IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Mobile Ad Hoc Networks Security: Challenges and solutions

Annan Naidu Paidi
Asst. Professor of CSE, Centurion University, India
annanpaidi@gmail.com

Abstract

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wire line networks, the unique characteristics of mobile ad hoc networks 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. In this article only focus on the fundamental security problem of protecting the multi hop network connectivity between mobile nodes in a MANET.

Keywords: MANET, Security Issues, routing attacks, Packet forwarding attacks, Multifence security solution.

Introduction

In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. A “Mobile ad hoc network” is a system of wireless mobile nodes with routing capabilities –the union of which form an arbitrary graph. Any group of them are capable of forming an autonomous network that require no infrastructure and is capable of organizing itself into arbitrary changeable topologies. Such a network may operate in a stand-alone fashion, or may be connected to the larger Internet .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. In this article I 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).One distinguishing characteristic of MANETs from the security design perspective is the lack of a clear line of defence. 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) [1] and Dynamic Source Routing (DSR) [2], and wireless MAC protocols, such as 802.11 [3], 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. 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 posterior and react accordingly. Due to the absence of a clear line of defence, 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. As argued in [4], 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. 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 soon 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 un addressed. 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.

This article is structured as follows, describe the attack model in the next section, and then identify the challenges in MANET security design. Next, overview the state-of the-art security proposals that protect MANET from different types of attacks in the link and network layers, respectively.

Security Attacks on MANET

A MANET provides network connectivity between mobile nodes over potentially multi hop wireless channels mainly through link-layer protocols that ensure one-hop connectivity, and network-layer protocols that extend the connectivity to multiple hops. These distributed protocols typically assume that all nodes are cooperative in the coordination process. This assumption is unfortunately not true in a hostile environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications.

The main network-layer operations in MANETs are ad hoc routing and data packet forwarding, which interact with each other and ful fill the functionality of delivering packets from the source to the destination. The ad hoc routing protocols exchange routing messages between nodes and maintain routing states at each node accordingly. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination. Nevertheless, both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. While a comprehensive enumeration of the attacks is out of our scope, such network-layer vulnerabilities generally fall into one of two categories: *routing attacks* and *packet forwarding attacks*, based on the target operation of the attacks.

The family of routing attacks refers to any action of advertising routing updates that does not follow the specifications of the routing protocol. The specific attack behaviours are related to the routing protocol used by the MANET. The attacker may modify the source route listed in the RREQ or RREP packets by deleting a node from the list, switching the order of nodes in th list, or appending a new node into the list [5].When distance-vector routing protocols such as AODV [1] are used, the attacker may advertise a route with a smaller distance metric than its actual distance to the destination, or advertise routing updates with a large sequence number and invalidate all the routing updates from other nodes [6]. By attacking the routing protocols, the attackers can attract traffic toward certain destinations in the nodes under their control, and cause the packets to be forwarded along a route that is not optimal or even nonexistent. The attackers can create routing loops in the network, and introduce severe network congestion and channel contention in certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, and partition the network in the worst case.

In addition to routing attacks, the adversary may launch attacks against packet forwarding operations as well. Such attacks do not disrupt the routing protocol and poison the routing states at each node. Instead, they cause the data packets to be delivered in a way that is intentionally inconsistent with the routing states. For example, the attacker along an established route may drop the packets, modify the content of the packets, or duplicate the packets it has already forwarded. Another type of packet forwarding attack is the denial-of-service (DoS) attack via network-layer packet blasting, in which the attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET.

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 defence 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 any time, 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 of computation capability, memory, communication capacity, and energy supply. Second, the security solution should span different layers of the protocol stack, with each layer contributing to a line of defence. No single-layer solution is possible to thwart all potential attacks. Third, the security solution should thwart threats from both outsiders who launch attacks on the wireless channel and network topology, and insiders who sneak into the system through compromised devices and gain access to certain system knowledge. Fourth, the security solution should encompass all three components of prevention, detection, and reaction, that work in concert to guard the system from collapse. Last but not least, the security solution should be practical and affordable in a highly dynamic and resource constrained networking scenario.

