World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:6, No:2, 2012

A Taxonomy of Internal Attacks in Wireless Sensor Network

Muhammad R Ahmed, Xu Huang, and Dharmendra Sharma

***Abstract*—**Developments in communication technologies especially in wireless have enabled the progress of low-cost and low-power wireless sensor networks (WSNs). The features of such WSN are holding minimal energy, weak computational capabilities, wireless communication and an open-medium nature where sensors are deployed. WSN is underpinned by application driven such as military applications, the health sector, etc. Due to the intrinsic nature of the network and application scenario, WSNs are vulnerable to many attacks externally and internally. In this paper we have focused on the types of internal attacks of WSNs based on OSI model and discussed some security requirements, characterizers and challenges of WSNs, by which to contribute to the WSN's security research.

***Keywords*—**Wireless sensor network, internal attacks, security, OSI model.

I. Introduction

WIRELESS sensor network (WSN) is underpinned by an application driven technology for information gathering and processing which consists of many resource-constrained sensor nodes. It can be used for many different applications range military implementations in the battlefield, environmental monitoring, in health sectors as well as emergency responses and various surveillances. Due to WSNs' natures such as low-cost, low power, open media, and multifunctional nodes that communicate at short distances through wireless links, etc. they have become one part of our daily life and drawn great attentions to those people who are working in this area. A typical WSN is shown in Figure 1.

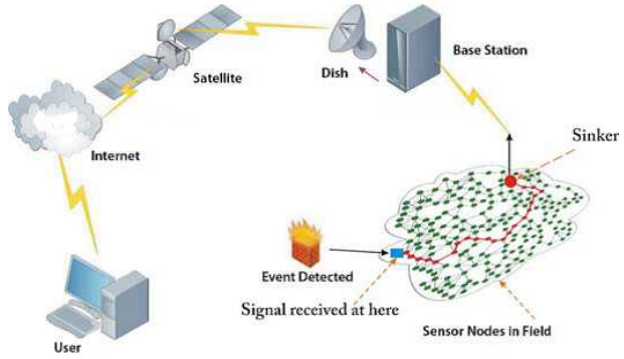

Fig. 1 A typical WSN [1]

Muhammad R Ahmed is with the Faculty of Information Science and Engineering, University of Canberra, Australia, (e-mail: muhammad.ahmed@canberra.edu.au)

Xu Huang is with Faculty of Information Science and Engineering, University of Canberra, Australia, (e-mail: xu.huang@canberra.edu.au)

Dharmendra Sharma is with Faculty of Information Science and Engineering, University of Canberra, Australia, (e-mail: dharmendra.sharma@canberra.edu.au)

In order to assure the functionality of a WSN, especially in malicious environments, security mechanisms become essential for all kinds of sensor networks. However, the resource constrains in the sensor nodes of a WSN and multihop communications in open wireless channel make the security of WSN even more heavy challenge. Since sensor nodes can (or have to) also be deployed in the hostile environment without any temper resistant protection. The nodes deployed in a network are relatively easy to be compromised, which is the case that the nodes are out of the system control and an adversary can easily get full access to those nodes. Hence, all the data could be modified and restored in those targeted nodes, including the cryptographic keys. Thus, developing new security mechanisms are necessary as the nodes under traditional security mechanisms based on conventional authentication become inefficient and an adversary is able to lunch attacks with a legitimate status of the network [2]. The node is called compromised node when an attacker gain a control of the node and appears as a legitimate node, after a network deployment done.

Though overall security is very important issue in any WSN, but very little work has been done to a secure WSN internally. In order to work on the internal security, researchers need to realize its features and different types of internal attacks. One of focuses of this paper is to give an overview different internal attack of a WSN based on the Open System Interconnect (OSI) model.

The following paper is organized as follows: section 2 is comprised of the overview of the generic security requirements for an WSN followed by vital security challenges in section 3. Section 4 covers the details of nature and the types of internal attacks followed by conclusion in section 5.

