 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

Applications and Damage Penetration of WSN: A Review

[1]Rina Sharma, [2]Dr. Himani
[1]Research Scholar, Punjab Technical University, Kapurthala, Punjab, India
[2]Professor, Dean, ECE, Marrilaxman Reddy Institute of Tech., Quthbullapur Mandal, Hyderabad, India

Abstract
All future application and Internet of Things will have high dependency on Wireless Sensor Network (WSN) it is an emerging technology showing a great promise to mass public, military and other relevant sectors like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios.In every aspects of life security is essential. In this paper we focus on the utilization of WSN technology in one part and in another part we focus on the review of some security considerations which shows the damage penetration on different kind of attacks. It is still very early in the lifetime of WSN because many different challenges exist.

Keyworks
Wireless Sensor Network, Continuous Monitoring, Provide Security, Attacks, Security Mechanism etc.

I. Introduction

One of the major challenges wireless sensor networks face today is security. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. Wireless sensor networks are characterized by severely constrained computational and energy resources, and an ad hoc operational environment.Wireless sensor networks (WSN) are currently receiving significant attention due to their unlimited potential. However, it is still very early in the lifetime of such systems and many research challenges exist.
Wireless Sensor Network (WSN) is an emerging technology which can be implemented in so many different areas for the betterment of society like medical application, civil health Monitoring, human health monitoring, use of multiagents system in WSN, University Campus security, designing testing method like simulator for simulation. In other words we can say WSN is basically used for the continuous monitoring and provide security.
The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. Wireless sensor networks are characterized by severely constrained computational and energy resources, and an ad hoc operational environment. Wireless sensor networks (WSN) are currently receiving significant attention due to their unlimited potential..
WSNs are composed of individual embedded systems that are capable of interacting with their environment through various sensors, processing information and communicating this information with neighbors. A Sensor node consists of three main components i.e. wireless modules or motes, sensor board and programming board.

Various Application Areas

- Military Applications
- Smart Dust
- Sniper Detection System
- Vigil net
- Environmental
- Great Duck Island
- CORIE
- Zebra Net
- Volcano Monitoring
- Flood Detection
- Health
- Artificial retina
- Patient Monitoring
- Emergency Response
- Home
- Water monitoring
- Security
- Industry
- Preventive Maintenance
- Structural Health Monitoring

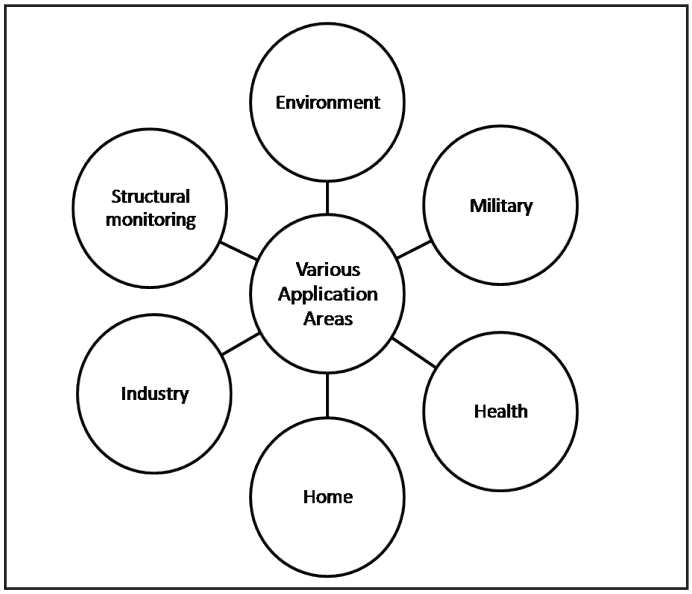

Fig. 1: Various Applications Area

II. Review Work

So many different researchers explore the different aspects of WSN to elaborates the concept which are as follows:- John Herbert, John O'Donoghue, Gao Ling, Kai Fei [1] describe that DMS deals with large volume of static date as well as dynamic data & its architecture is built mainly on JADE. The patient sensor node is combined of three layers: power; communicating and processing; and the sensor interface. The agilla middle ware executes on Tiny OS, initially developed for the Mica Mote.DMS Architecture consists of data collection, data integration, data analysis & data presentation. They have given various examples of the JADE-Agilla integration and also evaluated the results of two experiments.
B. F. Spencer Jr, Manuel E. Ruiz-Sandoval and NaritoKurata [2] explain the structured health Monitoring and control systems represent one of the primary applications for new sensor technologies. These concerns apply not only to civil engineering structures, such as bridges, highways and buildings, but also to other types of structures, like aging fleet of aircraft. It can provide advanced warning to allow for repair or removal of the structure before human lives are endangered. It is being used to enhance safety and reliability and to reduce maintenance and inspection

costs.
In the smart sensor computation to be done locally on sensor's embedded microprocessor. The size and cost of smart sensors has been decreasing with time. MEMS devices are manufactured using very large scale integration technology. Several protocols for transmitting data, one of the most popular are Bluetooth. However they explain the different smart sensors e.g. prototype smart sensor, Mica2 and mica2dot also explain their architecture & characteristics. Discuss some of the constraints for smart sensing application from both hardware as well as software perspective.

