ISSN No. 0976-5697

Volume 2, No. 4, July-August 2011

International Journal of Advanced Research in Computer Science

TECHNICAL NOTE

Available Online at www.ijarcs.info

Security Issues in Ad Hoc, Sensor and Mesh Networks

Abhishek Dixit
Technical Lead
HCL Technologies Ltd,
Noida, India
abhishekdixitg@gmail.com,Abhishek-D@hcl.com

Abstract**—** Network security in a wireless environment is a unique challenge. Whereas wired networks send electrical signals or pulses through cables, wireless signals propagate through the air. Because of this, it is much easier to intercept wireless signals. This extra level of security complexity adds to the challenges network administrators already face with traditional wired networks. There are a number of extremely serious risks and dangers if wireless networks are left open and exposed to the outside world. This paper studies the security aspects of these networks. The paper first introduces the types of wireless networks, and then presents its related security problems, threats, risks and characteristics.

Keywords - Wireless Sensor Networks (WSN); security; attack, threat model.

I. INTRODUCTION

Although the wireless medium has limited spectrum and additional constraints when compared to guided media, it provides the only means of mobile communication. In addition, more effective usage of the limited spectrum and advanced physical/data link layer protocols enable broadband communications and integrated services over the limited wireless spectrum. Moreover, random and rapid deployment of a large number of tetherless nodes is possible through wireless ad hoc networking, which is a technology with a wide range of applications such as tactical communications, disaster relief operations and temporary networking in areas that are not densely populated. As a result, the use of wireless ad hoc networking has become pervasive. However, wireless ad hoc networking also introduces additional security challenges [1] on top of those that exist for tethered networking:

A. the wireless broadcast medium is easier to tap than guided media;
B. the wireless medium has limited capacity and therefore requires more efficient schemes with less overhead;
C. the self-forming, self-organization and self-healing algorithms required for ad hoc networking, and the schemes that tackle challenges such as hidden and exposed terminals, may be targeted to design sophisticated security attacks;
D. The wireless medium is more susceptible to jamming and other denial-of-service attacks.

Wireless sensor and actuator networks (WSANs) are based on the random deployment of a large number of tiny sensor nodes and actuators into or very close to the phenomenon to be observed. They facilitate many application areas such as tactical surveillance by military unattended sensor networks, elderly and patient monitoring by body area networks (BANs) and building automation by building automation and control networks (BACnets). They are, in essence, ad hoc networks with additional and more stringent constraints. They need to be more energy efficient and scalable than conventional ad hoc networks, which exacerbates the security challenges. The security schemes for WSANs should require less computational power and memory because sensor nodes are tiny and have more limited capacity than the typical ad hoc network nodes such as a personal digital assistant (PDA) or a laptop computer.

The wireless mesh network (WMN) is another member of the ad hoc network domain. WMNs enable application areas such as infrastructure-less networks for developing regions, low-cost multi-hop wireless backhaul connections and community wireless networks. Actually, ad hoc networks can be considered a subset of WMNs because WMNs also provide a wireless backbone for working other mesh, ad hoc or infrastructure-based networks such as the Internet, IEEE 802.11, IEEE 802.15, IEEE 802.16, cellular, wireless sensor, wireless fidelity (Wi-Fi), worldwide interoperability for microwave access (WiMAX) and WiMedia networks. Lack of central authority and the availability of various access technologies to access the network make WMNs a more challenging domain in terms of security.

II. WIRELESS AD-HOC, SENSOR AND MESH NETWORKS

A. Mobile Ad-hoc Network

A mobile ad hoc network (MANET) [2] sometimes called a mobile mesh network, is a self configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other device frequently. Each most forward traffic unrelated to its own use and therefore be in router. The primary challenge in building a MANET is equipping device to continuously maintain the information required to property route traffic. In such networks, the wireless mobile nodes may dynamically enter the network as well as leave the network. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network

B. Sensor and Actuator Networks

Wireless sensor networks [3] form a particular class of Ad-hoc networks that operate with little or no infrastructure. WSNs are gaining momentum as they have great potential for both research and commercial applications. The sensor network nodes themselves are ideally low-priced, very small devices. They typically consist of a collection of application specific sensors, a wireless transceiver, a simple general purpose processor, possibly assisted by limited amount of special-purpose hardware, and an energy unit that may be a battery or a mechanism to obtain energy from the environment. We cannot assume that sensor nodes will be tamper- resistant, although we will consider the availability of such tamper-resistant nodes for future applications. Sensor nodes are distributed over a potentially vast geographical area to form a static, multi-hop, self-organizing network. However, also mobile WSNs and mobility within WSN are conceivable.

