ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Design and Implementation of Data Flow Routing With Energy Optimization under Different Attacks in WSN

Leena Rani[1], Er.Veena Rani[2]

Research Scholar, Department of ECE, JCDM Collage of Engineering, Sirsa, Haryana India

Assistant Professor, Department of ECE, JCDM Collage of Engineering, Sirsa, Haryana India

ABSTRACT: Wireless sensor networks (WSNs) deal with the major issue of energy limitation in their deployments. In this paper, we presents a data flow routing under various attacks in WSN. It also presents energy optimization scheme under clustering of nodes. The main attacks covered here are misdirection attack, worm hole attack and flooding attack etc. Sensor nodes are disposed to to failure due to energy reduction and their placement in an uncontrolled or even antagonistic environment. Simulation results will establish that the improved proposed scheme performs well in the above situation and increase the attack handling accuracy by using the new approach and reduce energy consumption. It also shows that proposed scheme improves the throughput value. The projected mechanism is implemented with MATLAB

KEYWORDS: Shortest Routing, path in Networks,wireless sensor networks, faults detection and recovery.

I. INTRODUCTION

Wireless Sensor Networks have seen tremendous advantages and utilization in the past two decades. These sensors with each other to sense some physical phenomenon and then information gathered is processed to get relevant results. They consist of protocols and algorithms with self organizing capabilities. Wireless sensor networks mainly use broadcast communication while Ad-hoc networks use point to point communication. Unlike Ad-hoc wireless sensor networks are limited by sensors limited power, energy and computational capability. Sensor nodes may not have Global ID because of large amount of overhead and large no. of sensors [1].

The applications of Wireless Sensor Networks can be divided in three categories: (a) monitoring of objects (b)monitoring of an area (c)monitoring of both area and objects. Monitoring of an object of Structural Monitoring, ECO Physiology, Condition based maintenance, Medical diagnostics etc. Monitoring area consists of Environmental and Habitat monitoring, precision agriculture, Indoor climate control, Military surveillance, Treaty verification, intelligent alarms etc.

Sensing is a technique used to gather information about a physical object or process, including the occurrence of events (i.e., changes in state such as a drop in temperature or pressure). An object performing such a detecting task is called a sensor. For instance, human body is equipped with sensors that are able to capture optical information from the environment (eyes), acoustic information such as sounds (ears), and smells (nose). These are examples of remote sensors, that is, they don't need to trace monitored object to gather information. From a practical perception, a sensor is a device that translates parameters or events in the physical world into signals that can be measured or analysed. Another commonly used term is transducer, which is often used to define a device that converts energy from one form to another [2].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

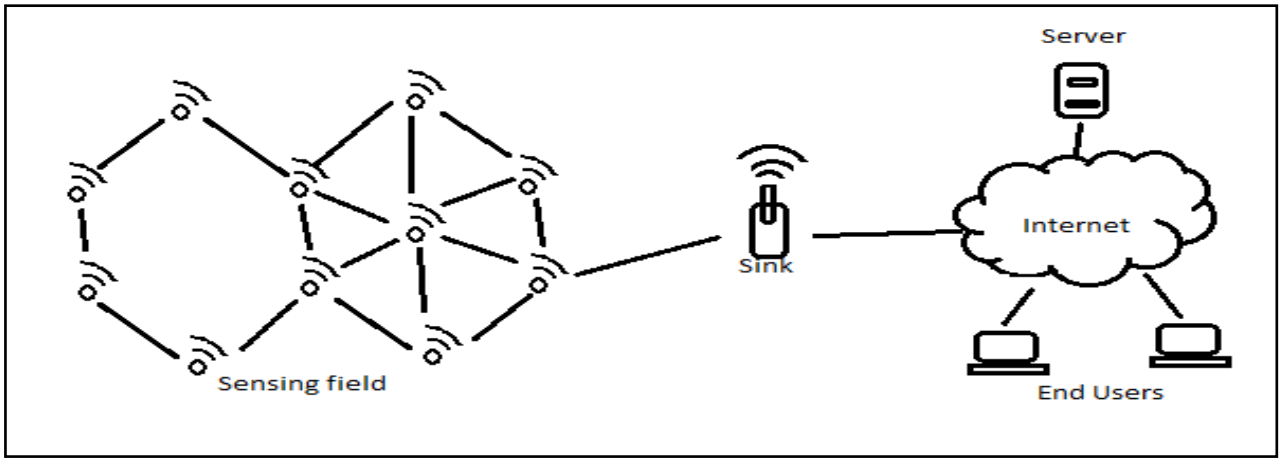

Figure 1: Wireless Sensor Architecture [1]

