International Journal of Interdisciplinary Telecommunications and Networking

April-June 2009, Vol. 1, No. 2

Table of Contents

Research Articles

1 **Hybrid Trust Structure in Self-Organizing Networks**
Tong Zhou, University of Missouri at Kansas City, USA
Lein Harn, University of Missouri at Kansas City, USA

16 **Error Probability for Coherent Modulations in Rician Fading Channel**
A. Chandra, N.I.T. Durgapur, India
C. Bose, Jadavpur University, India

28 **On Peer-to-Peer Location Management in Vehicular Ad Hoc Networks**
Zhaomin Mo, Florida International University, USA
Hao Zhu, Florida International University, USA
Kia Makki, Florida International University, USA
Niki Pissinou, Florida International University, USA
Masoumeh Karimi, Florida International University, USA

46 **Distributed Algorithms for Delay Bounded Minimum Energy Wireless Broadcasting**
Serkan Çiftlikli, Sabancı University, Turkey
Figen Öztoprak, Sabancı University, Turkey
Özgür Erçetin, Sabancı University, Turkey
Kerem Bülbül, Sabancı University, Turkey

66 **User-Based Channel Assignment Algorithm in a Load-Balanced IEEE 802.11 WLAN**
Mohamad Haidar, Ecole de Technolgie Superieure, Canada
Hussain Al-Rizzo, University of Arkansas at Little Rock, USA
Yupo Chan, University of Arkansas at Little Rock, USA
Robert Akl, University of North Texas, USA

Hybrid Trust Structure in Self-Organizing Networks

Tong Zhou, University of Missouri at Kansas City, USA

Lein Harn, University of Missouri at Kansas City, USA

ABSTRACT

A traditional service provider of telecommunications is recognized as an authority which is trusted by the subscribers and the public. Ad hoc and Peer to Peer (P2P) networks have demonstrated advantages that service provider controlled networks lack, and they also exhibit self-organizing behaviors. A pure self-organizing network does not rely on any hierarchical management. Instead, it utilizes a web of trust for security. Its trust management is complicated and varies from node to node. In this article, we discuss a hybrid trust structure that leverages the involvement of an authority in a self-organizing network to increase trust levels between disconnected small-worlds. The new model will help service providers design more robust and innovative solutions for next generation networks and applications. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: *Privacy; Public Key Encryption; Security Risk; Social Networks; Telecommunications; User; Wireless Technologies*

INTRODUCTION

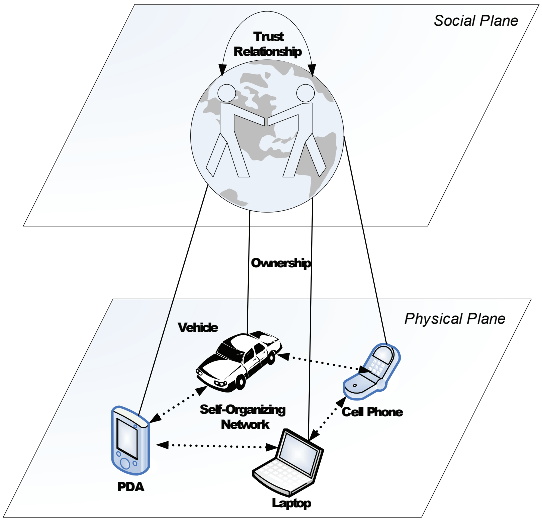
Wireless and internetworking technologies (i.e. IEEE 802.11 and the Internet) have provided opportunities for user equipment (UE) to directly communicate among themselves, bypassing traditional service providers' physical and logical controls. Today, UE (i.e. wireless handset, Personal Digital Assistant (PDA) or laptop computer) is a multifunction and multipurpose device. Not only does it provide a connection channel, makes a phone call and browse the Internet, but also stores personal data, makes electronic payments, determines its location, and so on. The traditional way of offering services is through telecommunications service providers. Service providers control the admissions to their network infrastructures, including access networks, such as Worldwide Interoperability for Microwave Access (WiMAX), Transmission Control Protocol/Internet Protocol (TCP/IP) transport networks and service networks, such as IP Multimedia Subsystems (IMS) through Authentication, Authorization and Accounting (AAA). Agreements may exist among different service providers for roaming and service peering purposes. A subscriber either shares a secret with the service provider or uses a digital certificate issued by the Public Key Infrastructures (PKI) of an authority for security. The issue of a service provider's complete control is that all users' service requests must be backhauled to a control point at a national or regional data center or the edge of the service provider's network. In an emergency, such as natural disaster or terrorist attack, this infrastructure centric control model is not robust enough to handle larger than the normal bursts traffic. Even during normal operations it is inefficient for a user to transmit large amounts of data (i.e. file sharing and streaming video) to another user through a server provider's network infrastructure when a self-organizing network provides a direct channel or a shorter path.

A self-organizing network, which can be a Mobile Ad hoc NETwork (MANET), a Peer-to-Peer (P2P) network, a mesh network or a wireless sensor network, is a promising approach for providing flexibilities for users to form a network and control applications by themselves. It can potentially reduce the burden on a service provider's network, increase service availability and reliability, and drive innovations. However, the challenge of a self-organizing network is the lack of a centralized control of authority. Without this it is difficult to establish secure communications. A pure self-organizing network does not assume any authority for managing communications. A user makes their own decision. A reputation system can be used to improve the performance of a self-organizing network. It helps users identify trusted nodes.

