International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

Intrusion Detection System Using WSN

Manoj L Patel[1], P R Bhole[2], N L Lokhande[3],
[1, 2,3]*Department of Electronics & Telecommunication, R C Patel Institute of Technology, Shirpur, Maharashtra, India*

Abstract*:*Wireless Sensor Networks (WSNs) are vulnerable to various kinds of security threats that can degrade the performance of the network and may cause the sensors to send wrong information to the sink. Key management, authentication and secure routing protocols cannot guarantee the required security for WSNs. Intrusion Detection System (IDS) provides a solution to this problem by analyzing the network in order to detect abnormal behavior of the sensor node(s). Researchers have proposed various approaches for detecting intrusions in WSNs during the past few years. In this survey, we classify these approaches into three categories and discuss them in detail.

Keywords: Xbee, Arduino Uno, Ultrasonic Sensor, Speed Sensor, LCD

I. INTRODUCTION

Security is today one of the primary concerns around the world. Recent trends have shown that surveillance of tactically important areas for suspicious activities is a high priority for organizations. Despite technological advances, the major threat that still lurks is from unauthorized humans who can gain access to a target location and compromise its integrity. This results in surveillance of key areas for possible intrusion to be one of the most desired goals for security. Wireless Sensor Networks (WSNs) are one of the most contemporary and successful technique used for environmental monitoring of certain physical parameters. WSNs can be effectively used to gather useful data from the physical environment they are deployed in and communicating that information wirelessly to base stations which can process it and extract useful information. WSNs are envisioned to reduce, and eventually, completely eliminate human involvement in information gathering in certain applications. However, they have their own limitations, the most important of which is the amount of energy available to a sensor node. With slow progress in energy scavenging, the current solutions need to be very energy-efficient; using the minimum amount of energy while having the maximum useful throughput. Other major challenges faced by WSNs are tamper resistance unobtrusiveness and real-time constraints despite these limitations; WSNs do have the advantage of deploying sensors in hostile environments autonomously.

II. OBJECTIVE

The general objective of such an application is to monitor the perimeter, in most cases a boundary wall for any human presence over the wall or within some distance of it. The base station, where all the information is sent, needs to have a map of the entire security perimeter and human detection at any segment of the wall must be reported to the base station with acceptable latency. Some applications requirements which must be satisfied to make our system useful in practice are following. First, continuous monitoring requires the sensor devices to be active all the time. Therefore, energy conservation schemes are required so that lifetime of sensor devices can be extended for uninterrupted active sensing. Second, the perimeter must be entirely covered without any unattended spaces in between any two nodes. This requires effective and acute positioning and orientation of the sensor devices. Third, it is crucial for the sensor nodes to have a very low possibility of being detected by the intruder which can then, possibly, find a way to bypass detection. Small physical size of sensor nodes along with zero RF communication is desired in absence of significant events. Fourth, effective detection of human presence along with low reporting latency is also required so that active countermeasures can be deployed against the threat well in time. Fifth, the sensor nodes need to communicate with each other in a line topology since wall coverage is done by placing sensor nodes in a semi-straight or straight line. Thus, the routing must be done in such a way to ensure that radio links are maintained even if any node goes down.

III.PROBLEM IDENTIFICATION

One of the key features of a WSN is its multihop distributed operations, which add more complexity in terms of security attack detection and prevention. In a multihop distributed environment, it is very difficult to locate attackers or malicious nodes. Many security attack detection and prevention mechanisms are designed for WSNs; however most of the existing solutions are capable of handling only a few security attacks. For example, most secure routing protocols are designed to counter few security attacks. Similarly new media access mechanisms are designed handle hidden-node problem or selfishness. Encryption mechanisms are designed to protect data against passive attacks. Hence, one can say that there is a need to design mechanisms that are capable

enough of detecting and preventing multiple security attacks in WSNs. An Intrusion Detection System (IDS) is one possible solution to it.

IV. HARDWARE REQUIREMENT

A. A.PIC Micro-controller

PIC18FX family offers the advantages of all PIC18 micro-controllers AS namely, high computational performance at an economical price âAS with the addition ofhigh-endurance, Enhanced Flash program memory. On top of these features, the PIC18F2420/2520/4420/ 4520 family introduces design enhancements that make these micro-controllers a logical choice for many high-performance, power sensitive applications. Devices in the PIC18F 2420/2520/4420/4520 family are available in 28-pin and 40/44-pin packages Like all Microchip PIC18 devices, members of the PIC18F2420/2520/4420/4520 family are available as both standard and low-voltage devices. Standard devices with Enhanced Flash memory, designated with an F in the part number (such as PIC18F2420), accommodate an operating VDD range o 4.2V to 5.5V. Low-voltage parts, designated by LF(such as PIC18LF2420), function over an extended VDD range of 2.0V to 5.5V.

