An Experimental setup to Detect and Defend Constant Jamming Attack in a Multi-sensor based Wireless Sensor Network

Divya K
Department of Computer Science Engineering
Govt. College of Engineering, Mananthavady, Wayanad-670 644, Kerala, India.

Abstract- *Wireless Sensor Network (WSN), a prominent technology has multiple security vulnerabilities. Jamming (DoS) is one of the active attacks which causes an interference with normal radio signal reception and affects the availability of data. The Constant jammer sends continuous radio signals into the wireless network keeping the channel busy and disrupting communication of legitimate nodes. It is important to detect and defend jamming attacks from malicious nodes for effective functioning of the network. In this paper we designed, developed and evaluated a WSN that can efficiently detect constant jamming attack using Packet Delivery Ratio (PDR). Also we present a defensive mechanism by using the technique of Channel Surfing, an adaptive form of FHSS. We use LabVIEW for data acquisition and analysis.*

Keywords- Wireless Sensor Networks, Jamming Attacks, Jamming Detection, Channel Surfing, Microcontroller, LabVIEW.

I. INTRODUCTION

Wireless Sensor Networks (WSN) [1] are an attractive technology nowadays due to its low cost solutions to many real time applications. This rapid development was contributed by the advances in sensor design, wireless communication technologies, embedded systems and energy efficient communication protocols. The initial use of wireless sensor network was in military domain, especially for battlefield surveillance. In present day, such networks are used in many applications such as environmental monitoring, health monitoring, habitat monitoring, disaster detection and management, industrial quality control and protection , transportation, law and order enforcement, agriculture, smart buildings and traffic monitoring [2] [3]. Most of these applications are security critical applications such as military applications, health monitoring and industrial monitoring in which the security and privacy of data is very critical. The selection of a suitable security scheme is critical in wireless sensor networks due to its sharing of communication channels, multihop communication, untrusted transmissions, deployment in hostile environments, and limited resource availability [4]. Thus security plays an important role in the design and development of WSN.

Due to the wireless transmission and deployment in hostile and unattended environments, the WSN is vulnerable to various security attacks, both active and passive types of attacks[3] [4] [5]. These attacks can occur at different layers of protocol stack of WSN. The security mechanisms used in traditional networks can not be applied directly, because of the constraints of sensor nodes such as limited energy, computation, and communication capabilities and their deployment in harsh environments. Efficient security mechanisms implemented in hardware plays a vital role in the design and development of WSN.

Jamming or Denial of Service (DoS) attacks are very common in WSN. Different types of jamming attacks like Constant, Deceptive, Random and Reactive jamming [6] [7] cause an inter- ference with normal radio signal reception. Various metrics are identified to efficiently detect constant jamming attacks including Packet Delivery Ratio, Energy, Distance, Packet Loss, Received Signal Strength, Noise Level and Carrier Sensing time [7] [11]. One of the most effective way to prevent jamming attack is the use of Spread Spectrum communication like DSSS, FHSS and hybrid form of these two. Other countermeasures against jamming include Regulated Transmitted Power, Ultra-wideband technology, Channel Surfing and the use of Directional antennas [7] [11].

This paper is organized to include an overview of jamming attacks in wireless sensor networks, experimental setup of a WSN to detect and defend jamming attack and its analysis. Section 2 gives a brief overview of constant jamming attacks, parameters used to detect this attack and various defensive measures avail- able. In Section 3, we discuss the network and attack model for conducting experiment, algorithm for detection and prevention of jamming attack and LabVIEW functions. Section 4 describes the experimental results and its analysis. Finally, concluding remarks are given in Section 5.

II. OVERVIEW OF JAMMING ATTACKS IN WSN

These type of attacks creates a forced interference with radio signals to disrupt the use of a communication channel. It is also termed as Denial of Service (DoS) attack and affects the availability of data. There are four types of jammers which affect a WSN - Constant, Deceptive, Random and Reactive Jammer. Jamming attack may occur at any layer of protocol stack of WSN. We consider physical layer attacks. Four types of jamming attacks can affect a WSN.

- Constant Jammer - During constant jamming attack the jammer emits continuous random radio signals into the wireless network and keeps the channel busy. Jammer will try to disrupting node communication or cause interference to nodes which have already started data transfers and corrupt their packets. This type of jammers have reduced energy efficiency.

- Deceptive Jammer - During deceptive jamming attack Con- tinuous regular packets are sent into wireless medium rather than sending random bits. Due to its regular packet structure it deceives other nodes to believe that a legal communication is happening and remain in receiving states while the jammer is on. This type of jammers also have reduced energy efficiency but can be easily implemented.

- Random Jammer - During random jamming attack either regular packets or random bits are send into wireless net- work. Compared to other jammers random jammers are more energy efficient due to its toggling capability between sleep and active states. Time periods between sleeping and jamming states are either fixed or random.

- Reactive Jammer - During Reactive jamming attack, mali- cious node monitors the channel activity and start sending jamming signals whenever a data transmission is observed. Energy efficiency of reactive jammers are low compared to random jammer due to its constant monitoring of the channels. However, it is very difficult to detect a reactive jammer due to its non-continuous ways.

A. Jamming Detection Techniques

Jamming attack detection in a wireless network is complicated. Sometimes it is difficult to distinguish jamming from the situa- tions like congestion and death of nodes. Various metrics can be used to detect jamming attacks in WSN and are as follows

- Packet Delivery Ratio - PDR is the ratio of total number of packets received successfully at sink node and total number of packets sent by the sensor node. We can compute the PDR of each node by coding the microcontroller at the sink node. PDR can be measured without any computational overhead.

- Energy - The residual energy calculations can be used to determine the transmission rate of a node. Although Direct and Prediction based approaches can be used, the overhead is much higher.

- Distance - Routing protocols can use the distance to a given destination path to detect jamming attack

- Packet Loss - The number of packets lost during a transmission

- Received Signal Strength - It is a measurement of the power present in a received radio signal

- Noise Level - The presence of unwanted data from malicious node can be used to detect jamming attack as well as to confirm the death of nodes

- Carrier Sensing time - If the network is jammed by a constant jammer, the channels will be busy all the time. Thus the channel sensing time used by sensor nodes can be used to detect jamming.

B. Countermeasures against Jamming

Various countermeasures are used to defend jamming attack. Some of them are listed below

- Spread Spectrum Communication - In Spread Spectrum modulation techniques, the Bandwidth of the transmitted signal is much higher than the bandwidth of the original message and is accomplished by the use of a Spreading code. It uses wide band, noise-like signals, which make it difficult to detect and jam compared to narrowband signals. Commonly used spread spectrum techniques are DSSS, FHSS and Hybrid form of these two.

- Regulated Transmitted Power - Sensor nodes are capable of changing their transmitting power

- Ultra-wideband technology - It is a recent research topic in which very short pulses are modulated and transmitted over a large spectrum of frequency bands.

- Channel Surfing - Channel surfing is a defensive measure for jamming attack in which the sink node or cluster heads informs all other nodes to switch to a secret frequency once jamming is detected.
- Directional antennas - Omni-directional antennas to accom- plish a directional communication.

III. PROPOSED SYSTEM

A. Network and Attack Model

We consider a single hop wireless sensor network with the nodes having limited battery power. The network contains differ- ent types of sensors. Each sensor node is uniquely identified by the sink node using an ID. The data from sensors are transmitted regularly to a sink node through an RF transmitter. The sink node receives data through a RF receiver and is connected to a PC through a wired channel. The data from sink node is acquired and processed using LabVIEW software and displayed on the PC. A malicious sensor node acts as a constant jammer that continuously emits radio signals to cause jamming. The block diagram of network model is shown in Fig. 1.

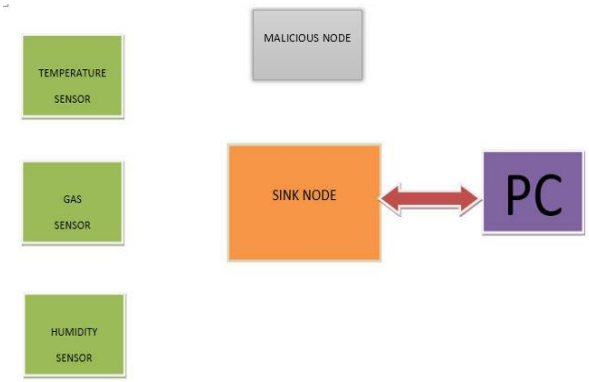

Fig. 1. Network Model

B. Proposed Framework

The proposed system consists of two functionalities - detecting and defending jamming attack. Our constant jammer continuously transmits a packet without sensing the channel. This type of attack substantially reduce the Packet Delivery Ratio and increases the overall noise level at the sink node. Our mechanism utilizes PDR value for jamming detection. Once the attack is detected, a Channel surfing technique is used to defend against it, by switching to a secret frequency. The proposed framework is shown in the flowchart shown in Fig. 2.

Jamming Detection

Our detection mechanism is based on Packet Delivery Ratio (PDR) of each sensor node.

– Packet Delivery Ratio (PDR)- PDR is the ratio of total number of packets received successfully at sink node and total number of packets sent by the sensor node. We can compute the PDR of each node by coding the microcontroller at the sink node. Once the network is jammed, the PDR of each node becomes 0. Thus the detection mechanism checks the PDR of all nodes at regular intervals and if it is 0, a jamming alarm is raised.

Defending Jamming Attack

– Channel Surfing - Channel surfing is a defensive mea- sure for jamming attack in which the sink node or cluster heads informs all other nodes to switch to a secret frequency once jamming is detected. It can be

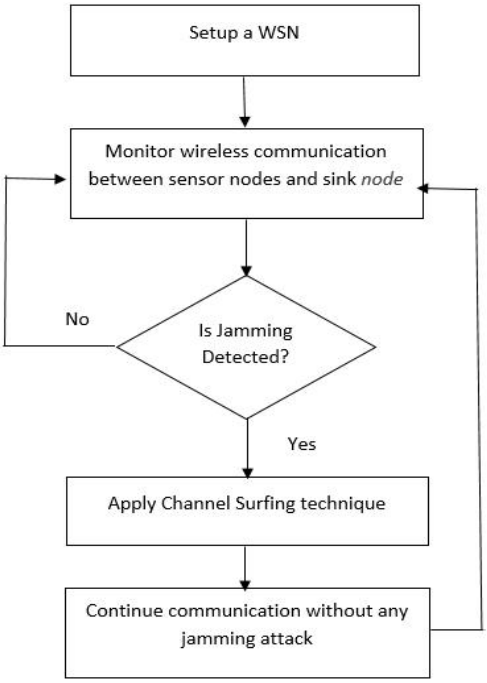

Fig. 2. Proposed Framework

considered as a low level implementation of FHSS (Frequency Hopping Spread Spectrum) in which the sensor nodes hops between multiple random frequencies during communication. The advantage is that switching is necessary only when jamming is detected, thus an efficient and fast jamming detection mechanism is re- quired. The problem arise when the adversaries could able to jam both of the network channels.

The flowchart for our jamming detection and defending mech- anism is shown in Fig. 3 and the algorithm is given below

Algorithm 1: Jamming Detection Algorithm

Step 1 : Monitor network communication between sensor nodes and sink node

Step 2 : Calculate PDR of each node at regular intervals at the sink node

Step 3 : If PDR of all nodes= 0 then goto Step 4 else goto Step 1

Step 4 : Display the alert message ”Some data break occurred” Step 5 : Display the message ”Switching Frequency” goto Step 1

C. LabVIEW Functions

The data acquisition from WSN and its analysis is done by using LabVIEW (Laboratory Virtual Instrument Engineering Workbench) [17]. LabVIEW from National Instruments (NI) is a system design, analysis and development environment for a visual programming language and are widely used for industrial automation. A data flow type, graphical programming language called G is used in LabVIEW. Graphical blocks define the execution structure. Programs/subroutines are called virtual instruments and has three components a front, a back and a connector panel. The front panel are designed using indicators and controls. Controls act as inputs for the VI and Indicators act as the outputs of VI. The back panel contains the graphical block diagram consisting of multiple VIs. All the objects kept on the front panel will

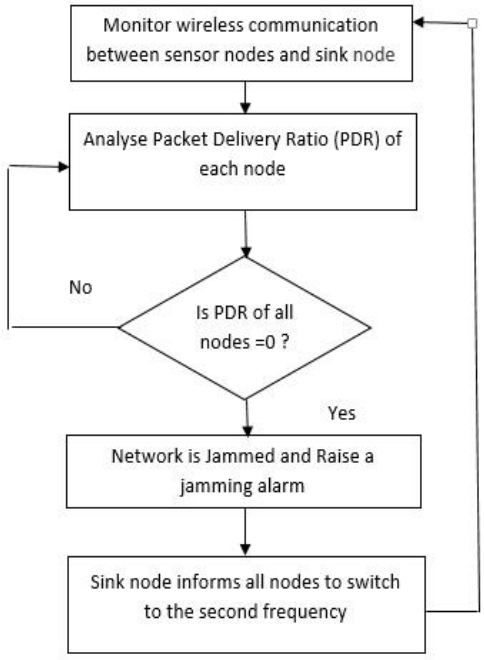

Fig. 3. Jamming Detection and defending mechanism

be displayed as a terminal on the back panel. The back panel containing structures and functions performing operations on controls and supply data to indicators. The following functions are implemented using LabVIEW as shown in Fig. 4.

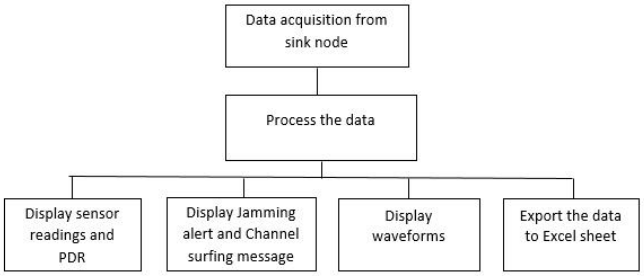

Fig. 4. LabVIEW Functions

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A WSN testbed is created with three sensor nodes, one sink node and two malicious node. All the nodes can communicate using two different frequencies through two different channels- a 433MHz channel and a 2.4 GHz channel. Three different types of sensors are used - one temperature sensor (LM35), one gas sensor (MQ5) and one humidity sensor (SY-HS-220). Each sensor node contains a Microcontroller, Transceiver, sensor and a power supply. In our project we use PIC 16F886 microcontroller. The microcontroller of sensor nodes are programmed in Embedded C using MPLAB IDE. The microcontroller programs are tested using Proteus simulation. The data from sensors are transmitted to a sink node through an RF transmitter. We use two constant jammers, one operates in 2.4 GHz frequency and the other in 433Mhz frequency. The indicators for channel selection, Trans- mission, reception plus manual resetting and channel selection is also provided in the circuit. The hardware setup is shown in Fig. 5.

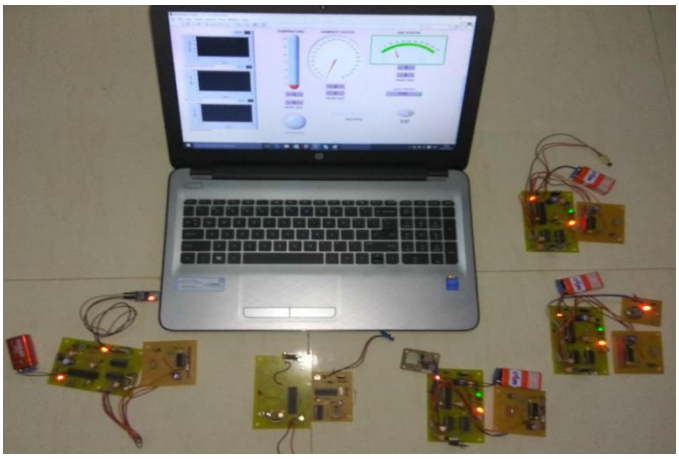

Fig. 5. Hardware setup of sensor network

The sink node receives data through a RF receiver and is connected to a PC through a wired channel. RS232 ethernet cable is used for serial communication. The data from sink node is acquired and processed using LabVIEW software and displayed on the PC. The VISA (Visual Instrumentation Soft- ware Architecture) tool kit enables LabVIEW to perform serial communication. The front panel displays the sensor readings, PDR and the appropriate waveforms. The sensor readings are uniquely identified using a ID such as T for temperature sensor, G for gas sensor and H for humidity sensor. These sensor values are displayed on corresponding front panel indicators. The PDR values that are computed and send by the sink node are also displayed in LabVIEW. Whenever the network gets jammed it is indicated as a red alert in the front panel. Our front panel in LabVIEW is given in Fig. 6.

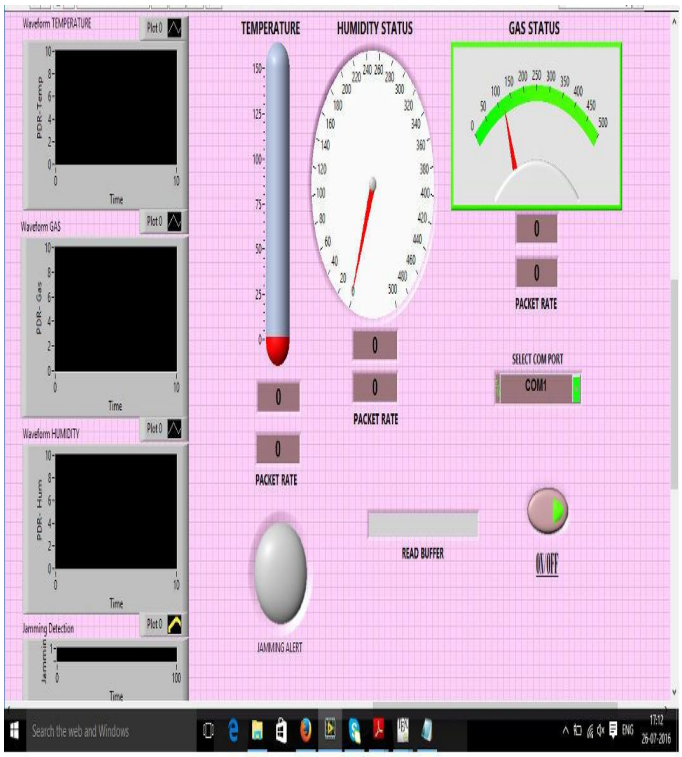

Fig. 6. Front Panel in LabVIEW

The entire processing steps are coded as a graphical block diagram in LabVIEW and is shown in Fig. 7.

The sensors reads the environmental temperature, humidity and presence of gas, and the voltage corresponding to this analog signal is given to a microcontroller. The Analog to Digital Converter in the microcontroller converts this voltage to a digital value, which is modulated and transmitted by a Transceiver.

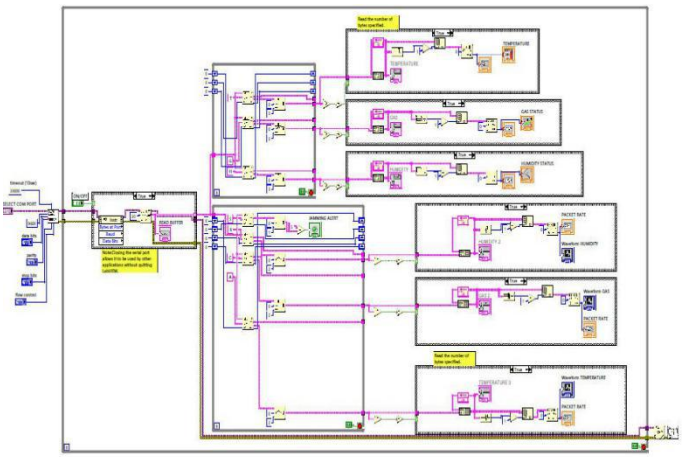

Fig. 7. Block Diagram in LabVIEW

The sink node receives all these data and communicates with LabVIEW through the ethernet port. Under normal condition, without any malicious node the sensor readings displayed on PC are shown in Fig. 8.

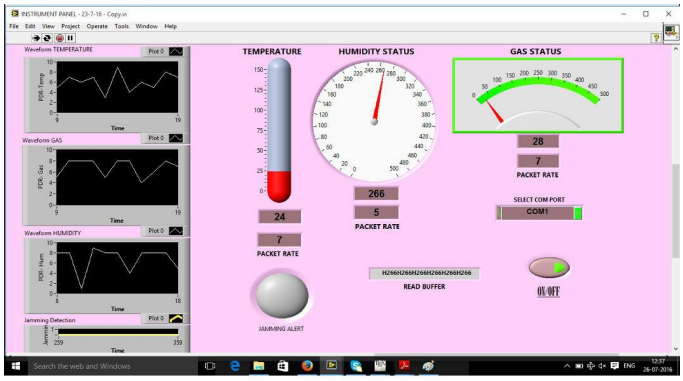

Fig. 8. Sensor readings under Normal condition

As soon as the malicious node is turned on, the communication from other nodes are disrupted and PDR becomes 0. This factor can be used to ensure that a jamming attack has occurred. The sink node calculates the PDR of each node at regular intervals which is sent to the labview for display and analysis. There is a possibility of death of all nodes in the network so that no data is received at sink node which results in a toggling state between two frequencies. A message ”Some data break occurred” is sent to the read buffer in labVIEW to indicate the jamming attack. A red LED Indication is also given and these are shown in Fig. 9. Whenever jamming is detected, the sink informs all other nodes in the network to switch to the second frequency. The sensor nodes in our network supports two frequencies so that whenever the first frequency is jammed, it switches to second frequency and vice versa. The channel switching is indicated in the circuit with the help of LEDs and a message ”switching channel” is displayed in LabVIEW. This scenario is shown in Fig. 10.

The PDR values received at regular intervals as well as the jamming detection points are plotted in a waveform chart as shown in Fig. 11. The first graph shows the values under normal working condition, second graph shows the jamming condition and third graph shows the condition when PDR of two nodes

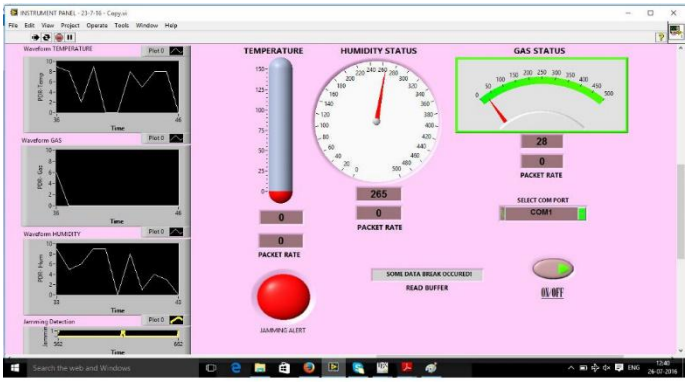

Fig. 9. Jamming Detection message in LabVIEW

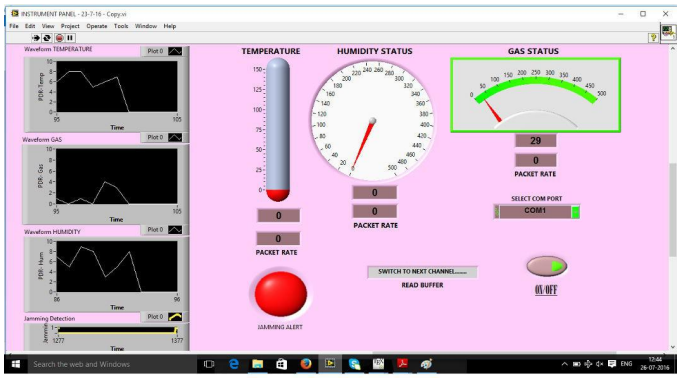

Fig. 10. Channel Surfing message in LabVIEW

equals 0. The values from each graph are exported to Excel sheets for future analysis.

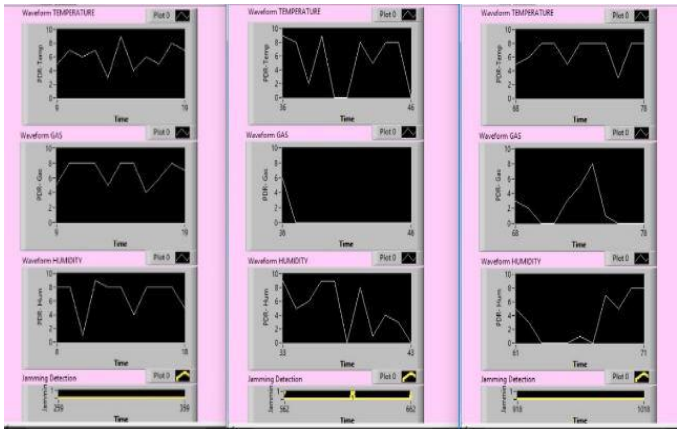

Fig. 11. Waveform charts displayed in LabVIEW

V. CONCLUSION

Present day engineers are looking for new and promising applications using wireless sensor networks with unprecedented security threats. These challenging networks can only be devel- oped with improved security mechanisms. This paper discussed the experimental setup of a WSN to detect and defend constant jamming attack. An effective security mechanism to prevent all types of jamming attacks has to be developed for future WSN.

ACKNOWLEDGMENT

The author would like to thank the Project guide Mr. Madhu K P, Assistant Professor, Department of Computer Science and Engineering, Govt. College of Engineering, Wayanad for valuable help and support.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ”A survey on sensor networks”, IEEE Communication Magazine, Aug 2002.

[2] David Culler, Deborah Estrin, ”Overview of sensor networks”, IEEE Com- puter Society, 2004.

[3] Dr. Shahriar Mohammadi and Hossein Jadidoleslamy, ”A comparison of physical attacks on wsn”, International Journal of Peer to Peer Networks, April 2011.

[4] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, ”A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International Journal of Computer Science and Information Security, Vol 4, No 1 and 2, 2009.

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudharyi, ”Wireless sensor network security: A survey”, Security in Distributed, Grid, and Pervasive Computing, 2006.

[6] Nadeem Sufyan, Nazar Abbass Saqib and Muhammad Zia, ”Detection of jamming attacks in 802.11b wireless networks”, EURASIP Journal on Wireless Communications and Networking, 2013.

[7] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou, ”A Survey on Jamming Attacks and Countermea- sures in WSNs”, IEEE Communications Surveys and Tutorials , 2009.

[8] Mohamed Lamine Messai, ”Classification of Attacks in Wireless Sensor Networks”, International Congress on Telecommunication and Application, April 2014.

[9] Abdul Wahid , Pavan Kumar, ”A survey on attacks, challenges and security mechanisms in wireless sensor network”, International Journal for Innovative Research in Science and Technology, January 2015.

[10] Shikha Jindal and Raman Maini, ”An Efficient Technique for Detection of Flooding and Jamming Attacks in Wireless Sensor Networks”, International Journal of Computer Applications, Volume 98 No.10, July 2014

[11] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang, ”Jamming Sensor Networks: Attack and Defense Strategies”, IEEE Network, May-June 2006

[12] Pritee V. Nikam and K. Sujatha, ”LabVIEW based real time data monitoring and control system”, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 12, December 2015

[13] http://pdf1.alldatasheet.com/datasheet-pdf/view/8866/NSC/LM35.html

[14] http://www.dfrobot.com/image/data/SEN0130/MQ-5.pdf

[15] https://www.foxytronics.com/files/file/80-hr202-humidity-sensor-datasheet

[16] http://extremeelectronics.co.in/microchip-pic-tutorials

[17] http://www.ni.com/labview