APPLICATIONS AND ASSOCIATED ATTACKS IN WIRELESS SENSOR NETWORK

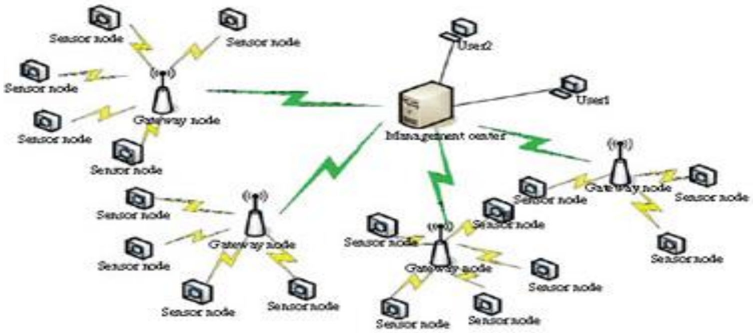
[1] V. Sandeep, [2]N.Venkateswaran, [3] G. Pranay Kumar, [4]G. Prashanth, [5]N. Pujith
[1,3,4,5] Students, [2]Associate Professor, Department of Computer Science and Engineering,
Jyothishmathi Institute of Technology and Science, Karimnagar, Telangana-505001.

Abstract: A wireless sensor network is a Wi-Fi community and which is consisting of circulated sufficiently using the sensor to reveal the conditions (environmental, physical). There are several applications of the wireless sensor network and these are mainly used for growth, sharing and security and sending the statics. These type of community consisting of the multiple sensors Or multiple detection sensors and they are called as" sensor nodes .each sensor node is small in size and light in weight and they are portable devices. Wireless communication technologies to undergo and rapid advancement. In the past years, research has been done over the WSN. Mainly found in military and civilian applications over the World Wide. These wireless sensor networks is an attractive technology with great promise for the future. On the basis, the challenges are also remained to be addressed and the problems belong to coverage, deployment, QOS (Quality of service), scalability. This paper publishes a piece of small information related to the applications and associated attacks found on WSN.

Indexed terms: Sensor, Attack, Network, wireless, applications, nodes. WSN

1. INTRODUCTION

A WSN(wireless sensor network) is a network consisting of spatially autonomous devices that can use a sensor for monitoring both physical and environmental conditions. These devices (portable) they are combined with network connecting devices like routers, gateways, bridges, switches, hubs, etc.. and they can confirm or create WSN system and these devices(nodes) communicate wirelessly with the gateways and that provide connection to the wired one then you can collect it. And these process can analyze the measurement of data regarding the part of distance and reliability in a wireless sensor network to gain additional information between these devices and gateways. We can also access the wireless network through the internet as shown in below fig(1) and that is to be considered as a physical network[1] & [2]. This particular technology mainly used for purposes such as home and smart spaces, transportation, military, and civilian, medical and environmental, etc.



In fact WSN they are more vulnerable to various attacks than those of guided transmission link. The nature of wireless sensor network communication is reliable and simple. Major challenges are also addressed. Apart from that security is the main issue over the wireless sensor network. This paper comes across various attacks and applications of WSN.

II.APPLICATIONS

In the WSN infrastructures, the software that depends on several constraints. WSN research has to be targeted to increase the solutions and also maintain the range of diverse sensor programs through integrating the software information [3]. Some of the applications associated with the wireless environment which follows

- Environment monitoring system
- Health-Care Monitoring System
- Pollution Monitoring System
- Fire Detection Monitoring Systems
- Routing Monitoring Protocol systems

The WSN is constructed with nodes that are used to monitoring the surroundings like temperature level of location, humidity, pressure, position, vibration, sound, etc. These nodes can be deployed into various real-time applications to operate different tasks like smart detecting, a discovery of neighbor node, data processing and storage, data collection, target tracking, monitor and controlling, synchronization, node localization, and effective routing between the base station and nodes.

III.CLASSIFICATION OF APPLICATIONS AND ITS ATTACKS

Smart Cities: By using these wireless sensor network we can know the city pollution and noisy points smart line in management and may other.

Health Care Monitoring: Generally, it is very difficult to find the heartbeat count of a patient. To overcome this problem a device (sensor) used to track the internet changes in the body. It is small in size and less portable [4].

Military Applications: These sensors are useful in the military. These are used to monitor each and every friendly motion. Different types of attacks can also be detected through sensors.

Disaster Rescue Applications: These sensor nodes are also useful when a disaster (or) natural calamity occurs. By using this we can find the proper ways to save the lives of the people from affected areas. Natural calamity like earthquakes, tsunami, floods, thunderstorm, etc.. By the sensors we will give some intimation to people just like some alarm sound has to produce. By this people can understand easily and then save their lives, property [5], etc.

