ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An UGC Approved Journal)

Website: www.ijareeie.com

Vol. 6, Issue 8, August 2017

A Novel Approach for Sinkhole Detection in WSN Using Encryption Approach with Reverse Tracking

Mitthatmeer Kaur[1], Manpreet Kaur[2], Dr. Charanjit Singh[3], Dr. Rajbir Kaur[4]

PG Student, Dept. of ECE, Punjabi University, Patiala, India[1]

PG Student, Dept. of ECE, Punjabi University, Patiala, India[2]

Assistant Professor, Dept. of ECE, Salem Punjabi University, Patiala, India[3]

Assistant Professor, Dept. of ECE, Salem Punjabi University, Patiala, India[4]

ABSTRACT: Wireless Sensor Network is a branch of networking that deals with sensing of information from deployed area. In Wireless Sensor Network, various malicious nodes have been introduced to perform various types of attacks on the network to degrade or collect some information. Sink hole attack is performed on sink node as attacking node replaces the actual sink node by advertising its availability and resumes all the data from the sensor node. In this paper, an approach has been developed that is combination of IDS with encryption approach so that better data transmission and data security can be provided. By analysing proposed approach we can predict that proposed model provides efficient security and reliable communication in WSN.

KEYWORDS: WSN, Sinkhole attack, IDS, AES and Hashing

I. INTRODUCTION

1.1 Wireless Sensor Network

A Wireless Sensor Network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. Most of the modern networks are bi-directional, also enabling control of sensor activity. The development of Wireless Sensor Networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring and so on.

1.2Attacks

In WSN, performance has been degraded due to vulnerable of various attacks over the network. In this process of attack over the network nodes goes through misbehavior. Various attacks affecting the efficiency of WSN have been listed below.

- **Fabrication Attack:** An aggressor can make this assault by sending wrong information into the system, the information could be wrong or the transmitter could assert that it is another person. This assault incorporates create messages, warnings, declarations, personalities [1].
- **Alteration Attack:** This assault happens when aggressor modifies current information, it incorporates deferring the transmission of the data, replaying prior transmission, or changing the genuine section of the information transmitted

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An UGC Approved Journal)

Website: www.ijareeie.com

Vol. 6, Issue 8, August 2017

[1]. For example, an aggressor can modify a message telling different vehicles that the current street is clear while the street is congested [2].

- **Black hole Attack:** When some malicious user enters into the network and stop forwarding messages to next nodes by dropping messages, this type of attack is referred to as black node.
- **Grey hole Attack:** This attack occurs if some node dropping 50% of the packets and rest 50% is sending by altering the message. In this way wrong information is broadcasted.
- **Sink Hole Attack:** In Sink hole attack, malicious node acts as a black hole to attract all the traffic in the sensor network. Attacker listens to requests for routes then replies to the target nodes. It inserts itself between the communicating nodes; it is able to do anything with the packets passing between them.
- **Cloning attack:** A node replication attack involves an attacker inserting a new node into a network which has been cloned from an existing node, such cloning being relatively simple task with current sensor node hardware. This new node can act exactly like the old node or it can have some extra behavior.

1.3 Sinkhole Attacks:

In a sinkhole attack, an intruder compromises a node or introduces a counterfeit node inside the network and uses it to launch an attack. The compromised node tries to attract all the traffic from neighbor nodes based on the routing metric used in the routing protocol. When the compromised node manages to achieve that, it will launch an attack. Sinkhole attacks are a type of network layer attack where the compromised node sends fake routing information to its neighbors to attract network traffic to itself [7].

