

Intrusion Detection System using Wireless Sensor Networks: a Review

Chandrabala P. Kothari

Dept. of Electronics and Telecommunication Engineering
SVKM's NMIMS MPSTME
Mumbai, India

Vaishali Kulkarni

Dept. of Electronics and Telecommunication Engineering
SVKM's NMIMS MPSTME
Mumbai, India

Abstract—IDS using WSN is the fast growing research area of recent times. WSN consists of tiny battery operated devices that are efficient of monitoring areas of varied interest. This paper provides general description of WSN and Sensor Nodes, the routing protocols utilized Application of WSN and thus a brief overview of IDS using WSN and its comparison with the available technology.

Index Terms—WSN, Sensor Nodes, Routing Protocols, IDS.

1. INTRODUCTION

A lot of research work and development in the field of Wireless systems and Micro Electro-Mechanical System technology (MEMS) has made WSN possible these days. It has an extremely wide scope of research and development and has an innovative structure and module, thus becoming one of the most promising and lucrative system. Sensing technology together with wireless communication finds varied interest areas. It provides the technology for a broad spectrum of systems in Defense, generating new capabilities for reconnaissance and surveillance as well as other tactical applications. WSN system has miniature size devices, with an ability to function in various climatic condition thus enabling it to become a suitable choice for IDS. IDS using WSN has become the area of major research interest since recent times

2. WIRELESS SENSOR NETWORK

2.1 Definition

A WSN is an adhoc network consisting of various battery-operated nodes which are capable of communicating with each other without relying on infrastructure. It is a self healing and self organizing unit which consists of autonomous Sensor modules that co-operate [1] in order to provide the environmental or surrounding information to the central or the sink node. These Sensor nodes are tiny, small, low cost [2] unit that communicate with each other in a decentralized manner using various hop methods. They have characteristics which are as explained [3].

a. *Self organization*: WSN system consists of deploying sensors in unguarded and hostile environment. It is supported by Sensor Network Protocols and algorithms which provides itself healing and self organizing property.

b. *Multihop routing*: This capability of WSN enables it to transmit data packet to upper node when used in Mesh Topology.

c. *Resource utilization*: This system has Short transmission range, limited battery lifetime and small memory capacity

2.2 Sensor Nodes.

WSN system consists of independent, intelligent [7] Sensor network or nodes communicating with each other in a collaborative manner. These nodes consist of Parameter sensing, Processing and communicating components mounted on a board. These nodes can be placed at distance and can be used in different topology [4,5] according to the need of the application. Multi hop communication proves to be better in terms of energy efficiency as compared to single hop, since the prime constraint of WSN system focuses on optimum power consumption in order to have better system performance [2, 7]. Since the Sensor nodes are deployed in harsh field in varied topology, energy saving becomes of utmost importance which gives rise to number of Protocols [7]. Also there are a number of routing protocols used for WSN based on design characteristics [5].

2.3 Classification of Routing Protocols.

Depending on the application of Wireless Sensor Networks, the Routing protocols are classified as following [16].

a. Flat Routing:

A node in need of data transmission, first searches for a valid route to the BS and then transmits the data. Nodes around the base station may drain their energy quickly. Its scalability is average.

Ex:-Rumor Routing (RR), Constrained Anisotropic Diffusion Routing (CADR),

b. Hierarchical Routing:

Its an energy efficient routing, higher energy nodes process and send the data whereas low energy nodes are used to perform the sensing in the area of interest.

Ex:- Low Energy Adaptive Clustering Hierarchy (LEACH), Power efficient gathering in sensor information systems (PEACH).

c. Location Based Routing:

It needs location information of the sensor nodes which can be obtained from GPS (Global Positioning System) signals, thus helping in forming an optimal path without using coding techniques.