MANETs are much more vulnerable to attack than wired network. This is because of following reasons:

A. Absence of Infrastructure

Ad hoc networks operate independently of any infrastructure, which makes inapplicable any classical solutions based on certification authorities and on line servers.

B. Limited physical security

Mobile wireless networks are generally more prone to physical security threats than a fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threat.

C. Restricted power Supply

Due to mobility of nodes in the ad hoc network, nodes will rely on battery as their power supply method, the problem that may be caused by restricted power supply is denial-of-service attacks and selfish manner.

D. Dynamically changing network topology

Nodes are free to move arbitrarily. The network topology may change randomly and have no restriction on their distance from other nodes. As a result of this random movement, the whole topology is changing in an unpredictable manner, which in turn gives rise to both directional as well as unidirectional links between the nodes.

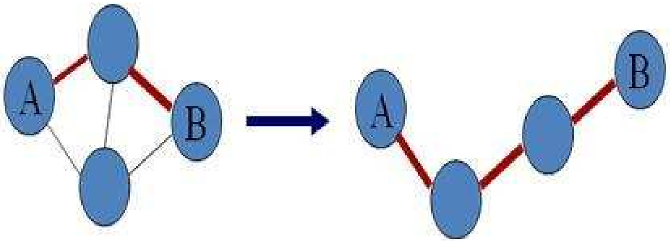

Figure 1. changing network topology

E. Lack of Centralized monitoring

Absence of any centralized monitoring makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly and large scale ad hoc network . It is rather common in the ad hoc network that benign failures such as transmission impairments and packet dropping.

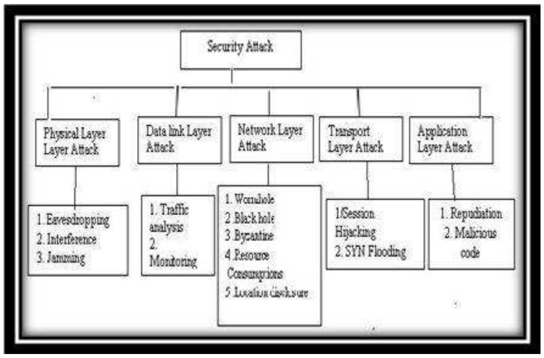

Figure.2.Classification of Attacks

Security Goals in Adhoc Networks

The goals of security mechanism of MANETs are similar to that of other networks. Security is a great issue in network especially in MANETs where security attacks can affect the nodes limited resources and consume them or waste the time before rote chain broke. Security is a vectored term of multi systems, procedures and functions that works together to reach certain level of security attributes.

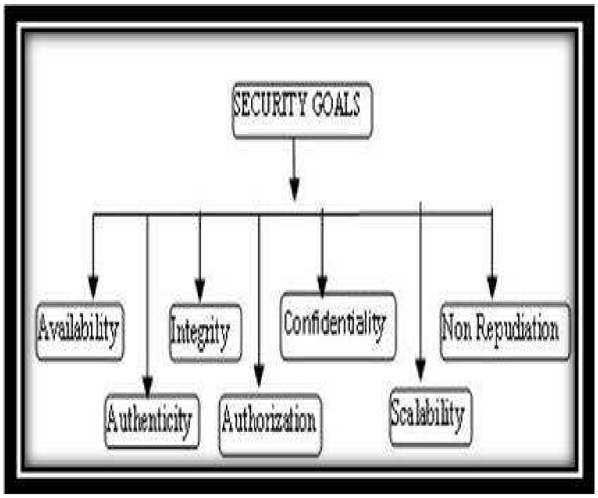

Fig.3. Types of Security Goals

A. Availability

The main goal of availability is to node will be available to its users when expected, i.e. survivability of network services despite denial of service attack. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network. Again, in higher levels, an adversary could bring down high-level services such as key management service, authentication service .