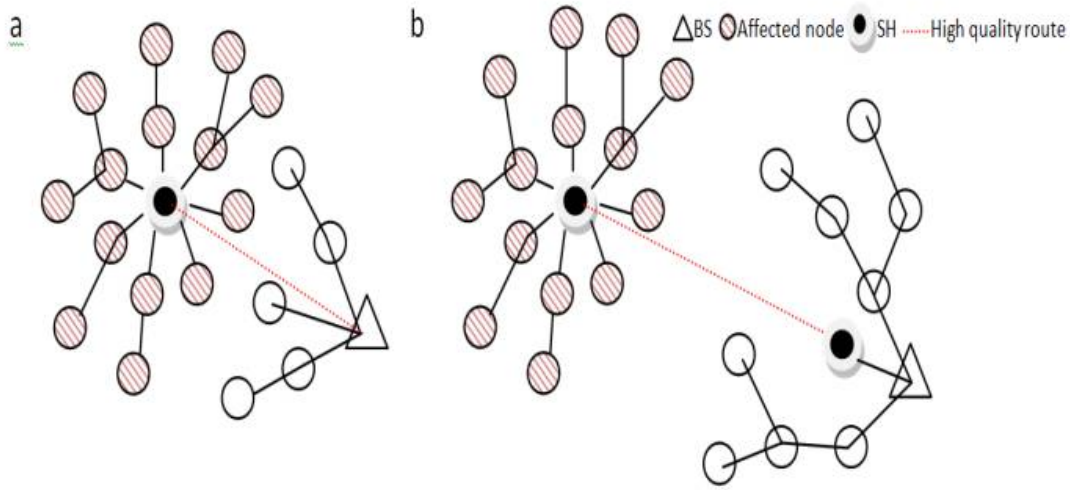

Fig. 1 Two illustrations of sinkhole attack in WSN a) using artificial high quality route b) using worm hole

In Figure 1(a); the intruder has greater computational and communication power than other nodes and has managed to create a high quality single hop connection with the base station. It then advertises its high quality routing message to its neighbors. After that all the neighbors will divert their traffic to the base station to pass through the intruder and the sinkhole attack is launched. In Figure 1(b) the sinkhole attack is launched in conjunction with a wormhole attack. This attack involves two compromised nodes linked via a tunnel or wormhole [6].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An UGC Approved Journal)

Website: www.ijareeie.com

Vol. 6, Issue 8, August 2017

1.4 Challenges in detection of sinkhole attack in WSNS

- **Communication Pattern in WSN**

All the messages from sensor nodes in Wireless Sensor Network are destined to base station. This created opportunity for sinkhole to launch an attack. Sinkhole attacks normally occur when compromised node send fake routing information to other nodes in the network with aim of attracting as many traffic as possible. Based on that communication pattern the intruder will only compromise the nodes which are close to base station instead of targeting all nodes in the network. This is considered as challenge because the communication pattern itself provides opportunity for attack.

- **Sinkhole attack is unpredictable;**

In Wireless Sensor Network the packets are transmitted based on routing metric that used by different routing protocols. The compromised node used its routing metric that used by routing protocol to lie to his neighbors in order to launch sinkhole attack. Then all the data from his neighbors to base station will pass through compromised node. For example the techniques used by compromised node in network that used TinyAODV protocol is different to the one used another protocol like Mint Route protocol.

- **Insider Attack and Outsider Attack**

Insider attack and outsider attack are two categories of attack in Wireless Sensor Network. Outsider attack is when intruder is not part of network. In insider attack the intruder compromises one of the legitimate node through node tempering or through weakness in its system software and then compromised node injects false information in network after listen to secret information. Insider attack can disrupt the network by modifying routing packet. Through compromised node, sinkhole attack attracts nearly all the traffic from particular area after making that compromised node attractive to other nodes.

II. REVIEW OF LITERATURE

A.Vijayalakshmi. et. al.[1] "Mobile Agent Middleware Security for Wireless Sensor Networks" Wireless Sensor Networks have gained much attention in recent applications. However, they are very much subjected to the security threats. To provide security arrangements in sensor nodes, the energy required to carry out the operation may reduce the lifetime of the sensor nodes. In order to optimize the energy usage in sensor nodes, middleware concept is introduced. The middleware to provide security for the Wireless Sensor Networks is arranged in the Mobile Agent with the capability of optimizing the power usage with the sensor nodes. An energy efficient Mobile Agent based algorithm is simulated. It will be established that the Mobile Agents provide the security arrangements to the Wireless Sensor Networks for the reduction of sinkhole and cloning attacks.

G. Kalnoor and J. Agarkhed, [2] "QoS based multipath routing for intrusion detection of sinkhole attack in Wireless Sensor Networks." As the number of nodes and size of the network increases, there will be rapid increase in internet traffic. In WSN, security is the major issue and needs to a system that can provide security. Intrusion Detection System (IDS) is the system which plays a vital role in security of a system. One of the major challenges of WSN is to provide consistent Quality of Service (QoS) such as reliability, congestion control, energy efficiency and end-to-end delay, by applying secured routing protocols along with detection of an intruder so that QoS of WSN does not get affected. In this research work, different routing protocols that are QoS based are discussed, to improve the overall performance of the network.

