Attacks in Wireless Sensor Networks(WSN)

Harpreet Kaur
Research scholar
Singhania University
harpreetsethi.27@gmail.com

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: Whitehat, Blackhat, Hacker, Phreaker, Cracker.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.

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 The attacks can also be classified into external attacks and internal attacks,according the domain of the 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

Table 1 Security Attacks on Each Layer of the internet model

Layer	**Attack**
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

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.

Table 2 Cryptographic Primitive Attacks

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

Eavesdropping: Eavesdropping is the intercepting and 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.Specificallyone-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.

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, injects 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].

.**2.6. Transport layer attacks**

The objectives of TCP-like Transport layer protocols inWSN include setting up of end-to-end connection, endto- end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection. However, a WSN has a higher channel error rate when compared 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.

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 vulnerabilitie 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 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 multilayer attacks are denial of service (DoS), man-in-the middle, and impersonation attacks.

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 isnot 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 messageattack, 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

.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,*.
[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*