A Threat Model Approach for Classification of Network Layer Attacks in WSN

Bhavna Arora, Ph.D
Assistant Professor
Department of Computer Science
Central University of Jammu
Jammu

ABSTRACT
Wireless sensor networks (WSN) comprise an emerging technology which has received a significant attention from the research community. Several small and low cost devices are included in the sensor networks which are self organizing ad hoc systems. WSNs are susceptible to many types of attacks at various layers of networks but due to limited resources most of traditional networks security techniques are unusable on WSNs. Hence security is a vital requirement for these networks. In this paper, the focus is on security of WSNs. A threat model has been considered; divided into four parts and has been used for evaluation of security at various layers of WSN. The paper also introduces the goals and effects of attacks in WSN based on the purpose and capabilities of the attackers. In addition, this paper discusses known approaches of security detection and defensive mechanisms against the layered attacks.

Keywords
Wireless Sensor Network (WSN), Layers of WSN, Attacks, Detection, Defensive Mechanism, Threat Model

1. INTRODUCTION
A WSN is a heterogeneous system consisting of hundreds or thousands of low-cost and low-power tiny sensors to monitor and gather information from environment and real time applications. The sensor network security is generally characterized by the same properties as traditional network security but WSNs are vulnerable to new methods of exploitation due to their unique characteristics. The sensor nodes gather and transmit the information by observing the physical environment to one or more sink, which is a high end node that collects information from these sensors and processes further. Normally, the radio transmission range of the sensor nodes are in the orders of magnitude which are smaller than the geographical extent of the entire network. Thus, data needs to be forwarded towards the sink node in hop-by-hop manner. If the amount of data which needs to transmitted are reduced, then the energy consumption of the network is also minimized. WSNs are susceptible to many types of link layer attacks [1] and most of traditional networks security techniques are unusable on WSNs due to wireless and shared nature of communication channel, untrusted transmissions, deployment in open environments, unattended nature and limited resources [1].
Sensor networks are just one form of ad hoc wireless networks, and hence we can consider them as s*ensor-based ad hoc mobile wireless networks*. This kind of network has four properties combined together [2]: *Sensors* nodes that can sense/capture information from the network, *ad- hoc*: network is established on need base, *Mobile*: Nodes are not located on fixed locations and *Wireless*: nodes can communicate wirelessly.
The paper is divided in 7 sections. The paper includes an overview of WSNs in section 1, security requirements of WSN in section 2,security classes in section 3, followed by the threat model of WSN in section 4.Section 5 discusses types of attacks against network layers of WSN and their defence techniques. Section 6 evaluates the defined attacks against the threat model followed by conclusion in section 7.

2. SECURITY REQUIREMENTS IN WSN
WSN though being a special type of network, shares some commonalities with a typical computer network. It also exhibits many distinctive characteristics. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehaviour of nodes. The most important security requirements in WSN are [3] [4]:

2.1 Data confidentiality
There is a clear need to protect sensitive transmitted data from passive attacks such as eavesdropping. Hence, cryptography based solutions are typically employed to alleviate this shortcoming. However, the sensor's power can be used quickly by the complicated encryption and decryption methods like multiplications of large numbers in public key based cryptosystems[5].The issue of confidentiality should address the following requirements [6] [7]: (i) a sensor node should not allow its readings to be accessed by its neighbours unless they are authorized to do so, (ii) key distribution mechanism should be extremely robust, (iii) public information such as sensor identities, and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks. Many applications like information surveillance, industrial management, key distribution etc. need to rely on confidentiality as the sensitivity of the data becomes an issue of concern.

2.2 Data integrity
It is very imperative that the data in transit should not be changed by the adversaries. Since sensor nodes lack expensive tampering resistant hardware, they can easily be compromised [8]. Data integrity is to ensure that information is not changed in transit in any case which may be due to malicious intent or accidently .The mechanism used for data integrity should ensure that no message could be altered by an entity as it traverses from the sender to the recipient.

2.3 Availability
Unavailability of sensor nodes may occur in case of hardware failure when the sensor runs out of battery power due to excess computation or communication. In other cases, it may happen that an attacker may jam communication to make sensor unavailable. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the network. This requirement ensures that the services of a WSN should be available always even in presence of an internal or external attacks such as a denial of service (DoS) attack.

