Main Types of Attacks in Wireless Sensor Networks

TEODOR-GRIGORE LUPU*
*Department of Computer and Software Engineering
University "Politehnica" of Timisoara, Faculty of Automatics and Computers
Vasile Parvan 2, 300223, Timisoara
ROMANIA
E-mail: teodor.lupu@hd.politiaromana.ro

Abstract - Security has become the forefront of network management and implementation. The challenge in the security issue is to find a well balanced situation between two of the most important requirements: the need of developing networks in order to sustain the evolving business opportunities and work level, and the need to protect classified, private and in some cases even strategic information.
The application of an effective security policy is the most important step that an institution can take to protect its network.
Networks have grown in both size and importance in a very short period of time. If the security is compromised, there could be serious consequences starting from theft of information, loss of privacy and reaching even bankruptcy of that institution. The types of potential threats to network are continuously evolving and must be at least theoretical known in order to fight them back, as the rise of wireless networks implies that the security solution become seamlessly integrated, more flexible.

Keywords: Wireless Sensor Network, security, attacks, passive and active attacks, diverse layer attacks, cryptographic attacks.

1. Introduction

As a result of the growth of networks, over the years the network attack tools and methods have greatly evolved. If in around 1985 and attacker had to have sophisticated computer, programming and network knowledge to have primary (rudimentary) tools, nowadays the attackers' methods and tools improved, and the attackers no longer need such sophisticated level of knowledge.
Since the types of threats, attacks and exploits have evolved, various terms have been coined to describe the individuals involved, some of the most common terms being:
White hat – Is an individual who looks for vulnerabilities in systems or networks and then reports these vulnerabilities to the owners of the system so that they can be fixed. They are ethically opposed to the abuse of computer systems. A white hat generally focuses on securing IT systems, whereas a black hat (the opposite) would like to break into them.
Hacker - A general term that has historically been used to describe a computer programming expert. More recently, this term is often used in a negative way to describe an individual that attempts to gain unauthorized access to network resources with malicious intent.
Black hat - Another term for individuals who use their knowledge of computer systems to break into systems or networks that they are not authorized to use, usually for personal or financial gain. A cracker is an example of a black hat.
Cracker - A more accurate term to describe someone who tries to gain unauthorized access to network resources with malicious intent.
Phreaker – Phreaker is an individual who manipulates the phone network to cause it to perform a function that is not allowed. A common goal of phreaking is breaking into the phone network, usually through a payphone, to make free long distance calls.
Spammer - An individual who sends large quantities of unsolicited e-mail messages. Spammers often use viruses to take control of home computers and use them to send out their bulk messages.
Phisher - Uses e-mail or other means to trick others into providing sensitive information, such as credit card numbers or passwords. A phisher masquerades as a trusted party that would have a legitimate need for the sensitive information.
A variety of attacks are possible in Wireless Sensor Network (WSN). These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks. These security attacks in WSN and all other networks can be roughly classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related [5].

2. Attacks Classifications

2.1. Passive and active attacks criteria

Attacks can be classified into two major categories, according the interruption of communication act, namely passive attacks and active attacks. From this regard, when it is referred to a passive attack it is said that the attack obtain data exchanged in the network without interrupting the communication. When it is referred to an active attack it can be affirmed that the attack implies the disruption of the normal functionality of the network, meaning information interruption, modification, or fabrication. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

Traffic analysis: Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication.

Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack): A Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers [5] [6].

Replay attack: A replay attack is a breach of security in which information is stored without authorization and then retransmitted to trick the receiver into unauthorized operations such as false identification or authentication or a duplicate transaction. For example, messages from an authorized user who is logging into a network may be captured by an attacker and resent (replayed) the next day. Even though the messages may be encrypted, and the attacker may not know what the actual keys and passwords are, the retransmission of valid logon messages is sufficient to gain access to the network.

