Wireless Network Security Threats
Satish Kumar Garg

Govt. PG College
Jind-126102 (Haryana),
India

Correspondence Author:
Satish Kumar Garg
sat.phy@gmail.com

1 Introduction:

The term "wireless" came into public use to refer to a radio receiver or transceiver, establishing its usage in the field of wireless telegraphy. Now the term is used to describe modern wireless connections such as in cellular networks and wireless broadband internet. It is also used in a general sense to refer to any type of operation that is implemented without the use of wires, such as "wireless remote control", "wireless energy transfer", etc. regardless of the specific technology (e.g., radio, infrared, ultrasonic, etc.) that is used to accomplish the operation.

The chief concerns at this time are:
1. Security problems resulting from the deployment of wireless appliances and networks
2. The need to adopt a uniform campus wireless standard in the face of evolving and changing industry standards to avoid incompatibility and the need to replace equipment that is incompatible with emerging standards.
3. Network resource demands resulting from the potential addition of a large number of new users and from the need to maintain network security.

Salient threats and vulnerabilities of wireless systems are:
- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an agency's computer or voice (IP telephony) network through wireless connections, potentially bypassing any firewall protections.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade them on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their physical movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and be subsequently introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other agencies for the purposes of launching attacks and concealing their activity.
Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

Malicious entities may use a third party, un-trusted wireless network services to gain access to an agency's network resources.

Internal attacks may be possible via ad hoc transmissions.

As with wired networks, agency officials need to be aware of liability issues for the loss of sensitive information or for any attacks launched from a compromised network.

2 Security Goals\textsuperscript{7,8}

In order to make secure the system one should consider the security primary attributes as confidentiality, integrity and availability and secondary attributes as authenticity, non-repudiation and accountability etc.

2.1 Primary Attributes \textsuperscript{4,9}:

2.1.1 Confidentiality: It 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.

2.1.2 Integrity: This implies that information cannot be altered except under properly authorized circumstances or it guarantees that a message being transferred is never corrupted.

2.1.3 Availability: This implies that resources are available, where desired or it can be considered that it provides survivability of network services despite denial of service attacks. The entire primary attributes can be maintained in the presence of malicious user and accidental.

2.2 Secondary Attributes:

2.2.1 Authenticity: It implies that apparent identity of the entity is genuine. That is 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.

2.2.2 Non-repudiation: It ensures that the origin of a message cannot deny having sent the message i.e. It implies that authenticity is sufficient trustworthy that later claims to its falsehood cannot be sustained. 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.

2.2.3 Accountability: It implies that it is possible to determine what has transpired, in terms of who did what operations or what resources at what time, as desired.

2.2.4 Data Freshness: It ensures that the data is recent and that no adversary replayed old message.

3 Key Security Issues \textsuperscript{4,10}

As ad hoc network works in wireless environment so nodes are more susceptible to attacks. That's why the key security issues must be discussed to attain the security for network.

3.1 End-to-End Information Security: In the wireless environment the communication, which a node performs to the other, is more susceptible to attacks. In ad hoc network there is no protection like firewall or access control. Any node can become vulnerable to attack from any direction. The attacking node could spoof the identity of node, it could temper the node's credentials, it could leak the node's confidential information or it could impersonate the node. This type of attack could leak the confidentiality, integrity and availability of the service provided by the node. The identification and authentication of node is also necessity in ad hoc network. The main issues in the identification and authentication is that the nodes can be confirmed to be authorized to gain access, without these methods the nodes may be given delegate certificates with which the node can access to the services. In some ad hoc networks the services may be centralized, while in other networks they are applied in distributed manner, which may require the use of different access control mechanisms. Moreover the required security level in access control also affects the way the access control must be implemented. To ensure the end-to-end security, the traditional security mechanisms such as authentication protocols, digital signature and encryption are used in achieving the primary and secondary security goals for ad hoc network.

3.2 Secure Routing: The routing protocols within ad hoc networks are more vulnerable to attacks as each device acts as a relay. Any tampering with the routing information can compromise the whole network. An attacker can introduce rogue information within
routing information or replay old logged or stored information.

The aim is to protect any information or behavior that can update or cause change to the routing tables on cooperating nodes involved in an ad hoc routing protocol. For completeness, timeliness and ordering are added to the list of desirable security properties that can eliminate or reduce the threat of attacks against routing protocols. Techniques that can be used to guarantee these properties are described in Table 11,12 (below).

