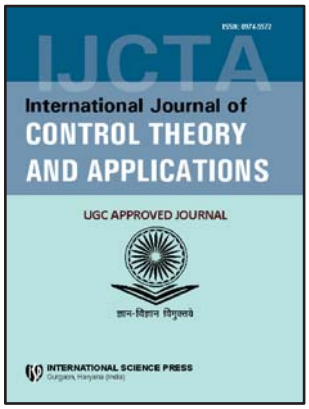

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 31 • 2017

Sinkhole Attack Detection in WSN using Fast Randomized Algorithm

S.Vidhya[a] and T. Sasilatha[b]

[a]*Asst. Professor, Department of Information Technology, Saveetha Engineering College,602002, Tamil Nadu, India.*

E-mail: vidhyas_1983@yahoo.com

[b]*Dean, AMET University, Chennai, 603112, Tamil Nadu, India.*

E-mail: sasi_saha@oyahoo.com

Abstract : Wireless sensor networks(WSN)consist of a large number of sensor nodes capable of sensing and monitoring the environment. The nature of sensor nodes makes it attractive to the intruders. Sinkhole attack is a major challenging attack in WSN. It occurs when an intruder introduces fake routing information in routing. The neighbour follows the same routing information leading to misrouting. The Attacker catches the information from the network. This paper proposes an algorithm called fast randomized algorithm to detect the intruder in sinkhole attack and providethe solution.

Keywords: *Wireless sensor network, sinkhole attack, randomized algorithm, routing.*

1. INTRODUCTION

WSN consists of nodes capable of storing and sensing the environment. It is deployed for large geographic environment. Sensor node sends the data collected from the environment and passes it to the BS. The sensor node makes it suitable for military applications,healthcare and monitoring applications. Securing the sensor network against the attackers is a serious issue. There are different types of attacks in WSN. In the sinkhole attack attackers try to hack the information passing between source to BS by misrouting them. A malicious node acts as a normal node introduces fake routing information.

Pushkar A. Chavan [1] indicates ETARF, a robust trust aware routing for WSNs against intruders in multi hop routing. This approach does not use any time synchronization or known geographic information to find the route from source to destination. Instead, it finds the efficient shortest route using the shortest path algorithm, which routes the logical link on physical path with least hop count. The results show energy savings and bandwidth through clusters and data aggregation.

Leovigildo Sánchez-Casado [2] discusses, in his work, an approach to detect sink hole attack in MANETs with AODV routing. It focuses on the contamination borders formed by legitimate nodes under the influence of intruders. The information collected from neighbour nodes at regular intervals is used for finding the sink holes.

Fang-Jiao Zhanga[3] discusses a novel approach for detecting serious security problems like sinkhole attack using the redundancy mechanism. Multi paths are used for sending the messages. After the evaluating the replies the attacker nodes are identified. The simulation results show the effectiveness of this approach.

Ngai et.al[5] discusses in his work, an algorithm to find a list of nodes by checking the data consistency and identifies the intruder by analyzing the network flow. This algorithm is analysed through numerical and simulation analysis and results are discussed.

Stefan and Antonopoulos [6] Implements a model to detect sinkhole attack and provides a solution using the AODV routing protocol. The results proved in terms of detection precision and agent overheads with simulation.

Fessant et.al [7] discusses a methodology implement a novel design and resilient protocol. This method implemented with simulation study and detailed analysis also discussed in practical.

Krontiris,et.al [8] discusses in his work that implement the sinkhole attack in TinyOS and rules framed to detect the intruders with IDS. Min route protocol is used for network deployment. The results present with the simulation with parameter discussed.

2. PROPOSED WORK

Networks are formed based on the distance between the nodes which, along with the sub node, are grouped together by the coverage area of the nodes. After the node selection process, network assigns the energy for each node in the network. In the routing process each node consumes energy consumption for transmitting and receiving. Initially the source node in the network tries to send data to the destination. The network first checks the source node id with the primary key for authentication. The proposed fast randomized algorithm (FRA) checks authentication of nodes in the network. When any unregistered node tries to attack the registered node in the network, its authentication is verified by the security algorithm. The mismatch in the id leads to the decision that node is an attacker.

