ABSTRACT

In Inter-Vehicle Communication (IVC) networks, the high mobility and lack of infrastructure pose major challenges in designing secure routing protocols. In this work, we present a new secure routing protocol called SERVEN (SEcure Routing in VEhicular Networks) that can achieve near-instantaneous secure communication in IVC networks. In particular, we concentrate on the design of the network setup phase of the protocol and we present simulation results using Network Simulator version 2.28 (ns-2.28). Secure setup means the appropriate formation of a network whose nodes are aware of each other and of the right topology. This is especially important for location-based routing protocols in IVC networks.

INTRODUCTION

Inter-Vehicle Communication (IVC) networks will become an important building block for Intelligent Transportation System (ITS) applications (Tian, Han, Rothermel, & Cseh, 2003). IVC networks can serve as local wireless ad hoc networks for exchanging information between cars for cooperative driver assistance and other vehicle safety applications. Nevertheless, the design of effective
inter-vehicular communication systems poses many technical challenges. First of all, IVC implies exchange of data between communication hosts whose location and velocity are changing continuously. Moreover, the communication patterns vary quickly as vehicles travel on different roads or in different areas. Therefore, routing of data in such a highly mobile wireless ad hoc network is liable to different attacks which motivate the research on new security mechanisms for IVC networks (Eishler, 2004). For example, the protection of route discovery is a critical prerequisite to ensure the robustness of the routing protocols. While security can be implemented at different levels, this paper focuses on the security mechanisms at the network level.

Secure routing protocols must be able to detect and isolate misbehaving nodes. A node may misbehave by agreeing to forward packets and then does not do so, because it is overloaded, selfish, malicious or broken. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets. A selfish node is unwilling to consume battery power, CPU cycles or available network bandwidth to forward packets not of direct interest to it. A malicious node launches a denial of service attack by dropping packets. A broken node might have a software fault that prevents it from forwarding packets. In addition to the routing challenges, IVC networks have to face many attacks on the security mechanisms, e.g., the key management mechanisms (Hubaux, Buttyan, & Capkun, 2001).

Before designing a secure routing protocol for an IVC network, the network setup should be properly executed. Proper or secure setup means the appropriate formation of a network whose nodes are aware of each other (correct node IDs) and of the right topology. After the secure formation of the network, the routing protocol should be able to maintain security and protect the network against possible attacks. The secure routing protocol SERVEN (SEcure Routing in VEHicular Networks), proposed in this paper, handles both secure network setup and secure routing sustainability in an IVC network. SERVEN is thus divided into two phases: Phase 1 is concerned with the secure formation of an IVC network which is the topic of this paper, and phase 2, which is concerned with maintaining secure routing after successful secure network setup.

The rest of the paper is organized as follows: We start by outlining the related work. Then, the proposed protocol design for secure network setup is explained followed by simulation results and analysis. Finally, we draw our conclusions.

**RELATED WORK**

Several secure routing protocols for Mobile Ad-hoc Networks (MANETs) have been proposed in the literature (Hubaux, et al., 2001; Marti, Giuli, Lai, & Baker. 2000; Zhou & Haas, 1999; Zapata, 2001; Kong, Zerfos, Luo, Lu, & Zhang, 2001; Papadimitratos & Haas, 2002; Hu, Johnson, & Perrig, 2002a; Hu, Perrig, & Johnson, 2002b; Sanzgiri, Dahill, Levine, Shields, & Royer, 2002; Eichler, Schwingenschlögl, Dötzer, & Eberspächer, 2004) with protection capabilities against only specific attacks in MANETs. Most of this previous work focuses on providing secure routing based on cryptographic operations, such as symmetric and asymmetric cryptography. Some approaches focus on distributing the certificate authority based on the fact that no one single node in an ad hoc network can be trusted, due to low physical security and availability (Zhou & Haas, 1999; Kong, et al., 2001). Marti, et al. (2000) and Buchegger, et al. (2002) focus on mitigating routing misbehavior by rating and isolating the nodes according to their behavior. A different approach is to provide incentive to nodes so that they properly relay user data by introducing the concept of fictitious currency (Buttyan & Hubaux, 2000). Yi, et al. (2001) propose an approach to routing that incorporates security levels of nodes into traditional routing metrics. The protection of the route discovery