta verkosta tai liittymisestä verkkoon. Kun verkon solmu haluaa julkaista uuden mainoksen resurssiin tai tietoon liittyen, se tutkii mainoksen sisällön. Sisällön perusteella solmu osaa lähettää mainoksen verkossa oikeaan paikkaan. Hajautus on yleisin tapa laskea mainoksen paikka tietoverkossa.

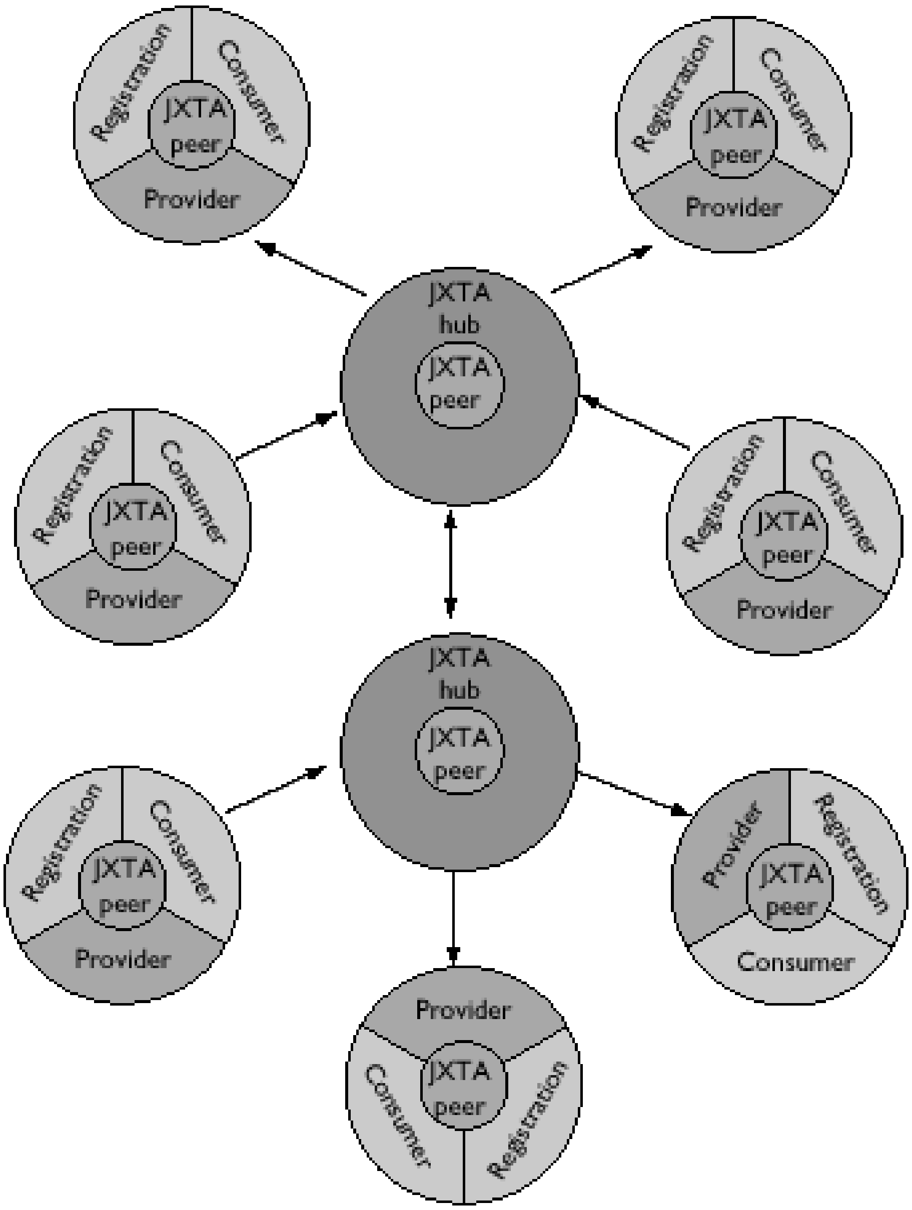
8.2 Tiedonhaku JXTA-verkossa

Haku JXTA-verkoissa pohjautuu keskitin-solmuihin (eng. Hub Peer) sekä XML-pohjaisiin viesteihin. Kuvassa 8.1 on esitetty JXTA-verkon verkkotopologia tiedonhaun yhteydessä.

Tietoa voidaan hakea JXTA-verkossa joko syvyys- tai leveyssuunnassa. Tämä mahdollistaa tehokkaat hakualgorimit sekä vähentää verkon kuormitusta. Kun vertaissolmut julkaisevat mainoksia, ne tallennetaan keskitin-vertaissolmuihin. Yksittäiset keskitin-vertaissolmut voivat ohjata kyselyjä toisiin keskitin-vertaissolmuihin. Lisäksi keskitin- vertaissolmut voivat keskittyä maantieteellisesti sekä sisällön tai sovelluksen perusteella.

JXTA-verkossa käytetään hakujen suorittamiseen Query Routing-protokollaa (QRP). Koska protokolla on XML-muotoinen viesti, on se kevyt ja yhteensopiva eri järjestelmien välillä. QRP koostuu kolmesta viestimuodosta, rekisteröinnistä (eng. Registration), pyynnöstä (eng. Request) sekä vastauksesta (eng. Response). Rekisteröinti-viestimuotoa käytetään uusien resurssien julkituomiseen, pyyntö-viestimuotoa tiedon ja resurssien hakemiseen sekä vastaus-viestimuotoa haun tuottamien vastausten palauttamiseen. Kaikki komponentit sijaitsevat kyselyavaruudessa (eng. Query Space), joka vastaa XML-standardin nimiavaruuksia (eng. Namespace). Kuvassa 8.2 esitetty pyyntö-viesti.