Network security plays a crucial role for service providers. Popular applications are often targeted by hackers. Various security attacks, such as Distributed Denial of Services (DDOS), Man-in-the-Middle and SPAM can negatively impact service performance. Implementing strong authentication and diverting unknown traffic can effectively avoid attacks. In cryptograph, a digital certificate is used to bind the public key and the identity of the owner using a digital signature of a Certification Authority (CA) to prevent impersonation attack. Both hierarchical, such as ITU X.509, and nonhierarchical, such as Pretty Good Privacy (PGP), certification structures can be used to secure communications between two nodes. Hierarchical PKI require a root CA, which may not exist in cross-domain scenarios. A nonhierarchical structure, which is also known as web of trust, has the flexibility to allow any user to be a CA. However, it is very challenging to manage the trust relationships between CAs. PGP defines trust levels and allows a user to assign three levels of trustworthiness (complete trust, marginal trust and no trust) to another user's certification capability. In PGP, a user only accepts a stranger's certificate if it is issued by a CA that is completely trusted, or two CAs that are marginally trusted by the user. Trust is based on context and subjective. Li, Li and Kato (2008) define trust as a belief level that one node can put on another node for a specific action according to previous direct or indirect information from the observation of behaviors. In this article, trust refers to the belief of certification capability of a user. Studying how people trust each other will help improve the design of self-organizing networks.

Small world phenomenon reveals the fact that people are connected through six or less acquaintances (six degrees of separation) (Watt, 1999). Figure 1 shows two planes in a self-organizing network. The physical plane includes a variety of UE that is capable of forming self-organizing networks using existing (i.e. WiFi and TCP/IP) or future networking technologies. The social plane reflects the trust relationships among users. It controls the self-organizing networks on the physical plane through equipment ownerships. The discovery of six degrees of separations supports the feasibility of establishing self-organizing networks as people are all connected through a small number of intermediate hops. However, it does not mean people on the connection path all trust each other. Additionally, there are different levels of trusts assessed by each individual. Therefore, from a trust perspective, the whole world is viewed as a collection of loosely connected or isolated groups. The services offered by Tier 1 service providers in the United States (U.S.)

Figure 1. Self-organizing network layers



are often targeted for 99.999% availability. A self-organizing network will not be highly available and scalable if there are too many loosely connected or isolated groups in it.

To solve the trust problem, we propose a novel method to utilize a hybrid trust structure for certification in order to connect groups where there is no strong trust between them. Within a group, the trust structure web can still be used for trust establishment. Between groups, a hierarchical trust structure is applied to bridge them. This solution will benefit both service providers and self-organizing networks. In human life, P2P services and mass collaboration, such as the online community for lending money (www.prosper.com) and wikipedia (www.wikipedia.com) are future trends, where trust is a fundamental issue that needs to be further studied.

The rest of the article is organized as follows: after a review of related works, we will explain the terminologies used in this article. Then the hybrid certification structure is described, followed by a section that provides a security protocol for exchanging private information between peers. The next section analyzes the effectiveness of endorsements, followed by the simulation results, with the final section summarizing the key contributions and introducing future work.

RELATED WORKS

A self-organizing network exhibits the structure of decentralization in many aspects, including signaling, data transportation, security, reputation management and charging. This section discusses prior art that is related to self-organizing security. Public-key and symmetric-key techniques can be used in self-organizing networks to establish security associations (Capkun, Hubaux, & Buttyan, 2006). Pairwise symmetric keys lack scalability (Zhang, Liu & Fang, 2006). In a P2P environment, public keys can be certified by an authority or individuals. In the scope of pure self-organizing networks, we do not assume any hierarchical certification structure. ID-based cryptography (IBC) is an alternative to certificate-based cryptography (CBC). Zhang et al. (2006) devise an ID-based key management scheme called IKM, which still requires a single authority. Suryanarayana, Erenkrantz and Taylor (2005) summarize different types of security threats. Sanzgirl, LaFlamme, Dahill, Levine, Shields and Belding-Royer (2005) design a protocol named 'authenticated routing' for ad hoc networks (ARAN), which uses public-key cryptography to defeat the identified attacks. Sun, Osborne, Xiao and Guizani (2007) present an overview of intrusion detection techniques and future research directions in MANET and wireless sensor networks.

There are many proposals on the web of trust based public-key certifications. Sun, Yu, Han and Liu (2006) propose entropy-based and probability based trust models. Caronni (2000) discusses the algorithms for computing multiple interconnected trust paths. Theodorakopoulos and Baras (2006) view the trust evaluation as a generalized shortest path problem on a weighted directed graph and propose a trust computation scheme. Li et al. (2008) design a robust and attack-resistant framework, which is called the objective trust management framework (OTMF) based on a modified Bayesian approach by which various weights are put on different information related to the observations of behaviors according to their occurrence time and providers. In previous research (Zhou & Harn, 2007), we discuss the method of utilizing the public key trust and validity levels to obtain an end-to-end trust, and summarize different thresholds for making a trust decision. When no connection with a newly joined node is found, and to mitigate the risks of blind trust, we introduce the macro and micro methods of analyzing the trust relationships among the CAs which issue certificates to the node (Zhou & Harn, 2008). More discussions on security and trust are found in Xiong and Liu, 2004; Josang, Hayward and Pope, 2006; Huynh, Jennings and Shadbolt, 2006; Papadimitratos and Hass, 2006; Yang, Shu, Meng and Lu, 2006; Ma and Orgun, 2006; Lin, Lu, Zhang, Zhu, Ho and Shen, 2008.