II. Generic Security Requirements In A WSN

The nature of a WSN leads a challenge to provide full security to the network. The ultimate security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. In order to provide the complete security in a WSN all message have to be encrypted and authenticated. An adversary can use natural impairments to modify the original message or information as well as can make the information unavailable because of WSN nature and uncontrolled environments. Security requirements in a WSN are similar to the wireless ad hoc network [3]. WSNs have the general security requirements of data confidentiality, authentication, integrity, freshness and secure management.

Confidentiality: an adversary can choose any node to eavesdrop as long as it is within the radio range as the signals are transmitted over the wireless channel. So, it is a threat for the data confidentiality as the attacker can gain the cryptographic information.

Authentication: to determine the legitimate node and whether the received data has come from the authorized node or not authentication is important.

Integrity: information moving through the network could be altered. So integrity is important to trust the received information from the network.

Freshness: to save the network from the replay packets it is important to ensure that the received data is fresh and unused.

Secure management: it is important to manage the distribution of cryptographic keying material in the network.

III. Vital Challenges For WSN Security

A WSN has three major properties that made the security mechanism challenging.

a. Resource Constraints

b. Operational Environment, and

c. Wireless Multihop Communication.

It is commonly assumed that sensor nodes are highly resource constrained; e.g., the resources are comparable to the Berkeley MICA2 motes and TMote mini is presented in the Table I Thus, security protocols for WSNs must be executable on the available hardware and especially must be very efficient in terms of energy consumption and execution time.

TABLE I
Existing Sensor Platform [4], [5]

Characteristics	Mica2	TMote mini
RAM (Kbytes)	4	10
Program Flesh Memory (Kbytes)	128	48
Maximum data rate (Kbps)	76.8	250
Power Draw: Receive (mW)	36.81	57
Power Draw: Transmit (mW)	87.90	57
Power Draw: sleep (mW)	0.048	0.003

The operational environment of most WSNs is assumed to be unattended or even hostile. Since sensor nodes are usually not assumed to be physically protected by some tamper-resistant hardware, an adversary is able to compromise sensor nodes. Thus, even if security mechanisms, such as node-based authentication, are deployed, an adversary is able to participate in the network since he has access to all data [6], e.g., cryptographic keys stored on the node. Thus, security protocols must be able to operate even if sensor nodes are compromised.

The wireless communication enables an adversary to eavesdrop, inject, drop, or alter messages or to perform denial of service (DoS) attacks by jamming the wireless channel. In contrast to most other wireless networks, the communication is performed in a multihop way. This introduces additional challenges. Compromised nodes may be part of a route, enabling them to modify forwarded messages, or a compromised node injects a large amount of false messages to drain the energy resources of all forwarding nodes.

IV. Natures And Types Of Internal Attacks

Wireless network transmission medium has broadcast nature because of this characteristic of the network; it is more susceptible to the security attack compare to the traditional wired network. In wireless sensor network nodes can be deployed randomly in the hostile environment an adversary can easily to make an attack to the targeted wireless sensor network (WSN) [7]. Regarding to the security of a WSN, it can be investigated in different perspectives, for example WSN attacks can be classified as two major categories: passive and active attack, or an attack can be identified as external and internal attack according to the domain of attacks [8]. Sometimes both reviews are applied, such as “internal active attack,” “internal passive attack,” etc. will be used to highlight the type of an attack. In this research paper, we focused on the internal attacks of WSN. In order to clarify all those mentioned terminologies the definitions are as follows [7], [8]:

Passive attack: The attack does not have any direct effect on the network as it is outside of the network. Passive attacks are in the nature of eavesdropping on, or monitoring of packets exchanged within a WSN.

Active Attack: the attacker transmits data to one or both of the nodes, or chunk the data stream in one or both directions in the communication channel. Active attackers can disrupt the normal functionality of the whole network, which means it may change the information, may modify the original data, or can gather falsehood data. Its behavior likes a legitimate node in the network.

External attack: The attack is defined as the attack does not belong to the network and it does not have any internal information about the network such as cryptographic information. In other word it can be defined as physical attack.

Internal attack: When a legitimate node of the network act abnormally or illicit way it is consider as an internal attack. It uses the compromised node to attack the network which can destroy or disrupt the network easily.