The development of sensor networks requires technologies from three different research zones: sensing, communication and computiong (as well as hardware, software, procedures). Thus, combined and separate progressions in each of these areas have driven investigation in sensor networks. Examples of early sensor networks comprise the radar networks used in air traffic regulator. The national power grid, with its numerous sensors can be viewed as one large sensor system. These systems were recognized computers and communication capabilities, and before the term "sensor networks" came into vogue[5].

The capabilities of sensor networks like self organization, rapid deployment and fault tolerance can make them an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting (C4ISRT). Some of the military applications include battlefield surveillance, battle demand assessment, reconnaissance of opposing forces and terrain and nuclear, biological and chemical attack detection.

The paper is ordered as follows. In section II, we discuss correlated work with wireless sensor networks. In setion III, It defines system architecture, routing techniques. In section IV, it describes proposed work of fault management system. After this, it designates the main results of this system. Finally, conclusion is explained in section VI.

FAULT TOLERANCE IN WSN

Generally, operation of WSN involves communication between sensor node and base station. The sensor node senses environment, perform some computation (if required) and report gathered information to the base station. If base station is connected with some actuator which triggers the alarm for human intervention in case of an event of interest [4]. Fault-tolerance is the quality or ability of a functional unit to perform a required task in the presence of some number of faults. Fault-tolerance is applied to increase the reliability of a system. Some expand the domain of the topic to dependability which encompasses availability, reliability, safety, integrity and maintainability [4].

A. Sources of Faults

At least two components of a sensor node, sensors and actuators, will directly interact with the environment and will be subject to a variety of physical, chemical, and biological forces. Therefore, they will have significantly lower intrinsic reliability than integrated circuits in fully enclosed packaging. In enterprise scenarios it becomes highly important to hide the details of the underlying sensor networks from the applications and to guarantee a minimum level of the system. One of the challenges faced to achieve this level of reliability is to overcome the failures frequently faced by sensor networks due to their tight integration with the environment. Failures can generate false information, which may trigger incorrect business processes, resulting in additional costs.

Sensor networks are inherently fault prone due to the shared wireless communication medium: message losses and corruption (due to fading, collision, and hidden node effect) are the norm rather than exception. Moreover, node failure (due to crash and energy exhaustion) are the comman place. They are also prone to failure due to hardware failure,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

communication link errors, malicious, malicious attack, and so on. Thus sensor nodes can lose synchrony and their programs can reach arbitrary states. Since on-site maintenance is not feasible, sensor network applications shoul be local and communication-efficient self healing.

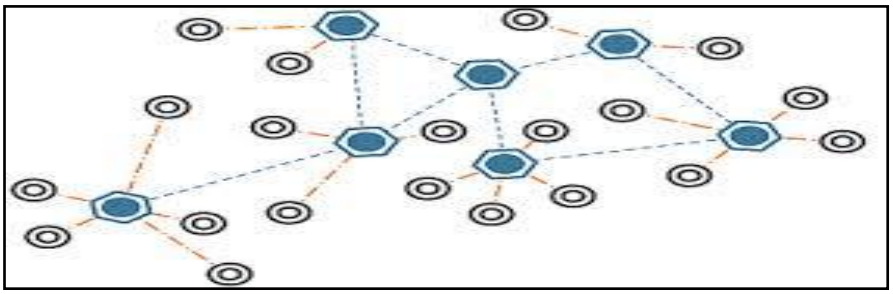

FIGURE 2: Wireless Sensor Network

Maintenance of continuous connectivity in a wireless sensor network after it is deployed in a hostile environment ia also a major issue. Constrained by the low user to node ratio, limited energy and bandwidth resources, entities that are usually mobile, networks without fixed infrastructure and frequent failure due to problems of energy, vulnerability to attack etc, a need for wireless sensor networks to be self-organizing and self-configuring so as to improve performance, increase energy efficiency, save resources and reduce data transmission arises. Data delivery in sensor networks is inherently faulty and unpredictable. Failures in wireless sensor networks can occur for various reasons. First, sensor nodes are fragile, and they may fail due to depletion of batteries or destruction by an external event. In addition nodes may capture and communicate incorrect readings because of environmental influence on their sensing components.