Debiao He et.al.[3] "A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks". With the development of wireless communication technology and sensor technology, the Wireless Sensor Network (WSN) has been widely used in various applications, such as military surveillance, environment monitoring industry control, medical monitoring, and so on. In most of the cases, WSNs are deployed in unattended environment. So, these are more vulnerable to various attacks than traditional networks. To protect communications in WSNs, mutual authentication and key agreement schemes for WSNs have been studied widely. Recently, Xue et al. proposed a temporal-credential-based mutual authentication and key agreement scheme for WSNs and claimed their scheme could withstand various attacks. However, in this paper, it is pointed out that this scheme is vulnerable to the off-line password guessing attack, the user impersonation attack, the sensor node impersonation attack and the modification attack. To overcome weaknesses in Xue et al.'s scheme, a new temporal-credential-based mutual authentication and key agreement scheme for WSNs is proposed. Security analysis shows that this scheme could overcome

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An UGC Approved Journal)

Website: www.ijareeie.com

Vol. 6, Issue 8, August 2017

weaknesses in Xue et al.'s scheme. Performance analysis shows this scheme also has better performance. Therefore, this scheme is more suitable for providing secure communication in WSNs.

Deshpande, P. et al [4] "Techniques improving throughput of wireless sensor network: A survey" In Wireless Sensor Networks, maintaining the higher throughput is the main concern. Wireless Sensor Networks are basically formed with a few powerful base stations and a large number of resource-constrained sensor nodes.The wireless sensor network composed of n number of sensors or nodes, where each and every node is connected to one or several nodes or sensors. Wireless Sensor nodes of zigbee system basically build on two aspects of protocol stack that are IEEE 802.15.4 standard and zigbee protocol. The problem that sensors usually face in Wireless Sensor Network is that when data packets are transferred from one node to another node, the throughput of the Wireless Sensor Network decreases because of packet collisions and high network traffic. In order to overcome this problem, various methods have been discussed to improve the throughput.

Guerroumi, M. et.al.[5] "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink" In this paper, an Intrusion Detection System (IDS) is proposed against Sinkhole attack in Wireless Sensor Networks with mobile sink. In the detection model, the network area is divided into a flat grid of cells, and the signature-based technique is used, which is represented by the detection rate of a cell, to distinguish between real and fake sink nodes. The proposed IDS consider two types of sink mobility: periodic and random. In addition, as the cell leaders do not activate their IDS agent simultaneously, the additional energy consumption incurred by the IDS is low. Simulation results show the efficiency of the proposed IDS in terms of detection rate, efficiency, and energy consumption.

III. METHDOLOGY

WSN has been used for data transmission from sensing nodes to base station. In the process of WSN various nodes have been deployed over the network that has been used for sensing and data transmission. In this research work malicious node detection has been done that is based on Advanced Encryption System and Intrusion Detection System. In this process of WSN nodes have been destined in such a way that sensing information has been encrypted using hashing function. On the basis of this information data has been transmitted to base station that has been decrypted using decryption key at station level.

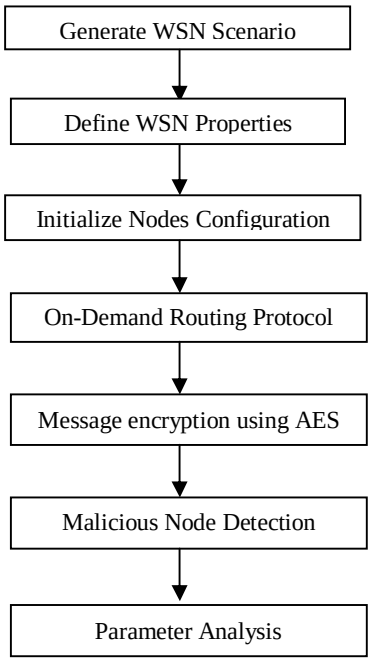

Fig.2 Flow of Work for proposed work

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An UGC Approved Journal)

Website: www.ijareeie.com

Vol. 6, Issue 8, August 2017

Fig. 2 represents the flow of the proposed work that represents various steps that must be carried out for evaluation of desired objectives. In the proposed work, malicious node detection has been done in Wireless Sensor Network. In the proposed work, Wireless Sensor Network has been initialized by defining various parameters in the proposed work. In WSN, sink nodes have been utilized for transmission of information from sensor to base station or to other sink nodes. Attackers encounter sinkhole attack in WSN for degrading network performance.
In this process, route has been discovered using RREQ and RREP format so that route from source to destination can be established. In this process, intrusion detection mechanism has been encounter that monitors whole process of information transmission. If a node in the desired path misbehave then reverse tracking mechanism has been used for ensuring security of the network that detects the nodes that comprises under sinkhole attack.