2.1. Node construction

In this proposed work, a network is constructed consisting of a number of Nodes shown in figure 1. A Node can request data from another node in the network. All nodes share their information with each other. They are connected in the network. So each network forms its group based on the coverage area.

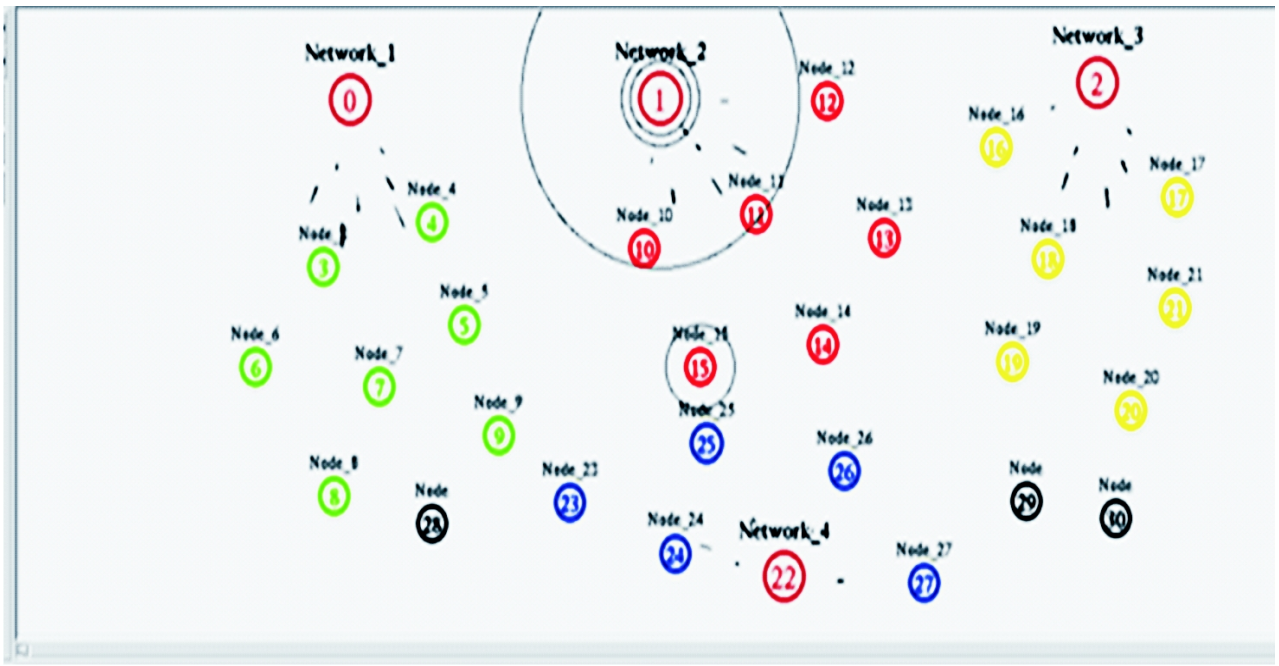

Figure 1: Node Construction in Network

2.2. Assigning Node ID and Primary Key

Each nodeis assigned a node ID and Primary key. A Primary key is assigned to each networkwhich monitors all the nodes communication for security purpose. This is shown in the figure2.