B. Need of Fault Tolerant Protocols

Sensor netwirs share comman failure issues (such as link failures and congestion) with traditional distributed wired and wireless networks, as well as introduce new fault sources (such as node failures). Fault tolerant techniques for distributed systems include tools that have become industry standard such as SNMP and TCP/IP, as well as more specialized and/or more efficient methods that have been extensively reseached. The faults in sensor networks can not be approached in the same way as in traditional wired or wireless networks due to the following reasons: Traditional network protocols are generally not concerned with energy consumption, since wirednetworks are constantly powered and wireless Ad-hoc devices can get rechaeged regularly;

- Traditional networks protocols aim to achieve point-to-point reliability, whereas wireless sensor networks are concerned with reliable event detection;
- In sensor networks, node failures occur much more frequently than in wired, where servers, routers, and client machines are assumed to operate normally most of the time;this iplies that closer monitoring of node health without incurringsignificant overhead is needed;
- Traditional wireless network protocols rely on functional MAC layer protocols that avoid packet collisions, hidden terminal problem,and channel errors by using physical carrier sense (RTS/CTS) and virtual carrier sense (monitoring the channel).

C. Different Attacks in WSN

Some routing protocols in WSN require nodes to broadcast hello messages to announce themselves to their neighbours. A node which receives such a message may assume that it is within a radio range of the sendor. However in some cases this assumption may be false;sometimes a laptop-class attacke broadcasting routing or other information with large enough transmission power could convince every other node in the network that the attacker is its neighbour.

In the wormwhole attack, an attacker tunnels messages received in one part of the network over a low latency link and replays them in a different part of the network. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

For instance in reactive routing protocols such as AODV or DSR , the attackers can tunnel each route request RREQ packet to another attacker which near to destination node of the RREQ. When the neighbours of the destination hear this RREQ , they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process.

Misdirection attack can be performed in different ways: Packets forwarded to a node close to the actual destination. This kind of misdirection attack is less intense, because packets reach to a node close to the actual destination. It's very harmful because all packets are forwarded to a node far away, preventing them to reach the destination so packets will not reach destination.

Intermediate node becomes selfish node. Here a node in the transmission path will behave selfishly and not forward the message packet to the actual destination. Thus here also the delay will be higher and throughput will be decrease. If packets forwarded to a node close to the destination then Predicted delay= Normal delay + Change in delay, Throughput predicted= Normal throughput – Change in throughput [12].

II. RELATED WORK

In this work, it presents data flow routing under various attacks with shortest path. It also covers energy optimization with clustering of nodes. As presented, the network fails due to the depletion of energy in the central ring of nodes around the sink node, leaving the sink node segmented from the remaining viable network nodes. With the existing protocol, at the extinction of the network (when the sink is isolated from the remaining live network nodes), the remaining energy is effectively consumed with zero efficiency because it is no longer available for useful work which negates the premise that their approach minimizes energy consumption within the network.

Two issues have been presented related to the proposed class of WSN. The first is the clear and consistent use of terminology with respect to Fault-Tolerant (FT) and WSN in general. This work addresses this shortcoming by defining the relevant terms of fault-tolerance, reliability, and dependability within the context of WSN. The second issue is specific to a class of WSN and deals with the depletion energy around the sink protocol. Then, a modified protocol is proposed to instill fault-tolerance into the network in response to network degradation. The Proposed protocol, in conjunction with the characterization of the remaining network energy, seeks to extend the useful life of the network, increasing efficiency in terms of energy expended, minimizing residual energy after network extinction.Fault detection is the first phase of fault management, where an unexpected failure should be properly identified by the network system. Centralized approach is a common solution to identify and localize the cause of failures or suspicious nodes in WSNs. Usually, a geographically or logically centralized sensor node takes responsibility for monitoring and tracing failed or misbehaviour nodes in the network. Most these approaches consider the central node has unlimited resources (e.g. energy) and is able to execute a wide range of fault management maintenance. They also believe the network lifetime can be extended if complex management work and message transmission can be shifted onto the central node. The central node normally adopts an active detection model to retrieve states of the network performance and individual sensor nodes by periodically injecting requests (or queries) into the network. It analyzes this information to identify and localize the failed or suspicious nodes. Distributed approach encourages the concept of local decision-making, which evenly distributes fault management into the network. The goal of it is to allow a node to make certain levels of decision before communicating with the central node. It believes the more decision a sensor can make, the less information needs to be delivered to the central node.