- **Reverse Tracking Method**

The main function of this process is to extract behavior of malicious nodes available in the network. In this process RREQ, message is transmitted from a node to the single hop neighbor nodes with a significant flag bit in the RREQ message. The nodes receive the messages and respond the message through RREP. On the basis of Bait reply message detection of malicious node has been done. If the respond is from single hop neighbor nodes then node to be treated as genuine node and if that is from other node that it has to be considered as malicious node. Neighbor node has been verified through routing table. After this process black hole and grey hole attack has been detected using packet delivery tracing of the node. On the basis of Packet Delivery Ratio of the node, malicious node has been detected in the network.

- **Security Preservation**

In proposed work solution has been provided for avoidance of data leakage over the network. In any cases, attack has been undergone process of data leakage then information that has been transmitted to malicious node has been prevented using AES encryption. On the basis of AES, data has been encrypted that convert original information to cipher text that is an encoded form. This information can be converted to original by using decryption key that is available at base station. So data security over WSN has been provided.

IV. RESULTS

In the proposed work WSN has been initialized for sensing information from environment. The sensor nodes have been deployed in the environment for capturing information. These nodes capture information from particular environment and transmit this information to base station. Various parameters have been used in WSN for sensing information. These nodes consume energy while sensing, receiving and transmitting information.

Table 1 Simulation Table

Number of nodes	100
Agent	TCP/TCP-Sink
Routing Protocol	AODV
Antenna Type	Omni
MAC type	802.11
Queue Type	Drop Tail
Queue Length	50
Simulation Time	50s
Traffic Type	CBR
Energy Model	Energy Model
Transmission Energy	0.9 J
Receiving Energy	0.5 J
Initial Energy	50 J

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An UGC Approved Journal)

Website: www.ijareeie.com

Vol. 6, Issue 8, August 2017

Table 1 represents various simulation parameters that have been used to define WSN communication. These different parameters have been defined for data transmission. In the proposed work, various parameters have been analyzed for performance evaluation of proposed work. Simulation has been done using NS 2.35 simulator. Detection of malicious nodes has been done using AES standard and reverse tracking approach.

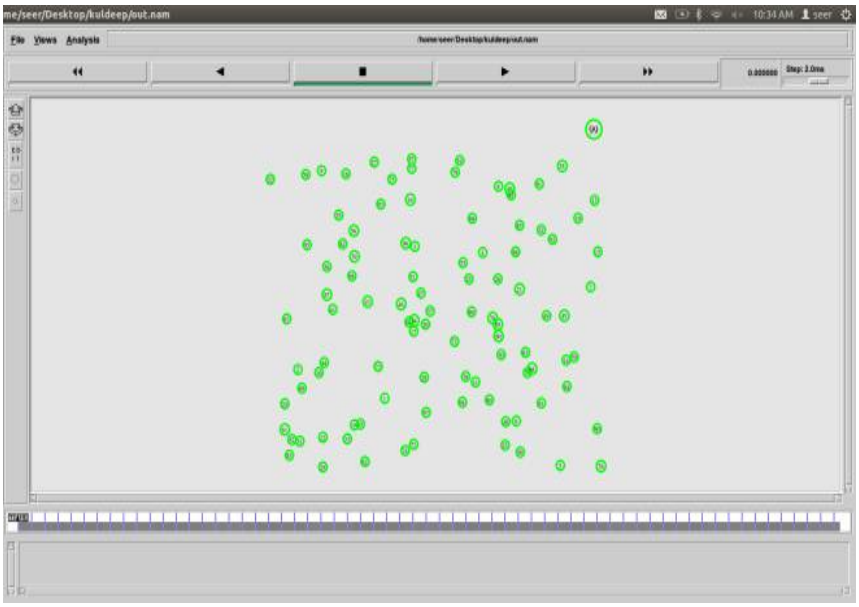

Fig.3 Initialization of Nodes

Fig. 3 represents initialization of Wireless Sensor Network for sensing information from environment. In this figure nodes have been initialized by defining various parameters about nodes location, nodes size and energy model. In WSN nodes sense information from a particular environment and transmit information to base station for decision making process.

