International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 5,May 2015

A survey on Wireless Sensor Network Attacks And Defenses

[1] Pramod Nath,[2] Pragya Rajput
[1] Department of Computer Science and Engineering, Jaypee Institute of Information Technology (JIIT),Student, Noida,U.P, India [2] Department of Computer Science and Engineering, SRM University,Student, NCR Campus, India
[1] er.pramodnath@gmail.com,[2] rajputpragya91@gmail.com

Abstract- **Wireless Sensor Networks (WSN) are combination of several thousand sensor nodes that have several capabilities such as to detect, to sense, to monitor, to process and to compute. WSN have many applications in real time scenarios such as in military, industries, health care and so on. WSN has infrastructure less structure, so the ability to cope with the node failure, fault tolerance and its security attack are the main concern. The sensor nodes are more vulnerable to security threats and attacks because of the harsh and hostile environment. Efficient implementation of different security protocols has huge impact to adverse the potential threat. The main aim of this paper is to present security issues and challenges faced by WSN. This paper explains attacks in WSN, its flaws and their countermeasures that can be used to handle the pitfall.**

Key Terms: **Wireless Sensor Networks (WSN); Denial of service (DOS); Attack; securitymechanism.**

INTRODUCTION

Wireless Sensor Network (WSN) consists of large number of low-cost, low-power, self-configured, resource constraint sensor nodes that are equipped with specialized sensors and wireless transceiver. These sensing nodes are scattered over the region and designed to do the specific task. The task includes capturing and gathering the data from the surrounding and forwarding the same to the reporting sites or control sites where the data can be observed and analyzed. The other task includes responding to the queries sent from the reporting sites or control sites to do the specific task without any glitches and provides sensing samples for further verification. Sometimes WSN are also called as Wireless Sensor and Actuator Networks (WSAN) as these sensor nodes are sometimes equipped with actuators to "act" upon specific condition.

With the recent development in micro-electro-mechanical system (MEMS), it became possible for us to manufacture large number of small sensing devices. These sensing devices have different components such as data analysis ormonitoring the communication. The structure or architecture of WSN device contains a processor, memory, transceiver, power source, and some interfaces for external sensors.

However, security of data at sensor node is the main concern. In this paper, various WSN attacks are discussed in detail including Denial of service (DOS) attack. Also discussed various defense mechanisms to counterattack the same. Possible solutions for each layer-wise attacks are also mentioned. This paper is organized into different sections as follows: Section II describes Goals, Application domain, and challenges faced by WSNs, Section III gives Literature Review, Section IV explains different Attacks and methods to countermeasures the same, Section V shows Result and Analysis for the same and finally Conclusion with Future Work has been presented

BACKGROUND

Security Goals for WSNs

Security is the important issue for transmission of any data. the security goals in wsn are as follows:
Integrity means data received at the end is not altered by the attacker.
Confidentiality means to keep the data confidential over transmit link from eavesdroppers.
availability means that the given service is available with the sensor node in given time.
Authentication means while communicating over the network, identity of communicating peer should be authenticated for security of data.
Self-Organization means the sensor nodes should be able to manage it for different conditions as required such as fault tolerance and node failure.
Non-repudiation means a sensor node cannot deny sending of sensing data or message to a node it has previously sent.
data freshness means the data or message is recent and it is not an old one.
Authorization means only the authorized nodes are able to use the desired services or resources on demand as required.

Application Domain

WSNs have been successfully applied in the following application domain:

1. Agriculture: WSNs have been used to control irrigation system according to the humidity of the terrain.
2. Military: Intrusion detection system based on WSNs has been used by the military.
3. Manufacturing: WSNs have been used to monitor the presence of lethal gases in refineries.
4. Transportation: Real-time traffic information is being collected by WSNs to later feed transportation models and alert drivers of congestion and traffic problems.
5. Environmental: WSNs have been installed to monitor water deposits in mountain to detect mudslides. WSNs have been utilized in intelligent building to automatically control the temperature.
6. Engineering: Civil engineers have used WSNs technology to monitor the condition of bridges.