The compromised node holds the following characteristics [9]:

- It usually runs some malicious code that is different from the code running on a legitimate node and seeks to steal information from the sensor network or disrupt its normal function.
- Node uses the same radio frequency as the other normal sensor nodes so that it can communicate with them.

• Node is authenticated and participates in the sensor network. Since secure communication in sensor networks is encrypted and authenticated using cryptographic keys, compromised nodes with the secret keys of a legitimate node can participate in the secret and authenticated communication of the network.

It is obviously that the compromised nodes are more dangerous as the adversary can easily obtain the access information from the cryptographic information and then to make further attacks with the trust of other sensors. This type of attack is difficult to break or stop. That is why it has become a challenging task to secure WSN from internal attack.In many applications, the data obtained by the sensing nodes needs to be kept confidential and it has to be authentic. In the absence of security a false or malicious node could intercept private information, or could send false messages to nodes in the network. The major attacks are: Denial of Service (DOS), Worm hole attack, Sinkhole attack, Sybil attack, Selective Forwarding attack, Spoofed and Altered, or Replayed routing information, Hello flood attack, flooding attack. Based on the Opes System Interconnect (OSI) model the attack can be tabulated in table II [10]:

TABLE II
LAYER BASED SECURITY ATTACKS [11]

Layer	Attacks
Physical layer	Jamming, Tampering, Sybil Attack
Data Link Layer	Collision, Sybil Attack, Spoofing and Altering Routing Attack, Replay attack
Network Layer	Internet smart attack, Sybil Attack, Blackhole Attack, Spoofing and Altering Routing Attack, wormhole attack, selective forwarding attack, Hello Flood Attack.
Transport Layer	Flooding Attack, Desynchronisation
Application	Spoofing and Altering Routing Attack, False Data Injection,

A. Denial of Service (DoS) attacks

Denial of service attack is an explicit attempt to prevent the legitimate user of a service or data. The common method of attack involves overloading the target system with requests, such that it cannot respond to legitimate traffic. As a result, it makes the system or service unavailable for the user. The basic types of attack are: Jamming, Tapering, collision, Homing, flooding, etc. If the sensor network encounters DoS attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network. Projected use of sensor networks in sensitive and critical applications makes the prospect of DoS attacks even more alarming. In WSN several types of Dos Can be performed in different layers which tabulated in the table 3 [10]

TABLE III
LAYER BASED DOS ATTACK [12]

Layer	Attacks
Physical layer	Jamming, Tampering
Data Link Layer	Collision, Exhaustion
Network Layer	Misdirection
Transport Layer	Desynchronisation
Application Layer	Path Based DoS

The discussed attacks are linking some terminologies that are defined as follows [11], [12]:

Jamming: Jamming is a popular Denial of Service (DOS) attack. In this attack the attacker attempts to jam the frequencies of the radio used for communication between the nodes in the network. In this attack, an adversary may use e few nodes in strategic positions to effectively jam most of the communications inside the network. In essence, an attacker needs only a few nodes in order to disseminate a large network.

Tampering: Because of the nature of wireless sensor networks, an adversary could easily get physical access to the sensor nodes. This may enable an attacker to compromise sensor nodes in a DOS like manner

Collision: This is a DOS attack, where a node induces a collision in some small part of a transmitted packet. The packet will then fail the checksum check, because of the changes brought on by the collision, and the receiver node will then ask for a retransmission of the packet.

Exhaustion: This attack is a collision attack taken a bit further. A malicious node may conduct a collision attack repeatedly in order to exhaust the power supply of the communicating nodes.

Misdirection: In this attack a malicious node, that is part of a route, can instead of dropping packets, quite simply send them on a different path where there does not exist a route to the destination. The malicious node can do this for certain packets, or all packets.

Desynchronisation: it can disrupt an existing connection between two end points. Adversary transmits forget packet with bogus sequence number or control flag to degrade or prevent the exchange of data.

Path based DoS: An adversary overwhelms sensor nodes by flooding a multihope end to end communication path with either replayed or injected false message to injected false message to waste secure energy resources.