B. NRF 24101

The nRF24L01 is a single chip 2.4GHz transceiver with an embedded baseband protocol engine, designed for ultra low power wireless applications. The nRF24L01 is designed for operation in the world wide ISM frequency band at 2.400 - 2.4835GHz. An MCU (microcontroller) and very few external passive components are needed to design a radio system with the nRF24L01. The nRF24L01 is configured and operated through a Serial Peripheral Interface (SPI.) Through this interface the register map is available. The register map contains all configuration registers in the nRF24L01 and is accessible in all operation modes of the chip. The embedded baseband protocol engine is based on packet communication and supports various modes from manual operation to advanced autonomous protocol operation.

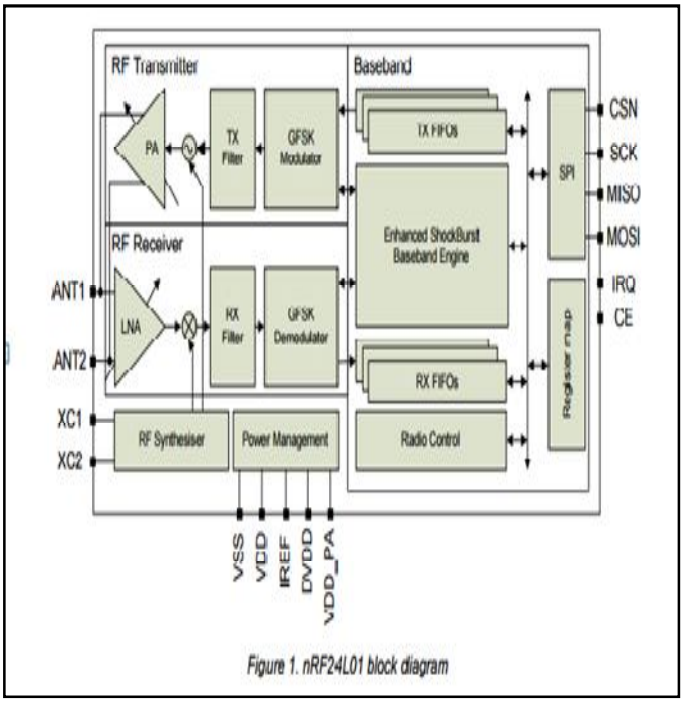

Fig. 1 Block Diagram of NRF 24L01

Internal FIFOs ensure a smooth data flow between the radio front end and the system AZs MCU. Enhanced Shock Burst reduces system cost by handling all the high-speed link layer operations. The radio front end uses GFSK modulation. It has user configurable parameters like frequency channel, output power and air data rate. The air data rate supported by the nRF 24L01 is configurable to 2 Mbps. The high air data rate combined with two powers saving modes makes the nRF24L01 very suitable for ultra low power designs. Internal voltage regulators ensure a high Power Supply Rejection Ratio (PSRR) and a wide power supply range.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

