ARTICLE N°3

SECURITY IN MOBILE AD HOC NETWORKS : CHALLENGES AND SOLUTIONS

HAO YANG , HAIYUN LUO , F ANYE , SONGWU LU , AND LIXIA ZHANG ,
UCLA COMPUTER SCIENCE DEPARTMENT

1. Introduction

1.1 Context

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment .Mobile ad hoc network got outstanding success as well as tremendous attention due to its self maintenance and self configuration properties or behavior. At early stage mostly people focused on its friendly and cooperative environment and due to this way many different problems came in being; security is one of the primary concerns in order to provide secure communication between different nodes in a mobile ad hoc network environment.

1.2 Background

A mobile ad-hoc network is a collection of mobile nodes forming an ad-hoc network without the assistance of any centralized structures. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective. There are quite a number of uses for mobile ad-hoc networks. For example, the military can track an enemy tank as it moves through the geographic area covered by the network. Your local community can use an ad-hoc network to detect your car moving though an intersection, checking the speed and direction of the car. In an environmental network, you can find out the temperature, atmospheric pressure, amount of sunlight, and the relative humidity at a number of locations.

The whole life-cycle of ad-hoc networks could be categorized into the first, second, and the third generation ad-hoc networks systems.

Present ad-hoc networks systems are considered the third generation.

The first generation goes back to 1972. At the time, they were called PRNET (Packet Radio Networks). In conjunction with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a kind of distance-vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment.

The second generation of ad-hoc networks emerged in1980s,when the ad-hoc network systems were further enhanced and implemented as a part of the SURAN (Survivable Adaptive Radio Networks) program. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure. This ram proved to be beneficial in improving the radios' performance by making them smaller, cheaper, and resilient to electronic attacks.

In the 1990s, the concept of commercial ad-hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences.

The IEEE 802.11 subcommittee had adopted the term &quot;ad-hoc networks&quot; and the research community had started to look into the possibility of deploying ad-hoc networks in other areas of application.

Meanwhile, work was going on to advance the previously built ad-hoc networks. GloMo (Global Mobile Information Systems) and the NTDR (Near-term Digital Radio) are some of the results of these efforts. GloMo was designed to provide an office environment with Ethernet-type multimedia connectivity anywhere and anytime in hand held devices.

3 Problem and research questions

In recent years mobile ad hoc networks(MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. While early research effort assumed friendly and cooperative environment and focused on problems such as wireless channel access and multi-hop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Although security has long been an active research topic in wireless networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Consequently,the existing security solutions for wired networks do not directly apply to the MANETdomain.The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity,anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. Table 1 describes the security issues in each layer. In this article we consider a fundamental security problem in MANET: the protection of its basic functionality to deliver data bits from one node to another. In other words, we seek to protect the network connectivity between mobile nodes over potentially multi-hop wireless channels, which is the basis to support any network security services. Multi hop connectivity is provided in MANETs through two steps: (1) ensuring one-hop connectivity through link-layer protocols (e.g., wireless medium access control, MAC); and (2) extending connectivity to multiple hops through network-layer routing and data forwarding protocols (e.g., ad hoc routing). Accordingly, we focus on the link- and network-layer security issues, challenges, and solutions in MANETs in this article.

3. **Methodology employed**

For the realization of this work,the autors employe a particular methodology We describe the attack model in the next section, and then identify the challenges in MANET security design. Next, we overview the state-of-the-art security proposals that protect MANET from different types of attacks in the link and network layers, respectively. Lastly, we discuss open challenges and possible future directions in this area.

One distinguishing characteristic of our work is to talk about security design perspective is the lack of a clear line of defense. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring or access control mechanisms can be deployed. As a result, the boundary that separates the inside network from the outside world becomes blurred.

4. **Results found and Perspectives**

The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multifence security solution that is embedded into possibly every component in the network,resulting in in-depth protection that offers multiple lines of defense against many both known and unknown security threats. This new design perspective is what we call resiliency-oriented security design.

We envision the resiliency-oriented security solution as possessing several features.

First, the solution seeks to attack a bigger problem space. It attempts not only to thwart malicious attacks,but also to cope with other network faults due to node misconfiguration, extreme network overload, or operational failures. In some sense,all such faults, whether incurred by attacks misconfiguration, share some common symptoms from both the network and end-user perspectives, and should be handled by the system.

Second, resiliency-oriented design takes a paradigm shift from conventional intrusion prevention to intrusion tolerance. In a sense, certain degrees of intrusions or compromised/captured nodes are the reality to face, not the problem to get rid of, in MANET security. The overall system has to be robust against the breakdown of any individual fence, and its performance does not critically depend on a single fence. Even though attackers intrude through an individual fence, the system still functions, but possibly with graceful performance degradation.

Third, as far as the solution space is concerned,cryptography-based techniques just offer a subset of toolkits in a resiliency-oriented design.

The solution also uses other non crypt-based schemes to ensure resiliency. For example, it may piggyback more “protocol invariant” information in the protocol messages, so that all nodes participating in the message exchanges can verify such information. The system may also exploit the rich connectivity of the network topology to detect inconsistency of the protocol operations. In many cases, routing messages are typically propagated through multiple paths and redundant copies of such messages can be used by downstream nodes. Fourth, the solution should be able to handle unexpected faults tosome extent. One possible approach worth exploring is to strengthen the correct operation mode of the network by enhancing more redundancy at the protocol and system levels.

5. Most important publications for this work.

- IEEE Std. 802.11, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 1997.

- D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, T. Imielinski and H. Korth, Ed., Kluwer, 1996.

- Y. Hu, A. Perrig, and D. Johnson, “Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks,“ ACM MOBICOM, 2002.

- P. Kyasanur, and N. Vaidya, “Detection and Handling of MAC Layer Misbehavior in Wireless Networks,” DCC, 2003.

- B. Dahill et al., “A Secure Protocol for Ad Hoc Networks,“ IEEE ICNP, 2002.

- B. Awerbuch et al., “An On-Demand Secure Routing Protocol Resilient to Byzantine Failures,” ACM WiSe, 2002.

another references

www.google.fr at 15 march 2017;
Mobile ad hoc network – Wikipedia att 15 march 2017
Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions – FULLTEXT01.pdf   at 16 march 2017
Security in mobile ad hoc networks: Challenges and solutions [http: eScholarship] at 16 march 2017