C. Mesh Networks

Wireless mesh networks (WMNs) have emerged as a promising concept to meet the challenges in next-generation networks such as providing flexible, adaptive, and reconfigurable architecture while offering cost-effective solutions to the service providers [4]. Unlike traditional Wi-Fi networks, with each access point (AP) connected to the wired network, in WMNs only a subset of the APs are required to be connected to the wired network. The APs that are connected to the wired network are called the Internet gateways (IGWs), while the APs that do not have wired connections are called the mesh routers (MRs). The MR's are connected to the IGWs using multi-hop communication. The IGWs provide access to conventional clients and interconnect ad hoc, sensor, cellular, and other networks

III. SECURITY ATTACKS IN AD HOC, SENSOR AND MESH NETWORKS

Security attacks can be categorized into two broad classes: passive and active attacks. Passive attacks, where adversaries do not make any emissions, are mainly against data confidentiality. In active attacks, malicious acts are carried out not only against data confidentiality but also data integrity. Active attacks can also aim for unauthorized access and usage of the resources or the disturbance of an opponent's communications. An active attacker makes an emission or action that can be detected. Apart from security attacks, needlessness is also an important security threat. By mistake, users can expose nodes to threats like tampering and destruction, and classified data and resources to unauthorized access. Security and fault-tolerance schemes should also tackle the security and safety challenges created by careless use or unpredicted events [5].

A. Passive Attacks

There are two types of passive attacks an attacker can mount:

a) Traffic Analysis
b) Passive Eavesdropping

a. Traffic Analysis

The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties

One of the following techniques may be used for traffic analysis:

i. Traffic Analysis at the Physical Layer:

In this attack only the carrier is sensed and the traffic rates are analysed for the nodes at a location.

ii. Traffic Analysis in MAC and Higher Layers:

MAC frames and data packets can be de-multiplexed and headers can be analysed. This can reveal the routing information, topology of the network and friendship trees.

iii. Traffic Analysis by Event Correlation:

events like detection in a sensor network or transmission by an end user can be correlated with the traffic and more detailed information, e.g. routes, etc., can be derived.

iv. Active Traffic Analysis:

Traffic analysis can also be conducted as an active attack. For example, a certain number of nodes can be destroyed, which stimulates self organization in the network, and valuable data about the topology can be gathered.

b. Passive Eavesdropping

Classified data can be eavesdropped by tapping communication lines, and wireless links are easier to tap. Therefore, wireless networks are more susceptible to passive attacks. In particular when known standards are used and plain data, i.e. not encrypted, are sent wirelessly, an adversary can easily receive and read the data and listen to or watch audio–visual transmissions. For example, adversaries can easily eaves-drop credit card numbers and passwords when they are transmitted plainly over unsecured wireless links.

The existence of wireless communications makes the implementation of multiple networks with different security levels at a single facility much more difficult. For example, if there are both classified networks and a network attached to the Internet in the same facility and wireless access to the classified networks is allowed, the decoupling of the Internet and the classified networks can become very difficult due to passive attacks and needlessness. Note that not allowing untethered communications does not make the security risks disappear, but allowing them increases the risks. Needlessness, insiders and emanation security are always issues whether wireless communications are allowed or not.

B. Active Attacks

a. Physical Attacks

An adversary may physically damage hardware to terminate the nodes. This is a security attack that can also be considered to fall in the domain of fault tolerance, which is the ability to sustain networking functionalities without any interruption due to node failures. Physical attacks against hardware may become a serious issue, especially in tactical communications and sensor networks [7]. Sensor nodes may be deployed unattended in regions accessible by the adversary. Therefore, they can be moved out of the sensor field or destroyed. When these risks are imminent, nodes need to be resilient to physical attacks. When nodes are unattended and can be reached physically by the adversary, they can be attacked by tampering techniques, such as micro probing, laser cutting, focused ion-beam manipulation, glitch attacks and power analysis [6]. Node tampering can help in masquerading and denial-of-service attacks, which we explain in the following sections. Therefore, tamper resilience is an issue that needs to be considered carefully in many sensor network and tactical communications applications.

We can group node-tampering schemes into two classes: invasive tampering and non-invasive tampering. Invasive techniques aim to gain unlimited access to a node. In non-invasive attacks, unlimited access to the node is not the intention. Instead, by analysing the behaviour of a node, such as the power consumption, or the execution timings of the algorithms for various inputs, confidential data about the procedures and keys used by the encryption schemes can be derived.