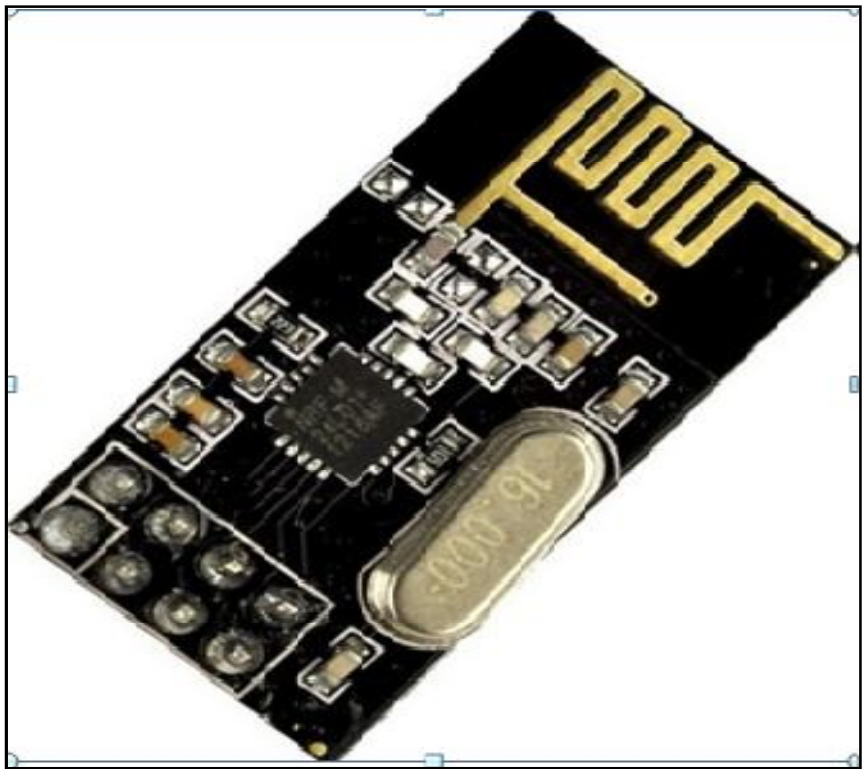

Fig. 2 NRF 24L01

C. RFID Reader

RFID, Radio frequency Identification and Detection system is to facilitate data transmission through the portable device known as tag that is read with the help of RFID reader; and process it as per the needs of an application. Information transmitted with the help of tag offers location or identification along with other specifics of product tagged as purchase date, color, and price. Typical RFID tag includes microchip with radio antenna, mounted on substrate. The RFID tags are configured to respond and receive signals from an RFID transceiver. This allows tags to be read from a distance, unlike other forms of authentication technology. The RFID system has gained wide acceptance in businesses, and is gradually replacing the bar code system.

V. ALGORITHM

Genetic algorithms are widely used in many areas of computing to solve a complex problem. It provides robust, adaptive and optimal solutions for many computing related problems. Genetic algorithms in computing are inspired from biological processes such as natural selection, evolution, theory of mutation, and genetic inheritance.

The general architecture of genetic algorithm used in computing is present in Figure 3. In genetic algorithm, the selection module derives most suitable answer or solution for some specific problem.

In crossover module, different parameters are exchange out of different solutions in order to get new solutions. Mutation module changes one or two parameters to get optimality in genetic algorithm. Genetic algorithm is widely used technique in network security especially in designing and proposing IDS. In IDS, genetic algorithm can be used for classification of security attacks and for generating specific rules for different security attacks. A lightweight IDS with reduced complexity using genetic algorithm for WSN is proposed in.

This work deals with measurement of sensor node suitability and attributes to International Journal of Distributed Sensor Networks Primary assumptions System activities are observe able Normal and intrusive activities have distinct evidence Perhaps effective Algorithmic (features or models)System architecture(Audit Data Processor, Knowledge Base, Decision Engine, Alarm Generation, and Responses)Information based on Genetic algorithm Applied to Intruder type External intruders Internal intruders Intruder behavior Attempted break-in Penetration of the security control system Leakage Denial of service Malicious use Type of approach Anomaly detection Misuse detection System Network-based Host-based Hybrid Masquerade attack.

