Review of Security in Ad Hoc Networks

SHIVA KHARBANDA
Dronacharya College Of Engineering

Abstract— Ad hoc networks are 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. The military tactical and other security-sensitive operations are one of the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this paper we analyse and focus on the existing problems and security challenges that are available in current Ad hoc Networks and summarizes key issues that should be solved for achieving the ad hoc security.

I. INTRODUCTION

A mobile ad hoc network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and service discovery without the help of an established infrastructure.

Nodes of an ad hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Figure 1 shows such an example: initially, nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken. However, the network is still connected, because A can reach D through C, E, and F

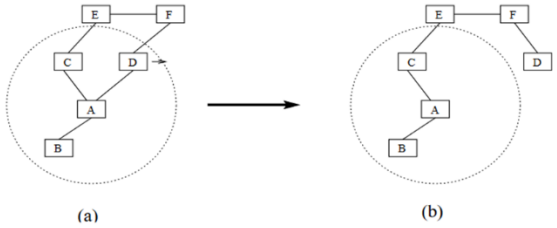

Figure 1: Topology change in ad hoc networks: nodes A, B, C, D, E, and F constitute an ad hoc network. The circle represents the radio range of node A. The network initially has the topology in (a). When node D moves out of the radio range of A, the network topology changes to the one in (b).

II. SECURITY IN AD HOC NETWORKS

In this section, we analyse the security in the ad hoc networks based on their idiosyncrasies

2.1 Idiosyncrasies of Ad Hoc Networks

As shown in Figure 1, mobile nodes within each other's radio range communicate directly via wireless link using a protocol such as IEEE 802.11 [1] or Bluetooth [2] , while those far apart rely on other nodes to relay messages as routers. Due to the mobility of the nodes, the network topology is frequently changed.

As can be seen from the above, the ad hoc networks are quite different from traditional, hardwired packet networks. In [3, 4], most noticeable idiosyncrasies of the ad hoc networks are analysed as the following.

- Dynamic topologies: Node mobility causes the network topology --which is typically multihop -- may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

- Bandwidth-constrained, variable capacity links:

Compared with hardwired counterparts, wireless links will continue to have significantly lower capacity. In addition, aggregate application demand will likely approach or exceed network capacity frequently. As the rapid extension of the traditional networks, similar services, such as multimedia commerce, are required to be supported by the ad hoc networks.

- Energy-constrained operation:

Most possibly, some or all of the nodes in an ad hoc network are actually mobile devices, which may rely on batteries or other exhaustible means for their energy. For these nodes, optimization for energy conservation is a critical design criterion.

- Wireless vulnerabilities and Limited physical security:

Operation in an ad hoc network introduces some new security problems in addition to the ones already present in fixed networks. Mobile wireless networks are generally more prone to physical security threats. The possibility of eavesdropping, spoofing, denial-of-service, band impersonation attacks is increased. Existing link security techniques are often applied within wireless networks to reduce security threats

2.2 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: *availability, confidentiality, integrity, authentication, and non-repudiation.*

- Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework.

- Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield.

- Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.
- Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

- Non-repudiation ensures that the origin of a message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised

2.3 Challenges and Key Issues

The salient features of the ad hoc networks pose challenges in achieving the security goals. First of all, the use of wireless link renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active interfering. Unlike fixed hardwired networks with physical defence at firewalls and gateways, attacks on an ad hoc network can come from all directions and target at any node. Damage can include leaking secret information, interfering message and impersonating nodes, thus violating the above security goals. All these mean that every node must be prepared for encounter with an adversary directly or indirectly.

Second, autonomous nodes in an ad hoc network have inadequate physical protection, and therefore more easily to be captured,
Compromised, and hijacked. We should consider malicious attacks launched from both outside and inside the network. Since it is difficult to track down a particular mobile node in a large scale of ad hoc network, attacks from a compromised node are more dangerous and much harder to detect. All these indicate that any node must be prepared to operate in a mode that trusts no peer.