Electromagnetic pulse (EMP) attacks are also among the threats that can be listed within physical security attacks. An EMP is a short-duration burst of high-intensity electromagnetic energy that can produce voltage surges, which can damage electronic devices within range. An EMP is a natural result of nuclear explosions. Today, portable devices that can generate EMPs are also available. Although there are still unsolved issues related to the practicability of EMP technologies, EMPs are a threat for all kinds of electrical devices in the tactical field. Again, this can be considered as part of the fault tolerance domain. It is possible to build electronic devices that are more resilient to EMPs. Therefore, we have listed EMP attacks as a type of security attack.

b. Masquerade, Replay and Message Modification

A masquerading node acts as if it is another node. Messages can be captured and replayed by masquerading nodes. Finally, the content of the captured messages can be modified before being replayed. Various scenarios and threats can be developed based on these approaches. Ad hoc and sensor networks introduce particular advantages for masquerading. In mobile ad hoc networks, nodes may change their location in the network. This location is not given or fixed, and self-forming and self-healing mechanisms are counted on to adapt to topology changes. Since reactive techniques are preferred for routing and topology may not be maintained, it may be difficult to check the consistency of a node’s access point to the network.

Masquerading, message replay and content modification can be used to attack the integrity of the content of messages or services in a network. For example, node localization schemes may be subject to one of the following security attacks:

i. A malicious node may act as a beacon and disseminate its location wrongly. This hampers the node localization procedure when the node uses beacon signals transmitted by the malicious node for triangulation or multilateration.
ii. A beacon may be tampered with and introduce wrong location data, transmit beacon signals with less or more power than expected to impair received signal strength indicator based schemes or slightly desynchronize the transmission of RF and ultrasonic signals if the time difference of arrival algorithm is used.
iii. Beacon signals may be replayed by a malicious node.
iv. Beacon nodes may be destroyed by physical attacks.
v. An obstacle may be placed between beacon nodes and the network to block the direct line of sight.

There are many more attack scenarios that may be detrimental to the node localization schemes.

i. In-network data aggregation and fusion make sensor networks more sensitive to replay and content modification attacks because changing the content of an aggregated message may change the data provided by many nodes.
ii. Time synchronization is also a vulnerable service for masquerading attacks. Several insiders that inject false time synchronization messages may prevent the system from achieving time synchronization. Time synchronization can be especially sensitive to replay attacks.

A malicious node can jam a time synchronization message at a certain part of a network, and then replay the message at that part after a very short delay. This may prevent correct time synchronization and create considerable detrimental effects on all services that rely on the accuracy of the synchronization protocol.

i. Data correlation and association techniques are also impaired when node localization or time synchronization services are attacked.
ii. By modifying the contents of the messages, event and event boundary detection algorithms can be hindered.
iii. Similarly, node management systems can be hampered by modifying the messages that report node status or convey commands for node management.

An improved version of masquerading is a sybil attack, where a malicious node introduces itself as multiple nodes. Having multiple identifications can be very useful for a malicious node. For example, a sybil attack can be conducted against data correlation and aggregation techniques. A node that sends multiple values with different identifications can change an aggregated value considerably. A sybil attack can also threaten multiple path routing schemes, node localization, etc. Multiple identifications can also help to keep the attacks hidden, i.e. stealthy attacks.

c. Denial-of-services-Attacks

A denial-of-service (DoS) attack mainly targets the availability of network services. A DoS is defined as any event that diminishes a network’s capacity to perform its expected function correctly or in a timely manner. A DoS attack is characterized by the following properties (Wood and Stankovic, 2005):

i. Malicious: it is carried out to prevent the network from fulfilling its intended functions. It is not accidental. Otherwise it is not in the domain of security but reliability and fault tolerance.
ii. Disruptive: it degrades the quality of services offered by the network.
iii. Asymmetric: the attacker puts in much less effort compared to the scale of the impact made on the network.

Every networking service may be subject to a DoS attack. In this section we will review important DoS scenarios for ad hoc and sensor networks [8].

d. DoS in the Physical Layer

All the physical attacks explained in Section 3.2.1 can also be perceived as DoS attacks because they prevent a network from performing its expected functions. In this section, the physical layer indicates the OSI layer responsible for representing 1s and 0s correctly in the wireless medium, and a DoS attack in the physical layer, which is called jamming, means a security threat against this.