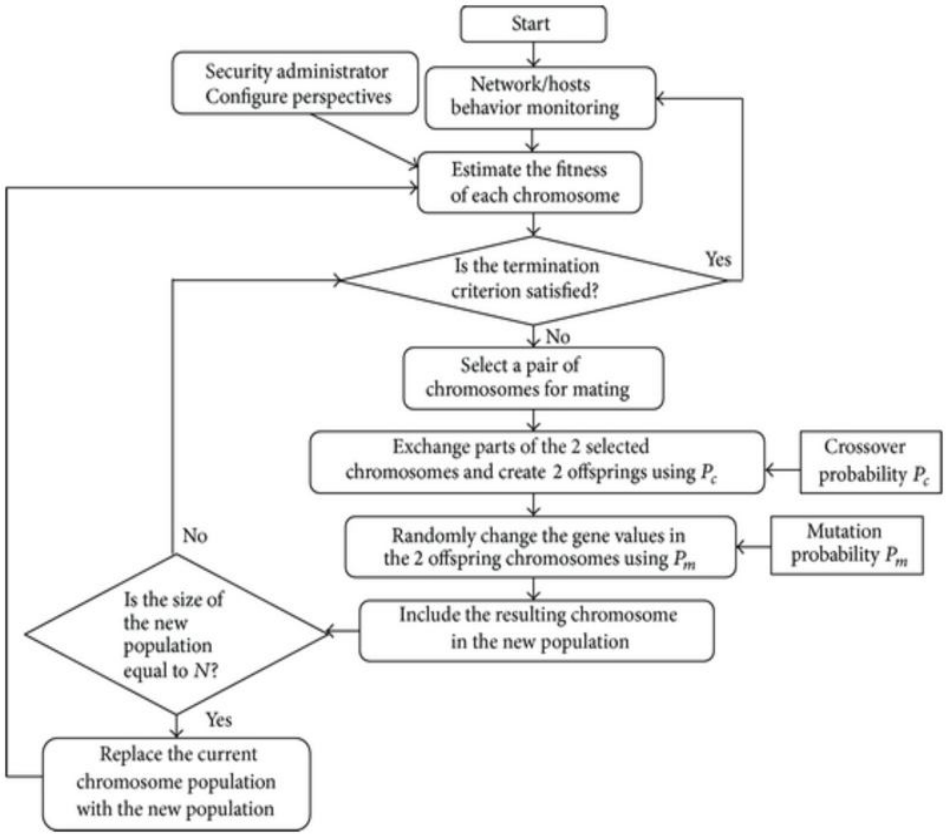

Fig. 3 Flow chart

Intrusion detection systems and element types where genetic algorithms can be applied for the perceived threat. A local monitoring node is introduced that acts like a proxy agent for the sink and is capable of monitoring neighbours. A Genetic algorithm based network IDS (GA-IDS) is present in. The proposed system considers many parameters such as protocol type, network services, and status of the connection to generate rules, the detection mechanism is trained on specific dataset, so that it can accurately identify and classify security attacks. In this mechanism, six rules are designed to detect six different types of denial of service (DoS) and probing attacks. The authors claim that the detection rate of DoS attacks. Many IDS several based where new and innovative attacks are not detected. An anomaly based IDS using concept of genetic algorithm is discussed in. This framework uses set of classification rules which are derived from network audit data. It uses these function to monitor quality and stability of eachthe perceived threat. A local monitoring node is introduced that acts like a proxy agent for the sink and is capable of monitoring neighbors. A Genetic algorithm based network IDS (GA-IDS) is present in. The proposed system considers many parameters such as protocol type, network services, and status of the connection to generate rules, detection mechanism is trained on specific dataset, so that it can accurately identify and classify security attacks. In this mechanism, six rules are designed to detect six different types of denial of service (DoS) and probing attacks. The authors claim that the detection rate of DoS attacks. Many IDS several based where new and innovative attacks are not detected. An anomaly based IDS using concept of genetic algorithm is discussed in. This framework uses set of classification rules which are derived from network audit data. It uses this function to monitor quality and stability of each rule.

VI. RESULTS

Intrusion detection systems add an early warning capability to your defenses, alerting you to any type of suspicious activity that typically occurs before and during an attack. Since most cannot stop an attack, intrusion detection systems should not be considered an alternative to traditional good security practices. There is no substitute for a carefully thought out corporate security policy, backed up by effective security procedures which are carried out by skilled staff using the necessary tools. Instead, intrusion detection systems should be viewed as an additional tool in the continuing battle against hackers and crackers.

VII. CONCLUSION

Research and implementation of diverse monitoring applications in the field of WSNs. The major lesson learned from this effort is that practical considerations and real-time factors must be taken into account while building such a monitoring application, so it can perform well not only in simulation, but also during practical deployment. has been very active. This work provides a study of deployment strategy for sensors. An intrusion detection model is implemented and evaluated for Homogeneous and Heterogeneous wireless sensor networks. It was programmed to identify the intruders coming in the confidential region and calculate the detection probability of intruders which provide the better results than previous work. During the detection model the detected information pass on to the base station where routing strategy is used with energy efficient way.

RFERENCES

[1] Absar-ul-Hasan, Ghalib A. Shah &Ather Ali, Intrusion detection system using wireless sensor network, National University of Science and Technology, Islamabad, Pakistan, Center for Advanced Research in Engineering, Islamabad Pakistan
[2] Aman V. Mankar, Tusher C. Ravekar, A Study of Intrusion Detection System using Advanced Genetic Algorithm, International Research Journal of Computer Science (IRJCS
[3] Mohamed HadiHabaebi, MahamatMahamat Ali, M. M. Hassan, M.S. Shoib, A. A. Zahrudin, A.A. Kamarulzaman, W.S. Wan Azhan, Md. Rafiqul Islam, Development of Physical Intrusion Detection System Using Wi-Fi/ZigBee RF Signals, Procedia Computer Science 76 (2015) 547–55
[4] K. Romer and F. Mattern, The design space of wireless sensor networks, Wireless Communications, IEEE, vol. 11, no. 6, pp. 54–61, 2004
[5] I. Onat and A. Miri, An intrusion detection system for wireless sensor networks, in Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005), IEEE International Conference on , vol. 3, pp. 253–259, IEEE, 2005.
[6] R. Roman, J. Zhou, and J. Lopez, Applying intrusion detection systems to wireless sensor networks, in Consumer Communications and Networking Conference , vol. 1, pp. 640–644, 2006
[7] DeependraBapna, Intrusion Detection System For Wireless Sensor Network, MTech Thesis, Department of Computer Science and Engineering, National Institute of Technology Rourkela, Odisha, 769 008, India, June 2014