Security Routing Protocols in Ad Hoc Networks: Challenges and Solutions

Sliman KA. A. Yaklaf
Azzaytuna University
Faculty of Engineering
Electrical and Electronics
Engineering Department
Tarhuna - Libya

Abdurrezagh S. Elmezughi
Azzaytuna University
Faculty of Engineering
Computer and Systems
Engineering Department
Tarhuna - Libya

Nasser Bashir Ekreem
Azzaytuna University
Faculty of Engineering
Electrical and Electronics
Engineering Department
Tarhuna - Libya

Adel A. M. Abosdel
Azzaytuna University
Faculty of Engineering,
Electrical and Electronics
Engineering Department
Tarhuna - Libya

***Abstract*—Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. This paper analyzes security challenges in ad hoc networks and summarizes key issues that should be solved for achieving the ad hoc security. It also gives an overview of the current state of solutions on such key issues in Mobile Ad Hoc Networks (MANETs). To develop suitable security solutions for such new environments, we must first understand how MANETs can be attacked. Then we discuss various proactive and reactive solutions proposed for MANETs. We outline secure routing solutions to avoid some attacks against the routing protocols based on cooperation between nodes.**

***Keywords*— *Security; Routing Protocols; Ad Hoc Networks; Attacks; Secure Routing Protocols*.**

1. INTRODUCTION

The Mobile Ad Hoc Network (MANET) is one of the wireless networks that have attracted most concentrations from many researchers. A MANET is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the MANET than in the wired network. Lack of secure boundaries makes the MANET susceptible to the attacks. The MANET suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. The attacks mainly include passive eavesdropping, active interfering, leakage of secret information, data tampering, message replay, message contamination, and denial of service [1]. 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 I describes the security issues in each layer. 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 posteriori and react accordingly. 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.

TABLE I

The security solutions for MANETs on the Protocol Stack

Layer	Security issues
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

2. ATTACKS ON MANET

The security goals of MANETs are not that different from other networks: most typically authentication, confidentiality, integrity, availability, and non-repudiation. Authentication is the verification of claims about the identity of a source of information. Confidentiality means that only authorized people or systems can read or execute protected data or programs. It should be noted that the sensitivity of information in MANETs may decay much more rapidly than in other information. For example, yesterday's troop location will typically be less sensitive than today's. Integrity means that the information is not modified or corrupted by unauthorized users or by the environment.

Availability refers to the ability of the network to provide services as required. Denials of Service (DoS) attacks have become one of the most worrying problems for network managers. In a military environment, a successful DoS attack is extremely dangerous, and the engineering of such attacks is a valid modern war-goal. Lastly, non-repudiation ensures that committed actions cannot be denied. The characteristics of MANETs make them susceptible to many new attacks. At the top level attacks can be classified according to network

protocol stacks. Table II gives a few examples of attacks at each layer.

TABLE II

Some Attacks on the Protocol Stack

Layer	Attacks
Application Layer	data corruption, viruses and worms
Transport Layer	TCP/UDP SYN flood
Network Layer	hello flood, black hole
Data Link Layer	monitoring, traffic analysis
Physical Layer	eavesdropping, active interference

Attacks against ad hoc networks can be divided into two groups: Passive attacks typically involve only eavesdropping of data [2]. Active attacks involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data. External attacks are typically active attacks that are targeted e.g. to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. External attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on. Internal attacks are typically more severe attacks.

3. CHALLENGES

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 [3].

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 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. Building multi-fence security solutions that achieve both broad protection and desirable network performance can be:

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 defense. 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.

4. SECURITY GOALS

Security is an important issue for Ad Hoc Networks, especially for those security-sensitive applications. To secure an Ad Hoc Network, we consider the following attributes: confidentiality, availability, integrity, authentication, and non-repudiation.

A. Confidentiality

Confidentiality ensures that certain information is never disclosed to unauthorized entities. In the Ad Hoc Network, not only sensitive information transmitted requires confidentiality; routing information must also remain secure in case it might be valuable for adversaries.

B. Availability

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the target of attack, and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service [4].

C. Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [5]:

- Malicious altering
- Accidental altering

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

D. Authentication

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

management function is only accessible by the network administrator. Therefore, there should be an authorization process before the network administrator accesses the network management functions.

E. Non-repudiation.

Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

5. SECURITY IN MANETS

The security of MANETs can be based on protection in the link or network layer. In some Ad-Hoc solutions, the link layer offers strong security services for protecting confidentiality and authenticity, in which case all of the security requirements need not be addressed in the network or upper layers. For instance in some wireless LANs, link layer encryption is applied. However, in most cases the security services are implemented in higher layers, for instance in network layer, since many ad hoc networks apply IP-based routing and recommend or suggest the use of IPSec.

In [6], an authentication architecture for MANETs is proposed. The proposed scheme details with the formats of messages, together with protocols that achieve authentication. The architecture can accommodate different authentication schemes.

6. AD HOC ROUTING PROTOCOLS

Ad hoc routing protocols can be classified into three classes: proactive, reactive and hybrid routing protocols. In proactive routing the routing table of every node is updated periodically. On the contrary, reactive routing is performed on-demand, i.e. the sending node searches for a route to the destination node only when it needs to communicate with it. Hybrid routing uses a mixture of these two routing approaches. That is, proactive routing is used in a limited area around the mobile node and reactive routing is used outside this area. MANET is the name of a working group in the Internet Engineering Task Force (IETF) and it serves as a meeting place for people dealing with MANET approaches.

The primary focus of the working group is to develop and evolve MANET routing specifications and introduce them to the Internet Standards track. The goal is to support networks scaling up to hundreds of routers according to the official web. Fig. 1 shows the prominent way of classifying MANETs routing protocols[7].

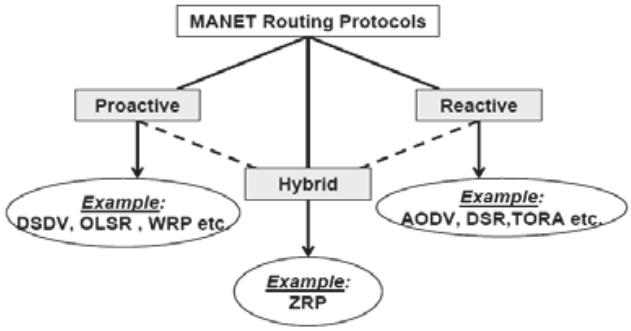

Fig. 1 Classification of MANET Routing Protocols

7. SECURE ROUTING PROTOCOLS

Routing protocols for Ad Hoc Networks are challenging to design: wired networks protocols (such as BGP) are not suitable for an environment where node mobility and network topology rapidly change; such protocols also have high communication overhead because they send periodic routing messages even when the network is not changing. So far, researchers in Ad Hoc Networking have studied the routing problem in a non-adversarial network setting, assuming a reasonably trusted environment. However, unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in Ad Hoc Networks, those functions are carried out by all available nodes. This difference is at the core of the increased sensitivity to node misbehavior in Ad Hoc Networks and the current proposed routing protocols are exposed to many different types of attacks.

The secure Ad Hoc Routing Protocols take the proactive approach and enhance the existing Ad Hoc routing protocols, such as DSR [8] and AODV [9], with security extensions. In these protocols, each mobile node proactively signs its routing messages using the cryptographic authentication primitives. In this way, the collaborative nodes can efficiently authenticate the legitimate traffic and differentiate the unauthenticated packets from outsider attackers. Following, the major secure routing protocols for ad hoc networks will be outlined and analyzed.

A. Secure Routing Protocol (SRP)

The Secure Routing Protocol [10] proposed by Papadimitratos and Haas is conceived as an extension that can be applied to a multitude of existing reactive routing protocols. SRP combats attacks that disrupt the route discovery process and guarantees the acquisition of correct topological information: a node initiating a route discovery is able to identify and discard replies providing false routing information or avoid receiving them.