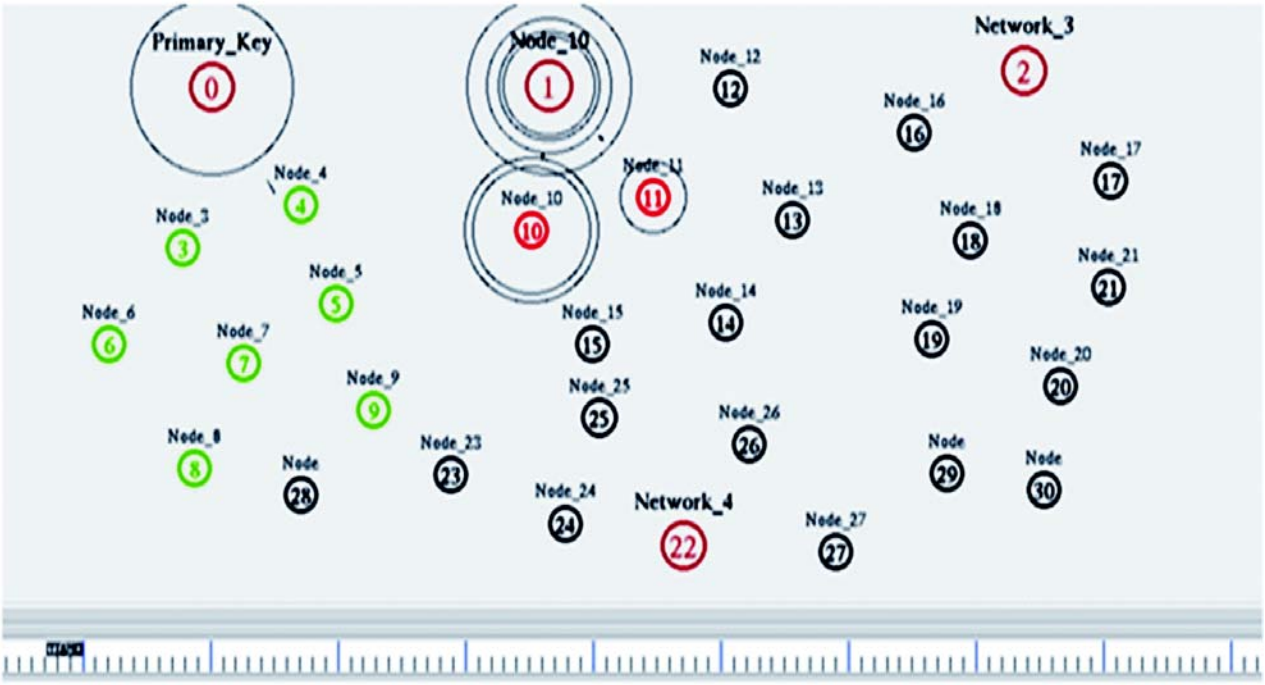

Figure 2: Assigning Node ID and Primary key

2.3. Network selection

Network is used to store all the information relating to nodes like Node Id, primary key and others.The network will also monitor all the Nodes Communication for security purpose. The number of nodes registered in a network is based on network coverage area. Although based on number of node connection, the network selects the nodes to transmit data. After network selection, server assigns energy level for each node.

2.4. Path selection and data transmission

In this module, the source node in a network sends data to another network.The network first checks the source node id with the and primary key then only it receives the data based on fast randomized algorithm which is shown in the figure 3. Using energy, node sends data to nodes in another network. So, after data transmission, each node loses some energy. After path selection and data transmission, the network checks energy level of each node. When the energy level is less than approximate energy, its goes into inactive state.

2.5. E.Identification or removal of attacker

In this module, the base station identifies the attacker on the basis of primary key.Suppose an unregistered node or registered node wants to send some virus file to a base station first checks its node id and the primary key. Any mismatchin the primary key is located easily another attacker is removed. This is shown in figure.4.