B. Confidentiality

The goal of confidentiality is to keeping information secret from unauthorized user or nodes. In other words, ensures payload data and header information is never disclosed to unauthorized nodes. The standard approach for keeping information confidential is to encrypt the data with a secret key that only intended receiver's posses, hence achieving confidentiality.

C. Integrity

The goal of integrity is to guarantee the message being transmitted is never corrupted. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways .

Malicious altering: – A message can be removed, replayed or revised by an adversary with malicious goal.

Accidental altering:- if the message is lost or its content is changed due to some benign failures, whichmaybe transmission errors in communication or hardware errors such as hard disk failure.

D .Authentication

The goal of authentication is too able to identify a node with which it is communicating and to prevent impersonation. In infrastructure-based wireless network, it is possible to implement a central authority at a point such as base station or access point. But in MANETs, no central administration so it is difficult to authenticate an entity.

E. Non repudiation

The main goal of non repudiation is sender of a message cannot deny having sent the message. This is useful when for detection and isolation of compromised nodes. When node P receives an erroneous message from Q, non repudiation allows P to access Q using this message and to convince other nodes that Q is compromised.

F. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users.

Security Solutions for MANETs

Layer	Attacks	Solution
Application Layer	Repudiation, data corruption	Detecting and preventing virus,worms, malicious codes and application abuses by use of Firewalls,IDS.
Transport Layer	Session hijacking, SYN Flooding	Authentication and securing end-to-end or point-to-point communication use of public cryptography(SSL , TLS, PCT) etc.
Network Layer	Routing protocol attacks (e.g. DSR, AODVetc.),Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks	Protecting the adhoc routing andforwarding protocols
Data Link Layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness etc.	Protecting the wireless MACprotocol and providing link layer security support.
Physical Layer	Eavesdropping, Jamming, Interceptions.	Preventing signal jamming denial-of-service attacks by using Spread Spectrum Mechanism.

Table 2. **Security solutions for MANETS**

Conclusions

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 prevent 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 call *resiliency-oriented* security design.

References

[1] Perkins and E Royer, "Ad Hoc On-Demand DistanceVector Routing," *2nd IEEE Wksp. Mobile Comp. Sys.and Apps.*, 1999.

[2] D. Johnson and D. Maltz, "Dynamic Source Routing inAd Hoc Wireless Networks," *Mobile Computing*, T.Imielinski and H. Korth, Ed., Kluwer,1996.

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

[4] B. Schneier, *Secret and Lies, Digital Security in a NetworkedWorld*, Wiley, 2000.

[5] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A SecureOn-demand Routing Protocol for Ad Hoc Networks,"*ACM MOBICOM*, 2002.

[6] M. Zapata, and N. Asokan, "Securing Ad Hoc RoutingProtocols," *ACM WiSe*, 2002.

[7] B. Dahill *et al.*, "A Secure Protocol for Ad Hoc Networks,"*IEEE ICNP*, 2002.

[8] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: ADefense against Wormhole Attacks in Wireless Networks," *IEEE INFOCOM*, 2002.

[9] N. Borisov, I. Goldberg, and D. Wagner, "InterceptingMobile Communications: The Insecurity of 802.11,"*ACM MOBICOM*, 2001.

[10] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denialof Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," *IEEE MILCOM*, 2002.

[11] Yanping Teng," A Study of Improved Approaches for TCP CongestionControl in Ad Hoc Networks" 2012 International Workshop on Information and Electronics Engineering (IWIEE).

[12] Christian Lochert Bj" orn s Scheuermann Martin Mauve, A Survey on Congestion Control for Mobile Ad-Hoc Network WileyWireless Communication and Mobile Computing 7 (5).Pp.655-676, June 2007.