Challenges faced by WSNs

1. Security: This is one of the important challenges faced by WSN. Due to hostile or unexpected environment, potential threat may occur over time. Therefore new security mechanisms or algorithms with low computational complexity and low energy requirement are needed.
2. Network lifetime: WSNs are battery powered; therefore the network lifetime depends on energy usage. It is considered good to have network lifetime in order of one or more years. In order to achieve such long network lifetime it is imperative to operate the sensors in a very low duty cycle.
3. Scalability: Some application requires hundreds or thousands of wireless sensor devices. Algorithms or protocols that work fine in small-scale network don't work necessarily well in large-scale networks.
4. Interconnectivity: WSNs need to be interconnected so that data reaches to its receiver and perform appropriate operations or actions. Today we have new protocols and mechanisms need to be designed to achieve interconnectivity and allows the transfer of data to and from WSNs.
5. Reliability: Wireless sensor devices are cheap devices with high failure rates. This can also be affected by available energy of sensor nodes or devices.
6. Heterogeneity: New WSNs are embedding wireless sensor devices with different capabilities and functionalities that require new algorithms and communication protocols. Thus the need for clustering and data aggregation algorithms is important challenge faced by WSNs.

LITERATURE REVIEW

Considering the security aspects, many authors have done survey regarding different issues to present the threat models in different perspectives.

Ritu Sharma et al[1], discussed different constraint in WSN, and security requirement in WSN. According to Author, attacks in WSN are classified into two types: invasive or non-invasive. A Non-invasive attack is based on frequency, time or power depending on its constraint. But invasive attacks are DoS attack or Node replication attacks or Routing attacks. Author has also explained different security protocols such as SPINS, SNEP, TINYSEC, MINISEC, LEAP and ZIGBEE. Finally Author has done comparison of these protocols considering different aspects.

Kalpana Sharma et al.[2], presented different application of WSNs. According to Author, attacks on WSN can be classified against security mechanism or routing mechanism. Author also explained possible DoS attacks and threats in different layer of WSN giving suitable defense mechanism.

G. Padmavathi et al. [3], discussed terminology used in security goals in WSN, challenges of WSN and also presented a flow chart depicting general classification of attacks and in-detail classification of attacks and an attempt is made to explain the same. Author also describes security mechanism as low level or high level to handle the attacks.

Al-Sakib et al. [4], has explained network security fundamentals such as cryptography, steganographic concepts. Different attacks in WSN are also explained and presented summary on various security schemes for WSN. According to Author, holistic security in WSN is the one of the great challenge.

David Martins et al. [5], came up with the architecture of WSN defining its topology etc, he then listed out the most current attack that are possible in WSN e.g. eavesdropping and many more. According to Author, there exists different security mechanism for WSN that can be used in different situation.

Fasee Ullah et al. [6], discussed literature review of different security protocols pointing strength and weakness of each protocol. He then compared those techniques stating problem identification, proposed solutions and limitations.

Manish M Patel et al. [7], presented security goals and challenges in WSN. Also author has explained about different attacks in wireless sensor networks. Finally Author has pointed research issue in future for detecting multiple wormhole attack and use of Intrusion Detection System.

K.H. Wandra et al. [8], describe WSN issues and challenges and different properties for WSN implementation. In this paper, Author has done survey and analyzed the outcome of different techniques to handle the challenges.

Saurabh Singh et al. [9], starts with the architecture of sensor network depicting different component. He then describes application and security goals in WSN. Description of Protocol stack is done and different attacks with their defense mechanism are also stated.

Manju V.C [10], gives layer Protocol architecture of WSN. The author also explains the necessary security requirement. According to Author, the attacks in WSN can be classified as based on domain of attack or the different techniques used. The Author also presents Link Layer Encryption techniques and various protocols in WSN. Different cryptographic modes have been explained as well.
Anser Ali et al. [11], discussed the typical architecture of wireless sensor network. In this paper, issues related to security, countermeasures and its challenges have been identified and future direction to some research issues has been pointed out.

Abhishek Pandey et al. [12], discussed comparative study of different motes such as Mica, µNode, Sun Spot. Author also described layered structure of WSN and also WSN layer attacks, its classification and existing protocols used. Author also described most commonly used simulator used in WSN such as TinyOS, NS2, OMNet++, GloMoSim and compared them as well.

Madhumita Panda [13], discussed operation and layered protocol stack of WSN. According to Author, the attack in WSN are classified into interception (attack on confidentiality), modification (attack on integrity) and fabrication (attack on authentication). The author also described different layer-wise attacks and cryptography can be used in WSN in order to provide security of data. Finally Author discussed different security schemes for WSN proposed till now.