However, to the best of our knowledge, there is no comparison on the service quality of a carrier's network and a self-organizing network. In self-organizing networks, low and no trust are common obstacles to achieving high availability and reliability while maintaining security. Without quality and security, the applications of self-organizing networks will be very limited to specific environments and only provide better than nothing services. To improve the performance of self-organizing networks, we propose a framework that allows an authority to bridge the trust gaps between loosely connected or isolated groups by leveraging its authority-endorsements on selected nodes, which become super-nodes. The introduction of super-nodes can help users establish a new certification path or short-cut a low trust path. We expect the confidence on the public key ownership can be increased. Therefore, self-organizing networks will be more practical and popular. The hybrid certification structure, which is detailed in a later section, inherits the advantages of hierarchical and non-hierarchical certifications.

DEFINITIONS AND BACKGROUND

Authority

In this article, an authority is a truly accountable administration in communications. Its judgments are completely or strongly trusted by the public. An authority is trusted is because it has proven records of being responsible for its behaviors. It must have AAA functions and is supposed to have a strict process for making sound decisions. Most authorities have AAA functions. As discussed in the following sections, an authority is expected to identify super-nodes and issue endorsement certificates properly to improve the performance of self-organizing networks.

Endorsement

An authority may provide a node in self-organizing networks with an endorsement certificate that not only binds the node's public key to its identity, but also includes the node's certification capability that the authority recognizes. In this article, this behavior is called endorsement. When compared to a PGP certificate, an endorsement certificate makes the trust level (i.e. gold, silver, or bronze) public and recognized. An example of an endorsement certificate is as follows:

Version: 10
Serial Number: 8390
Algorithm/Parameter: MD5, RSA
Issuer: Service Provider Company Name
Validity Period: mm/dd/yyyy – mm/dd/yyyy
Subject Identity: Bob.Rose@company.com
Subject's Public Key:
  00:c6:a9:d3:1b:25 …(RSA, 1024 bits)
Subject's Certification Capability: Gold
Signature: 45:9a:3b:12:8d …

Super-Node

An authority-endorsed node is referred as a super-node in this article. The certification capability of a super-node is described in the endorsement certificate example above. To become a super-node, a regular node must meet certain criteria, such as an excellent certification reputation and history, hardware and software capabilities, I/O throughput, and a willingness to assist other nodes in self-organizing networks. Through a common authority, a super-node trusts the other super-nodes. A similar concept exists in P2P VoIP (Voice over Internet Protocol) communications (i.e. Skype), where a super-node assumes the responsibility to assist other nodes to connect to each other as a routing hub. The super-node defined in this section functions as a reputable CA. The two types of super-nodes can coexist but are not necessarily in the same UE.

HYBRID CERTIFICATION STRUCTURE

In a service provider controlled network, a user can either share a secret with the service provider or use a service provider accepted certificate for security. As it is expensive for a service provider to build PKI, in most cases, an asymmetric key is not provided for the UE. In self-organizing networks, there is no centralized authority. A user stores the others' public keys in their key ring (local directory) and assigns a value of validity and trust to each key. Furthermore, a user can issue digital certificates to attest to the integrity and the ownership of the public keys. The certificates can be used by others who trust the issuer to verify the public keys and the identities.

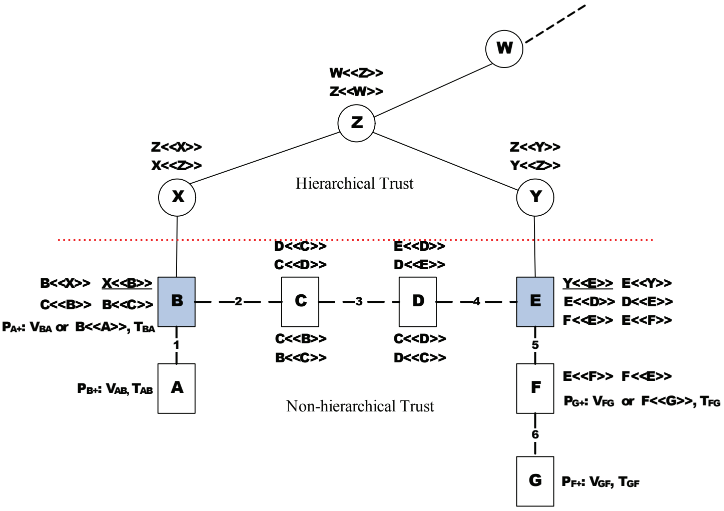
The advantage of hierarchical certification systems is that users completely trust the CAs' certifications capability. However, due to different reasons, such as Return on Investment (ROI), an authority may not build a hierarchical structure when users need it. Then an individual user must obtain the certificate from the authority. In contrast, a self-organizing network may be voluntarily formed by individual users to overcome the absence of authority control. High trust can possibly exist in a small group. In the real world, not all groups are strongly connected. Therefore, a self-organizing network is hard to scale. The hybrid trust structure we propose in this article combines the advantages of hierarchical and non-hierarchical trust structures to solve the no trust or low trust issue in self-organizing networks. The trusts among authority-endorsed super-nodes can be increased such that two super-nodes can establish a strong path to replace a weak link. This benefit does not exist in a pure non-hierarchical structure. An example of hybrid structure is a self-organizing community WiFi network. A resident may establish a strong trust with the neighbors in the community, but may not trust other residents in a different community. Without the involvement of an authority, the person can only be served within the neighborhood due to the lack of strong trust outside the community. In a hybrid structure, super-nodes bridge disconnected communities through the endorsements of an authority. Thus, residents in different communities can establish strong trusts, which results in improved service performance.

Figure 2 illustrates a self-organizing network with authority endorsements. Nodes X, Y, Z and W represent CAs in a hierarchical structure. X and Y are leave nodes and are under Z. The root of the tree is not shown. M<<N>> represents a certificate that M issues to N. V_{MN} and T_{MN} are the validity and trust levels that M assigns to N's public key, P_{N+} respectively. B and E are super-nodes endorsed by an authority through its local CAs, X and Y, respectively. B and E also sign the public keys of X and Y, respectively. Through certifications, trusts can be propagated in the network.