Chris Otto, AleksandarMilenković, Corey Sanders, Emil Jovanov [3] focus on prevention and early detection of disease or optimal maintenance. It helps to cope with the imminent crisis in the health care system. A WBAN consists of multiple sensor nodes each capable of sampling, processing and communicating one or more vital signs like heart rate, blood pressure, oxygen saturation, activity or environmental parameters e.g. Location, temperature, humidity and light etc. In this paper they describe a general WBAN architecture with the details of hardware and software architecture and introduces the energy effected WBAN communication protocol.
The medical server keeps electronic medical records of the registered users and provides various services to the user. A server may process the uploaded data and signal an alert in the case of potential medical problem. However, WBAN designers face a number of challenges to improve user's compliance that depends on the ease of use, size, reliability and security etc.

Alcides Montoya, Diana Carolina Restrepo and Demetrio Arturo Ovalle [4] throw the light on the implementation of Artificial Intelligence for Wireless Sensor networks in the first method which is based upon the global objective and design and second method the designer conceives & construct a set of self-interested agents. Some of the commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination, vibration and sound intensity, pollutant levels and vital body functions etc.

Berkeley Motes was the first commercial motes platform. Some others are Mica Mote, Tmote sky, BTnode, Waspmote, Sunspot & G-node etc. The modern approach of AI which gives the concept of rational agent which tries to optimize the performance measure. Agents are rarely individual, mostly they coexist and interact with other agents. Various functions of intelligent sensor are self calibration, self validation and compensation. Main research issues of the WSNs are focused on the coverage, connectivity and data fidelity.

However, it is important to note that most simulators are used to simulate a specific system like MAS or a WSN but not both of them. In this paper they proposed the multi agent model by a layered architecture which has three layers hardware layer, middle layer & application layer. Explain the different components of the layers and its working method. Moreover proposed model emphasizes about how a WSN works and how to make it intelligent.
AbdelhakimHamzi, MouloudKoudil, Jean-Paul Jamont, Michel Occello[5] explore the characteristics of WSN its background, requirements. They also elaborate the various design issue during the establishment of (WSN) Wireless Sensor Network i.e. node classification& agent types etc. Finally they proposed architecture of such network which is composed of functional modules. At last describe the application area e.g. Battlefield Surveillance.
A. Filippou, D. A. Karras [6] explain the concept of simulator architecture design through energy consumption, security and production cost. They highlight topology, simulation and hardware design issues. They proposed improved simulator architecture with agent, controller, interfaces & services. Elaborate the topic with algorithm and its detail diagram.

Min-Xiou Chen, Yin-Din wang [7] explore the important issue in the field of WSN (Wireless Sensor Network) which is known as "Object tracking". They proposed an efficient tracking tree method based on the physical structure of a wireless sensor networks. Design a tree construction algorithm which is also known as "Large Frequency First Tree (LFFT)". To reduce the update cost of object tracking tree they introduced the tree adaptation Procedure (TAP).

Alkhateeb& al. [8] represented a critical & important issue related to the security in university campus. The objective of this paper is to build an effective and low cost security system made by wireless sensor network and based on multi-agents to provide security. They represent a ACCESS Architecture to solve this problem. This architecture consists of two agents i.e. system agents and ACCESS agents. System Agents manage the platform and ACCESS agents consists of generic agents responsible for channeling context sensitive services. Different types of services are pull, push, tracking & emergency services. Explain the campus agent's security system with diagram. Simulate the system using laptops and it gives the better performance.
Various Attacks in WSN

S. No.	Attack Name	Symptom	Damage Penetration
1.	Sink/Black Hole Attack	This is a special kind of selective forwarding attack which draws attention on the compromised node. A compromised node attracts all maximum possible traffic of the network. Then it places malicious node to the closest base station and it enables the selective forwarding attack. It is a very complex attack. Detection of a sinkhole attack is very hard and it affects the higher layer applications.	• If Black hole attack occur in our sensor network then all network services gets down because it always try to attack on main node(or base station). • The whole network can be damage.