Ex:-Geographic and Energy-Aware Routing (GEAR)

2.4 Applications of WSN

The need to measure various parameters such as temperature, pressure, humidity, Sound, Strain, Acceleration, Infra-red, Visual, Acoustic were earlier met by traditional

wired network but due to its extreme cost of installation, maintenance and troubleshooting WSN systems have gained popularity in recent years because of their low cost and ability to survive in physical harsh and hostile conditions [1,5,6,7]. The typical need of WSN arises in battle-field surveillance and country Perimeter protection where these Sensor nodes can sense, detect, classify and give indication of possible unrecognized hostile intrusions in all weather situation year round[8]. The low cost factor enables it to be installed in various other civilian application, Environment and Habitat monitoring, Home Automation and Health care. Following gives a brief introduction to the application of WSN [2,9].

a. *Military.*

Due to its ability to function in rough and hostile terrain with capability to communicate remotely over distance using over the air mode of method, this system found its first application in defence organization where it can be used to track and Monitor Enemy activity, friendly troops ,Surveillance of battlefield, Missile Guidance system and Critical Ammunition reserve and Intrusion detection.

b. *Environment and Habitat Monitoring*

WSN system have made possible the observation of flora and fauna spread across a wide region because of its ability to communicate over a large range by means of remotely placed sensor nodes utilizing hop techniques. It is also used in forest fire detection, predict flood situation, Soil moisture and pesticide level.

c. *Home Automation and Health Care Unit*

With the advancement of research in field of Wireless sensor and the human need of having ease and comfort in daily schedule, this system has found a place of utmost importance. The various sensor nodes can be incorporated in equipments of utilities such as Air-Conditioners, Vacuum Cleaner, and Refrigerator. It can be embedded in furniture thus providing remote control facility. It does find application and use in Health care units for tracking and monitoring Patient's condition, Medicine level, Movement of Medical Personnel, Assistance to Elderly and the special ones.

3. INTRUSION DETECTION SYSTEM

Intrusion can be defined as the set of malicious activity undertaken by an outside agent or source in order to breach the security of a system or an Organization with a view of getting access into a highly monitored or secured location[10]. This Traditional approach of monitoring and security was being done by deploying Security Personnel and Guards, Alarm systems, fencing Automatic passage system, but these were highly inefficient and prone to false intrusion data and information. They had limitation in areas of being deployed in difficult and rough geographic terrain, cost of implementation and authentication of data obtained. IDS has the function of monitoring and reporting the suspicious activity within a particular system and report it to the central unit with higher efficiency than the old systems. IDS system can be implemented utilizing varied technology platform. Security and Surveillance being the prime concern, a number of IDS systems are available. Table.1 gives comparison of various systems.

TABLE I

DETECTION METHOD	MULTIPLE INTRUSION DETECTION	LOW FALSE POSITIVES	LONG DISTANCE CAPABILITIES	CONTINUOUS MONITORING	SYSTEM INTERACTION	LOW MAINTAINENCE REPAIR COST
BREAK TENSION WIRE			●	●		
INFRARED/LINE OF SIGHT	●			●	●	
MOTION DETECTION	●	●		●	●	
MICROWAVE DETECTION	●					
ELECTRICAL FENCE			●		●	●
SCHEDULE PATROLS		●	●		●	●

IDS has number of techniques of detecting intrusion [1, 12] of which here two types of methods are given.

a. *Signature based system*

In this system, detection of target is done by means of pre-fed data in the system. It is also known as rule based system, which has predefined set of rules for various security attacks. It can function and perform detection only if parameters or signatures are provided to it [3].

b. *Anomaly based system*

This system detects malicious activities based on a particular threshold value and signals it when the threshold level is exceeded. It can detect known and unknown suspicious movements in a system [1,3] and thus has an edge over Signature based system.

c. *Hybrid system*

It combines features of both the above methods. It detects attacks based on signatures and also the unknown activity [1]. But this method of detection is least energy efficient and hence not utilized for WSN based IDS where power consumption is important factor.

3.1 Recent Approaches to IDS using WSN

Intrusion detection system using WSN is the latest research trend considering the advancement of WSN with its approach to utilizing miniature sensors embedded on board, low cost. This system utilizing WSN consists of sensor node which measures various required parameters, such as Temperature, Pressure, Sound, Vibration, Humidity and Visual light, thus co-coordinating with other nodes wirelessly using wireless communication method such as Zig-bee[13], providing information to the Central unit or the Base-station, i.e. it Monitors, Analyzes and Alarms, thus finding application in unguarded and open environment.