Nodes A, B, C, D, F and G participate in a self-organizing network. Based on the small-world phenomenon, any nodes in a self-organizing network are connected by six or less intermediate nodes. Assume A does not know G directly and needs to communicate with it. A requests his or her friends to find connections to G. Among them, B's public key ownership (V_{AB}) and certification capability (T_{AB}) are trusted by A. B issues B<<C>> to C, and believes C's certification capability is T_{BC} (not shown); C issues C<<D>> to D, and believes B's certification capability is T_{CD} (not shown); D issues D<<E>> to E, and believes B's certification capability is T_{DE} (not shown); E issues E<<F>> to F, and believes B's certification capability is T_{EF} (not shown); F either issues F<<G>> to G or just stores the public key of G (P_{G+}) in its public key ring and assigns the validity of the key to V_{FG}.

Let the trust distance between two super-nodes be *d*. In the endorsement certificates that the authority issued to B and E, their certification capabilities (T_B and T_E) are included. There are different ways to calculate the end-to-end trust level (Sun et al., 2006; Zhou & Harn, 2007). For simplicity, we only discuss a single certification path in the following sections. The distance between two super nodes before endorsements can be different. Figure 2 shows B and E are three hops apart. For A to authenticate G, A needs to obtain the certificates on the certification path, which are B<<C>>, C<<D>>, D<<E>>, E<<F>> and F<<G>> or VFG, as well as the trust levels of certification capabilities, T_{BC}, T_{CD}, T_{DE} and T_{EF} . The following section discusses how to securely transmit trust levels and validity levels. Additionally, we assume A has securely obtained B's public key (P_{B+}), and can retrieve V_{AB} and T_{AB} from its key ring. With all the information received, A can verify the binding of G's public key and identity (Zhou & Harn, 2007). Similarly, G can assess the validity of A's public key for the purpose of mutual authentication.

Figure 2. Hybrid structure: a hypothetical example



With an authority's endorsements on nodes B and E, the hybrid certification path from A to G is B<<X>>, X<<Z>>, Z<<Y>>, Y<<E>>, E<<F>> and F<<G>> or V_{FG}. And the path from G to A is F<<E>>, E<<Y>>, Y<<Z>>, Z<<X>>, X<<B>> and B<<A>> or V_{BA}. The certification capabilities of super-nodes B and E are described in the endorsement certificates. As X, Y and Z are CAs in a hierarchical structure, they completely trust each other's certification capability. The hybrid certification path should have a higher trust than the self-organizing path. It is expected that the hybrid certification structure will improve the successful rate of communications in self-organizing networks. The quantitative studies are discussed in a later section.

PRIVATE INFORMATION EXCHANGE (PIE) PROTOCOL

This section describes a protocol for two nodes to securely exchange their personal information, such as trust levels and validity levels, in a self-organizing network. The following security requirements are identified for the design of the protocol (Sun et al., 2006):

- Mutual authentication – the two nodes involved in communications must authenticate each other.
- Data confidentiality – private information, such as trust level, transmitted between intermediate hops cannot be decoded by eavesdroppers.
- Data authenticity (integrity) – ensures data is from the intended source and not altered during transmission.
- Privacy protection – a receiver cannot prove to a third party that the received private information is from the sender.

To meet the requirements, we propose the PIE protocol, which is based on Internet Key Exchange - Secure Key Exchange MEchanism (IKE-SKEME) (Krawczyk, 1996) for the hop-by-hop private information exchange. In the following example, we assume that A stores the trust level (T_{AB}) and validity level (V_{AB}) for B's public key (P_{B+}) in its public key ring. A sends a SEARCH request to B to obtain B's confidence on C's public key (V_{BC}). In the message, A indicates that it accepts both direct and indirect trusts. For security, A encrypts its identity (A) and a random number (N_A) it generated using B's public key. Based on six degrees of separations, A chooses six as the maximum number of intermediate hops from it.

```
REQEUST SEARCH C <carol@example.com>, PIE/1.0
From: A <alice@example.com>
To: B <bob@example.com>
Search-ID: 49dks0230slwla
Information: Trust Level
Direct Trust: Yes
Indirect Trust: Yes
Max-Hops: 6 (maximum number of intermediate nodes)
Security: IKE-SKEME
Content: 87:6d:c2:fe:a4:45…
(E_B[A, N_A], where A = alice@example.com)
```

B sends back a provisional response (100 Trying) to inform A that B does not know C directly, and will forward the request to a number of trusted nodes. To avoid impersonation attacks, B only forwards the request to the nodes whose identities it trusts. If B is a super-node, it can also broadcast the request to other super-nodes. B reduces the Max-Hops it received by one and includes the new value in the forwarded message.

```
RESPONSE 100 Trying PIE/1.0
From: B <bob@example.com>
To: A <alice@example.com>
Search-ID: 49dks0230slwla
Direct Trust: Not found
Indirect Trust: Forwarding to n node(s), where n ≥ 1.
```

Assume one of the trusted nodes, J responds to B and provides V_{JC}, which J believes is the validity of C's public key, using the same

PIE protocol. B encrypts its identity (B), V_{JC}, B<<J>> (or V_{BJ}), T_{BJ} and a random number it generated (N_B) using A's public key and sends a 200 Found message to A.

B also attaches a Message Authentication Code (MAC) for data authenticity (secret key $K_0 = H(N_A, N_B)$). Therefore, A is assured that the data is from B. However, A cannot prove it to a 3rd party because the message from B does not include B's digital signature, and A can possibly forge the message by itself. The communication between B and J is protected in the same way.