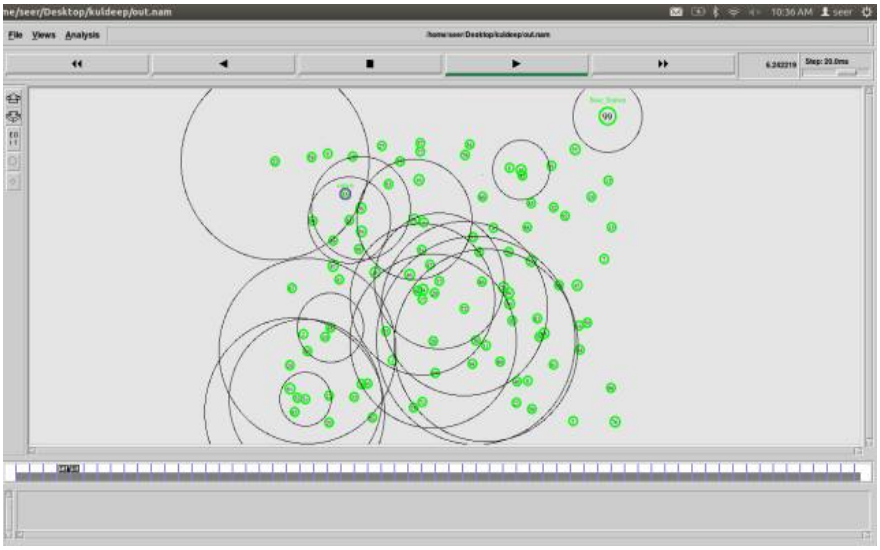

Fig 4. Attack occurred in the Network

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An UGC Approved Journal)

Website: www.ijareeie.com

Vol. 6, Issue 8, August 2017

Fig.4 is used to represent the Sinkhole attack occurred in the network. Sink hole attack is performed on sink node as attacking node replaces the actual sink node by advertising its availability and resumes all the data from the sensor node. Actual data isn't received at base station that ultimately results in the loss of the information of the network.

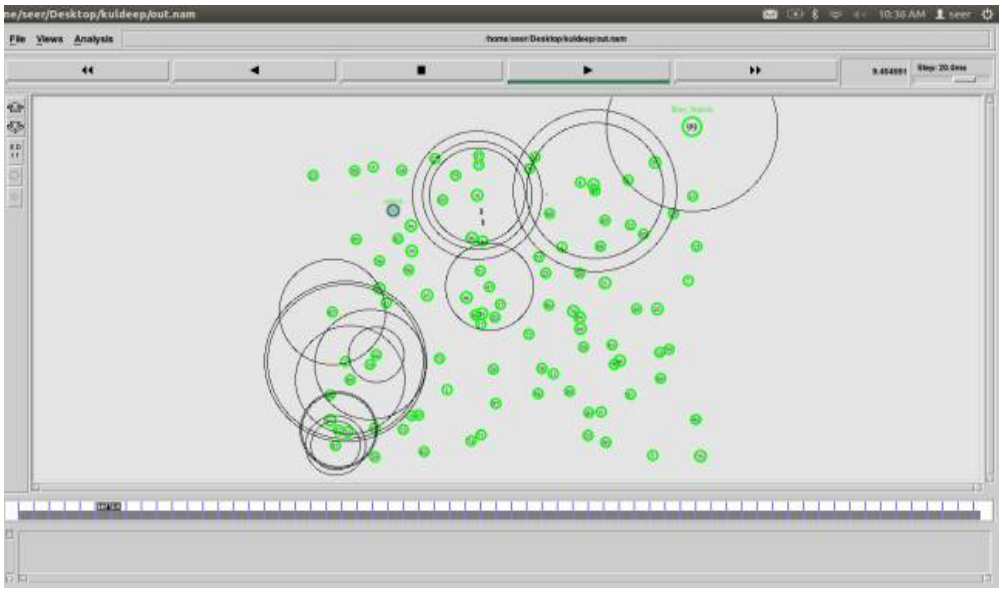

Fig. 5 Detection of Sinkhole Attack

In Wireless Sensor Network, the packets are transmitted based on routing metric that used by different routing protocols. The compromised node uses its routing metric that is used by routing protocol to lie to his neighbors in order to launch sinkhole attack. Then all the data from its neighbors to base station will pass through compromised node. In this, actual data isn't received at base station that loss the information of the network. Here, the sinkhole attack detection scheme has to be implemented that detects the attacking node and provide reliable information.