Authentication

Authentication ensures that the communicating node is the one that it claims to be. Essentially, it ensures for a receiver to have a mechanism to verify that the received packets have indeed come from the actual sender node and is recognizable. Fabrication of data packets and injecting fabricated packets in a packet stream is an attack on the authentication. Authentication is necessary during exchange of control information in the network. To ensure authentication, a message authentication code (MAC) can be used that is computed over a shared secret key among the nodes.

3. SECURITY CLASSES

Attacks on the computer system or network can be broadly classified [9] as interruption, interception, modification and fabrication. The attack on the availability of the network is called as interruption. Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it. Modification is an attack on integrity. Modification means an unauthorized party not only accesses the data but tampers it. Fabrication is an attack on authentication. In fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed. In order to implement secure WSNs, the design must simultaneously address several difficult research challenges.

- The vulnerability of the network to eavesdropping, unauthorized access, spoofing, replay, and denial-of-service (DoS) attacks is mainly due to the wireless medium of the network.

- Since the sensor nodes are highly resource-constrained in terms of power, memory, CPU, communication bandwidth, there is a limitation on the degree of encryption, decryption, and authentication that can be implemented on individual sensor nodes, and call into question the suitability of traditional security mechanisms such as computation-intensive public-key cryptography for such resource-constrained sensor nodes [6].

- Physical security of WSN is an additional risk as the sensor node may fall into wrong hands. Sensor nodes that are physically deployed in the field can be captured by an intruder, and can then be subject to attacks from the potentially well-equipped intruder in order to compromise a single resource-poor node [3].

The challenges that WSN face are that the devices have severe resource constraints in terms of energy, computation and memory.

4. THREAT MODEL

Based on the characteristics and goals of the attacks and attackers, threat model of WSN can be presented by comparing them on the most important classes. Threat model of WSNs is presented by attributes such as the damage level caused, location, network functionality and attacker's strength [1]. In this section each of these is explained with respect to the function and effect of the attacks. Figure 1 shows the threat model that has been used in this paper to evaluate various attacks and effects of these attacks on the network.

4.1 Attack based on access level and damage caused to the network

The attackers can be classified as active attackers and passive attackers depending on the kind of threat and the effect on the WSN. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack, such as attacks against privacy [10][11]. Passive attacks have to do with eavesdropping on, or monitoring, transmissions. Such an attack results in disclosure of information to attackers. Whereas, in the active attack, the unauthorized attackers monitor, listens to and modifies the data stream in the communication channel. Active attacks are used to break protection features; this may result into dissemination or loss of data, denial of service or abruption of important services. Table 1 discusses the functions of active attackers and Table 2 discusses the functions of passive attackers along with their effects on the security in WSN [1].

Table 1. Function and effect of Active Attack

Function	Effect of Attack (Active Attack)
Overloading the WSN	Disruption in functionality
Impersonation	Obstructing the operations/ cutting off certain nodes from their neighbours
Packet modification	Data alteration
Unauthorized access, monitor, eavesdrop and modify resources and data stream	Overall network performance degradation
Creating hole in security protocols	Inability in use the WSN's services, sensor nodes destruction

Table2. Function and effect of Passive Attack

Function	Effect of Attack (Passive Attack)
Gathering information from the WSN	Compromised privacy and confidentiality requirements
Analysing and Monitoring traffic, eavesdropping communication channel	Breach in confidentiality by eavesdropping, gathering and stealing information. Creating network partition.
Energy Drain	Preserving of energy by selfish nodes, avoiding cooperation
Attack against privacy	privacy degradation, open to threats