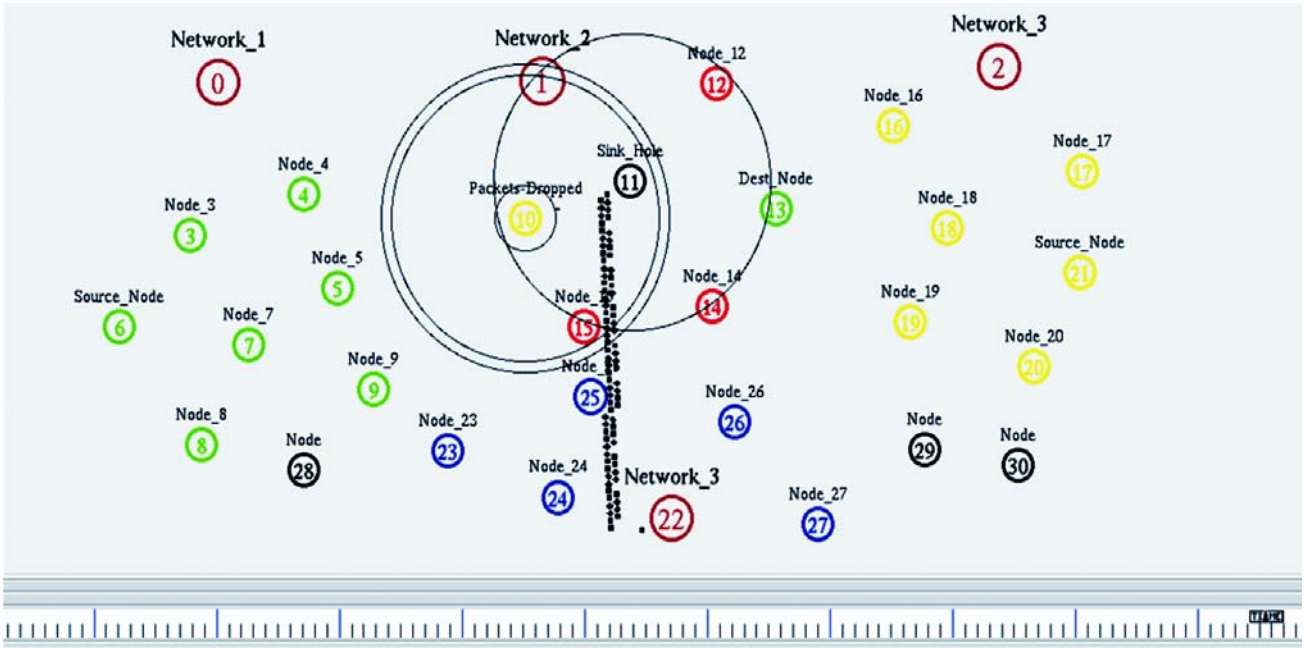

Figure 3: Path selection and packet transmission

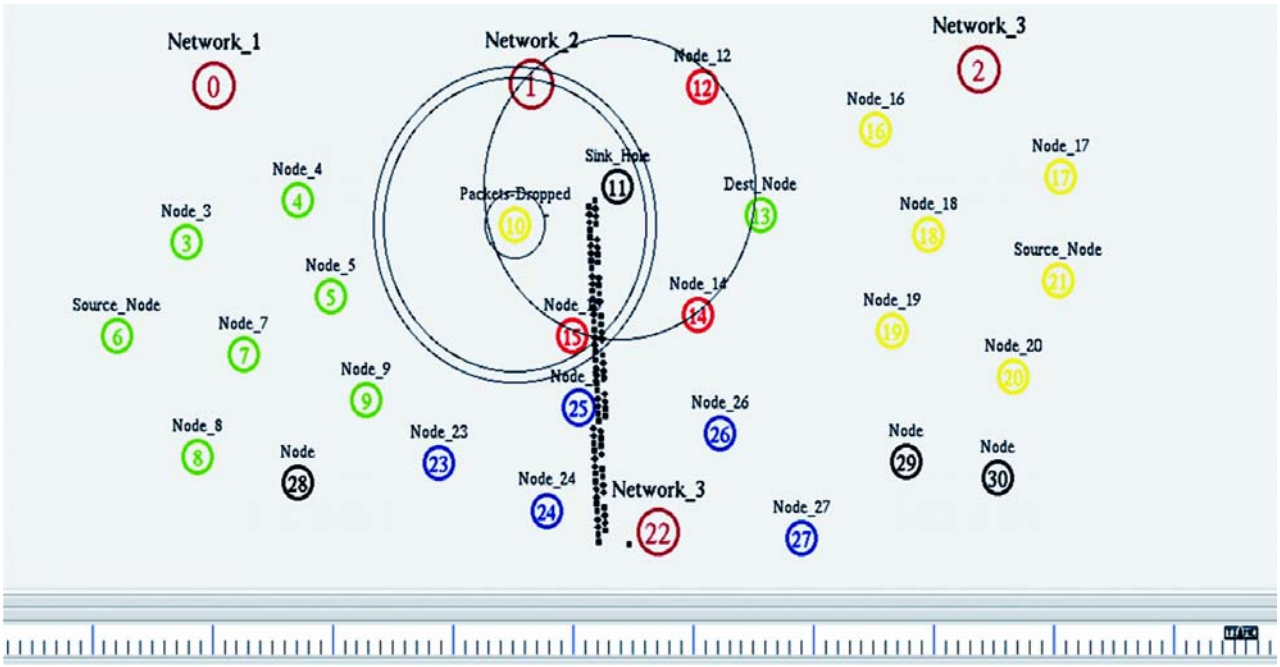

Figure 4: Removal of Attacker

3. SIMULATION

The simulation set up is designed using a NS2 simulator. The simulation landscape is designed as 1000X1000. The number of nodes in the simulation is 30. The DSDVrouting protocol is used and MAC protocol used is IEEE 802.11.the simulation parameters are shown in table 1.