Failure detection via neighbour coordination is another example of fault management distribution. Nodes coordinate with their neighbours to detect and identify the network faults (i.e. suspicious node or abnormal sensor readings) before consulting with the central node. For example, in a decentralized fault diagnosis system, a sensor node can execute a localized diagnosis algorithm in steps to identify the causes of a fault.Clustering has become an emerging technology for building scalable and energy balanced applications for WSNs. Some derive an efficient failure detection solution using a cluster-based communication hierarchy to achieve scalability, completeness, and accuracy simultaneously. They split the entire network into different clusters and subsequently distribute fault management into each individual region. Intra-cluster heartbeat diffusion is adopted to identify failed nodes in each cluster.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

III. PROPOSED ALGORITHM

The sensor nodes may be deployed in harsh or hostile environments leaving the nodes potentially vulnerable to environmentally induced failure or attack. As a result, sensor nodes may be easily damaged or depleted of energy altering the network topology and fragmenting routing paths. This dynamic characteristic of the network is especially critical to routing protocols where energy is lost in transmitting along failed routing paths. As noted above, sensor nodes are not readily replaced or recharged and hence the networks and employed protocols must complete their objectives in the presence of one or more failed nodes. This clearly establishes the value of employing mechanisms and protocols that persist correctly after the onset of network failures. This characteristic is referred to as fault-tolerance.
Fault tolerance is the ability to sustain the functionalities of the sensor network without any interruption due to failure of sensor nodes. The hardware and the software constraints greatly affect the failure rate of a sensor node. Since sensor nodes are embedded with the low cost devices, so majority of the node failures are caused by hardware problems. The fault tolerance of a sensor network is also application dependent, for example, if sensor nodes are deployed in home applications, the fault tolerance requirement may be low because here sensor network is not easily damaged. But if sensor nodes are deployed in military applications, then the fault tolerance requirement will be high because sensor nodes can be destroyed by hostile action. The fault tolerance of a sensor network can be improved by depending on more than a single node. As a result, even if a sensor node dies then other nodes can be used for connectivity of the network. [3].

These protocols offer fault tolerance by having at least one alternate path (from source to sink) and thus, increasing energy consumption and traffic generation. These paths are kept alive by sending periodic messages. The path is switched whenever a better path is discovered. The primary path will be used until its energy is below the energy of the backup path. By means of this approach, the nodes in the primary path will not deplete their energy resources through continual use of the same route, thus achieving longer lifetime. A disadvantage for applications that require mobility on the nodes, is that the protocol is oriented to solve routing problem in static wireless networks. Hierarchical Power-aware Routing in Sensor Networks protocol enhances the reliability of WSN by using multipath routing. It is useful for delivering data in unreliable environments. The idea is to define many paths from source to sink and send through them the same sub-packets.