Also known as a "man-in-the-middle attack", a replay attack can be prevented using strong digital signatures that include time stamps and inclusion of unique information from the previous transaction such as the value of a constantly incremented sequence number.

Internal vs. external attacks: The attacks can also be classified into external attacks and internal attacks, according the domain of the attacks. Some papers refer to outsider and insider attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

Attacks on different layers of the Internet model: The attacks can be further classified according to the five layers of the Internet model. Table1 presents a classification of various security attacks on each layer of the Internet model. Some attacks can be launched at multiple layers.

2.2. Cryptography and non-cryptography related attacks

Some attacks are non-cryptography related, and others are cryptographic primitive attacks. Table 2 shows cryptographic primitive attacks and the examples.

2.3. Physical layer attacks

Wireless communication is broadcast by nature. A common radio signal is easy to jam or intercept. An attacker could overhear or disrupt the service of a wireless network physically.

Eavesdropping: Eavesdropping is the intercepting and

Table 1 Security Attacks on Each Layer of the Internet Model

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

Table 2 Cryptographic Primitive Attacks

Cryptographic Primitive Attacks	Examples
Pseudorandom number attack	Nonce, timestamp, initialization vector (IV)
Digital signature attack	RSA signature, ElGamal signature, digital signature standard (DSS)
Hash collision attack	SHA-0, MD4, MD5, HAVAL-128, RIPEMD

reading of messages and conversations by unintended receivers. The mobile hosts in mobile ad hoc networks share a wireless medium.

The majorities of wireless communications use the RF spectrum and broadcast by nature. Signals broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency. Thus, messages transmitted can be overheard, and fake messages can be injected into network.

Interference and Jamming: Radio signals can be jammed or interfered with, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. The most common types of this form of signal jamming are random noise and pulse. Jamming equipment is readily available. In addition, jamming attacks can be mounted from a location remote to the target networks.

2.4. Link layer attacks

The Mobile Ad Hoc Network (MANET) is an open multipoint peer-to-peer network architecture. Specifically, one-hop connectivity among neighbors is maintained by the link layer protocols, and the network layer protocols extend the connectivity to other nodes in the network. Attacks may target the link layer by disrupting the cooperation of the layer's protocols.

Wireless medium access control (MAC) protocols have to coordinate the transmissions of the nodes on the common transmission medium. Because a token-passing bus MAC protocol is not suitable for controlling a radio channel, IEEE 802.11 protocol is specifically devoted to wireless LANs. The IEEE 802.11 MAC protocol uses distributed contention resolution mechanisms for sharing the wireless channel. The IEEE 802.11 working group proposed two algorithms for contention resolution. One is a fully distributed access protocol called the distributed coordination function (DCF). The other is a centralized access protocol called the point coordination function (PCF). PCF requires a central decision maker such as a base station. DCF uses a carrier sense multiple access/collision avoidance protocol (CSMA/CA) for resolving channel contention among multiple wireless hosts.

Three values for interframe space (IFS) are defined to provide priority-based access to the radio channel. SIFS is the shortest interframe space and is used for ACK, CTS and poll response frames. DIFS is the longest IFS and is used as the minimum delay for asynchronous frames contending for access. PIFS is the middle IFS and is used for issuing polls by the centralized controller in the PCF scheme. In case there is a collision, the sender waits a random unit of time, based on the binary exponential backoff algorithm, before retransmitting.

Disruption on MAC DCF and backoff mechanism

Current wireless MAC protocols assume cooperative behaviors among all nodes. Obviously the malicious or selfish nodes are not forced to follow the normal operation of the protocols. In the link layer, a selfish or malicious node could interrupt either contention-based or reservation-based MAC protocols.