RESPONSE 200 Found PIE/1.0
From: B <bob@example.com>
To: A <alice@example.com>
Search-ID: 49dks0230slwla
Indirect Trust: Found
Content: 32:1d:b2:5c:6a:f0 …
(E_A[Data, B, N_B], MAC_{K0}(Data, B, A),
where Data = T_{BJ} || V_{BJ} or B<<J>> || V_{JC} or J<<C>>, $K_0 = H(N_A, N_B)$,
B = bob@example.com, and A = alice@example.com.)

A decrypts the received message to obtain the data using A's private key and sends back an ACKnowledgement to B. A uses B<<J>> to verify J's identity and calculates the trust distance to J by calculating $T_{AB} \times T_{BJ}$. If J<<C>> is received, A concludes that the validity level of C's public key is $T_{AB} \times T_{BJ}$. If J does not issue a certificate to C, A verifies that a friend's friend, J trusts C's public key at the V_{JC} level. So the validity of C's public key is $T_{AB} \times T_{BJ} \times V_{JC}$. When A uses multiple certification paths for public key validity evaluation, it is important to identify if the paths are independent or interconnected.

ACK <carol@example.com>, PIE/1.0
From: A <alice@example.com>
To: B <bob@example.com>
Search-ID: 49dks0230slwla
Security: IKE-SKEME
Content: 14:7c:a2:df:58:93… (MAC_{K0}(A, B))

QUANTITY ANALYSIS

Trust Gain

In this section, we discuss the effectiveness of introducing two super-nodes on a certification path (see Figure 2). The super-node at the beginning of a directional path is called the upstream super-node, and the super-node at the end is called the downstream super-node. The end-to-end trust on G's public key from A is in Equation 1. After the endorsements on B and E, the trust is increased to Equation 2. The trust gain is defined in Equation 3.

$$T_{AG} = T_{AB} \times T_{BC} \times T_{CD} \times T_{DE} \times T_{EF} \times V_{FG} \qquad (1)$$

$$T_{AG}' = T_{AB} \times T_E \times T_{EF} \times V_{FG} \qquad (2)$$

$$T_{gain} = \frac{T_{AG}'}{T_{AG}} - 1 = \frac{T_{\sup er-node}}{T_{SON-path}} - 1 \qquad (3),$$

where $T_{\text{super-node}}$ is the certification capability of the downstream super-node recognized by an authority in the endorsement certificate, and $T_{\text{SON-path}}$ is the trust level between the upstream and downstream super-nodes. In Figure 2, $T_{\text{super-node}}$ and $T_{\text{SON-path}}$ are T_E and $T_{BC} \times T_{CD} \times T_{DE}$, respectively. Equation 3 indicates that the endorsement will be more effective if the downstream super-node, E improves its certification capability, $T_{\text{super-node}}$ and/or $T_{\text{SON-path}}$ is a weak link (low trust or no trust).

Assume a super-node obtains a gold level certification from an authority, the weak link length is l, and the average trust per hop is T_0. The lower limit of trust gain can be obtained from Equation 4. This is because the arithmetic mean is greater than the geometric mean (see Equation 5).

$$T_{gain} \geq \frac{T_{Gold}}{T_0^{\,l}} - 1 \qquad (4)$$

$$\frac{1}{n}\sum_{i=1}^{n} x_i \geq (\prod_{i=1}^{n} x_i)^{1/n} \qquad (5),$$

where $x_i \geq 0$

Figure 3 shows the increases of trusts for different average trusts (0.1, 0.5 and 0.9) and path lengths (1, 2, 3 and 4). The X-axis is the distance, *d* between two super-nodes in terms of the number of intermediate hops, and the Y-axis is the trust increase in a logarithmic scale. In the case of low trust (avg. trust = 0.1), the super-nodes improve the trusts significantly.

End-to-End Trust with Authority Endorsements

In a self-organizing network, a node needs to determine the end-to-end trust level (Z) to another node it encounters. Z is the product of an upstream trust level, X, and a downstream trust level, Y (see Equation 6).

$$Z = X \times Y \qquad (6)$$

Assume the Probability Density Functions (PDF) of upstream and downstream trusts are $f_X(x)$ and $f_Y(y)$, respectively (see Figure 4). The PDF varies from group to group. Figure 4 illustrates a hypothetical example, where the upstream group has strong trusts within it while, on average, the downstream group has marginal trusts.

The PDF of Z is calculated in Equation 7, where X and Y are independent trust variables.

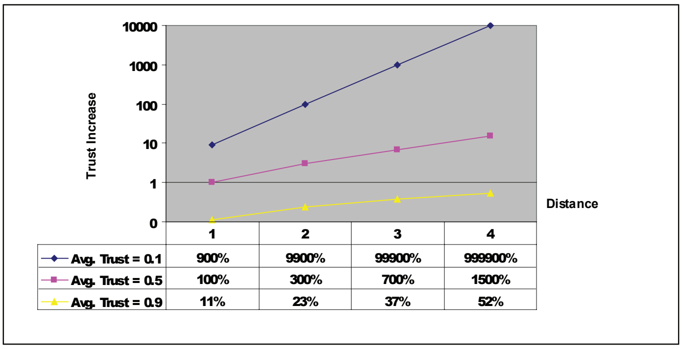
$$f_Z(z) = \int_0^1 f(z/y, y)dy = \int_0^1 f(z/x, x)dx \qquad (7)$$

As $f(x,y) = f_X(x)f_Y(y)$, $f_Y(y)$ can be obtained from Equation 8.