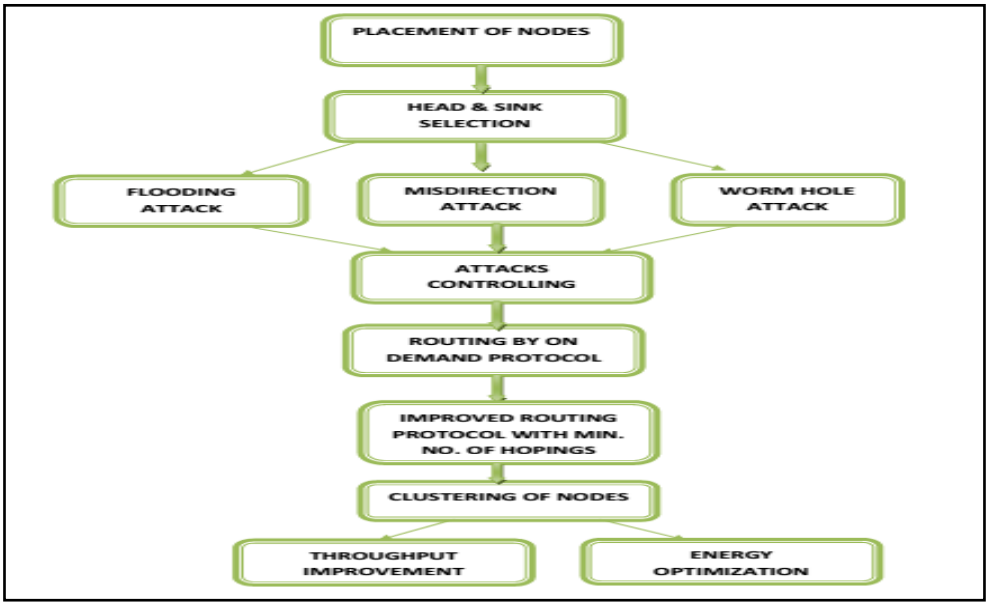

Figure 3: Proposed Steps of a System

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Routing protocols provide different mechanisms to develop and maintain the routing tables of the nodes of the network and find a path between all nodes of the network. Routing protocols must be adaptable to any type of topology to allow reaching any remote host in any network. In this approach a new scheme is suggested to deal with various attacks. It proposes a hierarchical structure to properly distribute fault management tasks among sensor nodes by heavily presenting more self-managing functions. To proficiently detect the node sudden death, our fault management system engaged an active detection mode. In this method, the message of updating the node residual battery is applied to track the existence of sensor nodes.

Short-path algorithms generally have polynomial complexity and generally only produce a single path between a source and destination. In shortest path routing, the topology network is represented using a directed weighted graph. The nodes in the graph represent switching elements and the directed arcs in the graph represent communication links between switching elements. Each arc has a weight that represents the cost of sending a packet between two nodes in a particular direction. This cost is generally a positive value that can inculcates such factors as delay, throughput, and error rate, monetary cost etc.

IV. SIMULATION RESULTS

Since the ultimate goal of this work is to assess the performance of routing algorithm, it is essential that it comes up with tests that are fair measures of the performance of these algorithms.

A. Proposed Results

In this work, take the scenario for 50 nodes and following result will show the information about the placement of sensor nodes in an area.