Table 1
Simulation parameters

Parameter	*Value*
Simulator	Ns2 - 2.34
Number of nodes	30
Simulation Time	15 min
Packet Interval	0.01 sec
Simulation Landscape	1000 x 1000
Background Data Traffic	CBR
Packet Size	1000 bytes
Queue Length	50
Transmission Range	100 Kbytes
Node Transmission range	250 m
Antenna Type	Omni directional
Mobility Models	Random-waypoint (0-30 m/s)
Radio Frequency	850-950 MHz
Routing Protocol	DSDV
MAC Protocol	IEEE 802.11

4. RESULTS AND DISCUSSION

The performance of the network can be estimated by using the parameters such as energy consumption, alive nodes, end to end delay, transmission rate, and the throughput which can be explained using graphs. The effect of the sinkhole attack is reduced by using a fast randomized algorithm. By this algorithm we can enhance the security of the network.

4.1. Throughput

Throughput is the ratio of the total data received for the certain period of time shown in figure 5. The proposed scheme detects the sinkhole nodes at the earliest and minimizes the packet drop rate.

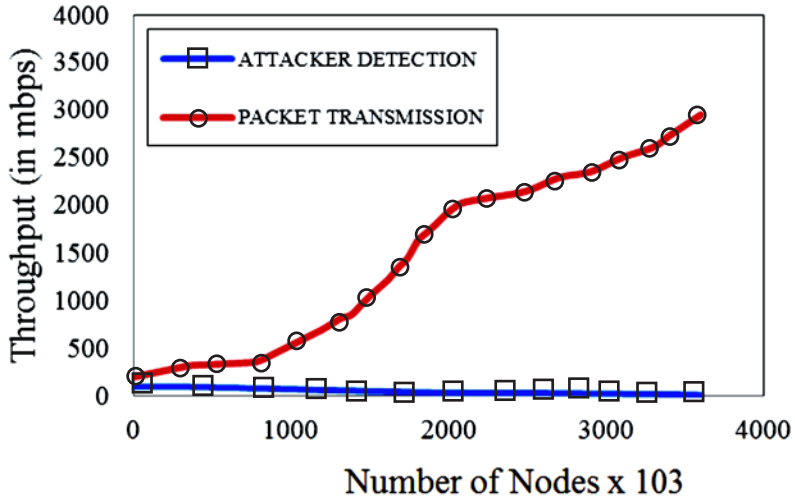

Figure 5: Throughput in network

4.2. Packet delivery ratio

Packet Delivery Ratio (PDR) shown in figure 6.isthe number of packets reaching the destination to the number of packets seeded at the source. The ratio will always be less than 1 (unity) as there will be packet drop due to congestion or due to attacks.

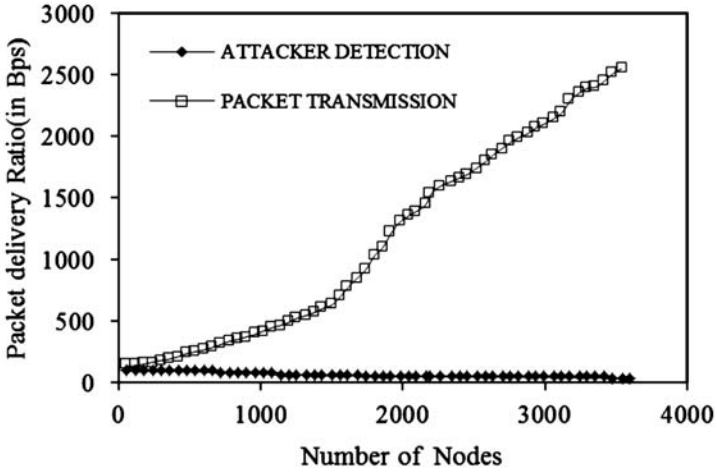

Figure 6: Packet Delivery Ratio in Network

4.3. End to end delay

The End- to-End Delay is the transit time difference for the packet to reach the destination from the source. This delay depends on the number of intermediate nodes that are taken up in the chosen route. Thus, if shortest path is chosen, the delay will be minimized.