Pyyntöjen palauttamiin hakutuloksiin voidaan vaikuttaa Query Node Pattern-tekniikan (QNP) avulla. Se on tekniikka, jossa loogisia predikaatteja käytetään kuvamaan tietoa tai resurssia. Predikaatit voivat olla yksittäisiä sanoja tai loogisia operaattoreita, kuten "Tai"(eng. Or) ja "Ja"(eng. And). Kuvassa 8.3 on esitetty rekisteröinti-viesti. Viestissä rivi "http://big-bookseller.com/jxtasearch"määrää käytettävän kyselyavaruuden. Tämä viesti rekisteröi kyselyavaruuteen uudet avainsanat "Joy", "Stephenson", "Java", "JXTA", "XML"ja "Cryptography". Kaikki pyyntö-viestit, jotka hakevat edellä mainittuja sanoja (esimerkiksi kuvan 8.2 viesti), suoritetaan "http://big-bookseller.com/jxtasearch-palvelimella.



Kuva 8.1: Tiedon haku JXTA-verkossa (© IEEE).

```
<?xml version=‘1.0’?>
<request id=“1C8DAC3036A811D584AEC2C23”
       query-space=“http://bigbookseller.com/js”
       xmlns=“http://jxta.org/search”>
       <query>
              <author> Joy </author>
              <title> Java </title>
       </query>
</request>
```

Kuva 8.2: Eräs XML-muotoinen pyyntö-viesti (© IEEE).

```
<?xml version=‘1.0’?>
<register xmlns=“http://search.jxta.org”>
    <query-server>
       http://bigbookseller.com/exec/jxtasearch
    </query-server>
    <query-space
uri=“http://bigbookseller.com/jxtasearch”>
       <predicate>
       <query>
          <author> Joy Stephenson </author>
          <title> Java JXTA XML Cryptography </title>
       </query>
       </predicate>
    </query-space>
</register>
```

Kuva 8.3: Eräs XML-muotoinen rekisteröinti-viesti (© IEEE).

9 Yhteenveto

JXTA-projektin tuotoksena on syntynyt monipuolinen vertaisverkkojärjestelmä. Avoimuus, tietoturva, sovellusten yhteensopivuus sekä laitteistoriippumattomuus ovat asioita, jotka erottavat JXTA-arkkitehtuurin muista vertaisverkkojärjestelmistä. Erityisesti JXTAn kehittynyt tietoturva-arkkitehtuuri mahdollistaa vertaisverkkosovellusten käytön tilanteissa, joihin aiemmat vertaisverkkotekniikat eivät ole soveltuneet. JXTA-arkkitehtuuri auttaa sovelluskehittäjiä keskittymään olennaiseen. Ohjelmoijan ei tarvitse syventyä erilaisiin yksityikohtiin, vaan voi heti alkaa kehittämään turvallisia ja tehokkaita ja ennen kaikkea hajautettuja sovelluksia vertaisverkkoympäristöön

10 Kirjallisuutta

[1] Botros Sherif, Waterhouse Steve, ”Search in JXTA and Other Distributed Networks”, 0-7695-1503-07/02 IEEE, 2002

[2] Dabek F. ym., ”Building Peer-to-Peer Systems with Chord”, a Distributed Lookup Service, 2001

[3] Dierks T., Allen C., ”The TLS Protocol”, IETF RFC2246, January 1999

[4] Gong Li, ”Project JXTA: A Technology Overview”, saatavilla WWW-muodossa <URL: `http://www.jxta.org/project/www/docs/TechOverview.pdf`>, viitattu 11.10.2002

[5] Gong Li, ”JXTA: A Network Programming Environment”, 1089-7801/01 IEEE / IEEE Internet Computing May-June 2001

[6] Oram Andy, ”Harnessing the Power of Disruptive Technologies”, O’Reilly, 2001

[7] Ratnasamy S. ym., ”A Scalable Content Addressable Network”, ACM SIGCOM, 2001

[8] Traversat Bernard ym., ”Project JXTA Virtual Netowk”, saatavilla WWW-muodossa <URL: `http://www.jxta.org/project/www/docs/JXTAprotocols.pdf`>, viitattu 11.10.2002

[9] Yeager William, William Joseph, ”Secure Peer-to-Peer Networking, The JXTA Example”, 1520-9202/02 IEEE / IT Professional Volume: 4; Issue: 2, March-April 2002

[10] Waterhouse Steve ym., ”Distributed Serach in P2P Networks”, 1089-7801/02 IEEE / IEEE Internet Computing, January-February 2002

[11] "Project JXTA: An Open, Innovative Colloboration", saatavilla WWW-muodossa <URL: `http://www.jxta.org/project/www/docs/OpenInnovative.pdf`>, viitattu 11.10.2002

[12] JXTA-projekti, saatavilla WWW-muodossa <URL: `http://www.jxta.org`>, viitattu 11.10.2002

[13] Gnutella, saatavilla WWW-muodossa <URL: `http://www.gnutella.wego.com`>, viitattu 11.10.2002

[14] Napster, saatavilla WWW-muodossa <URL: `http://www.napster.com`>, viitattu 11.10.2002

[15] Zeropaid Portal, saatavilla WWW-muodossa <URL: `http://www.zeropaid.com`>, viitattu 11.10.2002

[16] IEEE 802.11 WLAN WORKING GROUP, saatavilla WWW-muodossa <URL: `http://grouper.ieee.org/groups/802/11/`>, viitattu 11.10.2002

[17] Poblano, a Distributed Trust Model for Peer-to-Peer Networks, saatavilla WWW-muodossa <URL: `http://www.jxta.org/project/www/docs/trust.pdf`>, viitattu 11.10.2002