$$f_Z(z) = \int_0^1 f_X(x) f_Y(z/x)dx = \int_0^1 f_X(z/y) f_Y(y)dy \qquad (8)$$

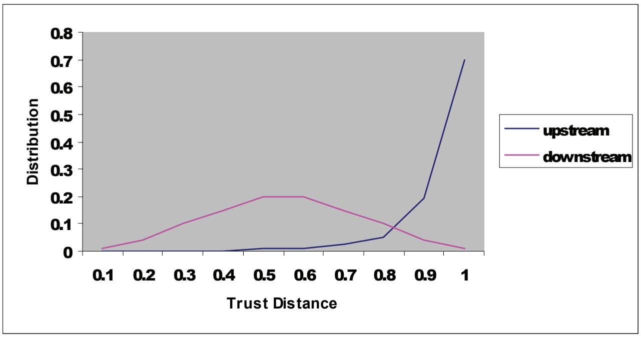
If a node selects a trust threshold T (0≤T≤1), the possibility that the end-to-end trust is higher than T is obtained from Equation 9. The higher the trust threshold used, the stronger the security achieved. The tradeoff is that the successful rate of inter-group communications becomes lower. The goal of the hybrid trust structure is to connect isolated groups which have high or medium internal trusts through endorsing super-nodes. With this approach, it is expected that the successful rate of communications is higher than 80% if a medium trust threshold is selected. The following section uses simulation to explain this in detail.

Figure 3. Trust gains



	1	2	3	4
◆ Avg. Trust = 0.1	900%	9900%	99900%	999900%
■ Avg. Trust = 0.5	100%	300%	700%	1500%
▲ Avg. Trust = 0.9	11%	23%	37%	52%

Figure 4. Upstream and downstream trust distribution example



$$P(Z > T) = 1 - \int_0^T f_Z(z)dz \qquad (9)$$

Caveman Model

Watts (1999) describes a caveman world, "Everybody you know knows everybody else you know and no on else." However, this model does not include how well a node knows other nodes. This missing part is important for people to make trust decisions. In this section, we discuss three types of caves, where the internal trusts are High, Medium and Low (see Table 1). In each cave, we assume the trusts among the nodes are identical.

An authority should focus on connecting isolated high trust and medium trust caves (see Figure 5). Although super-nodes serve as hubs connecting isolated groups, the end-to-end trust still includes the intra-group trust.

When comparing connecting two high trust groups and connecting two low trust groups, the end-to-end trust of the former is higher than that of the latter. It is unlikely that two low trust groups can establish trust unless the acceptable trust threshold is very low, which increases the risk of trusting a malicious node. Figure 6 exhibits the results of connecting H, M and L groups. There are six different combinations, HH, HM, HL, MM, ML and LL, which have the trust values of 0.81, 0.45, 0.09, 0.25, 0.05 and 0.01, respectively.

Table 1. H/M/L trusts

Intra-cave Trust Level	Quantification
High (H)	0.9
Medium (M)	0.5
Low (L)	0.1

SIMULATION

We created two groups A and B, each of which has 10 nodes (see Figure 7). The weights on the lines represent mutual trust levels. Initially, the two groups were disconnected. Group A includes Nodes 1 to 10 and Group B includes Nodes 11 to 20. The average intra-group trust is the arithmetic mean of inter-nodes direct trusts (see Equation 10).

$$T_{avg} = \sum_{i,j=1,n,i\neq j} T_{ij} / N_{MAX} \qquad (10)$$

where N_{MAX} is equal to $n^2 - n$. n is the number of nodes in a group. For Groups A and B, the average intra-group trusts are 0.767 and 0.770 respectively (see Figure 10). Nodes 10 and 20 were identified and then endorsed by an authority to become super-nodes. Thus, inter-group communications are possible. For example, we

Figure 5. Connecting caves

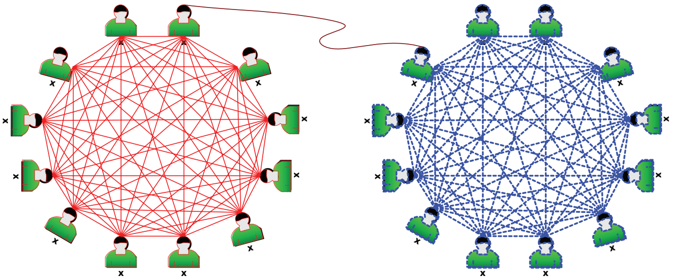


Figure 6. Connecting groups with high (H), medium (M) and low (L) trusts

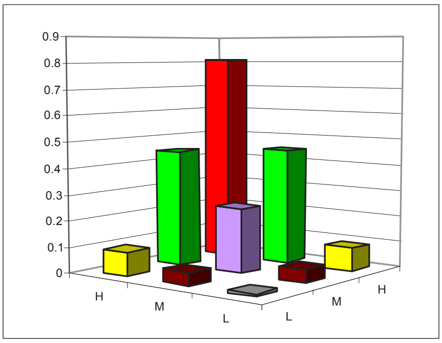
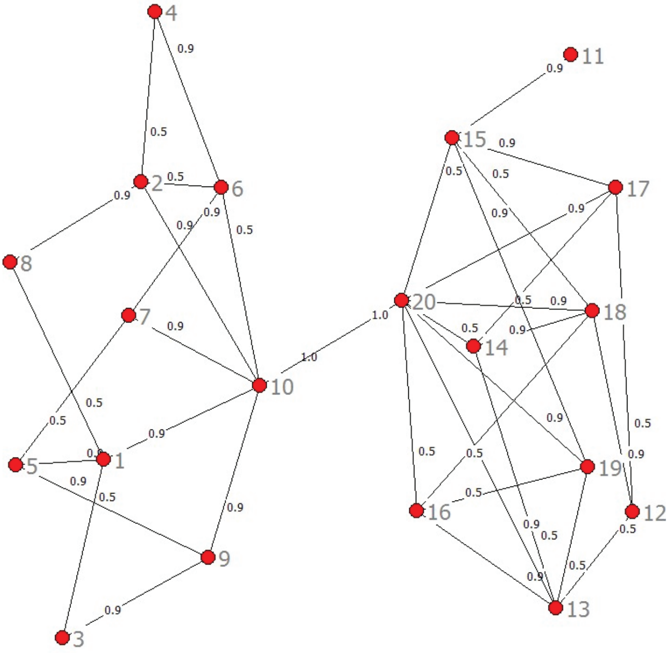