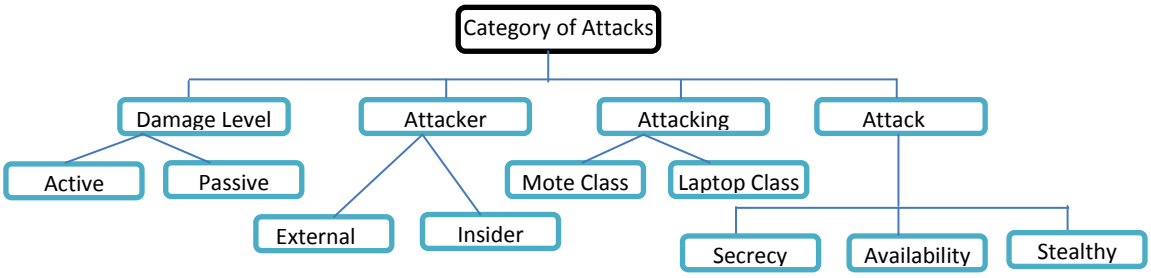

Figure 1.Threat Model

4.2 Attacks based on Attacker's Location

Based on the location of attackers, the network attacks in WSN can be categorized as outsider or insider i.e. external or internal respectively. It is based on whether the attacker is a legitimate node of the network or is not a part of the network. If the intruding node is not an authorized participant of the sensor network it can be used to launch passive attacks. In such cases, the attacker has no special access to the sensor network. Whereas an inside attacker or internal threat is an authorized participant in the sensor network which has gone hostile [4]. Insider attacks may be mounted from either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes, and who then use one or more laptop-class devices to attack the network. Threats that are external may cause passive eavesdropping on data transmissions. They may also extend to injecting bogus data into the network so that network resources are consumed and then raise Denial of Service (DoS) attack. To prevent such attacks the best methods are the authentication and encryption techniques that shall prevent such attackers from gaining any special access to the network. Table 3 defines the various functions and effects of external based (Outside) attacks. Table 4 defines the various functions and effects of internal based (Inside) attacks [13].

Table 3.Functions and effects of Attacks (Outside or External)

Functions	Effect of Attack (Outside or External)
Unauthenticated initiation of attack	Eavesdropping and stealing information
Overload/Jam communications	Consumption of WSN's resources
Traffic analysis and eavesdropping	Attack on confidentiality
Trigger DoS Attacks	Network functionality deprivation

Table 4.Functions and effects of Attacks (Inside or Internal)

Functions	Effects
Injecting irrelevant/ faulty data into WSN	Compromise on WSN codes/ secret keys
Impersonation (Behaving as other node)	Data modification
Unauthorized access to resources and hence modification of data	Blocking nodes from their adjoining nodes /neighbours
Overloading the network	Denial of Service in WSN
Performing malicious exploits or use of legitimate cryptographic content	High threat to the functional efficiency of the whole network

4.3 Attacks based on attacker's functional capabilities and resource access

Based on the resources like computation power, transmission range and power, and other such capabilities, the attackers can use different types of devices to attack the targeted network. Based on these parameters attackers can be classified in two categories [12] i.e. laptop-class and mote-class attackers. Laptop-class attackers may possess powerful hardware such as faster CPU, larger battery, and high-power radio transmitter. Using such specialized hardware allows more broad range of attacks which are difficult to control. Such attacks may be used to run some malicious code and seek to extract secret keys and information from the sensor network and hence disrupt its normal functions. On the other hand, mote-class attackers are constrained to the CPU, power, bandwidth, and range limitations of the used mote platform. In such cases, they have access to a few sensor nodes with similar capabilities, but not much more than this. They may try to jam a radio link, but only in the sensor node's immediate vicinity. However, these attacks are more limited since the attackers try to exploit the network's vulnerabilities using only the sensor's node capabilities. Table 5 briefs out the functions and effects of mote-class or laptop class attacker.

Table 5. Functions and effects based on attackers functional capabilities.

Function	Effect of Attack (Mote-class or Laptop Class)
Extract secret keys from the nodes	Breach Confidentiality Gain access to network
Node Capturing	Partial/Complete Disruption of functionality of WSN
Eavesdropping and Monitoring traffic	Compromise on confidentiality
Jam communications	Network's resource consumption
Trigger DoS Attacks	WSN functionality degradation

4.4 Attacks based on functionality

Based on the functionality and security requirements, the attacks in WSNs have been classified into three types namely Secrecy, Availability and Stealthy [1][12]:

- Attacks on secrecy and authentication: Attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets can be handled by using standard cryptographic techniques. They can protect the secrecy and authenticity of communication channels.

• Attacks on network availability: Attacks on availability are often referred to as denial-of-service (DoS) attacks and may target any layer of the sensor network.

• Stealthy attacks against service integrity: In a stealthy attack, the goal of the attacker is to attack the communication channel and make the network accept a false data value by injecting bogus data.

