A Secure On-Demand Source Routing Scheme Using Hierarchical Clustering in Mobile Ad Hoc Networks*

Woei-Jiunn Tsaur and Haw-Tyng Pai

Department of Information Management
Dayeh University, Changhua, Taiwan, R.O.C.
{wjtsaur, paioknol_27}@yahoo.com.tw

Abstract. In mobile ad hoc networks (MANETs), since all of the nodes communicate each other based on the routing protocol, and an attacker could manipulate a lower-level protocol to interrupt a security mechanism in a higher-level one, securing routing protocol is an important issue in MANETs. Recently, there exist several proposals that attempt to develop a secure routing protocol for MANETs. However, those methods are not actually secure against a variety of attacks, including the Sybil, wormhole, black hole, replay, blackmail, denial of service, and routing table poisoning attacks. Therefore, in this paper we design a secure hierarchical-clustering-based routing scheme using the self-certified public key cryptosystem, elliptic curve cryptosystem, pre-hashing, and nonce techniques against such attacks. Finally, we also analyze the advantages of our proposed scheme in terms of security and superiority.

1 Introduction

Mobile ad hoc networks (MANETs) [1] are an occasional infrastructureless network, formed by a set of wireless mobile hosts that dynamically establish their own network on the fly, without relying on any central administration. In other words, MANETs dynamically handle the joining or leaving of nodes in the network by self-organizing. This is a challenging task [2], since these devices have limited resources (CPU, storage, energy, etc.). Moreover, the network’s environment has some features that add extra complications, such as the nodes’ mobility bringing about frequent topology changes, as well as the unreliability and the limited bandwidth of wireless channels.

Most of the existing routing protocols follow two different design approaches [3] to confront the inherent characteristics of MANETs: the table-driven and the source-initiated on-demand approaches. Owing to limited bandwidth and power in MANETs, the source-initiated on-demand routing protocols are more suitable for such features. Moreover, securing routing protocol is an important issue in MANETs [2-3, 5-9]. In the cause of maintaining connectivity in MANETs, all participating nodes have to perform routing of network traffic. However, the previous research trust all the

* This work was supported by the National Science Council of Republic of China under contract numbers NSC 95-2219-E-212-001 and NSC 95-2218-E-212-008.
participants to correctly forward routing and data traffic [4]. Furthermore, an attacker could manipulate a lower-level protocol to interrupt a security mechanism in a higher-level.

Recently, there exist several proposals [3] that attempt to develop a secure routing protocol for MANETs. Each proposal has a different set of operational requirements and provides protection against different attacks by utilizing particular approaches. Ariadne [10] is the flagship protocol for securing dynamic source routing (DSR) [11]. It can defend against the alteration of route message and prevent various types of denial of service (DoS) attacks. Unfortunately, Acs et al. [12] stated Ariadne will suffer from a new attack, and proposed a provably secure on-demand source routing protocol, called ENDAIRA, against such an attack. However, they must assume (1) nodes are identified by identifiers in the neighbor discovery protocol and in the routing protocol. The identifiers are authenticated during neighbor discovery; (2) nodes that are not within each other’s radio range are not able to run the neighbor discovery protocol successfully. In other words, the Sybil attack [13] and wormhole attack [14] will occur in ENDAIRA unless the above two assumptions are actually achieved. The Sybil attack exists if a single faulty entity can present multiple identities. Such attackers can control a substantial fraction of the system, and then causing a serious damage in MANETs. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them there into the network. Due to most existing ad hoc network routing protocols without some mechanism to defend against the wormhole attack, it would be unable to find routes longer than one or two hops, severely disrupting communication. The wormhole attack can also form a serious threat in wireless networks, especially against many ad hoc network routing protocols.

Therefore, Argyroudis et al.’s [3] affirmed that there is a need for a solution that offers a lightweight approach to the problem of secure ad hoc routing, while taking into account the security prerequisites of different application scenarios, offering a flexible approach to the required security-performance balance. On the other hand, Yu and Chong [15] survey that clustering is an effective technique for regulating nodes in MANETs. It is because clustering makes it possible to guarantee basic levels of system performance [16], such as throughput and delay, in the presence of both mobility and a large number of mobile terminals. Hence, using the self-certified public key cryptosystem, elliptic curve cryptosystem, pre-hashing, and nonce [17] techniques, we propose a hierarchical-clustering-based secure and available routing scheme to actually overcome the above weaknesses in MANETs.

The rest of this paper is organized as follows. In Section 2, we propose a new hierarchical-clustering-based secure on-demand source routing scheme. Then in Section 3, the advantages of our proposed scheme will be analyzed in terms of security and superiority. Finally, some concluding remarks are presented in Section 4.

2 The Proposed Hierarchical-Clustering-Based Secure Routing Scheme

Inspired by Acs et al.’s solution [12], we comprehend a digital signature scheme that can avoid malicious nodes to fake route messages. However, the limited resources of