IV ATTACKS IN WSN

The major attacks in wireless sensor network are as follows:

1. Denial Of Service (Dos) attack: in this type of attack, the resources available to victim nodes are made exhausted by sending continuous unnecessary messages. the intent of the attacker is to disrupt the normal functioning of sensor node. this type of attack can be at different layer, for example, at physical layer it could be jamming or tampering, at link layer it could be collision, exhaustion, or unfairness, at network layer it could be spoofing, homing, black holes, or neglect and greed, at transport layer it could be flooding or de-synchronization.
2. Wormhole Attack: in this type of attack, the attacker node uses tunneling mechanism to interfere between two communicating sensor nodes. this attack does not require establishing a complete network rather it can have its adverse impact even at initial phase of network.
3. Sybil Attack: in this type of attack, the malicious node pretend to be set of nodes and start sending incorrect information such as position of nodes, number of nodes and their strength, to all other nodes in the network. for outsider, authentication and encryption techniques are used, but for insider, public key cryptography mechanism is used.
4. Selective Forwarding Attack: in this type of attack, the attacker node misguide the intermediate nodes regarding the path to forward to base station and it starts dropping those messages and create a black hole in the network hence no message is forwarded.
5. Sinkhole Attack: in this type of attack, the goal of attacker node is to attract nearby all traffic from particular area through compromised node. thus all the information is being routed through malicious node and the attacker can do anything with those messages.
6. Hello Flood Attack: In this type of attack, the attacker node send hello packet with very high transmission power to sender or receiver in the network. the sender or receiver thinks that the node is very near to them and starts communicating with the malicious node, thus leading to congestion in the network.
7. Flooding Attack: In this type of attack, the attacker nodes send useless messages in the network making the link highly congested, thus destroying the bandwidth and energy of the node.
8. Node Replication Attack: In this type of attack, the attacker node insert a node in the network which is cloned to some existing node, thus performing the same function as the old one. this cloned node has some extra features that it sends the information back to the attacker.

9. Attacks On Information On Transit: in this of attack, while a sensor node communicate with the sink node for any updates, the attacker nodes in-between can cause serious damage by altering, eavesdropping the information being sent. the malicious node indirectly monitor the traffic flow and can modify the packet or message while transmission.
10. Malicious Node: in this type of attack, the attacker node send false information within the network, thus disrupting the normal flow.

11. METHODS TO COUNTERMEASURES THE ATTACKS

THREATS	COUNTERMEASURES
DOS	Protect Network ID and other network specific data. Inspect and protect the network physically.
SYBIL	Reset the devices and change the session keys.
Selective forwarding Wormhole	Regularly monitor the network by Source Routing. Regularly monitor the network physically and by Source Routing. Using the Packet Leach technique for monitoring.
Hello Flood	Bi-Directional Verification Of Link
Sink Hole	GEO-GRAPHIC ROUTING PROTOCOLS
Traffic Analysis	Regularly monitor WSN and send dummy packets when network is quite.
Eavesdropping	Protecting NPDU from Eavesdropper through Session keys.

12. TABLE1. WSN THREATS AND THEIR COUNTERMEASURES

link	1. collision	ecc (error correcting codes)
	2. exhaustion	rate limitation
	3. unfairness	small frames
network or routing	1. spoofing	monitoring, or authentication
	2. homing	encryption
	3. black holes	monitoring, or authentication
	4. neglect and greed	probing, or redundancy
transport	1. flooding	client puzzles
	2. desynchronization	authentication

TABLE2. WSN LAYER-WISE ATTACKS AND THEIR DEFENSE MECHANISMS.

RESULT AND ANALYSIS

All the above mentioned attacks can be classified as active attacks or passive attacks because it directly or indirectly disrupt the normal functioning of sensor nodes in the network.

When wormhole attack come up with sybil attack and selective forwarding, then it becomes very much difficult to detect them, and can cause serious damage to sensor nodes and the base station in the network.

CONCLUSION AND FUTURE WORK

Wsn security is one of the most challenging issues that capture the interest of many research authors in this present scenario. in this paper, we have made attempt to explain the security threats and also different defense mechanism to handle those attacks. possible solutions to countermeasure the attack at different layer of wsn are also outlined. but even though due to unexpected and hostile environment, the need for security of sensor nodes are raising at an alarming rate and demands more improvement in the defense mechanisms. in this paper, existing work done on security from different authors are also reviewed.