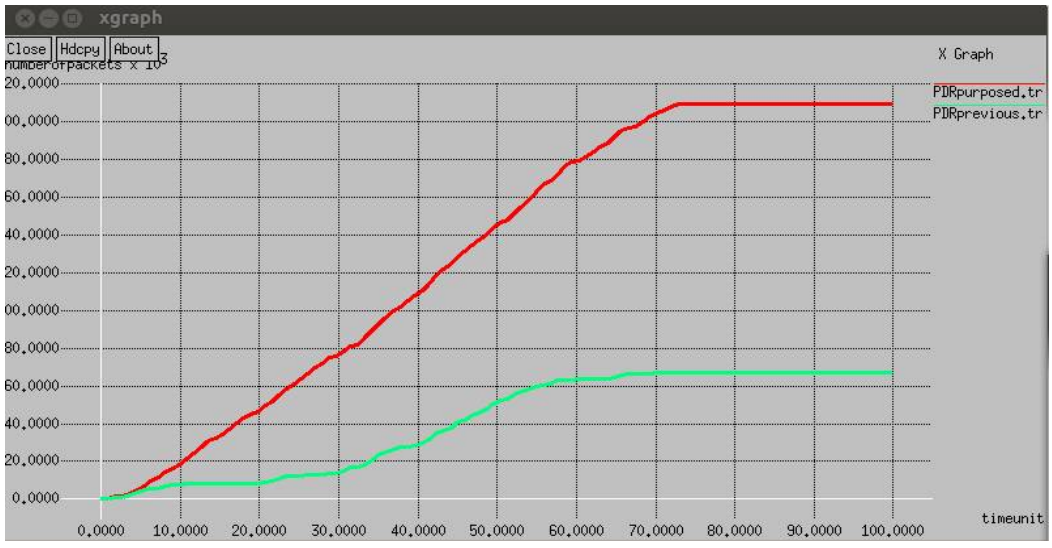

Fig.6 Packet Delivery Ratio

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An UGC Approved Journal)

Website: www.ijareeie.com

Vol. 6, Issue 8, August 2017

Packet Delivery Ratio is defined as the number of packets delivered with respect to time. Packet Delivery Ratio by proposed AES based approach is much higher than that of the previous approach.