Figure 7. Two isolated groups with one connection



can find a trust path from Node 3 to Node 12, which is 3 → 9 → 10 → 20 → 18 → 12. The end-to-end trust level from Node 3 to Node 9 is 0.66. If we divide the trust into 10 equal levels, 0.66 falls into the 0.6 to 0.7 range. The PDFs of the trust levels from regular nodes to the super-nodes in group A and B have the same distribution (see Figure 8). After the introduction of super-nodes, the inter-group trust distribution is shown in Figure 9.

In our study, we used UCINET Version 6 software (UCINET, 2007) for the social network analysis to find connections between Groups A and B. (Under the main manual, select Network, Cohesion, Reachability, and then Probabilities in the "Type of data" field.) The probability of a path is equal to the product of the probabilities of its edges. The algorithm finds the probability of the most probable path between each pair of nodes (UCINET, 2007).

It is the user's decision to select a trust threshold. Different thresholds incur different successful rates and risks of communication. Figure 11 shows when the thresholds are 0.6 and 0.8 the communication successful rates are 90.0% and 26.7%, respectively. Trust is a dynamic learning process in self-organizing networks. After a positive experience is obtained, the trust on the path will be increased. A UE can cache the certificates and the trust data. So next time when the same path is found, the trust will be increased to $T_{current} = T_{past} + \Delta T$, where $T_{current}$ is the current trust level to be determined, T_{past} is the trust level used in the last event, and ΔT is recommended to be a fraction of T_{past} until $T_{current}$ reaches the maximum trust value (1.0). With this approach, self-organizing networks will become more successful with increasing trusts from past experiences.

Figure 8. Simulation of upstream and downstream PDFs - $f_X(x)$ and $f_Y(y)$

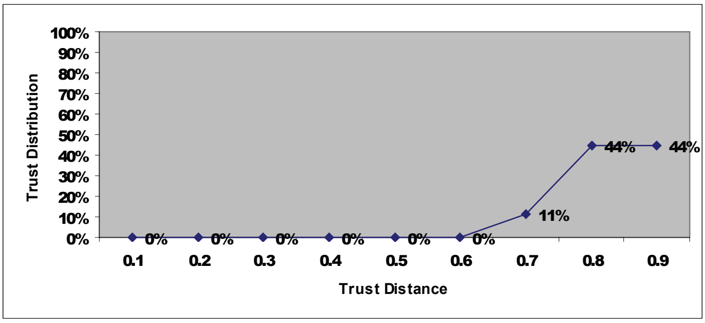


Figure 9. End-to-end trust PDF - fZ(z)

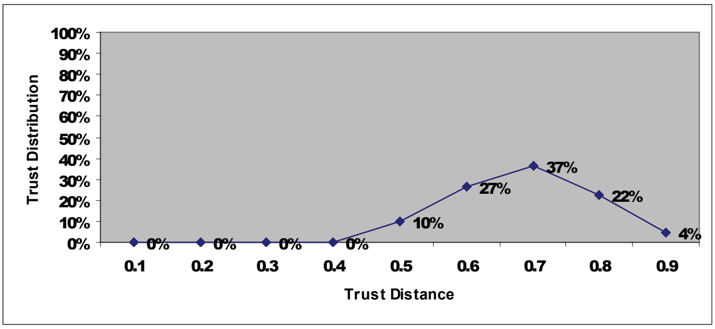


Figure 10. Average trust

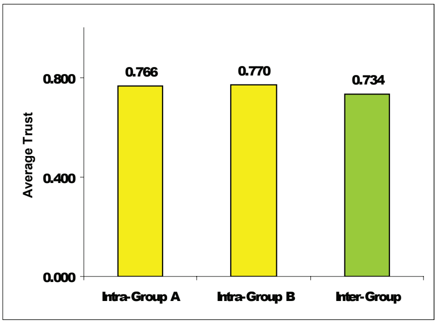
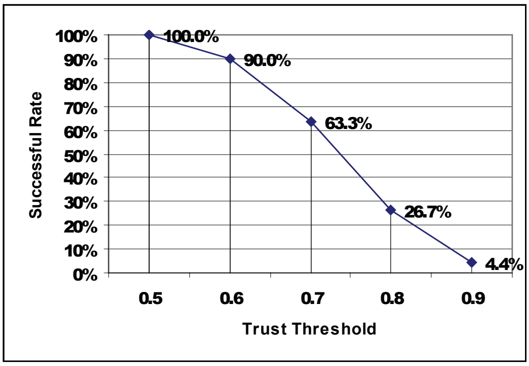