Table 6 details out the functions and effects of attacks based on operations.

Table 6. Attacks and effects of attacks based on functions

Function	Effect of attack
Secrecy Monitoring secretly communication channel, Replay Packets ,Snooping spoofing or modification , Injecting false data	Spoofing or modification Passive eavesdrop Packet replication
Availability Denial of Services (DoS)	Performance degradation, Destruction/disruption of network services, Network unavailability
Stealthy Eavesdropping & Bogus data injection in network	Partial/entire degradation/ disruption of services and functionality

5. ATTACKS AGAINST LAYERS OF WSN AND DEFENCE TECHNIQUES

In WSN, the nodes are vulnerable to security threats due to the unique characteristics of their underlying networking protocols and their limited resources. Attacks can occur in different layers such as physical, link (MAC), network, transportation, and application layer. The vulnerability increases as most of the routing protocols used in these layers are not designed having security threats in mind and hence leave open the chances of attacks. Hence the probability of attacks in such scenarios becomes very strong and the attacker doesn't need much effort to launch any attack. Though there is no such standard layered architecture of the communication protocol for wireless sensor network, here we have summarized possible attacks and their security solution approaches in different layers with respect to ISO OSI layer in Table-7 [4][12][13].

Table 7. Layered architecture, threats and possible security approaches in WSN

Threat	Layer	Defence Techniques
Jamming Tampering	Physical Layer	Spread-spectrum, lower duty cycle, Tamper-proofing, hiding Effective Key Management Schemes, region mapping, mode change
Exhaustion Collision Unfairness	Link Layer	Rate Limitation Error Correcting Code Small frames
HELLO Flood, Packet drop, bogus routing information and tunnelling, Spoofed, altered or replayed routing information Selective forwarding Sinkhole, Sybil, Wormholes Acknowledgment spoofing	Network	Two-way authentication, Three-way Hand-shake, Authentication, Monitoring, Flexible Routing, Monitoring Redundancy Authentication Egress filtering, Probing Authentication, packet leashes by using geographic and temporal information, verify the bidirectional link authentication
Flooding Energy drain attacks De-synchronization	Transport Layer	Limited Connection Numbers, Client Puzzles, Authentication
Cloning Denial-of-Service Attacks on reliability	Application Layer	Unique Pair-Wise Keys Cryptographic approach Client puzzles

6. EVALUATION OF THREATS AND ATTACKS

In this section, the attacks that exist in networking layers of WSN have been evaluated in context to the security class, attack threat and threat model. These parameters have been chosen keeping in mind the vulnerabilities that exists in various layers of the network. Table 8 briefly categorizes the attacks and threats of layered architecture of WSN and provides a quick glance with respect to the underlying threat model. The threat model has been evaluated under various parameters. The baseline for the threat model based comparison has been the work that has been considered in [1].

Brief descriptions of parameters used in threat model used for evaluation are as under:-

A. Security Classes – Interruption, Interception, Fabrication, Modification

B. Attack Threat- Availability, Authentication, Integrity and Confidentiality

C. Threat Model-4 levels of the threat model have been considered -(1)Attacks based on Damage/Access Level

(Active/Passive type),(2)Based on Attacker's Location(Internal or External), (3)Attacker's functional capabilities and resource access(Laptop class or mote class),(4) Attacks based on function (operation)- (Secrecy, availability, Stealthy)

Table 8. Evaluation of attacks based on threat model

Type of Attack	**Type of Security Class (A)**	**Type of Attack Threat (B)**	**Threat Model (C)**			
			1 (Active/Passive)	**2 (External/Internal)**	**3 (Laptop/MoteClass)**	**4 (Function)**
Jamming	Modification	Availability, Integrity	Active	External	Both	Availability
Collision	Modification	Availability, Integrity	Active	External	Both	Availability
Resource Exhaustion	Modification	Availability, Integrity	Active	External	Both	Availability
Unfairness	Modification	Availability, Integrity	Active	External	Both	Availability
Acknowledgement spoofing	Modification, Fabrication	Integrity, Authenticity	Active	Both	Both	Secrecy, Stealthy
Sinkhole	Modification Fabrication	Availability Integrity, Authenticity	Active	Both	Both	Availability, Secrecy, Stealthy
Eavesdropping	Interception	Confidentiality	Passive	External	Both	Stealthy, Secrecy
Impersonation	Fabrication, Modification Interception	Availability, Integrity, Authentication Confidentiality	Active	External	Both	Stealthy, Secrecy
DoS	Interception, Fabrication, Interruption, Modification	Availability, Authentication Integrity Confidentiality	Active	Both	Both	Availability, Stealthy, Secrecy
Wormhole	Interception , Fabrication	Confidentiality Authenticity	Active	Both	Both	Availability, Stealthy, Secrecy

