IGI PUBLISHING **ITJ 4683**

701 E. Chocolate Avenue, Suite 200, 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 1
edited by **Steven Powell © 2009, IGI Global**

Time-Based Confidentiality Enhancement Scheme for Mobile Wireless Networks

Qunwei Zheng, Cerqa, USA

Xiaoyan Hong, Rice University, USA

Jun Liu, University of Alabama, USA

Lei Tang, University of Alabama, USA

ABSTRACT

A multi-hop wireless network with highly dynamic members and mobility is vulnerable to many attacks. To address this problem, we propose a novel time-based approach that exploits mobility. In our scheme, the source sends shares at different times. Due to node mobility, these shares will be routed through different intermediate nodes. It is highly unlikely that a particular intermediate node is able to be on many of these routes and to collect enough shares to reconstruct the original message. The scheme is particularly suitable for applications that can tolerate long message delays, as studied in Delay Tolerant Networks. The article focuses on analyzing the feasibility of this scheme. We describe a general approach to calculate the probability of intercepting enough shares by arbitrary nodes, together with simulations. The results show that the probability is small. The scheme provides a valuable alternative for delay tolerant applications to enhance message confidentiality.

Keywords: Data Security; Mobile Technologies; Networking; Secret Sharing; Wireless Technologies

INTRODUCTION

Multi-hop wireless networks, e.g., mobile ad hoc networks, mesh networks, vehicular ad hoc networks, and moveable wireless sensor networks, are peer-to-peer networks where users act not only as hosts but also as routers to forward packets for others. Such networks are self-organizing and highly dynamic due to node mobility, frequent node join and leave, and possible long distances between nodes. In this work, we focus on the challenging mobile ad hoc networks (MANETs). MANETs are vulnerable to many attacks. Possible attackers may want to eavesdrop other nodes' communication, to disrupt communication, or to deplete network resources. In the scenarios where ad hoc networks are deployed in hostile environments, a legitimate node could be captured and turned into malicious. Moreover, the open nature of wireless media allows the attacks to be

launched with great ease. Any nodes within the reception range of a transmission can overhear, intercept and alter transmitted messages; or, a malicious node can position itself to be within a network field and emit bogus messages. All these situations require a secure network to protect communications. One important secure aspect is the confidentiality of the messages. In this work, we study the confidentiality issue targeting at defending against the eavesdropping attack that is interested in learning the contents of the messages.

Message confidentiality (or secrecy) can be achieved using encryption or an approach that spreads message shares. Encrypting messages before sending is a common practice. Yet for encryption to work, the keys for encryption and decryption must be available. However, both symmetric key cryptography and public key cryptography face challenges due to the dynamic nature of network members. Several early works have proposed to address the problem (Balfanz, Smetters, Stewart, & Wong, 2002; Zhang & Fang, 2008; Capkun, Hubaux, & Buttyan, 2003; Hubaux, Buttyan, & Capkun, 2001; Luo, Kong, Zerfos, Lu, & Zhang, 2004; Stajano & Anderson, 1999; Zhou, Schneider, & Renesse, 2002). Still, there is no one-fit-all strict security mechanism. In addition, cryptographic approaches usually require additional computation time and bandwidth (for exchanging secure credentials needed in handshake), which could be crucial for nodes that are resource constrained. Also, nodes could be compromised and a compromised node gives away all the keys stored in its memory. Moreover, cryptography cannot defend against adversaries that simply drop messages. After all, with these considerations, sending messages in MANET with needed secrecy remains a challenging issue.

Spreading a message through multiple paths is another approach to achieve secrecy. The basic idea is to split a message into multiple shares and send them to different paths. Usually, the threshold secret share scheme can be used to generate the shares. Several related secure data transmission schemes have been proposed following the idea, e.g., using node-disjoint paths (Lou, Liu, & Fang, 2004; Papadimitratos & Haas, 2003). Multi-path routing in MANET is used to select these paths (Tsirigos, 2001; Wu, 2001; Radunovic, Gkantsidis, Key, & Rodriguez, 2008; Lee, 2001). These schemes fit well for scenarios where the space is large enough for these paths to spread apart. But they are not appropriate when a network is sparse or deployed in a restricted geographic area, where no enough node-disjoint multiple paths can be found.

Our scheme works differently. It explores node mobility by sending shares at different times. Thus it is not limited by geographical features. Notice that nodes in mobile ad hoc networks move all the time. If the time interval is large enough, two shares will be routed through different intermediate nodes. Thus it is very difficult for a node (including the eavesdropping attacker) other than the source and the destination to hear enough shares - unless it physically follows the source and the destination or it has enough collaborators in the network to help collecting the shares. A node having enough shares is able to reconstruct the original message by combining these shares. Otherwise, no information about the original message will be revealed.

Such a time-based multi-path message dissemination scheme has a natural fit for applications and scenarios where delay can be tolerated, similar to applications studied in Delay Tolerant Networks (DTN) (Jain, Fall, & Patra, 2004). It is also suitable for scenarios where multiple paths do not exist or are hard to find, such as a sparse network, or a network deployed in a restricted geographical area. For these scenarios, our scheme can provide message secrecy, yet does not rely on the presence of in-network key distribution and cryptography approaches.

For this scheme to work, the key issue is the guarantee (with probability) that nodes other than the source and the destination will not intercept enough shares. In this article, we introduce the scheme and analyze the feasibility of this scheme. We describe a general approach to calculate the probability, and use the isotropic