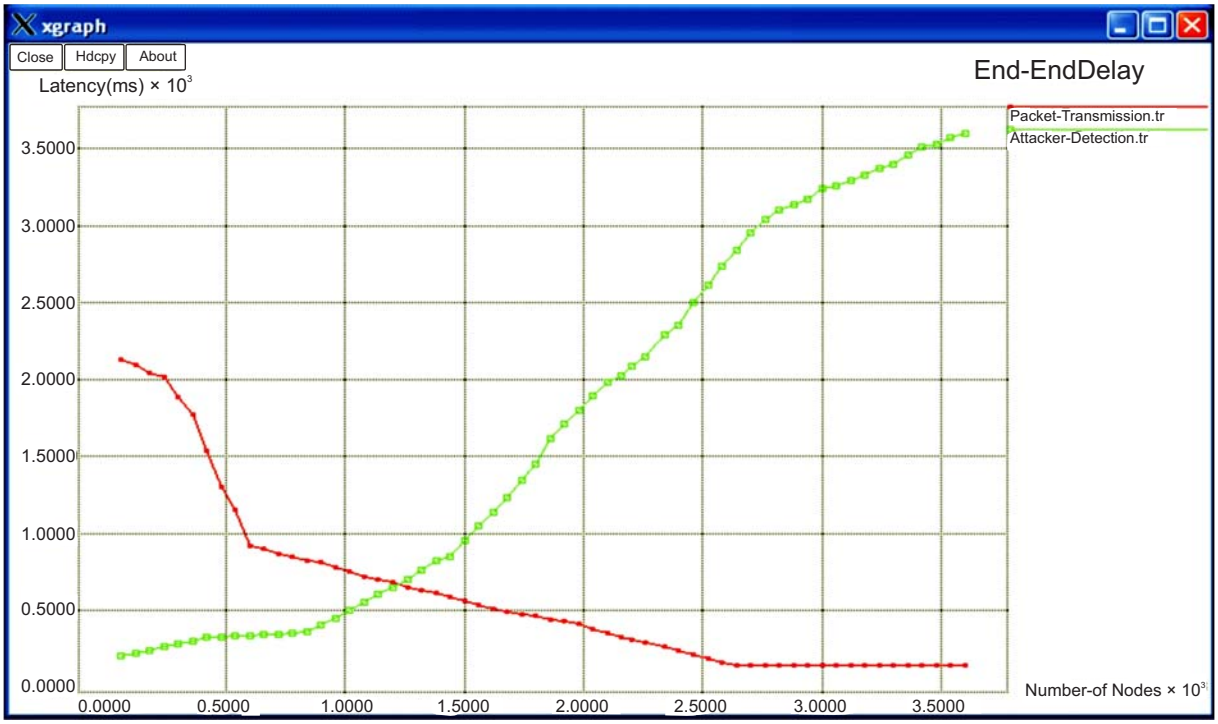

Figure 7: End to End delay in Network

4.4. Alive nodes

The lifetime of the node is influenced mainly by the energy node possesses.