Third, any security solution with static configuration would not be sufficient because of the dynamic topology of the networks. In order to achieve high availability, distributed architecture without central entities should be applied. . This is because introducing any central entity into security solution may cause fatal attack on the entire network once the centralized entity is compromised. Generally, decision making in the ad hoc networks is decentralized and many ad hoc network algorithms rely on the cooperation of all nodes or partial nodes. But new type of attacks can be designed to break the cooperative algorithm. s can be seen from the above, no matter what security measures are deployed, there are always some vulnerability that can be exploited to break in.

Based on the above analysis, we further summarize three key issues for achieving the security of ad hoc networks

- Intrusion detection
- Secure routing
- Key management service

III. FURTHER DISCUSSION ON KEY ISSUES

In this section we will further study the current state of the issues discussed above.

3.1 Intrusion detection

An intrusion is defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability" [5]. Intrusion protection techniques work as the first line of defence. However, intrusion protection alone is not sufficient because there is no perfect security in any network system, especially in the ad hoc networks. Intrusion detection can be used as the second line of protection to capture audit data and dig out evidence in the data to determine whether the system is under attack. Because once an intrusion is detected, e.g. in the early stage of a DDOS (Distributed Denial -of- Services), measures can be taken to minimize the damages, gather evidence for prosecution and even launch counter-attacks. This is very important in the ad hoc network to find compromised nodes promptly and take corresponding actions to against.

Generally speaking, intrusion detection system (IDS) can be classified as network -based or host -based according to the type of audit data used. A network -based IDS runs at the gateway of a network and captures and examines the packets going through it. This kind of IDS is not suitable for the ad hoc networks where there are no traffic concentration points. A host -based IDS relies on operating system audit data to monitor and analyse the events generated by programs or users on the node. In the ad hoc networks, the useful audit data at the node include system and user activities within the mobile node, communication activities by this node, as well as communication activities within the radio range and observation of the node

The intrusion detection techniques can be categorized into misuse detection n and anomaly detection. The misuse detection uses patterns of well -known attacks to match and identify known intrusions. It can accurately and efficiently detect instances of known attacks, but it lacks ability to find out newly invented attacks. In the ad hoc networks, it is more difficult to model the pattern of known attacks due to the complexity and mobility of the networks. The anomaly detection flags observed activities that deviate significantly from the established normal usage as possible intrusions. This detection does not require prior knowledge of intrusion and can thus detect new intrusions. The disadvantage is it may not be able to indicate what intrusion is and may have high false rate. Furthermore, there may not be a clear separation between normalcy and anomaly in the ad hoc networks. This model may not be suitable to deploy for the ad hoc environment.

3.2 Secure Routing

In MANET, routing functions are carried out by all available nodes. Likewise, common routing security mechanisms consist of node and message authentication referring to apriority trust model in which legitimate routers are believed to perform correct operations. Authentication of a node or its messages does not guarantee the correct execution of routing functions in open environments with lack of a priori trust like MANET.

Ad Hoc routing protocols can be divided into three classes [6]. Table-driven or proactive protocols require the periodical refreshing or updating of the routing information so that every node can operate with consistent and up -to-date routing tables. The advantage of the proactive approach is that once a route is formed, its use is efficient. But the pure proactive protocols do not suite the ad -hoc networks due to the heavy routing information exchange. Source-initiated on –demand driven or reactive protocols, in contrary, do not periodically update the routing information - the data is propagated to the necessary nodes only when necessary. Many of the ad hoc protocols fall into this class. They create network traffic only when the routing fabric must really be changed. The disadvantage of the reactive protocols is that they create a lot of overhead when the route is being determined. The third class, hybrid protocols, make use of both approaches by adapting the protocol to the specific conditions. For instance, table - driven protocols could be used between networks and on-demand protocols inside the networks or vice versa.

To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. Routing protocols [7, 8, 9, 10, 11, 12, 13, and 14] proposed for ad hoc networks cope well
with the dynamically changing topology. However, none of them, to our knowledge, have accommodated mechanisms to defend against malicious attacks. Routing protocols for ad hoc networks are still under active research. There is no single standard routing protocol. Therefore, we aim to capture the common security threats and to provide guidelines to secure routing protocols

In most routing protocols, routers exchange information on the topology of the network in order to establish routes between nodes. Such information could become a target for malicious adversaries who intend to bring the network down.