A malicious device can jam a wireless carrier by transmitting a signal at that frequency. The jamming signal contributes to the noise in the carrier and its strength is enough to reduce the signal-to-noise ratio below the level that the nodes using that channel need to receive data correctly. Jamming can be conducted continuously in a region, which thwarts all the nodes in that region from communication. Alternatively, jamming can be done temporarily with random time intervals, which can still very effectively hamper the transmissions.

e. DoS in the Link Layer

The algorithms in the link layer, especially MAC schemes, present many exploitation opportunities for DoS attacks. For example, MAC layer DoS attacks such as the following may continuously jam a channel:

i. Whenever an RTS signal is received, a signal that collides with the CTS signal is transmitted. Since the nodes cannot start transmitting data before receiving the CTS, they continue sending RTS signals.

ii. If the MAC scheme is based on sleeping and active periods, jamming only the active periods can continuously block the channel.

iii. False RTS or CTS signals with long data transmission parameters are continuously sent out, which makes the other nodes that do virtual carrier sensing wait forever.

iv. Acknowledgement spoofing, where an adversary sends false link layer acknowledgements for overheard packets addressed to neighbouring nodes, can also be an effective link layer DoS attack.

More complex DoS attacks can be designed based on MAC layer addressing schemes. For example, in sensor networks, global addressing schemes are not used. Instead, schemes like data-centric routing; attribute-based naming and address reuse can be used. A malicious node can conduct a sybil attack in the MAC layer to make the other nodes in the region think that all the addresses available are used. This prevents the nodes from even being a part of the network.

f. DoS against Routing Schemes

Ad hoc networks are infrastructure less and have special routing challenges, which bear additional opportunities for new types of DoS attack against the network layer protocols for ad hoc and sensor networks. These attacks generally fall into one of two categories (Hu et al., 2005): routing disruption attacks or resource consumption attacks. Routing disruption attacks aim to make the routing scheme dysfunction, making it unable to provide the required networking services. The goal of resource consumption attacks is to consume network resources such as bandwidth, memory, computational power and energy. Both are denial-of-service attacks and examples of them are listed below (Karlof and Wagner, 2003):

i. Spoofed, Altered or Replayed Routing Information:

Routing information exchanged among nodes can be altered by malicious nodes to have a detrimental effect on the routing scheme.

ii. Hello Flood Attack (Karlof and Wagner, 2003):

A malicious node may broadcast routing or other information with high enough transmission power to convince every node in the network that it is their neighbour. When the other nodes send their packets to the malicious node, those packets are not received by any node.

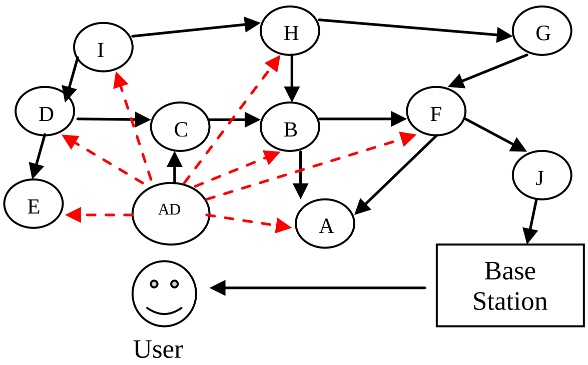

Figure 1 Hello Flood Attack

iii. Wormhole Attack:

A malicious node can eavesdrop or receive data packets at a point and transfer them to another malicious node, which is at another part of the network, through an out-of-band channel. The second malici us node then replays the packets. This makes all the nodes that can hear the transmissions by the second malicious node believe that the node that sent the packets to the first malicious node is their single-hop neighbour and they are receiving the packets directly from it. Wormholes are very difficult to detect and can impact on the performance of many network services such as time synchronization, localization and data fusion.

iv. Detour Attack:

An attacker can attempt to detour traffic to a suboptimal route or to partition the network. Various techniques can be used for this. For example, Hu et al. (2005) define a gratuitous detour attack, where a node on a route adds virtual nodes to the route such that the route becomes more costly compared to another route to which the attacker tries to detour traffic.

v. Sink Hole Attacks:

A malicious node can be made very attractive to the surrounding nodes with respect to the routing algorithm. For example, very attractive routing advertisements can be broadcast and all the neighbouring nodes can be convinced that the malicious node is the best next hop for sending the packets to the base station. When a node becomes a sink hole, it becomes the hub for its vicinity and starts receiving all the packets going to the base station. This creates many opportunities for follow-on attacks.

vi. Black Hole Attack:

A malicious node may drop all the packets that it receives for forwarding. This attack is especially effective when the black hole node is also a sink hole. Such an attack combination may stop all the data traffic around the black hole.

vii. Selective Forwarding (Gray Hole Attack):

When a malicious node drops all the packets, this may be detected easily by its neighbours. Therefore, it may drop only selected packets and forward the others.

viii. Routing Loop Attack:

Detour or sink hole types of attack can be used to create routing loops to consume energy and bandwidth as well as disrupting the routing.