7. CONCLUSION

Security is a vital requirement and intricate attribute in deploying and extending WSNs in different application domains. Various attacks on WSNs target most important network security dimensions such as integrity, confidentiality, authenticity and availability. In this paper, different dimensions of WSN's security have been analyzed. A wide variety of WSNs' attacks at various layers and their classification based on type of attack and security class have been discussed. Further, an approach to classify and compare the WSN's layer attacks have been evaluated on the parameters such as attacks' and attackers' properties and threat model. WSN's layered attacks, nature and goals have been analyzed in detail.

The key work in this paper includes:

• Outline of WSNs' key security requirements and classes.

•A precise classification and comprehensive comparison of WSNs' layered based attacks along with their defence techniques.

•Finally, the classification and comparison of various attacks based on the proposed threat model.

8. REFERENCES

[1] Mohammadi Shahriar, Hossein J. , "A Comparison Of Link Layer Attacks On Wireless Sensor Networks", International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC), Vol.3, No.1.March 2011

[2] Habib Asif, ,"Sensor Network security issues at network layer", Proceeding of 2nd International Conference on Advances in Space Technologies Islamabad, Pakistan, 29th – 30th November 2008

[3] Sen Jaydip, "Routing Security Issues in Wireless Sensor Networks: Attacks and Defences", Book Chapter, "Sustainable Wireless Sensor Networks",2010

[4] Mohanty Prabhudutta, Panigrahi Sangram, Sarma Nityananda and Siddhartha Satapathy Sankar, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", Journal Of Theoretical And Applied Information Technology, JATIT.14-27. © 2005 – 2010

[5] Bhavna Arora Makin and Prof. Devanand, "An Intra-Cluster Trust-Based Secure Data Aggregation Framework for Wireless Sensor Networks", International Journal for Next Generation Computing,Vol.2, No.1 March 2011, pp 325-338

[6] Carman, D.W. , Krus, P.S. & Matt, B.J., ," Constraints and approaches for distributed sensor network security". Technical Report No : 00-010, NAI Labs, Associates Inc., Glenwood, MD, USA. Network,2000.

[7] Perrig A. , Szewczyk R. , Tygar J. D. , V. Wen and Culler D. E. , "SPINS: security protocols for sensor networks ", Wireless Networks, vol. 8, no. 5, pp. 521-34. 2002.

[8] Bhavna Arora Makin and Prof. Devanand, "Trust Based Secure Data Aggregation Protocol in Wireless Sensor Networks", IUP Journal of Information Technology, Vol. VI, No. 3, pp. 7-22, September 2010.

[9] Stallings, W., "Cryptography and Network Security Principles and Practice", Cryptography Book, 2nd Edition, Prentice- Hall, 0-13-869017-0, 2000.

[10] Khelifa Benahmed, Hafid Haffaf and Madjid Merabti, "Monitoring of Wireless Sensor Networks", Book Chapter, "Sustainable Wireless Sensor Networks",2010.

[11] Karlof Chris and Wagner David ,"Secure routing in wireless sensor networks: attacks and countermeasures", Proceedings of the First IEEE International Workshop on In Sensor Network Protocols and Applications,2003.

[12] Wang Yong , Garhan Attebury, Byrav Ramamurthy,"A Survey of Security Issues In Wireless Sensor Networks", CSE, Journal Articles, paper 84, 2006.

[13] Giannetsos Athanasios, "Security Threats in Wireless Sensor Networks: Implementation of Attacks & Defense Mechanisms", Ph.D Dissertation Submitted to the Department of Electronic Systems and the Committee on Graduate Studies of Aalborg University in Wireless Communications, 2011.