There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce excessive traffic load into the network by causing retransmission and inefficient routing

The second and also the more severe kind of threats comes from compromised nodes, which might advertise incorrect routing information to other nodes. Detection of such incorrect information is difficult: merely requiring routing information to be signed by each node would not work, because compromised nodes are able to generate valid signatures using their private keys.

To defend against the first kind of threats, nodes can protect routing information in the same way they protect data traffic, i.e., through the use of cryptographic schemes such as digital signature. However, this defence is ineffective against attacks from compromised servers. Worse yet, as we have argued, we cannot neglect the possibility of nodes being compromised in an ad hoc network. Detection of compromised nodes
through routing information is also difficult in an ad hoc network because of its dynamically changing topology: when a piece of routing information is found invalid, the information could be generated by a compromised node, or, it could have become invalid as a result of topology changes. It is difficult to distinguish between the two cases. On the other hand, we can exploit certain properties of ad hoc networks to achieve secure routing.

3.3 Key Management Service

Traditional cryptographic mechanisms, such as digital signature and public key encryption, still play vital roles in achieving security goals in the ad hoc networks. All these mechanisms require a key management service to keep track of key and node binding and assist the establishment of mutual trust

between communication nodes. Traditionally, the key management service is based on a trusted entity called a certificate authority (CA) to issue public key certificate of every node. The trusted CA is required to be online in many cases to support public key revocation and renewal. But it is dangerous to set up a key management service using a single CA in an ad hoc network. Single CA will be the vulnerable point of the network. If the CA is compromised, the security of the entire network is crashed. How to set up a trusted key management service for the ad hoc network is also a big issue.

We employ cryptographic schemes, such as digital signatures, to protect both routing information and data traffic. Use of such schemes usually requires a key management service.

We adopt a public key infrastructure because of its superiority in distributing keys and in achieving integrity and non-repudiation. Efficient secret key schemes are used to secure further communication after
nodes authenticate each other and establish a shared secret session key.

In a public key infrastructure, each node has a public/private key pair. Public keys can be distributed to other nodes, while private keys should be kept confidential to individual nodes. There is a trusted entity
called Certification Authority (CA) [15, 16, and 17] for key management. The CA has a public/private key pair, with its public key known to every node, and signs certificates binding public keys to nodes.

The trusted CA has to stay on-line to reflect the current bindings, because the bindings could change over time: a public key should be revoked if the owner node is no longer trusted or is out of the network; a node may refresh its key pair periodically to reduce the chance of a successful brute-force attack on its private key.

As discussed above, key management service is the basic issue on the ad hoc security if traditional cryptographic way is deployed. The most popular ideas today are introduced below.

3.3.1 Key agreement

In [18], Asokan and Ginzboorg presented a new protocol for password -based multi-party key agreement in an ad hoc scenario that a group people in a meeting room do not have access to public key infrastructure or third party key management service, but need to set up a secure session among their computers. The protocol illustrates Diffie Hellman key exchange base d on shared password authentication between two parties and among multiple parties. It derives a strong -shared session key from the weak shared password. Key agreement is a fundamental building block for various security services. But this protocol is only suitable for the above special scenario. A password has to be shared by all the nodes involved in the ad hoc network. The authors do not consider how to renew the password in case some nodes leave or are compromised.

3.3.2 Threshold Cryptography

Distribution of trust in our key management service is accomplished using threshold cryptography [19, 20]. An (n, t + 1) threshold cryptography scheme allows n parties to share the ability to perform a cryptographic operation (e.g., creating a digital signature), so that any t + 1 parties can perform this operation jointly, whereas it is infeasible for at most t parties to do so, even by collusion.

In [5] and [8], threshold cryptography is used to provide robust and ubiquitous security support for the ad hoc networks. The basic idea is the CA functions are distributed through a threshold secret sharing mechanism, in which each entity holds a secret share and multiple entities jointly provide complete services. In the proposed designs for an ad hoc network with totally N nodes, K nodes hold secret share of the CA's private key, K nodes jointly can provide a complete CA signature.
The system security cannot be compromised as long as 6 here are less than K shareholders to be broken. That is an adversary must destroy (N-K+1) nodes in order to turn off certification services. To further resist intrusions, the secret shares are updated periodically.