With reference to all the facilities provided by WSN, it is used in order to guard high security buildings and premises, Large Industrial Estate, Government Embassies and reserve. The system used for Human intrusion detection [10] consists of smart wireless sensor unit, low power processing unit, radio transceiver, battery in a compact pack, called as Motes. It utilized TinyOS as operating system and Nesc as programming platform. It made use of PIR, Seismic, Magnetic, Acoustic and Optical sensors for detecting

possibility of possible intrusion. Other project as mentioned in [15] utilizes Magnetic and Radar sensors, Intrusion if any is processed locally, shared with neighbouring node and communicated to Gateway. WSN can be utilized for detecting and tracking position of moving object [10]. As per the need of today's Security and Reconnaissance application, Continuous monitoring, long distance together with System interaction and low false alarm rates are the necessities which are better provided by IDS using WSN. As per the observation from above given table, WSN proves to be a promising technology in terms all the mentioned comparison factors.

4. FUTURE SCOPE AND CONCLUSION

Future sees a wide scope and development in the field of Wireless Networks, thus becoming an important part of our lives. The flexibility, low cost, small size makes it first choice to proceed with new areas of research when compared to other existing methods. Its remote access mode of operation and least possibility of false alarm rate enable it to be used for Security and Surveillance systems. According to the need of detection, various types of IDS can be used. Further research in making it highly power efficient, memory requirement, fault tolerances, possibility of reducing the number of nodes required will cause it to be one of the most sought after technology in varied areas of application.

REFERENCES

- [1] Nabil Ali Alrajeh, S. Khan and Bilal Shams, "Intrusion Detection System in Wireless Sensor Network: A Review", International Journal of distributed Sensor Network, Vol.2013, Article ID 167575.
- [2] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci," Wireless sensor networks: a survey", Computer Networks 38 (2002) 393–422, 12 December 2001.
- [3] Md. Safiqul Islam, Syed Ashiqur Rahman," Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches", International Journal of Advanced Science and Technology Vol. 36, November, 2011.
- [4] Bc. Lumír Honus,"Design , implementation and simulation of intrusion detection system for wireless sensor networks",Masarykova Univerzita,Master Thesis, Spring 2009.
- [5] Swati Sharma, Dr. Pradeep Mittal," Wireless Sensor Networks: Architecture, Protocols", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 1, January 2013.
- [6] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary,"Wireless Sensor Network Security: A Survey",Security in Distributed, Grid, and Pervasive Computing Yang Xiao,2006 Auerbach Publications, CRC Press
- [7] Eiko Yoneki, Jean Bacon,"A survey of Wireless Sensor Network technologies: research trends and middleware's role",Technical Report,UCAM-CL-TR-646,ISSN 1476-2986.
- [8] Telecommunication Standardization Sector of ITU, Technical report,28 feb.2014.
- [9] Chee-ye Chong and Srikanta P. Kumar, Invited paper, Sensor Networks: Evolution, Opportunities, and Challenges,IEEE.
- [10] Anurag Kumar et.all,"Wireless sensor networks for human intruder detection: A Review", Journal of the Indian Institute of Science VOL 90:3 Jul–Sep 2010.
- [11] Rodrigo Roman et.all, "Applying Intrusion Detection Systems to Wireless Sensor Networks",
- [12] Robert Mitchell, Ing-Ray Chen, "Review:A survey of intrusion detection in wireless network applications", Computer Communications 42 (2014) 1–23.
- [13] Meng-Shiuan Pan, Yu-Chee Tseng, "ZigBee-Based Long-ThinWireless Sensor Networks: Address Assignment and Routing Schemes",IJAHUC.
- [14] Peter Rothenpieler, Daniela Kruger, Dennis Pfisterer, Stefan Fischer,"FleGSens — Secure Area Monitoring Using Wireless Sensor Networks".
- [15] A. Arora, et. all, "A Line in the Sand: A Wireless Sensor Network for Target, Detection, Classification, and Tracking.
- [16] Darpan Dekivadiya,"Power Aware Routing protocols In Wireless Sensor Networks",CSE,Nirma University, April 2012.