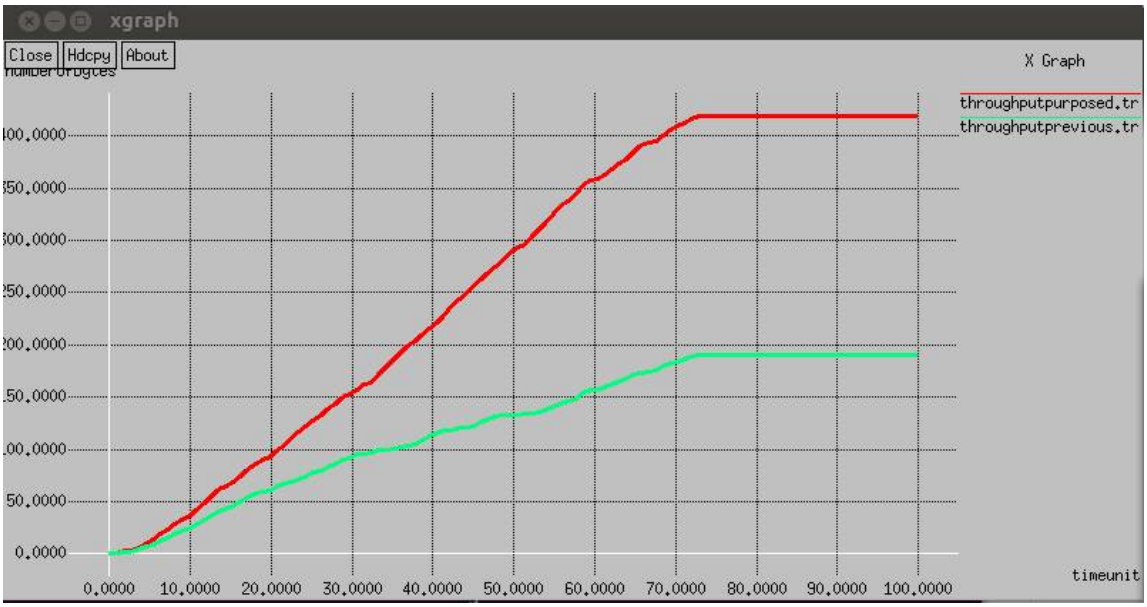

Fig.7 Throughput

Throughput is defined as the number of packets delivered successfully over the network. Throughput represents bytes transmitted per unit time. This graph represents comparison between proposed and AODV routing protocol. By analyzing graph plotting one can say that proposed approach provides much higher throughput than that of AODV based detection approach.

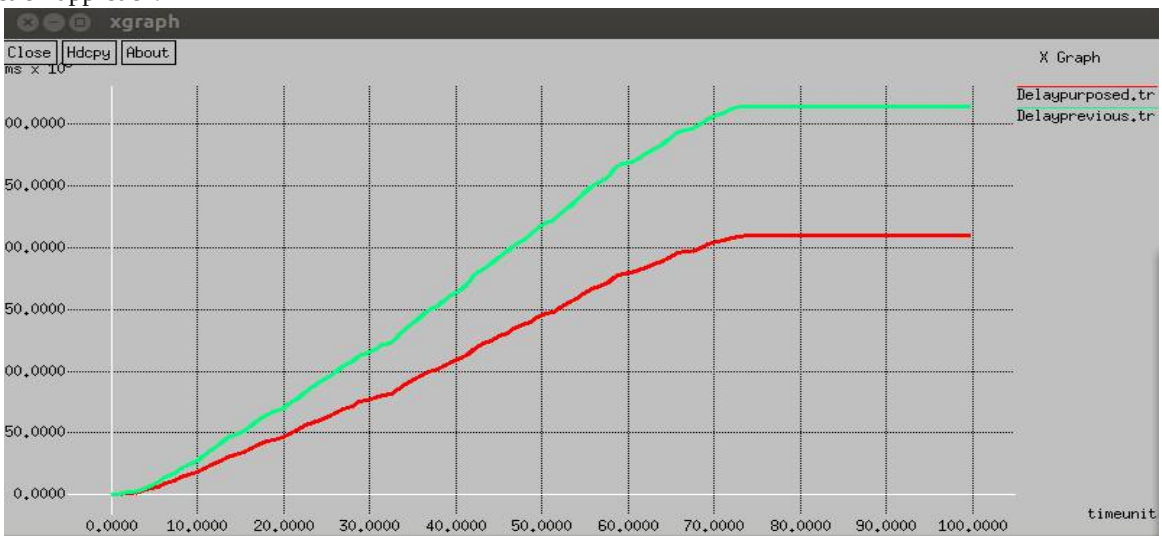

Fig.8 Packet Delay

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An UGC Approved Journal)

Website: www.ijareeie.com

Vol. 6, Issue 8, August 2017

Packet Delay is defined as the delay between packets during transmission. Delay has been measured in terms of time units. Proposed approach has lesser delay than that of previous approach due to transmission of enquiry packets over the network for detection of sinkhole attack.