House Hold Applications: These are useful in home appliances like Refrigerator s, Vaccum Cleaners, Door control, microwaves, etc. As technology is developing this kind of sensors will be created.

Programs on Environment: Ecological applications of sensor network which is mainly consisting of monitoring and movement birds and animals and insects and observing the conditions which may affect the vegetation and livestock irrigation macro gods for huge amount of scale of earth tracking and planetary exploration and also agriculture organic earth and environmental monitoring in marine and atmospheric contexts wooded area and fire detection geophysical., studies on flood detection bio-complexity mapping of the environment and pollution observe[6].

Agriculture: The wireless sensor network is mainly used in the point of agricultural industry increasingly common.using of these WSN frees the farmer from the Maintenance of wiring and it is to difficult environment irrigation automation enables more efficient water usage and reduced waste.

Environmental Applications: These type of applications include the movements of insects and animals and birds.

Infrastructural Monitoring: WSN is mainly used to monitor the movements of buildings and any other infrastructures such as bridges, flyovers, tunnels, etc. enabling the emerging practices to monitor assets remotely without the need for costly. size visits. mainly advantage of daily data, traditionally this data can be collected monthly, weekly using physical site visits involving transportation as roads and rails some cases. It is also far more accurate than any visual accepts or inceptions that would be carried act.

IV.TYPES OF ATTACKS ON WIRELESS SENSOR NETWORKS:

i) **COMMON ATTACKS:** It is an attack in which an opponent can perform some operations on the data packets like

a) **Message modification:** In this opponent can modify the data packets.
b) **Caves dropping:** In this data is retrieved by the opponent from packets that are transmitted.
c) **Message replay**: In this attack the modification which is done to the message that is retransmitted later.

ii) **NODE COMPROMISE ATTACK:** Various complex attacks can be easily launched from compromised nodes. This is a common attack in wireless sensor networks. When an attacker gains control to the sensor node then it said to be compromised[8].

iii) **IMPERSONATION ATTACK:** The attack which is launched during a compromised node is an impersonation attack. In this legitimate node is impersonated by the node and by using its identity it mounts an active attack.

iv) **PROTOCOL-SPECIFIC ATTACK:**

The devices obey many rules when performing network activities. The protocol ARP, TCP, UDP, CMP, IP& Application protocols-They may leave openings for network Intrusions via protocol Impersonation[7].

-Protocol-specific attacks can easily compromise on a network.

v) **DOS ATTACK:**

This attack has several forms

a) **Node collaboration**: In this same nodes acts as malicosly& prevent broadcast messages from reaching other sections in sensor networks.

b**) Jamming Attack:** In this hacker jams communication channel& avoids any member of the network to receiver send any packet.

c) **Exhaustion power**: To deplete the battery life of packets attacker repeatedly requests packets[9].

V.CONCLUSION

Wireless sensor network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative being exploited in abundance for the first time. The applications and related attacks of the wireless sensor network are military, civilian, water, environment, agriculture, etc.. The security is the main issue over the WSN and in this paper we publish those different types of attacks over WSN.

REFERENCES:

[1] A. D. Wood and J. A Avancha, s.pinkstan " Sensor networks", computer vol 35, no 10,200w, pp, 54- 22.

[2] J. Hill, R. SZEWCZYK, A, Woo, S. Hollar, D, collar and K. Poster system Architecture Directions for networked System sensor, Apols, November 2000

[3] S. Prasanna, Srinivasarao "An overview of wireless sensor networks applications and security".Volume - 2, issue-2, may 2002.

[4] B. P sreeja, L. Jaykumar, G. Sarathadevic " Wireless sensor network applications" Vol 118, No.11, 2018,385-389.

[5] S.V manikanthan and K. Baskaran "Low cast VLSI Design and the implementation of sorting Network for wireless sensor network". ISSN 0974-973X ISSUE : November 2011,Pocs 112011008.

[6] Dr. J. Cook and S. K Das" Smart environments technologies, protocols, and applications " New York: Jhon widely, PP 13-15, 2004.

[7].Umapathi, N. & Ramaraj, N and Adlin Mano, R (2012), "A Proactive Ant Colony Algorithm for Efficient Power Routing using MANET", International Journal of Computer Applications, 58(20): 33-36.

Umapathi, N., and Ramaraj, N. (2016), "Wireless Adhoc Telemedicine System: Improving Network Performance for Multimedia

[8].Data', Journal of Medical Imagining and Health Informatics, vol. 6, pp.1-5, https://doi.org/10.1166/jmihi.2016.1954

[9].Umapathi.N, (2010), “A Novel Approach to Packet Loss Analysis in a Wireless Network”, International Journal of Wireless Networks and Communications. ISSN 0975-6507 Volume 2, Number 3 pp.119-124.