International Journal of Information Technology and Knowledge Management
January-June 2008, Volume 1, No. 1, pp. 57-61

SECURE INFORMATION FLOW IN MOBILE AD-HOC NETWORK: A CHALLENGE

Rajender Nath & Pankaj Kumar Sehgal

Abstract

The emergence of the Mobile Ad Hoc Networking (*MANET*) technology advocates self-organized wireless interconnection of communication devices that would either extend or operate in concert with the wired networking infrastructure or, possibly, evolve to autonomous networks. In either case, the proliferation of *MANET*-based applications depends on a multitude of factors, with trustworthiness being one of the primary challenges to be met. Despite the existence of well-known security mechanisms, additional vulnerabilities and features pertinent to this new networking paradigm might render such traditional solutions inapplicable. In particular, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. In *MANET*, any node may compromise the routing protocol functionality by disrupting the route discovery process.

Unlike the wireline networks, the unique characteristics of *MANETs* pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. In this paper we focus on the fundamental security challenges, discuss the challenges to security design, and review the state-of-the-art security proposals that protect the MANET link- and network-layer operations of delivering packets over the multihop wireless channel.

Keywords: mobile network, ad-hoc network, challenges, security solutions.

1. Introduction

In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration [6] and self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop 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 wireline 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 MANET domain.

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. A fundamental security problem in MANET: the protection of its basic functionality to deliver data bits from one node to another. The network connectivity between mobile nodes over potentially multihop wireless channels, which is the basis to support any network security services. Multihop 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).

Table1
The Security Solutions for MANETs at Different Layer

Layer	*Security issue*
Application layer	Detecting and preventing viruses, worms, malicious codes and application abuses
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

One distinguishing characteristic of MANETs from the 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. On the other hand, the existing ad hoc routing protocols, such as Ad Hoc On Demand Distance Vector (AODV) [17] and Dynamic Source Routing (DSR) [10], and wireless MAC protocols, such as 802.11 [11], typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by intentionally disobeying the protocol specifications.

There are basically two approaches to protecting MANETs: proactive and reactive [9]. The proactive approach attempts to prevent an attacker from launching attacks in the first place, typically through various cryptographic techniques. In contrast, the reactive approach seeks to detect security threats a posteriori and react accordingly. Due to the absence of a clear line of defense, a complete security solution for MANETs

should integrate both approaches and encompass all three components: prevention, detection, and reaction. For example, the proactive approach can be used to ensure the correctness of routing states, while the reactive approach can be used to protect packet forwarding operations. Security is a chain, and it is only as secure as the weakest link. Missing a single component may significantly degrade the strength of the overall security solution.

2. CHALLENGES

One fundamental vulnerability of MANETs comes from their open peer-to-peer architecture. 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 nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defense in MANETs from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. There is no well defined place/infrastructure where we may deploy a single security solution. Moreover, portable devices, as well as the system security information they store, are vulnerable to compromises or physical capture, especially low-end devices with weak protection. Attackers may sneak into the network through these subverted nodes, which pose the weakest link and incur a domino effect of security breaches in the system.

The stringent resource constraints in MANETs constitute another nontrivial challenge to security design. The wireless channel is bandwidth-constrained and shared among multiple networking entities. The computation capability of a mobile node is also constrained. For example, some low-end devices, such as PDAs, can hardly perform computation-intensive tasks like asymmetric cryptographic computation. Because mobile devices are typically powered by batteries, they may have very limited energy resources. The wireless medium and node mobility poses far more dynamics in MANETs compared to the wireline networks. The network topology is highly dynamic as nodes frequently join or leave the network, and roam in the network on their own will. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay. Despite such dynamics, mobile users may request for anytime, anywhere security services as they move from one place to another. The above characteristics of MANETs clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. First, the security solution should spread across many individual components and rely on their collective protection power to secure the entire network. The security scheme adopted by each device has to work within its own resource limitations in terms ication protocols in the ad-hoc wireless networks is challenging because of the limited wireless transmission range, broadcast nature of the wireless medium (hidden terminal and exposed terminal problems [6]), node mobility, limited

power resources, and limited physical security. Advantages of using an ad-hoc wireless networks include easy and speedy deployment, robustness (no infrastructure required), adaptive and self-organizing network.

