Need to Secure a Adhoc Network

Saoud Sarwar¹ Sana Saif² Almas Zahra³ Syed Tariq⁴ Shikha Mishra⁵
¹³Department of Computer Science, Al-Falah School of Eng. & Tech. Faridabad, India
²Duxconcept, New Delhi ⁴Accenture-IT-System Analyst, Okhla, New Delhi
⁵Department of Computer Science JB Knowledge Park, Faridabad, India

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. The military tactical and other security-sensitive operations are the main applications of adhoc networks. Other commercial uses are also trying to adopt the usage of the adhoc networks.

One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved.

In light of this paper we have reviewed opportunities posed by this new networking environment. We have reviewed the main threats focused on Adhoc Networks, the major security features, secure routing and key management services.

Keywords: Secure Routing, Security Trinity, MANET

I. INTRODUCTION

Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). An adhoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. In it there is no fixed infrastructure such as base stations or mobile switching centers. These can be formed, merged together or partitioned into separate networks on the fly, without necessarily relying on a fixed infrastructure to manage the operation. 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.

Nodes of a adhoc network are mobile, which states that they apply wireless communication to maintain the connectivity. As such these may be referred as mobile adhoc networks -MANET

Military tactical operations are still the main application of ad hoc networks today. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

II. 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.

A. Availability

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.

B. Confidentiality

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.

C. Integrity

It 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.

D. Authentication

It 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.

E. Non-repudiation

It ensures that the origin of a message cannot deny having sent the message. Nonrepudiation 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.

III. THE SECURITY TRINITY

The three legs of the "security trinity,” prevention, detection, and response, comprise the basis for adhoc security. The security trinity should be the foundation for all security
policies and measures that an organization develops and deploys as in the figure below:

![Fig.1: The security trinity](image)

**A. Prevention**

The foundation of the security trinity is prevention. To provide some level of security, it is necessary to implement measures to prevent the exploitation of vulnerabilities. In developing network security schemes, organizations should emphasize preventative measures over detection and response: It is easier, more efficient, and much more cost-effective to prevent a security breach than to detect or respond to one.

**B. Detection**

Once preventative measures are implemented, procedures need to be put in place to detect potential problems or security breaches; in the event preventative measures fail.

**C. Response**

Organizations need to develop a plan that identifies the appropriate response to a security breach. The plan should be in writing and should identify who is responsible for what actions and the varying responses and levels of escalation.

**IV. SECURITY THREATS IN AN ADHOC NETWORKS**

**A. Types of Attacks**

Attacks against ad hoc networks can be divided into two groups: Passive attacks typically involve only eavesdropping of data. 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. Internal attacks are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer.

**B. Denial of Service**

The denial of service threat either produced by an unintentional failure or malicious action forms a severe security risk in any distributed system. The consequences of such attacks, however, depend on the area of application of the ad hoc network. If the enemy can shut down the network, the group may be separated into vulnerable units that cannot communicate with each other or to the headquarters.

**C. Impersonation**

Impersonation attacks form a serious security risk in all levels of ad hoc networking. If proper authentication of parties is not supported, compromised nodes may in network layer be able to e.g. join the network undetectably or send false routing information masqueraded as some other, trusted node. Within network management the attacker could gain access to the configuration system as a super user. In service level, a malicious party could have its public key certified even without proper credentials. Thus impersonation attacks concern all critical operations in ad hoc networks. Impersonation threats are mitigated by applying strong authentication mechanisms in contexts where a party has to be able to trust the origin of data it has received or stored. Most often this means in every layer the application of digital signature or keyed fingerprints over routing messages, configuration or status information or exchanged payload data of the services in use.

**D. Disclosure**

Any communication must be protected from eavesdropping, whenever confidential information is exchanged. Also critical data the nodes store must be protected from unauthorized access. In ad hoc networks such information can include almost anything e.g. specific status details of a node, the location of nodes, private or secret keys, passwords and -phrases and so on. Sometimes the control data is more critical information in respect of the security than the actual exchanged data.

**V. SECURE ROUTING**

To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. Routing protocols \([30, 25, 43, 32, 49, 16, 23, 35]\) 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 defense 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.

On the other hand, we can exploit certain properties of ad hoc networks to achieve secure routing. Note that routing protocols for ad hoc networks must handle outdated routing information to accommodate the dynamically changing topology. False routing information generated by compromised nodes could, to some extent, be considered outdated information. As long as there are sufficiently many correct nodes, the routing protocol should be able to find routes that go around these compromised nodes. Such capability of the routing protocols usually relies on the inherent redundancies — multiple, possibly disjoint, routes between nodes — in ad hoc networks. If routing protocols can discover multiple routes, nodes can switch to an alternative route when the primary route appears to have failed.

VI. KEY MANAGEMENT SERVICE

Cryptographic schemes, such as digital signatures are applied 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) [11, 47, 26] 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.

It is problematic to establish a key management service using a single CA in ad hoc networks. The CA, responsible for the security of the entire network, is a vulnerable point of the network: if the CA is unavailable, nodes cannot get the current public keys of other nodes or to establish secure communication with others. If the CA is compromised and leaks its private key to an adversary, the adversary can then sign any erroneous certificate using this private key to impersonate any node or to revoke any certificate.

A standard approach to improve availability of a service is replication. But a naive replication of the CA makes the service more vulnerable: compromise of any single replica, which possesses the service private key, could lead to collapse of the entire system. To solve this problem, we distribute the trust to a set of nodes by letting these nodes share the key management responsibility.

VII. CONCLUSION

In this paper, we have analyzed the security threats an ad hoc network faces and presented the security objectives that need to be achieved. On one hand, the security-sensitive applications of ad hoc networks require high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks. The idiosyncrasy of ad hoc networks poses both challenges and opportunities for these mechanisms.

This paper focuses on how to secure routing and how to establish a secure key management service in an ad hoc networking environment. These two issues are essential to achieving our security goals. Besides the standard security mechanisms, we take advantage of the redundancies in ad hoc network topology and use diversity coding on multiple routes to tolerate both benign and Byzantine failures. To build a highly available and highly secure key management service, we propose to use threshold cryptography to distribute trust among a set of servers. Furthermore, our key management service employs share refreshing to achieve proactive security and to adapt to changes in the network in a scalable way. Finally, by relaxing the consistency requirement on the servers, our service does not rely on synchrony assumptions. Such assumptions could lead to vulnerability. A prototype of the key management service has been implemented, which shows its feasibility.

REFERENCES