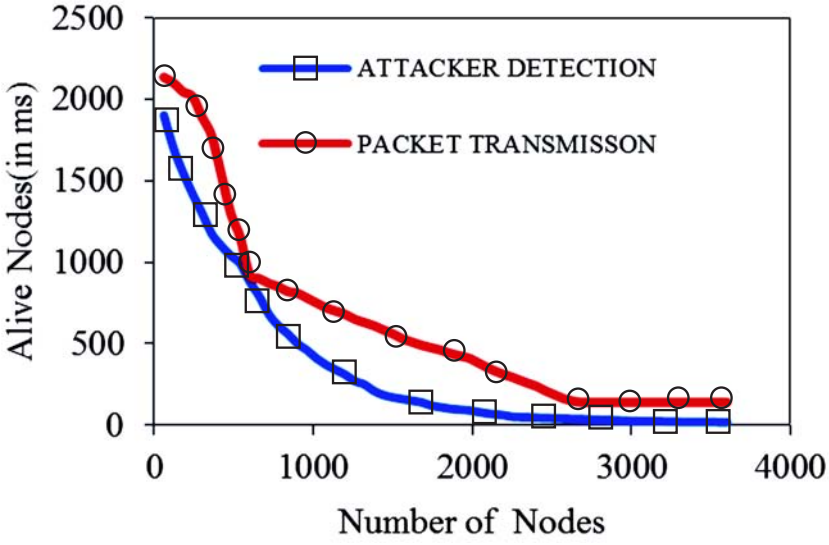

Figure 8: Alive Nodes in Network

4.5. Energy consumption

The energy consumption for the transmission of a packet from source to destination is basically dependent on the number of the intermediate hopstaken in that route.

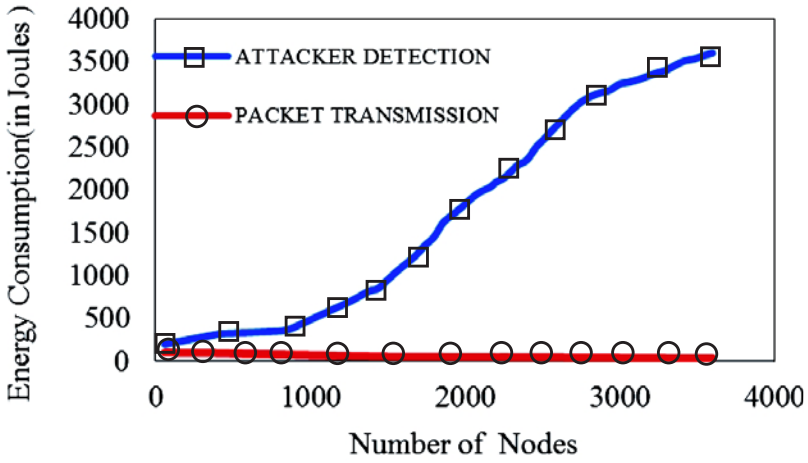

Figure 9: Energy Consumption in Network

5. CONCLUSION

Thus the proposed work can help a better performance than the existing work in wireless senor networks. Results indicate that the proposed work provides security and confidentiality of the message transferred. It increases the network lifetime and ensures the security and integrity of the data transferred along the sensor nodes. It avoids taking malicious nodes by calculating the primary key for each node in the network.

The future work may be based on increasing the efficiency of network when there is a large number of nodes present it. The proposed algorithm can also be modified to select nodes that will be a part of the communication structure. In this proposed work the value of the security and the reliability model are considered. For future work, the value based on mobility of sensor nodes can also be included in order to provide better security.

REFERENCES

[1] Pushkar A. Chavan, Rashmi D. Aher, Kamlesh V. Khairnar, Hemant D. Sonawane -, "Enhanced Trust Aware Routing Framework against Sinkhole Attacks in Wireless Sensor Networks", International Journal of Engineering and Technical Research.Vol.No.3 pp. 2321-0869 Jan. 2015.

[2] Leovigildo Sánchez-Casado, Gabriel Maciá-Fernández, Pedro García- Teodoro, Nils Aschenbruck, "A Novel Collaborative Approach for Sinkhole Detection in MANETs" ,Springer, Adhoc Networks and Wireless, Vol.No.8629.pp.123-136, 2015.

[3] Fang-Jiao Zhanga,b, Li-Dong Zhaia, Jin-Cui Yangb, and Xiang Cuic, (2014), "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks", Elsevier Procedia Computer Science, Vol.No.31 pp. 711 – 720s,2014.

[4] Vivek Tank and Amit Lathigara(2015), "A Survey on Sinkhole Attack Techniques in Mobile Ad hoc Networks",2015.

[5] Ngai , Liu, and Lyu(2007), "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks" Elsevier Computer Communications, Vol.No.30pp. 2353–2364,2004.

[6] Stefan and Antonopoulos(2010), "Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks", ElsevierComputer Communications, Vol.No.33.pp. 619–638,2010.

[7] Fessant, Papadimitriou, Viana, Sengul, Palomar,"A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis", Elsevier Computer Communications Vol.No.35 pp. 234–248,2012.

[8] Krontiris, Dimitriou, Giannetsos, and Mpasoukos, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks".