International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-1, 2019

ISSN: 2581-3404 (Online)

Performance Analysis for the Malicious Attacks in Wireless Sensor Network

Yogendra Kumar Mishra[1], Prof. Jitendra Mishra[2]

[1]M. Tech Scholar, Department of EC, PCST, Bhopal (India)

[2]Head & Professor, Department of EC, PCST, Bhopal (India)

[1]yogendramishra782@gmail.com, [2]jitendramishra@gmail.com

ABSTRACT

Wireless ad-hoc sensor networks have recently emerged as a premier research topic. They have great long-term economic potential, ability to transform our lives and pose many new system-building challenges. Sensor networks pose a number of new conceptual and optimization problems such as location, deployment and tracking in that many applications rely on them for needed information. In this paper we present the comparative performance analysis for the wireless sensor networks using existing and presents techniques for the robustness and reduce the attack in network.

Keywords: Wireless sensor networks, Attack, Fault detection, denial of services, Mobile ad-hoc networks.

INTRODUCTION

A wireless sensor network (WSN) is a wireless network that consists of distributed sensor nodes that monitor specific physical or environmental events or phenomena, such as temperature, sound, vibration, pressure, or motion, at different locations [2]. The first development of WSN was first motivated by military purposes in order to do battlefield surveillance. Nowadays, new technologies have reduced the size, cost and power of these sensor nodes besides the development of wireless interfaces making the WSN one of the hottest topics of wireless communication [4-5].

There are four basic components in any WSN: (1) a group of distributed sensor nodes; (2) an interconnecting wireless network; (3) a gathering-information base station(Sink); (4) a set of computing devices at the base station (or beyond) to interpret and analyze the received data from the nodes; sometimes the computing is done through the network itself [2].

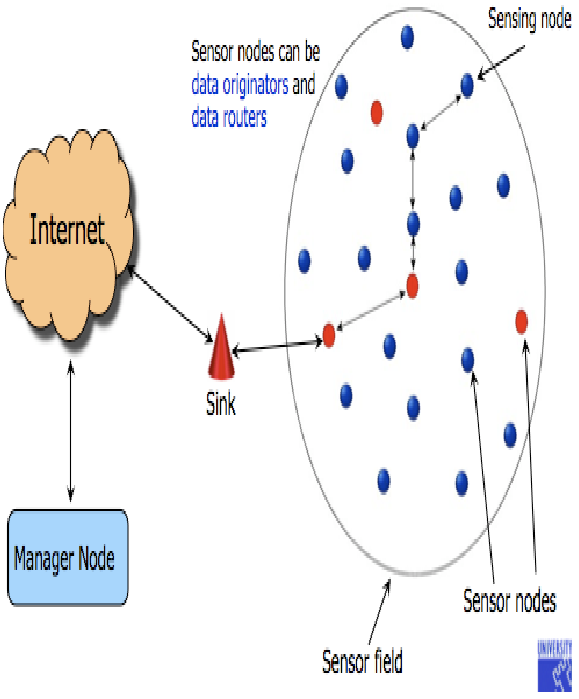


Fig 1: Overview of wireless sensor networks.

Sensor nodes, as mention earlier, are low-cost and low-power devices used to accumulate the desired data and forward it to the base station. A sensor node is composed of four parts, the nodes are equipped with a sensing unit, a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery, some sensor nodes have an additional memory component [11].

Functionality of sensor nodes lies behind the ability of the node to either being the source of the data (i.e. senses the event) then transmits it, or just being a pure transceiver that received data from other sources then forwards it to other nodes in order to reach the base station. Actually, this functionality depends on the network architecture that depends in turn on the application. Fig.2 shows different available sensor nodes in the market followed by Table1 showing the specifications for each node [6].

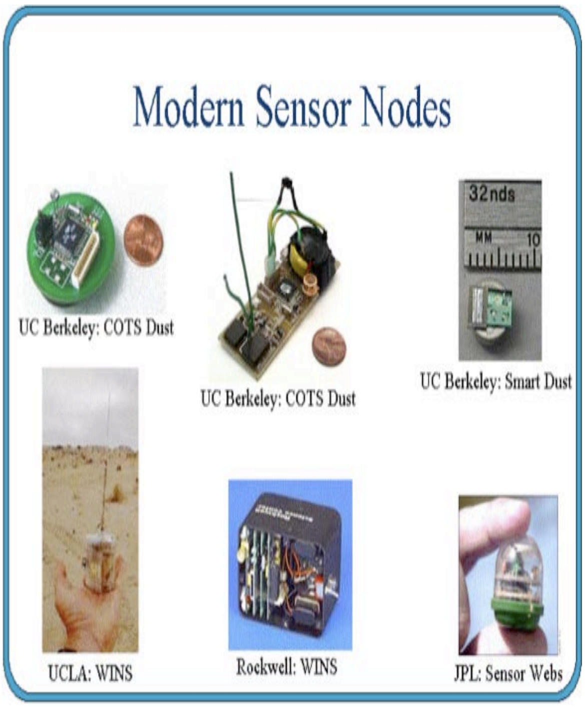


Fig 2: List of sensor nodes.

The rest of this paper is organized as follows in the first section we describe an introduction of about the wireless sensor network. In section II we discuss about the various number of wireless sensor network application, In section III we discuss about the various element in sensor nodes. In section IV we discuss about the proposed experimental results, finally in section V we conclude the about our paper.

II APPLICATION OF WSN

The applications for WSNs are many and varied. They are used in commercial and industrial applications to monitor data that would be difficult or expensive to monitor using wired sensors. They could be deployed in wilderness areas, where they would remain for many years (monitoring some environmental variable) without the need to recharge/replace their power supplies. They could form a perimeter about a property and monitor the progression of intruders (passing information from one node to the next). There are a many uses for WSNs.

Typical applications of WSNs include monitoring, tracking, and controlling. Some of the specific applications are habitat monitoring, object tracking, nuclear reactor controlling, fire detection, traffic monitoring, etc. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes.

- Environmental monitoring
- Habitat monitoring
- Acoustic detection
- Seismic Detection
- Military surveillance
- Inventory tracking
- Medical monitoring
- Smart spaces
- Process Monitoring

III SENSOR NODE ELEMENT

Each sensor node is a device which has a transceiver, a microcontroller, and a sensitive element. Usually sensor node is an autonomous device. Each sensor node in WSN measures some physical conditions, such as temperature, humidity, pressure, vibration, and converts them into digital data. Sensor node can also process and store measured data before transmission. Network sink is a kind of a sensor node which aggregates useful data from other sensor nodes. As a rule, network sink has a stationary power source and is connected to a *server* which is processing data received from WSN. Such connection is implemented directly, if server and WSN are placed on the same object. If it is necessary to provide a remote access to WSN, network sink also functions as a gate, and it is possible to interact with WSN through global network such as the Internet.

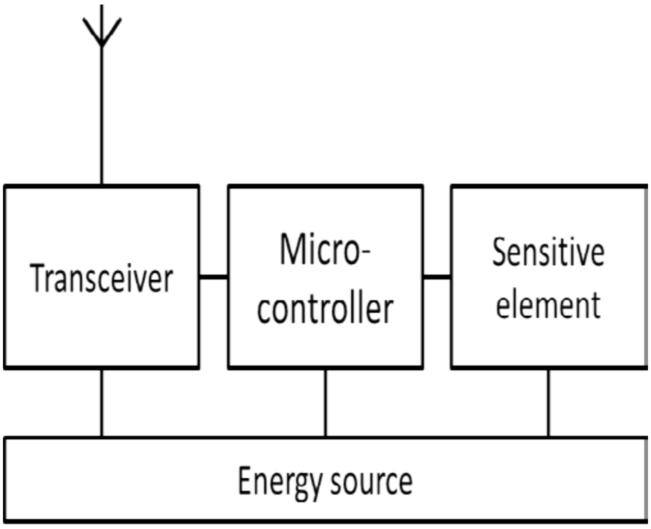


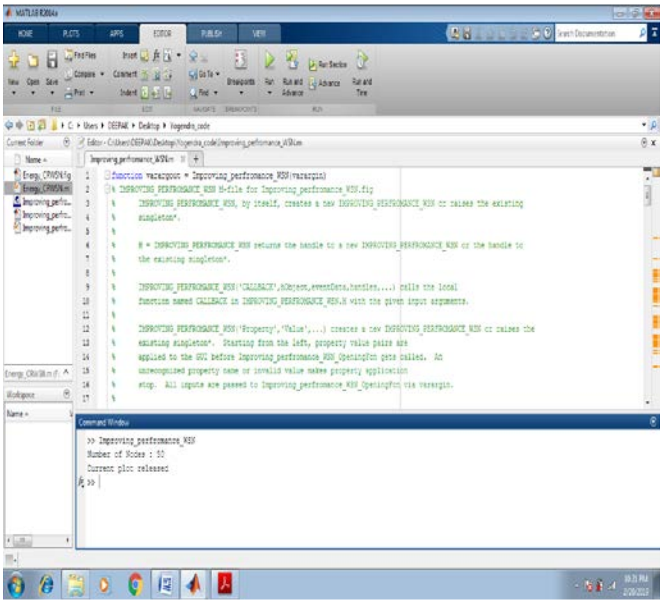
Fig 3: Sensor node inner structure.