A malicious neighbor of either the sender or the receiver could intentionally not follow the protocol specifications. For example, the attacker may corrupt the frames easily by introducing some bits or ignoring the ongoing transmission. It could also just wait SIFS or exploit its binary exponential backoff scheme to launch DoS attacks in IEEE 802.11 MAC. The binary exponential scheme favors the last winner amongst the contending nodes. This leads to what is called the capture effect. Nodes that are heavily loaded tend to capture the channel by continually transmitting data, thereby causing lightly loaded neighbors to backoff endlessly. Malicious nodes could take advantage of this capture effect vulnerability. Moreover, a backoff at the link layer can cause a chain reaction in any upper layer protocols that use a backoff scheme, like TCP window management.

The network allocation vector (NAV) field carried in RTS/CTS frames exposes another vulnerability to DoS attacks in the link layer. Initially the NAV field was proposed to mitigate the hidden terminal problem in the carrier sense mechanism. During the RTS/CTS handshake the sender first sends a small RTS frame containing the time needed to complete the CTS, data, and ACK frames. Each neighbor of the sender and receiver will update the NAV field and defer their transmission for the duration of the future transaction according to the time that they overheard. An attacker may also overhear the NAV information and then intentionally corrupt the link layer frame by interfering with the ongoing transmission.

2.5. Network layer attacks

A variety of attacks targeting the network layer have been identified and heavily studied in research papers. By attacking the routing protocols, attackers can absorb network traffic, inject themselves into the path between the source and destination, and thus control the network traffic flow. The traffic packets could be forwarded to a non-optimal path, which could introduce significant delay. In addition, the packets could be forwarded to a nonexistent path and get lost. The attackers can create routing loops, introduce severe network congestion, and channel contention into certain areas. Multiple colluding attackers may even prevent a source node from finding

any route to the destination, causing the network to partition, which triggers excessive network control traffic, and further intensifies network congestion and performance degradation [4].

Attacks at the routing discovery phase: There are malicious routing attacks that target the routing discovery or maintenance phase by not following the specifications of the routing protocols. Routing message flooding attacks, such as hello flooding, RREQ flooding, acknowledgement flooding, routing table overflow, routing cache poisoning, and routing loop are simple examples of routing attacks targeting the route discovery phase. Proactive routing algorithms, such as DSDV and OLSR, attempt to discover routing information before it is needed, while reactive algorithms, such as DSR and AODV, create routes only when they are needed. Thus, proactive algorithms performs worse than on demand schemes because they do not accommodate the dynamic of WSN and MANETs, clearly proactive algorithms require many costly broadcasts. Proactive algorithms are more vulnerable to routing table overflow attacks. Some of these attacks are listed below.

Routing table overflow attack: A malicious node advertises routes that go to non-existent nodes to the authorized nodes present in the network. It usually happens in proactive routing algorithms, which update routing information periodically. The attacker tries to create enough routes to prevent new routes from being created. The proactive routing algorithms are more vulnerable to table overflow attacks because proactive routing algorithms attempt to discover routing information before it is actually needed. An attacker can simply send excessive route advertisements to overflow the victim's routing table.

Routing cache poisoning attack: In route cache poisoning attacks, attackers take advantage of the promiscuous mode of routing table updating, where a node overhearing any packet may add the routing information contained in that packet header to its own route cache, even if that node is not on the path. Suppose a malicious node M wants to poison routes to node X. M could broadcast spoofed packets with source route to X via M itself; thus, neighboring nodes that overhear the packet may add the route to their route caches.

Attacks at the routing maintenance phase: There are attacks that target the route maintenance phase by broadcasting false control messages, such as link-broken error messages, which cause the invocation of the costly route maintenance or repairing operation. For example, AODV and DSR implement path maintenance procedures to recover broken paths when nodes move. If the destination node or an intermediate node along an active path moves, the upstream node of the broken link broadcasts a route error message to all active upstream neighbors. The node also invalidates the route for this destination in its routing table. Attackers could take advantage of this mechanism to launch attacks by sending false route error messages.