2.	Worm Hole Attack	In this type of attack, an attacker copies the whole packet or message by tunneling them to another network from the originator. Then the attacker transmits them to the destination node. When the attacker transmits the copied messages or packets to the destination node, she/he transmits it speedily in such a way that copied packets reach the destination node before the original packets (from the legitimate user) reach it. To do that, the attacker uses a wormhole tunnel. Wormhole nodes are fully invisible.	• The invisible nodes when occur in the wireless sensor network these nodes try to send fake messages to the other network nodes then the all network nodes look like busy node that time sender always waits for destination node.
3.	HELLO Flood Attack	New sensor node broadcasts "Hello" to find its neighbors. Also broadcast its route to the base station. Other nodes may choose to route data through this new node if the path is shorter. Adversary node broadcast a short path to the base station using a high power transmission. Target nodes attempt to reply, but the adversary node is out of range. This attack puts the network in a state of confusion.	• The whole network is got confused be a newly added sensor node which is continuously try to send HELLO message to each and every node within the network. • As result the network is got jammed by HELLO packets. • Due to the increase of HELLO packet flooding the sensor battery gets down and may be enter into dead state.
4.	Sybil Attack	This attack is very common and well known. The attacker may obtain the legitimate person's IP address or MAC address in order to steal his/her identity and make it his/her own. Then the attacker may attack another victim and can do plenty of things with that new stolen identity of the legitimate user. A Sybil attack is an advanced version of an impersonate attack in which a malicious user (attacker) may steal multiple identities. In technical terms, a malicious node represents itself to the other fellow nodes by acquiring multiple identities within it-self. Impacts will be the same as in an impersonate attack.	• The will not be secure if Sybil attack will occur within sensor network. • Theconfidential information can be stolen by unauthorized user. • A fake user will come into the existence which call leak out the sensitive data on the public network. • Unimportant data can be broadcasted by attacker over the wireless sensor network.
5.	Cryptographic Attack	In cryptanalysis, attack models or attack types are a classification of cryptographic attacks specifying the kind of access a cryptanalyst has to a system under attack when attempting to "break" an encrypted message (also known as cipher-text) generated by the system. The more elaborate the access the cryptanalyst can gain, the more useful information it can extracted and utilize for breaking the system.	• The man in the middle problem can be occurring then all information can be stolen by that person. • The encryption key can fetched by that person and can open confidential data without any permission of actual user. • Encryption and decryption can be easily captured and data can be convert into readable form.
6.	Selective Forwarding Attack/ Gray Hole Attack	It may also refer as 'Gray Hole attack'. In this form of attack, an attacker may stop the node to pass packets through by forwarding or dropping those messages. In one form of selective forwarding attack, a node selectively rejects the packets by dropping them from coming into that network from an individual node or a group of individual nodes.	• Our important data can be lost because the attacker drops the original message. • The high confidential data which is needed at a time will not be available for the end user.
7.	Denial of Service Attack	There are plenty of DoS attacks which reduce the network lifetime in different ways. One of the common methods is Denial of Service attack. An attacker sends a huge amount of packets in order to stop the network from communicating with different nodes. The main aim of this attack is to exhaust the resources on the victim's machine.	• Directly impact the battery of the sensor network. • Attacker tries to send unwanted data to reduce battery life of the sensor node then offer the few hours the sensor node can be properly dead.

8.	Acknowledgement Spoofing	Adversary can easily intercept messages between two parties Spoofs acknowledge of a message to the sender. Goal is to convince the sender that a weak link is strong, or a dead line is still active. Counter the attack by appending a random number to the message and encrypt the whole thing. Acknowledge by sending the decrypted random number.	• Whole network can come into busy state because an intermediate person will receive the original messages and tries to send unwanted material to the end user.

III. Security Mechanism

Security Threats in WSN [9]:- It is an emerging technology that shows great promise for various futuristic application for both general public and national security.

- Spoofed, altered, or replayed routing Information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes
- HELLO flood attacks

Challenges in Wireless Sensor Networks [10]:- It has great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges wireless sensor networks face today is security.

Passive Attacks

- Attacks Against

Active Attacks

- Routing attacks in sensor Networks
- Denial of Service Attacks
- Node Subversion
- Node Malfunction
- Node outage
- Physical Attacks
- Message Corruption
- False Node
- Node Replication Attacks
- Passive Information gathering

Security in cognitive wireless sensor networks [11]- A wide variety of attacks on CWSNs, their taxonomy and different security measures available to handle the attacks.

- Communication attacks
- Against Privacy Attacks.
- Node Targeted Attacks.
- Power Consumption Attacks.
- Policy Attacks
- Cryptographic Attacks

Security attacks And intrusion detection schemes in Wireless sensor network [12] :- Maintenance of complex systems and fine-grain monitoring of indoor and outdoor environments. However security is one of the major aspects of Wireless sensor networks due to the resource limitations of sensor nodes.

- Spoofed, altered or replayed routing information
- Selective forwarding
- Worm hole attack
- Sybil attack
- Black hole attack
- Hello Flooding
- Acknowledgement spoofing
- Denial-of-Service Attacks
- Various Attacks and Their Security

Various Attacks and Their Security Mechanisms in Wireless Sensor Network [13]:- It examines the security related problems and challenges in wireless sensor networks.