Figure 11. Communication successful rate



CONCLUSION AND FUTURE WORKS

In contrast to traditional communication services provided by government authorized service providers, self-organizing networks are formed by individual users using their own equipment. Each of the two models has advantages and disadvantages. The service providers provide so-called carrier grade services with strong authentication control which should yield high quality and security. Self-organizing networks can be applied to P2P and ad hoc environments. Due to the lack of a central authority in self-organizing networks, it is difficult to verify the identity of the participating users. The studies on the web of trust and small world phenomenon have revealed the possibility of establishing trusts among users who do not directly know each other. However, the end-to-end trust level decreases when the path length of certification gets longer, which results in low success rates of communications. To solve the problem, we propose a hybrid trust structure for certification by combining the strengths of both models, and introducing the concept of authority endorsement and super-node for public key certification. In other words, an authority is involved in self-organizing networks to improve their performance. Through quantity analysis and simulations, we have shown the trust gain and the successful rate against different trust thresholds. In addition, the proposed PIE protocol provides security and privacy protection for transporting user sensitive information over open networks. In summary, the hybrid trust structure for certification will achieve improved security and performance. For our future research, we plan to focus on studying the trust development process (from a stranger to a friend) and cryptographic processing times.

REFERENCES

Capkun, S., Hubaux, J-P., & Buttyan, L. 2006. Mobility Helps Peer-to-Peer Security. *IEEE Transactions on Mobile Computing. 5,* 43 – 51.

Caronni, G. 2000. Walking the Web of Trust. *Proceedings of IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises* (pp. 153-158).

Huynh, T., Jennings, N., & Shadbolt, N. 2006. Certified Reputation: How an Agent Can Trust a Stranger. *Proceedings of the Fifth International Joint Conference on Autonomous Agents and Multiagent Systems.*

Josang, A., Hayward, R., & Pope, S. 2006. Trust Network Analysis with Subjective Logic. *Proceedings of the Twenty-Ninth Australian Computer Science Conference* (pp. 85-94).

Krawczyk, H. 1996. SKEME: A Versatile Secure Key Exchange Mechanism for Internet. *Proceedings of the 1996 Internet Society Symposium on Network and Distributed Systems Security* (pp. 114-127).

Li, J., Li, R., & Kato, J. 2008. Future Trust Management Framework for Mobile Ad Hoc Networks. *IEEE Communications Magazine, 46,* 108-114.

Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P., & Shen, X. 2008 Security in Vehicular Ad Hoc Networks. *IEEE Communications Magazine, 46,* 88-95.

Ma, J., & Orgun, M. 2006. Trust Management and Trust Theory Revision. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans, 36.* 451-460.

Papadimitratos, P., & Hass, Z. 2006. Secure Data Communication in Mobile Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications, 24.* 343-356.

Sanzgirl, K., LaFlamme, D., Dahill, B., Levine B., Shields, C., & Belding-Royer, E. 2005. Authenticated Routing for Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications, 23,* 598-610.

Sun, B., Osborne, L., Xiao Y., & Guizani, S. 2007. Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks. *IEEE Wireless Communications, 14,* 56-63.

Sun, Y., Yu, W., Han, Z. & Liu, K.J. 2006. Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications, 24,* 305-317.

Suryanarayana, G., Erenkrantz, J., & Taylor, R. 2005. An Architectural Approach for Decentralized Trust Management. *IEEE Internet Computing, 9*, 16-23.

Theodorakopoulos, G., & Baras, J.S. 2006. On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications, 24*, 318-328.

UCINET. 2007. Received September 25, 2007 from http://www.analytictech.com/

Watts, D., 1999. *Small Worlds: The Dynamics of Networks between Order and Randomness.* Princeton, NJ: Princeton University Press.

Xiong, L., & Liu, L. 2004. PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. *IEEE Transactions on Knowledge and Data Engineering, 16,* 843-857.

Yang, H., Shu, J., Meng X., & Lu, S. 2006. SCAN: Self-Organized Network Layer Security in Mobile Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications, 24,* 261-273.

Zhang, Y., Liu, W., & Fang, Y. 2006. Securing Mobile Ad Hoc Networks with Certificateless Public Keys. *IEEE Transactions on Dependable and Secure Computing, 3,* 386 – 399.

Zhou, T., & Harn, L. 2007. Security in User-Assisted Communications. *Proceedings of IEEE Wireless Telecommunications Symposium (WTS).*

Zhou, T., & Harn, L. 2008. Risk Management of Digital Certification in Ad Hoc and P2P Networks. *Proceedings of the 21st Canadian Conference on Electrical and Computer Engineering.*

Tong Zhou is a PhD candidate in interdisciplinary studies at University of Missouri - Kansas City, USA and a principal engineer at Comcast Cable, USA. He received his BEng in communications engineering from Beijing Information Science & Technology University, P. R. China in 1991 and MS in electrical and computer engineering from State University of New York - Stony Brook, USA in 1998. He worked at Sprint Nextel, USA as a principal engineer from 1998 to 2007 and Motorola China Electronics Ltd. as a cellular field engineer from 1993 to 1997. His research interests are in the areas of information security, next generation networks and services, peer-to-peer trust management, social networks and ad hoc networks. He has over twenty patents issued/pending in USA.

Lein Harn received his BS degree in electrical engineering from the National Taiwan University in 1977. In 1980, he received his MS in electrical engineering from the State University of New York at Stony Brook and in 1984 he received his doctorate degree in electrical engineering from the University of Minnesota. He joined as an assistant professor in the department of electrical and computer engineering at the University of Missouri-Columbia in 1984 and in 1986, he moved to Computer Science and Telecommunication Program (CSTP) of University of Missouri-Kansas City (UMKC). While at UMKC he went on development leave to work in Racal Data Group in Florida for a year. His research interests are cryptography, network security and wireless communication security. He has published a number of papers on digital signature design and applications, wireless and network security. He has written two books on security. At present he is investigating new ways of using digital signature in various applications.