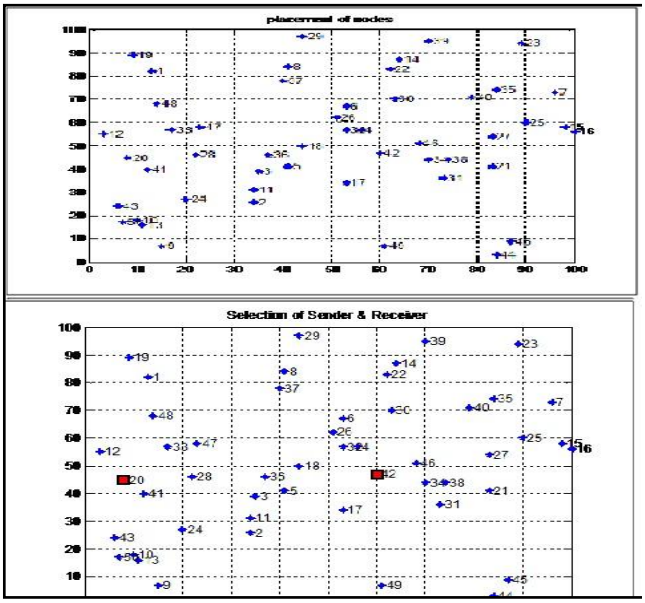

Figure 4: Ideal Placement of the Sensor Nodes

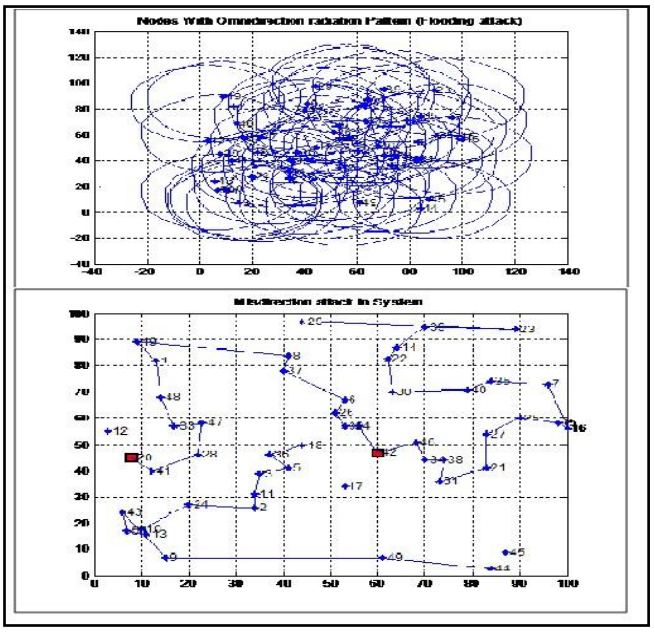

Figure 5: Various Attacks Scenario in WSN

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

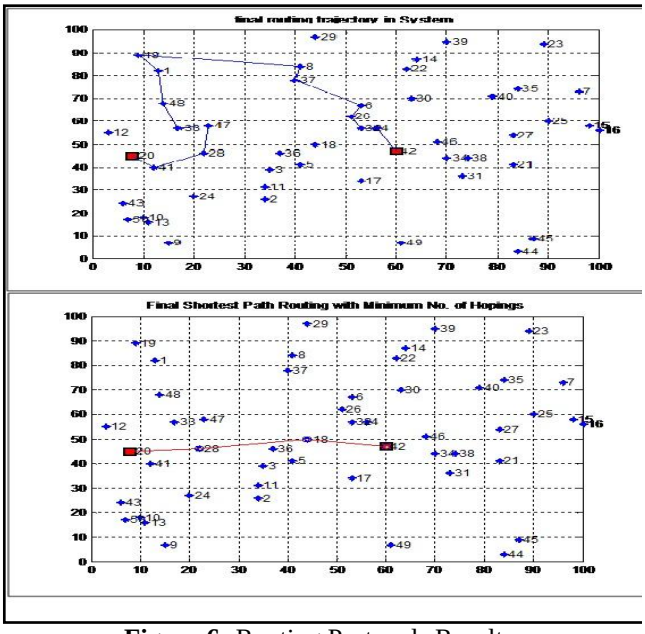

Figure 6: Routing Protocols Result

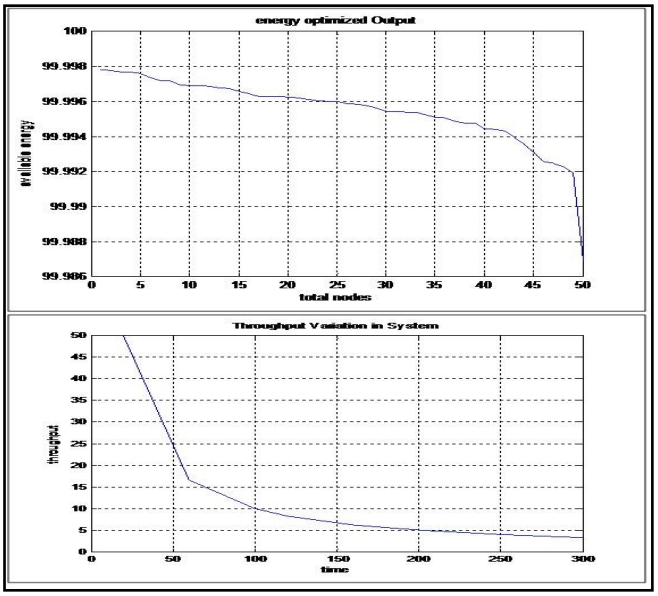

Figure 7: Performance Parameters of System

The above scenario, displays how the sensors are being deployed in an area. Sensors are randomly spread over the area. Each sensor has a sensor ID shown along with it. It will be used to address any sensor throughout the process. They are random in nature. No two nodes overlap each other.
After the deployment of the sensor nodes, the system will ask you to enter one sender id and one receiver id. That sender will become the master node and will send acknowledgement request to all the other nodes in the scenario. The nodes which will be able to reply back properly.

After mastering the node, it sends the signal to each node for knowing the distance between them. All nodes sends acknowledge to master node. In this, it also describes the distance between them. After this, various attacks occurred in network. After controlling of attacks, an on demand routing is occurred. The routing consists of two basic mechanisms: Route Discovery and Route Maintenance. Route Discovery is the mechanism by which a node S wishing to send a packet to a destination obtains a source route. To reduce the cost of Route Discovery, each node maintains a Route Cache of source routes it has learned or overheard..