- Sybil Attack
- Node Replication Attacks
- HELLO Flood Attack
- Sinkhole Attack
- Eavesdropping Attack

Attacks and Countermeasures in Wireless Sensor Network [14]:-It discusses a Security Issues, limitation and wide variety of Attack in WSN and then classification mechanisms and different securities available to handle them.

- Sybil Attack
- HELLO Flood Attack
- Sinkhole Attack
- Worm Hole

Routing Attacks in Wireless Sensor Networks [15] :- The security of a wireless sensor network is compromised because of the random deployment of sensor nodes in open environment, memory limitations, power limitations and unattended nature.

- Sybil Attack
- Gray Hole Attack
- Black Hole Attack
- Hello Flood Attack
- Worm Hole Attack

Security Mechanisms and Attacks in Wireless Sensor Networks [16]:-It discusses the holistic view of security for ensuring layered and robust security in wireless sensor networks.

- Black Hole Attack
- Hello Flood Attack
- Sybil Attack
- Worm Hole Attack

IV. Conclusion

The Design and construction of smart structures is one of the ultimate challenges of now days. Use of Wireless Sensor Network (WSN) shows that it is the vital part of our life, industry, environment, security & most important is our health. In future more and more research work is to be carried out to make human being life much better and secure.In Future more emphasis is be given on security due to the security threats in security mechanism.

References

[1] John Herbert, John O'Donoghue, Gao Ling, Kai Fei "Mobile Agent Architecture Integration for a Wireless Sensor MedicalApplication" Proceedings of the 2006 IEEE/WIC/ ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT 2006 Workshops)

(WI-IATW'06) 0-7695-2749-3/06.
[2] B. F. Spencer Jr, Manuel E. Ruiz-Sandoval and NaritoKurata"Smart sensing technology: opportunities and challenges" STRUCTURAL CONTROL AND HEALTH MONITORING , 2004; 11:349–368 (DOI: 10.1002/stc.48).
[3] Chris Otto, AleksandarMilenković, Corey Sanders, Emil Jovanov"System Architecture Of A Wireless Body Area Sensor Network For Ubiquitous Health Monitoring" Journal of Mobile Multimedia, Vol. 1, No.4 (2006) 307-326
[4] Alcides Montoya, Diana Carolina Restrepo and Demetrio Arturo Ovalle"Artificial Intelligence for wireless Sensor Networks Enhancement"
[5] AbdelhakimHamzi, MouloudKoudil, Jean-Paul Jamont, Michel Occello "Multi-Agent Architecture for the Design of WSN Applications" Wireless Sensor Network, 2013, 5, 14-25http://dx.doi.org/10.4236/wsn.2013.52003 Published Online February 2013 (http://www.scirp.org/journal/wsn)
[6] Filippou, D. A. Karras "Introducing Intelligent Agents Potential into a competent Integral Multi-Agent Sensor Network Simulation Architecture Design"Journal of Software Engineering and Applications, 2013, 6, 42-48doi:10.4236/jsea.2013.67B008 Published Online July 2013 (http://www.scirp.org/journal/jsea)
[7] Min-Xiou Chen , Yin-Din Wang "An efficient location tracking structure for wireless sensor networks" Computer Communications 32 (2009) 1495–1504
[8] Faisal Alkhateeb et al. "A Multi-Agent-Based System for Securing University Campus" IJRRAS 2 (3) March 2010
[9] IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011ISSN (Online): 2231 –5268 www.ijcsms.com
[10] International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009
[11] Journal on Wireless Communications and Networking 2012, 2012:48
[12] International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 6, December 2013
[13] International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-2, Issue-8, June 2014
[14] International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012
[15] Deepali Virmani et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, pp. 2665-2671
[16] International Journal of Engineering and Innovative Technology (IJEIT) Vol. 2, Issue 3, September 2012.

Rina Sharma, Research Scholar, Punjab Technical University, Kapurthala is working as a HOD (CSE) in GPE-Ganpati Group Of Institution, Bilaspur, Yamuna Nagar, Haryana, India from 01-10-2008.
She is pursuing Ph.D. in Computer Applications from Punjab Technical University, Jalandhar,Punjab,India. She has Published One Review paper in International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS).

Dr. Himani,Professor, Dean, ECE,Marrilaxman Reddy Institute of Technology, Quthbullapur Mandal,Dundigal, Hyderabad-500043. Senior Member IEEE. IEEE Nanotechnology Council, IEEE Sensors Council, Editorial Board Member of IEEE Transactions of Industrial Electronics (Impact factor 6.5) Vice Editor In Chief Blue Eyes Intelligence Engineering & Sciences Publication Pvt. Ltd.(BEI-ESP) Editorial Board Member IJARSET.