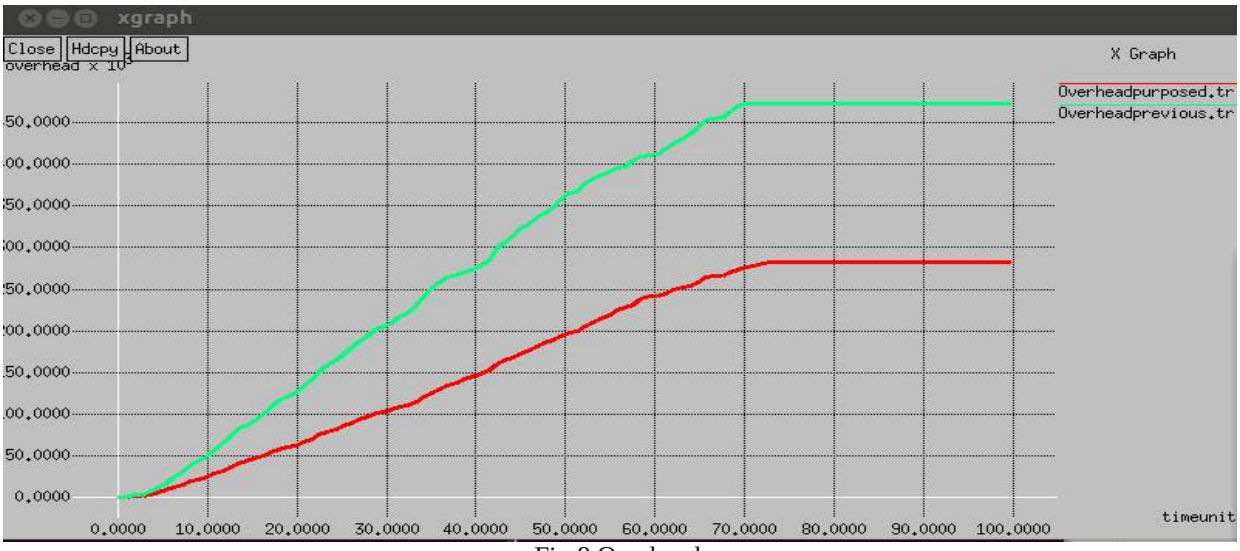

Fig.9 Overhead

Fig.9 is used to represent the network overhead. Overhead has been caused due to routing packets that has been transmitted over the network. Overhead causes various problems over the network. Minimum routing overhead causes better data management and transmission over the network.

V. CONCLUSION

Wireless Sensor Network has been used for sensing various types of information from sensing environment. In the proposed work, AES based encryption approach has been used with AODV routing protocol so that data integrity and confidentiality can be achieved. In the proposed work, reverse tracking mechanism has been used for detection of malicious nodes that degrades performance of the network. In the process of reverse tracking mechanism, all the nodes that are one hop neighbor from the source node are identified by transmitting a message. Then, a reply message is sent and that message is verified if any message has been occurred from other than single hop communication node. Then, the detection mechanism has been enabled for detection of black hole and grey hole attack over the network. In this simulation, various performance evaluation parameters have been analyzed that are used for validation of proposed work. On the basis of these parameters it can be concluded that proposed approach provides better efficiency and performance as compared to previous one.

REFERENCES

[1] A. Vijayalakshmi., "Mobile Agent Middleware Security for Wireless Sensor Networks" IEEE International Conference on Communication and Signal Processing, 2014, pp. 1669- 1673.

[2] G. Kalnoor and J. Agarkhed, "QoS based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks,"*2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, 2016, pp. 1-6.*

[3] Debiao He "A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks" IEEE international Conference on Wireless and Pervasive Computing, pp-453-459, 2014.

[4] Deshpande, P., "Techniques improving throughput of wireless sensor network: A survey", IEEE Conf. on Electric Information and Control Engineering (ICEICE), 2011, pp. 3683 – 3686.

[5] Guerroumi, M., "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink" IEEE International Conference on Information Technology - New Generations, 2015, pp. 307 – 313.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An UGC Approved Journal)

Website: www.ijareeie.com

Vol. 6, Issue 8, August 2017

[6] Geetha, R. "Fuzzy logic based compromised node detection and revocation in clustered wireless sensor networks" IEEE Conf. on Information Communication and Embedded Systems (ICICES),2014, pp. 1 – 6.
[7] Mohamed Guerroumi "Intrusion detection system against Sinkhole attack in wireless sensor networks with mobile sink" IEEE International Conference on Information Technology, 2015, pp. 307- 313.
[8] Mittal, R. "Wireless sensor networks for monitoring the environmental activities" IEEE Conf on Computational Intelligence and Computing Research (ICCIC), 2010, pp. 1 – 5.
[9] Marriwala, N. Rathee, P. "An approach to increase the wireless sensor network lifetime" IEEE Conf. on Information and Communication Technologies (WICT), 2012, 495 – 499.
[10] Mittal, R. "Wireless sensor networks for monitoring the environmental activities" *IEEE Conf on Computational Intelligence and Computing Research (ICCIC)*, 2010, pp. 1 – 5.
[11] Marriwala, N. Rathee, P. "An approach to increase the wireless sensor network lifetime" IEEE Conf. on Information and Communication Technologies (WICT), 2012, 495 – 499.
[12] N.deepika "Secure enhanced energy efficient two tier scheme", IEEE international Conference on Emerging Trends in Engineering, Technology and Science,pp. 32-39, 2016.
.