B. Wormhole attack

Just like the theoretical wormholes in space, this attacker can send packets, routing information, ACK etc, through a link outside the network to another node somewhere else in the same network. This way an attacker can fool nodes into thinking they are neighbours, when they are actually in different parts of the network. This can also confuse routing

mechanisms that rely on knowing distances between nodes. A wormhole attack can be used as a base for eaves dropping, not forwarding packets in a DOS like manner, alter information in packets before forwarding them etc.

C. Sinkhole attack

This is a DOS attack, where a malicious node advertises a zero cost route through itself. If the routing protocol in the network is a "low cost route first "protocol, like distance vector, other nodes will chose this node as an intermediate node in routing paths. The neighbours of this node will also chose this node in routes, and compete for the bandwidth. This way the malicious node creates a black hole inside the network.

D. Sybil attack

The Sybil attack targets fault tolerant schemes such as distributed storage, dispersity, multipath routing and topology maintenance. This is done by having a malicious node present multiple identities to the network. This attack is especially confusing to geographic routing protocols as the adversary appears to be in multiple locations at once

E. Selective forwarding attack

In this attack, malicious nodes can decide not to forward packets of certain types or to from certain nodes. Even though the protocol is completely resistant to the sinkholes, wormholes, and the Sybil attack, a compromised node has a significant probability of including itself on a data flow to launch this type of attack if it is strategically located near the source or a base station.

F. Spoofing attack

In this attack, a malicious node may be able to create routing loops, wormholes, black holes, partition the network and etc., by spoofing, altering or replaying routing information.

G. Hello flood attack

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbours. A node receiving such a packet may assume that it is within the radio range of the sender but this assumption may be false.

H. Flooding attack

In this attack, a malicious node may send continuous connection requests to a victim node effectively flooding the victim's network link

All of the above mentioned attacks has the common purpose that is to compromise the integrity or workability of the network that they attack. In order to make the network function the network need to saved internally and externally. This work will give a understanding the internal attacks of WSN to the researchers.

V. Conclusion

Provisioning internal security is a significant task in WSN. In this paper we have presented a foundation of OSI layer based internal attacks of WSN. This will lead the researchers to develop the resilient security mechanism by considering internal attacks induced in WSN.

References

[1] X, Huang, M, Ahmed, D, Sharma, "The node became compromised when an attacker gain control of the node that acts as a legitimate node, after network deployment", 2011 Ninth IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. October 2011 Melbourne, Australia

[2] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," IEEE Communications Surveys & Tutorials, 3rd Quarter 2008.

[3] K. Lu et al., "A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks", IEEE Transactions on Wireless Communications, vol. 7, no. 2, Feb. 2008, pp. 639-647.

[4] https://www.eol.ucar.edu/rtf/facilities/isa/internal/CrossBow/DataSheets/mica2.pdf, [accessed on November 24, 2011]

[5] http://sentilla.com/files/pdf/eol/Tmote_Mini_Datasheet.pdf, [accessed on November 24, 2011].

[6] O. E. Ochirkhand, M. Marine, V. Fabrice and K. Apostotlos, "Resiliency of Wireless Sensor Networks: Definitions and Analyses", 17th international conference on Telecommunications 2010.

[7] S. K. Singh, M. P. Singh, and D. K. Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", International Journal of Computer Trends and Technology- May to June Issue 2011

[8] T. G. Lupu "Main Types of Attacks in Wireless Sensor Networks" International Conference in Recent Advances in Signals and Systems 2009, ISSN: 1790-5109, ISBN: 978-960-474- 114-4.

[9] M.Y. Hsieh, Y. M. Huang, "Adaptive Security Modules in Increment-ally Deployed Sensor Networks", International Journal on Smart Sensing and Intelligent Systems, vol. 1, no. 1, March 2008

[10] K. Sharma, M. K. Gosh, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on Mobile Ad-hoc Networks MANETs, 2010.

[11] H. K. D. Sharma, A. Kar, "Security Threats in Wireless Sensor Networks", Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International.

[12] H. Ghamgin, M. S. Akhger, M. T. Jafari, Z. Branch, "Attackes in wireless sensor networks", Australian journal of Basic and applied Sciences, 2011.