In WSNs communication is implemented through wireless transmission channel using low power transceivers of sensor nodes. Communication range of such transceivers is set up in the first place for reasons of energy efficiency and density of nodes spatial disposition, and, as a rule of thumb, this quantity is about a few dozens meters. Sensor node’s transceiver has limited energy content, and this fact makes it impossible for the most spatially remote sensor nodes to transmit their data directly to the sink. So, in WSN every sensor node transmits its data only to a few nearest sensor nodes which, in turn, retransmit those data to theirs nearest sensor nodes and so on. As a result, after a lot of retransmissions data from all the sensor nodes reach the network sink.

IV EXPERIMENTAL RESULT ANALYSIS

The limited capabilities of a sensor node, such as restricted processing capabilities and a limited amount of energy, have an impact on all the parameters of a WSN. Taking into account the energy characteristics of transmitters in sensor nodes and their high susceptibility to interference, the quality of communication between sensor nodes can vary significantly with time. That is why the information loss and substantial delays often occur in wireless sensor networks. Providing security from attackers is a very important task in the field of wireless sensor networks, as well as in every computer network. Successful security problem solving defines if one or other technology will be used for crucial tasks or its applications will be used in laboratory researches and high-tech entertainment only.

In this section we proposed a new scheme for the wireless sensor network to improve the robustness in network topology, here our proposed scheme gives better results than the existing techniques, and shows that the reduce number of malicious attack. A number of WSN peculiarities complicate the task of security providing. A part of these peculiarities deals with the physical level of WSNs. Data transmission via radio makes it possible for a attacker to capture transmitted information (eavesdropping), to misrepresent it (man-in-the-middle attacks), to disable the whole network or a part of it (denial-of-service, DoS attacks).



```
function varargout = Improving_perfromance_WSN(varargin)
% IMPROVING_PERFROMANCE_WSN M-file for Improving_perfromance_WSN.fig
%      IMPROVING_PERFROMANCE_WSN, by itself, creates a new IMPROVING_PERFROMANCE_WSN or raises the existing
%      singleton*.
%
%      H = IMPROVING_PERFROMANCE_WSN returns the handle to a new IMPROVING_PERFROMANCE_WSN or the handle to
%      the existing singleton*.
%
%      IMPROVING_PERFROMANCE_WSN('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in IMPROVING_PERFROMANCE_WSN.M with the given input arguments.
%
%      IMPROVING_PERFROMANCE_WSN('Property','Value',...) creates a new IMPROVING_PERFROMANCE_WSN or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before Improving_perfromance_WSN_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to Improving_perfromance_WSN_OpeningFcn via varargin.
%
```

```
>> Improving_perfromance_WSN
Number of Nodes : 50
Current plot released
>>
```

Fig 4: Shows that the simulation enviornemnt window.

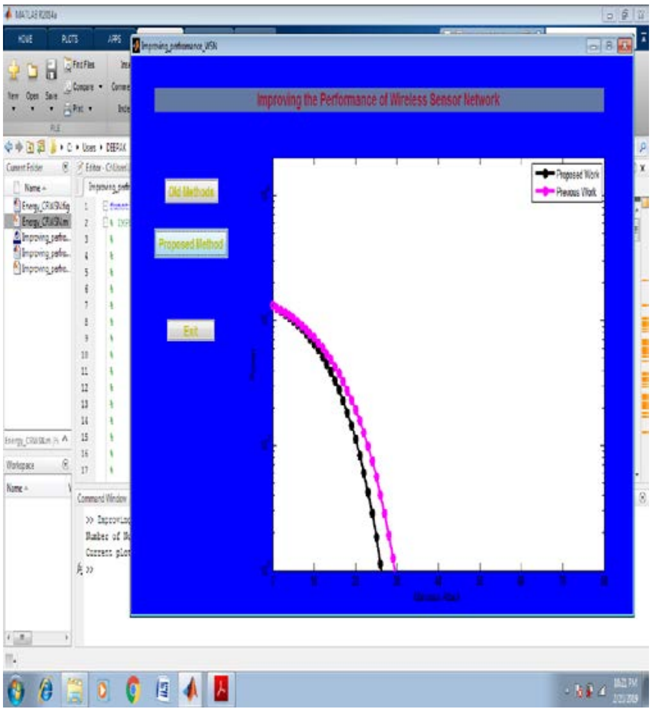

Improving_perfromance_WSN
Improving the Performance of Wireless Sensor Network
Old Methods
Proposed Method
Exit
Proposed Work
Previous Work

Fig 5: Shows that the comparative result performacne simulation enviornemnt window for th emalicious attack.

V CONCLUSIONS AND FUTURE SCOPE

In the foreseeable future sensor networks have wide applicability from Observing scientific phenomenon to use in various sector such as agricultural monitors and warehouse inventory management. WSNs a number of probe devices are distributed throughout a geographic region to observe local scientific conditions. In addition to sensors, probes are equipped with computational resources for in-network data processing, as well as wireless transceivers for communication with neighboring probes. Here we presents the comparative performance for malicious attack and improve the performance of network.