CONCLUSION

Designing a secure ad hoc wireless networks communication is a challenging task due to (1) insecure wireless communication links, (2) absence of a fixed infrastructure, (3) resource constraints (e.g. battery power, bandwidth, memory, CPU processing capacity), and (4) node mobility that triggers a dynamic network topology. The majority of traditional routing protocols design fail to provide security. The main requirements of a secure routing protocol are: (1) detection of malicious nodes; such nodes should be avoided in the routing process, (2) guarantee of correct route discovery, (3) confidentiality of network topology; if an attacker learns the network topology, he can attack the bottleneck nodes, detected by studying the traffic patters. This will result in disturbing the routing process and DoS, and (4) stability against attacks; the routing protocol must be able to resume the normal operation within a finite amount of time after an attack.

Security never comes for free. When more security features are introduced into the network, in parallel with the enhanced security strength is the ever-increasing computation, communication, and management overhead. Consequently, network performance, in terms of scalability, service availability, robustness, and so on of the security solutions, becomes an important concern in a resource-constrained ad hoc network. While many contemporary proposals focus on the security vigor of their solutions from the cryptographic standpoint, they leave the network performance aspect largely unaddressed. In fact, both dimensions of security strength and network performance are equally important, and achieving a good trade-off between two extremes is one fundamental challenge in security design for MANETs.

REFERENCES

[1] Gergely Acs, Levente Buttyan and Istvan Vajda, (November-2006), "Provably Secure On-demand Source Routing in Mobile Ad-hoc Networks", *IEEE Transactions on Mobile Computing*, **5**(11), 1533-1546.

[2] Jaier Gomez, Andrew T. Campbell, (January-2007), "Variable – Range Transmission Power Control in Wireless Ad-hoc Networks", *IEEE Transactions on Mobile Computing*, **6**(1), 87-99.

[3] Ting-Yao Jiang, Qing-hua Li, (Augest-2004), "A Secure Routing Protocol for Mobile Ad-hoc Network", Proceeding of the Third International Conference on Machine Learning and Cybernetics, 2825-2829.

[4] Rendong Bai and Mukesh Singhal, (October-2006), DOA: DSR Over AODV Routing for Mobile Ad-hoc Network, *IEEE Transactions on Mobile Computing*, **5**(10), 1403-1416.

[5] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen and J.-P. Sheu, (March-2002), The Broadcast Storm Problem in a Mobile Ad-hoc Network, *ACM Wireless Networks*, **8**(2), 153-167.

[6] C. S. R. Murthy and B. S. Manoj, (2004), Ad-hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR.

[7] Ljubica Blazevic, Jean-Yves Le Boudec and Silvia Giordano, (March/April-2005), A Location-Bases Routing Method for Mobile Ad-hoc Networks, *IEEE Transactions on Mobile Computing*, **4(2),** 97-109.

[8] Adnan Vora and Mikhail Nesterenko, (October/December-2006), Secure Location Verification Using Radio Broadcast, *IEEE Transactions on Dependable and Secure Computing*, **3**(4), 377-385.

[9] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, (February-2004), Security in Mobile Ad-hoc Networks: Challenges and Solutions, *IEEE Wireless Commnications*, 38-47.

[10] D. B. Johnson and D. A. Maltz, (1996), Dynamic Source Routing in Ad-hoc Wireless Networks, *Mobile Computing*, Kluwer Academic Publishers, **353**, 153-181.

[11] IEEE Std. 802.11, (1997), "Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) Specifications".

[12] Y. Zhang, Wenjing Lou and Yuguang Fang, (Octuber/December-2006), "Securing Mobile Ad-hoc Networks with Certificate Less Public Keys", *IEEE Transactions on Dependable and Secure Computing*, **3**(4), 386-399.

[13] Williams, B. and Camp T., (June-2002), Comparison of Broadcasting Techniques for Mobile Ad-hoc Networks, In: Proceedings of the 3rd ACM International Symposium on Mobile Ad-hoc Networking & Computing (MOBIHOC '02), 194-205. Lausanne, Switzerland.

[14] R. Kravets, S. Yi and P. Naldurg, (2001), A Security-Aware Routing Protocol for Wireless Ad-hoc Networks, In ACM Symp, *On Mobile Ad-hoc Networking and Computing*.

[15] P. Papadimitratos and Z. J. Haas, (January-2002), Secure Routing for Mobile Ad-hoc Networks, In Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002).

[16] J. Newsome, E. Shi, D. Song and A. Perrig, (2004), The Sybil Attack in Sensor Networks: Analysis & Defenses, Proc. of the 3rd Intl. Symp., *On Information Processing in Sensor Networks*.

Rajender Nath
Dept. of Computer Science and Application
Kurukshetra University
Kurukshetra (Haryana), INDIA
E-mail: rnath2k3@gmail.com

Pankaj Kumar Sehgal
MM Institute of Computer Technology and Business Management
MM University, Mullana (Ambala), Haryana, INDIA
E-mail: pankajkumar.sehgal@gmail.com