Attacks at data forwarding phase: Some attacks also target data packet forwarding functionality in the network layer. In this scenario the malicious nodes participate cooperatively in the routing protocol routing discovery and maintenance phases, but in the data forwarding phase they do not forward data packets consistently according to the routing table. Malicious nodes simply drop data packets quietly, modify data content, replay, or flood data packets; they can also delay forwarding time-sensitive data packets selectively or inject junk packets.

Attacks on particular routing protocols: There are attacks that target some particular routing protocols. In DSR, the attacker may modify the source route listed in the RREQ or RREP packets. It can delete a node from the list, switch the order, or append a new node into the list. In AODV, the attacker may advertise a route with a smaller instance metric than the actual distance, or advertise a routing update with a large sequence number and invalidate all routing updates from other nodes.

More sophisticated and subtle routing attacks have been identified in recent research papers. The black hole (or sinkhole), Byzantine, and wormhole attacks are the typical examples, which are described in detail below.

Wormhole attack: An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to WSN routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

Rushing attack: Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial of-service attack against all currently proposed on-demand WSN routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne.

Resource consumption attack: This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

Location disclosure attack: An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location

information, such as a route map, and then plans further attack scenarios. Traffic analysis, one of the subtlest security attacks against WSN, is unsolved. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security-sensitive scenarios.

2.6. Transport layer attacks

The objectives of TCP-like Transport layer protocols in WSN include setting up of end-to-end connection, end-to-end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection. Similar to TCP protocols in the Internet, the mobile node is vulnerable to the classic SYN flooding attack or session hijacking attacks [1] [3] [4]. However, a WSN has a higher channel error rate when compared with wired networks. Because TCP does not have any mechanism to distinguish whether a loss was caused by congestion, random error, or malicious attacks, TCP multiplicatively decreases its congestion window upon experiencing losses, which degrades network performance significantly.

SYN flooding attack: The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection. For two nodes to communicate using TCP, they must first establish a TCP connection using a three-way handshake. The three messages exchanged during the handshake allow both nodes to learn that the other is ready to communicate and to agree on initial sequence numbers for the conversation.

During the attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The SYN-ACK packets are sent out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the response of ACK packet. Without receiving the ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed size table while it awaits the acknowledgement of the three-way handshake, all of these pending connections could overflow the buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection.

Session hijacking: Session hijacking takes advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter. In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. Thus the attacker impersonates the victim node and continues the session with the target.

Hijacking a session over UDP is the same as over TCP, except that UDP attackers do not have to worry about the overhead of managing sequence numbers and other TCP mechanisms. Since UDP is connectionless, edging into a session without being detected is much easier than the TCP session attacks.

2.7. Application layer attacks

The application layer communication is also vulnerable in terms of security compared with other layers. The application layer contains user data, and it normally supports many protocols such as HTTP, SMTP, TELNET, and FTP, which provide many vulnerabilities and access points for attackers. The application layer attacks are attractive to attackers because the information they seek ultimately resides within the application and it is direct for them to make an impact and reach their goals.

Malicious code attacks: Malicious code, such as viruses, worms, spywares, and Trojan Horses, can attack both operating systems and user applications. These malicious programs usually can spread themselves through the network and cause the computer system and networks to slow down or even damaged.

Repudiation attacks: Repudiation refers to a denial of participation in all or part of the communication.

2.8. Multi-layer attacks

Some security attacks can be launched from multiple layers instead of a particular layer. Examples of multi-layer attacks are denial of service (DoS), man-in-the-middle, and impersonation attacks.

Denial of service: Denial of service (DoS) attacks could be launched from several layers. An attacker can employ signal jamming at the physical layer, which disrupts normal communications. At the link layer, malicious nodes can occupy channels through the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks.

Impersonation attacks: Impersonation attacks are launched by using other node's identity, such as MAC or IP address. Impersonation attacks sometimes are the first step for most attacks, and are used to launch further, more sophisticated attacks.