ix. Sybil Attack:

A single node presents multiple identities to the other nodes in the network. This reduces the effectiveness of fault-tolerance schemes and poses a significant threat to geographic routing protocols. Apart from these services it may also affect the performance of other schemes such as misbehaviour detection, voting-based algorithms, data aggregation and fusion and distributed storage.

x. Rushing Attack (Hu et al., 2005):

An attacker disseminates route request and reply messages quickly throughout the network. This suppresses any later legitimate route request messages, i.e. nodes drop them, because nodes suppress the other copies of a route request that they have already processed.

xi. Attacks that Exploit Node-Penalizing Schemes:

Schemes that avoid low performance nodes can be exploited by adversaries. For example, malicious nodes can report error messages for a node which is actually performing well. Therefore, the routing scheme may avoid using a route that includes this node. Similarly, a link may be jammed for a short time but since error messages are generated about the link during that time interval, the routing scheme may continue to avoid the link even though it is not jammed any more.

xii. *Attacks to Deplete Network Resources:*

When nodes are unattended and rely on their onboard resources, those resources may be depleted by malicious actions. This is especially the case for sensor networks. For example, a malicious node may continuously generate packets to be sent to the data-collecting node, i.e. the base station, and the nodes that relay these messages deplete their energy.

g. DoS in the Transport Layer

Transport layer protocols are also susceptible to security threats. Some attack scenarios applicable at this layer are listed below:

i. Transport layer Acknowledgement Spoofing:

False acknowledgement or acknowledgement with large receiver windows may make the source node generate more segments than the network can handle, causing congestion and degrading the network capacity.

ii. Replaying Acknowledgement:

In some transport layer protocols, such as TCP-Reno, acknowledging the same segment multiple times indicates negative acknowledgement. A malicious node can replay an acknowledgement multiple times to make the source node believe that the message was not delivered successfully.

iii. Jamming Acknowledgements:

A malicious node can jam the segments that convey acknowledgements. This may lead to the termination of a connection.

iv. Changing Sequence Number:

In protocols like RMST and PSFQ, a malicious node may change the sequence number of a fragment and make the destination believe that some fragments have been lost.

v. Connection Request Spoofing:

A malicious node can send many connection requests to a node, using up its resources such that it cannot accept any other connection request.

This list of scenarios is not exhaustive. Many different tactics can be developed based on the protocol used in the transport layer.

h. DoS in the Application Layer

Application layer protocols can also be exploited in DoS attacks. A malicious node that impersonates a beacon node and gives false location information or cheats with regard to its transmission power, i.e. transmitting with less or more power than it is supposed to do, may hamper the node localization scheme. Since these kinds of attack diminish the related network service, they can also be categorized as DoS attacks.

IV. CONCLUSION

The attacks that I have described above are quite brief and further information can be obtained by following up the references. The attacks have countermeasure to them which are not covered in this paper. Cryptographic techniques are sometimes employed to protect against some of the attacks. Although this particular taxonomy used in this paper is not a set standard, but it can be used as a starting point for the WLAN designer .For the future scope more study needs to be analysed for security in WLAN. Understand and analyse Cryptographic techniques and implementation of the solutions, risk involved in implementation of the solutions for the above discussed attacks.

V. REFERENCES

[1] Erdal Çayırcı, Chunming “Security in Wireless Ad Hoc and Sensor Networks” c- 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-02748-6

[2] Peter P.Pham, Sylvie Perreau, “Increasing the network performance using multi path routing mechanism with load balance,” Ad Hoc Networks 2 (2004) 433-459

[3] Snehlata Yadav, Kamlesh Gupta and Sanjay Silakari “Security issues in wireless sensor networks” Journal of Information Systems and Communication, ISSN: 0976-8742, Volume 1, Issue 2, 2010, pp-01-06

[4] Akyildiz, I.F.; Wang, X.; & Wang, W. (2005). Wireless mesh networks: a survey. Journal of Computer Networks, Vol 47, No 4, pp. 445 – 487

[5] Wenjing Lou, “Security, Privacy, and Accountability in Wireless Access Network” IEEE Wireless Communications • August 2009

[6] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002) ‘Wireless Sensor Networks: A Survey’,Computer Networks, 38, 393–422.

[7] Roman, R., Zhou, J. and Lopez, J. (2005) ‘On the Security of Wireless Sensor Networks’, proceedings of the 2005 ICCSA Workshop on Internet Communications Security, Singapore, LNCS, 3482, 681–690.

[8] Wood, A. and Stankovic, J.A. (2005) “A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks’, in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC” Press, pp. 32:1–20.