The basic version of SRP suffers from the route cache poisoning attack: routing information gathered by nodes that operate in promiscuous mode in order to improve the efficiency of the DSR protocol could be invalid, because fabricated by malicious nodes. The authors propose two alternative designs of SRP that uses an Intermediate Node Reply Token (INRT). INRT allows intermediate nodes that belong to the same group that share a common key (KG) to validate RREQ and provide valid RREP messages.

SRP suffers also from the lack of a validation of route maintenance messages: route errors packets are not verified. However, in order to minimize the effects of fabricated error messages, SRP source-routes error packets along the prefix of the route reported as broken: as a consequence the source node can verify that the provided route error feedback refers to the actual route and is not generated by a node that is not even part of the route. A malicious node can harm only the route it belongs. However, SRP is not immune to the wormhole attack: two colluding malicious nodes can misroute the routing packets on a private network connection and alter the network topology vision a benign node can collect.

B. Securing Link-State Protocol(SLSP)

Secure Link-State Protocol (SLSP), which uses digital signatures and one-way hash chains to ensure the security of link-state updates. We can use SLSP as the Intrazone Routing Protocol in the Zone Routing Protocol (ZRP). SLSP is a periodic protocol that receives link state information through a periodic Neighbor Location Protocol (NLP). As a part of NLP, each node broadcasts a signed pairing between its IP address and its MAC address. A node's NLP can notify SLSP when one MAC address uses two IP addresses, when two MAC addresses claim the same IP address, and when another node uses the same MAC address as the detecting node. These protocols ensure some level of integrity of MAC and IP addresses within a two-hop radius. SLSP link-state updates are signed and propagated a limited number of hops.

SLSP uses the same lightweight flooding prevention mechanism as SRP, where in nodes that relay or generate fewer link-state updates are given priority over any node that sends more link-state updates. As in SRP, an attacker can masquerade as a victim node and flood the victim's neighbors with link-state updates that appear to originate at the victim. Although the victim might be able to detect the attack, due to NLP's duplicate MAC address detection functionality, the victim will have no way to protest [11].

C. Securing Ad hoc On-demand Distance Vector(SAODV)

The idea behind SAODV is to use a signature to authenticate most fields of a route request (RREQ) and route reply (RREP) and to use hash chains to authenticate the hop count. SAODV designs signature extensions to AODV. Network nodes authenticate AODV routing packets with an SAODV signature extension, which prevents certain impersonation attacks. In SAODV, an RREQ packet includes a route request single signature extension (RREQ-SSE). When forwarding an RREQ in SAODV, a node first authenticates the RREQ to ensure that each field is valid. It then performs duplicate suppression to ensure that it forwards only a single RREQ for each route discovery. The node then increments the hop-count field in the RREQ header, hashes the hop count authenticator, and rebroadcasts the RREQ, together with its RREQ-SSE extension [12].

When the RREQ reaches the target, the target checks the authentication in the RREQ-SSE. If the RREQ is valid, the target returns an RREP as in AODV. A route reply single signature extension (RREP-SSE) provides authentication for the RREP. A node forwarding an RREP checks the signature extension. If the signature is valid, then the forwarding node sets its routing table entry for the RREP's original source, specifying that packets to that destination should be forwarded to the node from which the forwarding node heard the RREP.

SAODV also uses signatures to protect the route error (RERR) message used in route maintenance. In SAODV, each node signs the RERR and it transmits, whether it's originating the RERR or forwarding it. Nodes implementing SAODV don't change their destination sequence number information when receiving an RERR, because the destination doesn't authenticate the destination sequence number.

D. Securing Authenticated Routing for Ad Hoc Networks(SARAN)

ARAN is a secure, on-demand, distance-vector routing protocol for ad hoc networks proposed in [13]. ARAN uses public key cryptography to ensure routing message integrity and non-repudiation to the route discovery process. ARAN requires the use of a trusted certificate server T, whose public key is known to all valid nodes. This server sends to each node a certificate, containing the IP address of the node, its public key, a timestamp t of when the certificate was created, and a time e at which the certificate expires, all signed with the private key of T. As an example, when a node n gets certified by T, it receives a certificate of the form {n,Kn+,t,e}KT−. All nodes use certificates issued by T to authenticate themselves during the protocol.