IV. CONCLUSION

This paper analysed the security challenges in the ad hoc networks. We summarized three key issues that should be firstly solved for achieving the ad hoc security. Furthermore, we gave an overview of the current state of solutions on intrusion detection, secure routing and key management service respectively. This paper focuses more on the problems existing In the current state of Ad hoc Networks.

REFERENCES

[1] IEEE Wireless Local Area Networks, <http://www.ieee802.org/11/ >

[2] Official Bluetooth Website, <http://www.bluetooth.com/>

[3] S. Corson, J. Macker: Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, 1999, ftp://ftp.funet.fi/pub/standards/RFC/rfc2501.txt

[4] S. Corson, J. Macker, G. Cirincione: I nternet-Based Mobile Ad Hoc Networking, IEEE Internet
Computing, Jul/Aug 1999.

[5] Yongguang Zhang, Wenke Lee: Intrusion Detection in Wireless Ad -Hoc Networks, Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking,
Boston, MA, USA, 6-11 Aug. 2000.

[6] Vesa Kärpijoki: Signalling and Routing Security in Mobile and Ad -hoc Networ ks, May, 2000, < http://www.tml.hut.fi/Opinnot/Tik-110.551/2000/papers/signalling_security/index.ht

[7] S. Murphy and J. J. Garcia-Luna-Aceves. An efficient routing algorithm for mobile wireless networks. MONET, 1(2):183–197, October 1996.

[8] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad-hoc wireless networks. Mobile Computing,1996.

[9] J. Sharony. A mobile radio network architecture with dynamically changing topology using virtual subnets. In Proceedings of ICC/SUPERCOM'96, pages 807–812, Dallas, TX, June 1996.

[10] V. D. Park and M. S. Corson. A highly adaptable distributed routing algorithm for mobile wireless networks. In IEEE INFOCOMM'97, Kobe, Japan, 1997.

[11] C.-K. Toh. Associativity-based routing for ad hoc mobile networks. Wireless Personal Communications Journal, Special Issue on Mobile Networking and Computing Systems, 4(2):103–139, March 1997

[12] Z. J. Haas and M. Perlman. The performance of query control schemes for zone routing protocol. In SIGCOMM'98, June 1998.

[13] P. Jacquet, P. Muhlethaler, and A. Qayyum. Optimized link state routing protocol. IETF MANET, Internet Draft, November 1998.

[14] C. E. Perkins and E. M. Royer. Ad hoc on-demand distance vector routing. In IEEE WMCSA'99, New Orleans, LA, February 1999.

[15] M. Gasser, A. Goldstein, C. Kaufman, and B. Lampson. The digital distributed systems security architecture. In Proceedings of the 12th National Computer Security Conference, pages 305–319, Baltimore, MD USA, October 10–13, 1989. National Institute of Standards and Technology (NIST), National Computer Security Center (NCSC).

[16] J. J. Tardo and K. Algappan. SPX: Global authentication using public key certificates. In Proceedings
of the 1991 IEEE Symposium on Security and Privacy, pages 232–244, Oakland, CA USA, May 1991. IEEE Computer Society Press.

[17] C. Kaufman. DASS: Distributed authentication security service. Request for Comments 1507, September 1993.

[18] Asokan-N, Ginzboorg -P: Key agreement in ad hoc networks, Computer Com munications (Netherlands), vol.23, no.17, p.1627 -37, 1 Nov. 2000.

[19] Y. Desmedt. Threshold cryptography. European Transactions on Telecommunications, 5(4):449–457, July–August 1994.

[20] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In G. Brassard, editor, Advances in Cryptology— Crypto'89, the 9th Annual International Cryptology Conference, Santa

Barbara, CA USA, August 20–24, 1989, Proceedings, volume 435 of Lecture Notes in Computer Science, pages 307–315. Springer, 1990.

[21] Security in Ad Hoc Networks Zheng Yan Networking Laboratory Helsinki University of Technologyzheng.yan@hut.fi

[22] Securing Ad Hoc Networks∗ Lidong Zhou Department of Computer Science Zygmunt J. Haas School of Electrical Engineering Cornell University Ithaca, NY 14853

[23] Security in Ad Hoc Networks * Refik Molva and Pietro Michiardi Institut Eurecom2229 Route des Crêtes 06904 Sophia-Antipolis, France