Table: Properties of secured routing

<table>
<thead>
<tr>
<th>Properties</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeliness</td>
<td>Time stamping, Slotted Time</td>
</tr>
<tr>
<td>Ordering</td>
<td>Sequence Numbering</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Password, Certificate</td>
</tr>
<tr>
<td>Authorization</td>
<td>Credential</td>
</tr>
<tr>
<td>Integrity</td>
<td>Digest, Digital Signature</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Encryption</td>
</tr>
<tr>
<td>Non-Repudiation</td>
<td>Chaining of Digital Signature</td>
</tr>
</tbody>
</table>

The following properties can be integrated into routing protocol messages to prevent attacks that exploit the vulnerability of unprotected information in transit:

3.2.1 Timeliness: Routing updates need to be delivered in a timely fashion. Update messages that arrive late may not reflect the true state of the links or routers on the network. They can cause incorrect forwarding or even propagate false information and weaken the credibility of the update information. Most ad hoc routing protocols have timestamps and timeout mechanisms to guarantee the freshness of the routes they provide.

3.2.2 Ordering: Out-of-order updates can also affect the correctness of the routing protocols. These messages may not reflect the true state of the network and may propagate false information. Ad hoc routing protocols have sequence numbers that are unique within the routing domain to keep updates in order.

3.2.3 Authenticity: Routing updates must originate from authenticated nodes and users. Mutual authentication is the basis of a trust relationship. Simple passwords can be used for weak authentication. Each entity can append a public key certificate, attested by a trusted third party to claim its authenticity. The certifying authority can implement a password based login or a challenge-response mechanism to authenticate the identity in the first place. The receiving node can then verify this claim by examining the certificate. One of the problems in ad hoc networking is the absence of a centralized authority to issue and validate certificates of authenticity.

3.2.4 Authorization: An authenticated user or node is issued an unforgivable credential by the certificate authority. These credentials specify the privileges and permissions associated by the users or the nodes. Currently, credentials are not used in routing protocol packets, and any packet can trigger update propagations and modifications to the routing table.

3.2.5 Integrity: The information carried in the routing updates can cause the routing table to change and alter the flow of packets in the network. Therefore, the integrity of the content of these messages must be guaranteed. This can be accomplished by using message digests and digital signatures.

3.2.6 Non-repudiation: Routers cannot repudiate ownership of routing protocol messages they send. A major concern with the updates is the trust model associated with the propagation of updates that originate from distant nodes. Ad-hoc nodes obtain information from their neighbors and forward it to their other neighbors. These neighbors may forward it to other neighbors and so on. In most existing protocols, nodes cannot vouch for the authenticity of updates that are not generated by their immediate neighbors. In order to preserve trust relationships, it becomes necessary to form a chain of routers (using signatures to protect integrity) and authenticate every one in turn, following the chain to the source. This is necessary because trust relationships are not transitive. Alternative solutions that avoid chaining include the path attribute mechanism developed for Secure BGP and secure distance vector routing.

3.2.7 Confidentiality: In addition to integrity, sometimes it may be necessary to prevent intermediate or non-trusted nodes from understanding the contents of packets as they are exchanged between routers. Encrypting the routing protocol packets themselves can prevent unauthorized users from reading it. Only routers that have the decryption key can decrypt these messages and participate in the routing. This is employed when a node cannot trust one or more of its immediate neighbors to route packets correctly. Each
of these desirable properties has a cost and performance penalty associated with it. Some options such as enforcing access control to routing tables using credentials and providing non repudiation by chaining signatures are extremely expensive and impractical to implement and enforce in a generalized routing protocol.

4 Proposed Solution

Key management is the process by which cryptographic keys are generated, stored, protected, transferred, loaded, used, and destroyed. At the initial stage, the data packet will be transmitted from source to destination over transmission media using efficient cryptographic algorithm to encrypt the entire packet. Cryptography is the process used to make a meaningful message appear meaningless. An algorithm is a set of rules or procedures used to scramble, or encrypt the plaintext to produce Cipher text. The algorithm applies a key to text [13]. Encryption is the procedure that guarantees secrecy of the data exchanged. Any encryption algorithm depends on some key, and keys are normally generated during authentication phase, so the two phases are strictly connected [14]. In the proposed architecture, an extended flavor of link level encryption will be used to encrypt the entire data packet. The packet encryption algorithm at the originating site encrypts the entire packet including the packet header and provides it a new header. This readable new header also includes a dynamic key-id. The key-id controls the behavior of encryption and decryption mechanism. It specifies the information as the encryption algorithm, the encryption block size, the error checking code and lifetime of the key.

References