V. CONCLUSION AND FUTURE WORK

In this work, it presents a data flow routing under various attacks in WSN. It also presents energy optimization scheme under clustering of nodes. The main attacks covered here are misdirection attack, wormhole attack and flooding attack etc. Sensor nodes are disposed to failure due to energy reduction and their placement in an uncontrolled or even antagonistic environment. Simulation results established that the improved proposed scheme performs well in the above situation and increase the attack handling accuracy by using the new approach and reduce energy consumption. In this, the proposed routing scheme covers minimum no. of hoping to send data from sender to receiver because it uses shortest path to travel under situation. Also the existing on demand protocol response is shown. It also shows that proposed scheme improves the throughput value. The results show that proposed path transfers packets completely without any loss as compared to path hoping mechanisms. As number of nodes increases in network, its complexity increases.

REFERENCES

1. N.Gaur, A. Chakraborty, B.S. Manoj,'Load Aware Routing for Non Persistant Small World Wireless Mesh Networks',IEEE,pp. 8-14,2014.
2. Madhu B.M., Abhilash C B,'Implementation of Improved Robust Energy Efficient Routing Protocol', IEEE, pp.5-14,2014 .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

3. Roberto D Pietro, Gabriele Oligeri, Claudio Soriente, Gene Tsudik,'United We Stand: Intrusion Resilience in Mobile Unattended WSNs',. IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 7,pp.1456-1468,2013.
4. Pinaki Sarkar, Sarbajeet Mukharji,'Source Connected Scalable Combinational KPS in WSN: Deterministic Merging, Localization'38th Annual IEEE Conference on Local Computer Networks,pp.622-629,2013.
5. Basel Alomair, Andrew Clark, Jorge Cuellar, Radha Poovendran 'Toward A Statistical Framework For Source Anonymity in Sensor Networks'IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2,pp.248-260,2013.
6. Junfeng Xiao, Rose Quingyang Hu, Yi Qian, Lei Gong, BO Wang'Expanding LTE Network Spectrum With Cognitive Radios: From Concept of Implementation'IEEE Wireless Communications,pp.12-19,April 2013.
7. P. Chanak, Indrajit Banergee, Hafizur Rahaman,'Distributed Multipath Fault Tolerance Routing Scheme of Wireless Sensor Network'2013 Third International Conference on Advanced Computing & Communication Technologies ,pp.241-247,2013.
8. Messaoud Doudou, Djamel Djenouri, Nadjib Badache,'Survey on Latancy Issue of Asynchronous MAC Protocols in Delay Sensitive WSN' IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER,pp.528-550,2013
9. Chih-Min Chao, Lin- Fei Lien, Chien-Yu Hsu,'Rendezvous Enhancement in Arbitrary-Duty-Cycled WSN'. IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 8,pp.4080-4091,2013.
10. V.Gabale, B.Raman, P.Dutta, S.Kalyanraman,'A Classification Framework For Scheduling Algorithms in Wireless Mesh Networks'IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 1, FIRST QUARTER,pp199-222,2013.
11. Wei Liu, Hiroki Nishiyama,Nei Kato, Yoshitaka Shimizu, Tomoaki Kumagai,'A Novel Gateway Selection Method to Maximize the System Throughput of Wireless Mesh Network Deployed in Disaster Areas' 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC) ,pp.771-776,2012.
12. ZHAO Jun, CHEN Xiang-guang, Xie Ying-xin,'The Application of Multipath Fault Tolerant Algorithm in WSN Codes'IEEE,pp.7323-7326,2011.
13. Chi Lin, Guowei Wu, Mingchu Li, Xiaojie Chen, Zuosong Liu, Lin Yao,'A Selfish node Preventive Real Time Fault Tolerant Routing Protocol For WSNs'2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing ,pp.330-337,2011.
14. P.Ghosh, Michael Mayo, V. Chaitankar, T. Habib, Ed Perkins, Sajal K Das,'Principles of Genomic Robustness Inspire Fault Tolerant WSN Topologies: A Network Science Base Case Study'Seventh IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing,pp.160-165,2011.
15. Kiyotaka Imai, Hisao Yamamoto,'A Study on Large Scale Wireless Mesh Networks Cooprating With High Speed External Networks2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery',pp.71-74,2010.