IGI PUBLISHING **ITJ 4924**

701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Interdisciplinary Telecommunications and Networking, Volume 1, Issue 2
edited by **Michael R. Bartolacci and Steven R. Powell © 2009, IGI Global**

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.)