Rapid growth in the software and hardware implementations may eliminate the resource constraint such as low memory, low processing speed, and battery life thus upgrading the existing security mechanisms.

ACKNOWLEDGEMENT

we would like to thanks many anonymous reviewers for their valuable suggestions and comments that help us to improve the readability of this paper.

REFERENCES

[1]. sharma, ritu, yogesh chaba, and yudhvir singh. "analysis of security protocols in wireless sensor

network." *international journal of advanced networking and applications* 2.3 (2010): 707-713.

[2]. sharma, kalpana, and m. k. ghose. "wireless sensor networks: an overview on its security threats." *ijca, special issue on "mobile ad-hoc networks" manets* (2010): 42-45.

[3]. padmavathi, dr g., and mrs shanmugapriya. "a survey of attacks, security mechanisms and challenges in wireless sensor networks." *arxiv preprint arxiv:0909.0576* (2009).

[4]. pathan, a. s. k., hyung-woo lee, and choong seon hong. "security in wireless sensor networks: issues and challenges." *advanced communication technology, 2006. icact 2006. the 8th international conference*. vol. 2. ieee, 2006.

[5]. martins, david, and hervé guyennet. "wireless sensor network attacks and security mechanisms: a short survey." *network-based information systems (nbis), 2010 13th international conference on*. ieee, 2010.

[6]. ullah, fasee, et al. "analysis of security protocols for wireless sensor networks." *computer research and development (iccrd), 2011 3rd international conference on*. vol. 2. ieee, 2011.

[7]. patel, manish m., and akshai aggarwal. "security attacks in wireless sensor networks: a survey." *intelligent systems and signal processing (issp), 2013 international conference on*. ieee, 2013.

[8]. wandra, k. h., and sharnil pandya. "a survey on various issues in wireless sensor networks."*international journal of scientific & engineering research* volume 3, issue 12, december-2012

[9]. singh, saurabh, and harsh kumar verma. "security for wireless sensor network." *international journal on computer science and engineering* 3.6 (2011): 2393-2399.

[10]. manju, v. c. "a survey on wireless sensor network attacks." *international journal of engineering and innovative technology (ijeit)* volume 2, issue 2, august 2012.

[11]. anser ali, aasim z., syed h."security issues in wireless sensor networks" *magnt research report* vol.2(4):pp.82-91.

[12]. pandey, abhishek, and r. c. tripathi. "a survey on wireless sensor networks security." *international journal of computer applications* 3.2 (2010): 43-49.

[13]. panda, madhumita. "security threats at each layer of wireless sensor networks". *international journal of advanced research in computer science and software engineering* volume 3, issue 11, november 2013

[14]. perrig, adrian, john stankovic, and david wagner."security in wireless sensor networks." *communications of the acm* 47.6 (2004): 53-57.

[15]. akyildiz, ian f., et al. "wireless sensor networks: a survey." *computer networks* 38.4 (2002): 393-422.

[16]. wang, yong, garhan attebury, and byrav ramamurthy. "a survey of security issues in wireless sensor networks." (2006).

[17]. bojkovic, zoran s., bojan m. bakmaz, and miodrag r. bakmaz. "security issues in wireless sensor networks." *international journal of communications*2.1 (2008): 106-115.

[18]. sen, jaydip. "a survey on wireless sensor network security." *arxiv preprint arxiv:1011.1529* (2010).

[19]. akyildiz, ian f., et al. "wireless sensor networks: a survey." *computer networks* 38.4 (2002): 393-422.

[20]. sharifnejad, mona, et al. "a survey on wireless sensor networks security." *4th international conference: sciences of electronic, technologies of information and telecommunications (seit), tunisia, march 2007*. 2007.

[21]. wang, yong, garhan attebury, and byrav ramamurthy. "a survey of security issues in wireless sensor networks." (2006).

[22]. pathan, a. s. k., hyung-woo lee, and choong seon hong. "security in wireless sensor networks: issues and challenges." *advanced communication technology, 2006. icact 2006. the 8th international conference*. vol. 2. ieee, 2006.

● ● ●