Figure 2 shows a scheme of the ARAN protocol with four nodes: a source node A, a destination node X, and two intermediate nodes B and C, one close to the source and the other close to the destination. A graphical representation is provided of the flow of messages: dashed arrows denote the broadcast of Route Discovery Packets (RDP), while the continuous arrows denote the unicast sending of Reply Packets (REP). The figure doesn't show the preliminary phase in which each node receives a certificate from T, assuming it has been already performed.

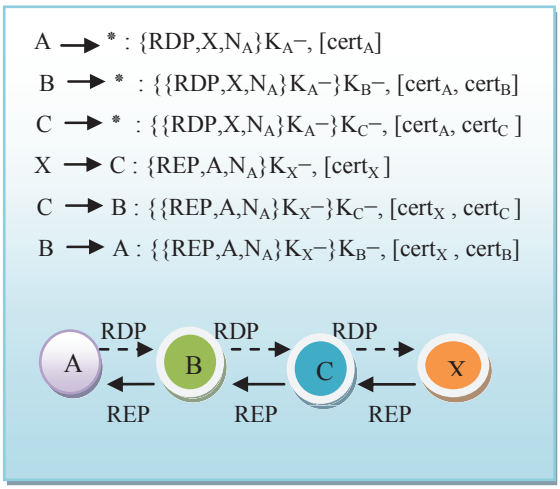

Fig. 2 The ARAN Protocol with Four Nodes

8. CONCLUSIONS

In order to avoid the same problems that raised in wired networks like the Internet, security has to be taken into account at the early stages of the design of basic networking mechanisms like the data link layer and the network layer protocols. The need for security mechanisms that cope with the threats that are specific to the Ad Hoc environment has recently gained attention among the research community. A number of challenges remain in the area of securing wireless Ad Hoc Networks. First, the secure routing problem in such networks isn't well modeled. A more complete model of possible attacks would let protocol designers evaluate the security of their routing protocol. In addition, such a model would form the basis for using formal methods to verify protocol security.

More work needs to be done to deploy these security mechanisms in Ad Hoc Network and to investigate the impact of these security mechanisms on the network performance. SRP combats attacks that disrupt the route discovery process and guarantees the acquisition of correct topological information. SLSP is a periodic protocol that receives link-state information through a periodic Neighbor Location Protocol. SAODV also uses signatures to protect the route error (RERR) message used in route maintenance. ARAN is a simple protocol that does not require significant additional work from nodes within the group.

REFERENCES

[1] A. Mishra and K. M. Nadkarni, "Security in Wireless Ad Hoc Networks". The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[2] J. Kong., X. Hong, and M. Gerla., "A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks", In IEEE MILCOM, 2003.

[3] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions" (2004). IEEE Wireless Communications. 11 (1), pp. 38-47.

[4] L. Zhou and Z. J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.

[5] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.

[6] S. Jacobs and M. S. Corson. MANET authentication architecture. Internet Draft . February 1999.

[7] S. K. Yakhlef, N. A. Shashoa, I.l shrena, and O. Abusaeeda " Properties Evaluation of Proactive, Reactive, and Hybrid Protocols for Mobile ad-hoc Networks". International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882, Volume 4, Issue 3, March 2015, pages 230 – 235.

[8] D. B. Johnson, D. A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[9] C. Perkins, Ad hoc On Demand Distance Vector (AODV) Routing, Internet draft, draft-ietf-manet-aodv-00.txt.

[10] P. Papadimitratos, Z. Haas, Secure Routing for Mobile Ad Hoc Networks, in proceedings of CNDS 2002.

[11] P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks, IEEE Press, 2003, pp. 27–31.

[12] M. Guerrero Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. ACM Workshop on Wireless Security (WiSe), ACM Press, 2002, pp. 1–10.

[13] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks," IEEE Journal on Selected Areas in Communication, special issue on Wireless Ad Hoc Networks, vol. 23, no. 3, pp. 598–610, 2005.