REFERENCES:-

[1] Tie Qiu, Aoyang Zhao, Feng Xia, Weisheng Si, Dapeng Oliver Wu, "ROSE: Robustness Strategy for Scale-Free Wireless Sensor Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 25, NO. 5, OCTOBER 2017, pp 2944-2960.

[2] Xuxun Liu, "Node Deployment Based on Extra Path Creation for Wireless Sensor Networks on Mountain Roads", IEEE COMMUNICATIONS LETTERS, VOL. 21, NO. 11, NOVEMBER 2017, pp 2376-2381.

[3] Nengsong Peng, Weiwei Zhang, Hongfei Ling, Yuzhao Zhang, Lixin Zheng, "Fault-Tolerant Anomaly Detection Method in Wireless Sensor Networks", Licensee MDPI, Basel, Switzerland, 2018. Pp 1-16.

[4] Yong Cheng, Qiuyue Liu, JunWang, ShaohuaWan , Tariq Umer, "Distributed Fault Detection for Wireless Sensor Networks Based on Support Vector Regression", Hindawi Wireless Communications and Mobile Computing Volume 2018, pp 1-9.

[5] Yaqiang Zhang, Zhenhua Wang, Lin Meng, Zhangbing Zhou, "Boundary Region Detection for Continuous Objects in Wireless Sensor Networks", Hindawi Wireless Communications and Mobile Computing Volume 2018, pp 1-14.

[6] XUXUN LIU, “Routing Protocols Based on Ant Colony Optimization in Wireless Sensor Networks: A Survey”, IEEE volume-5, 2015. pp 26303-26317.

[7] Nan Ding , Huanbo Gao, Hongyu Bu, Haoxuan Ma, Huaiwei Si, “Multivariate-Time-Series-Driven Real-time Anomaly Detection Based on Bayesian Network”, Licensee MDPI, Basel, Switzerland, 2018. pp 1-13.

[8] YAO YU, LEI GUO, JINLI HUANG, FENGYAN ZHANG, AND YUE ZONG, “A Cross-Layer Security Monitoring Selection Algorithm Based on Traffic Prediction”, IEEE Access volume-6, 2018. pp 35382-35391.

[9] ZHANGBING ZHOU, JIABEI XU, ZHENJIANG ZHANG, FEI LEI, AND WEI FANG, “Energy-Efficient Optimization for Concurrent Compositions of WSN Services”, IEEE Access, volume-5, 2017. pp 19994-20008.

[10] Tarek AlSkaif, Boris Bellalta, Manel Guerrero Zapata, Jose M. Barcelo Ordinas, “Energy Efficiency of MAC Protocols in Low Data Rate Wireless Multimedia Sensor Networks: A Comparative Study”, Preprint submitted to Journal of Ad Hoc Networks, 2016. Pp 1-19.

[11] T.R.Saravanan, M. Jayapriya, M.Gayathri, “A wireless sensor application for energy management in home appliances using smart”, International Research Journal of Engineering and Technology, Vol-5, 2018. Pp 1218-1224.

[12] Anzar Mahmood, NadeemJavaid, SohailRazzaq, “A review of wireless communications for smart grid”, Elsevier ltd. 2015. Pp 248-260.

[13] Edoardo Patti, Angeliki Lydia Antonia Syrri, Marco Jahn, Pierluigi Mancarella, Andrea Acquaviva, Enrico Macii, “Distributed Software Infrastructure for General Purpose Services in Smart Grid”, IEEE, 2016. Pp 1156-1163.

[14] German C. Madueno, Jimmy J. Nielsen, Dong Min Kim, Nuno K. Pratas, Cedomir Stefanovic, Petar Popovski, “Assessment of LTE Wireless Access for Monitoring of Energy Distribution in the Smart Grid”, 2015. Pp 1-33.

Yogendra Kumar Mishra received his Bachelor`s degree in Electronics & comunication Engineering, from PCRT, Bhopal M.P. in 2015. Currently he is pursuing Master of Technology Degree in Electronics & comunication (Digital communication) from PCST, (RGPV), Bhopal, Madhya Pradesh India. His research area include Wireless sesnor networks.

Mr. **Jitendra Kumar Mishra** he is Associate Professor and Head of the Department of Electronics and Communication Engineering in PCST, Bhopal (RGPV). His received Master of Technology and Bachelor’s of engineering respectively in Digital communication from BUIT, Bhopal and from RGPV, Bhopal. He has more than 10 years of teaching experience and publish 30+ papers in International journals, conferences etc. His areas of Interests are Antenna & Wave Propagation, Digital Signal Processing, Wireless Communication, Wireless Sensor Networks etc.