Man-in-the-middle attacks: An attacker sits between the sender and the receiver and sniffs any information being sent between two ends. In some cases the attacker may impersonate the sender to communicate with the receiver, or impersonate the receiver to reply to the sender.

2.9. Cryptographic primitive attacks

Most security holes are due to poor implementation, i.e. weakness in security protocols. For example, authentication protocols and key exchange protocols are often the target of malicious attacks. Cryptographic primitives are considered to be secure; however, recently some problems were discovered, such as collision attacks on hash function, e.g. SHA-1. Pseudorandom number attacks, digital signature attacks, and hash collision attacks are discussed as following. [8]

Pseudorandom number attacks: To make packets fresh, a timestamp or random number (nonce) is used to prevent a replay attack. The session key is often generated from a random number. In the public key infrastructure the shared secret key can be generated from a random number too. The conventional random number generators in most programming languages are designed for statistical randomness, not to resist prediction by cryptanalysts. In the optimal case, random numbers are generated based on physical sources of randomness that cannot be predicted. The noise from an electronic device or the position of a pointer device is a source of such randomness. However, true random numbers are difficult to generate. When true physical randomness is not available, pseudorandom numbers must be used. Cryptographic pseudorandom generators typically have a large pool (seed value) containing randomness.

Digital signature attacks: The RSA public key algorithm can be used to generate a digital signature. The signature scheme has one problem: it could suffer the blind signature attack. The user can get the signature of a message and use the signature and the message to fake another message's signature. The attack models for digital signature can be classified into known-message, chosen-message, and key- only attacks. In the known-message attack, the attacker knows a list of messages previously signed by the victim. In the chosen-message attack, the attacker can choose a specific message that it wants the victim to sign. But in the key-only attack, the adversary only knows the verification algorithm, which is public. Hash collision attacks: The goal of a collision attack is to find two messages with the same hash, but the attacker cannot pick what the hash will be. Collision attacks were announced in SHA-0, MD4, MD5, HAVAL-128, and RIPEMD. Normally all major digital signature techniques (including DSA and RSA) involve first hashing the data and then signing the hash value. The original message data is not signed directly by the digital signature algorithm for both performance and security reasons. Collision attacks could be used to tamper with existing certificates. An adversary might be able to construct a valid certificate corresponding to the hash collision.

Key management vulnerability: Key management protocols deal with the key generation, storage, distribution, updating, revocation, and certificate service. Attackers can launch attacks to disclose the cryptographic key at the local host or during the key distribution procedure. The lack of a central trusted entity in WSN makes it more vulnerable to key management attacks.

3. Conclusion

Thinking like the attacker people understands better their goals and intentions. This will help them to protect thier systems and networks better for the future intrusions; it will help us to create better intrusion detection systems and so on [2][7].

Even if there are so many types of attacks and the possibility of having the system compromised people must not give up to the security systems like firewalls, antivirus software, cryptographic systems and software.

References

[1]. Danny McPherson, *BGP Security Techniques*, APRICOT, 2005

[2]. Hralambos Mouratidis, Paolo Giorgini, Gordon Manson, *Using Security Attack scenarios to Analyse Security During Information System Design*, in the 6th International Conference on Enterprise Information Systems, 2004

[3]. Taka Mizuguchi, Tomoya Yoshida, *BGP Route Hijacking*, APRICOT, 2007.

[4]. Su-Chiu Yang, *Flow-based Flooding Detection System*, APRICOT,2004.

[5]. Ray Hunt, Network Security: *The Principles of Threats, Attacks and Intrusions, part1 and part 2*, APRICOT, 2004.

[6]. Ehab Al-Shaer, "Network Security Attacks I: DDOS", DePaul University, 2007.

[7]. Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad, *Security Patterns- Integrating Security and System Engineering*, John Wiley & Sons, Ltd., 2006.

[8]. William Stallings, *Cryptography and Network Security Principles and Practices*, Fourth Edition, Prentice Hall, 2005.