International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

Detection of Wormhole Attacks using AODV: A Proposed Scheme

Moumita Pramanik, Samarjeet Borah, Diksha Giri

Abstract*: Sensor Networks (WSN) are often vulnerable to several types of attacks due to its open space deployment and large area of applications. Wormhole is one of such attack, which falls under the category of Denial of Service (DoS). In this attack, an attacker takes control of the network services by developing an overlay tunnel called wormhole channel. In this paper, a mechanism has been proposed by appending extra four-bit information to RREP packets which is known to both sender and receiver; thus, reducing chances of wormhole tunnel. The work is based on AODV protocol and simulated in OMNeT, which effectively detect illegitimate attack carriers.

***Index Terms*: Wireless Sensor Network, Energy, AODV, DoS, Wormhole Attack, Detection**

I. INTRODUCTION

Wireless sensor network is a mixture of tiny devices known as sensor nodes with sensing and computing power [3,4]. The sensor nodes act as transmission node which has partial memory and computational capabilities. Each of these sensor nodes has a cell in it as source of its energy [4,8]. In general, we can say that wireless sensor network is distributed in an area where the main aim of the sensor nodes is to collect data from the network. Due to the wide nature of network, the security is one of the major concerns to protect its sensor nodes and protocol from any attackers. Similar to any network technology, WSN is also vulnerable to numerous security attacks in its packet transmission process due to the nature of mobility of sensor nodes [19]. There are some limitations in the security to the wireless sensor network because of its limited storage, computation, communication and processing capabilities. The sensor nodes are densely distributed with limited resources and power in the wireless sensor network to sense and collect data from the region. Mainly the confidential data that are collected by the sensor node must be protected from the unauthorized exposer. This is the main cause of interest to the attacker which leads to various kind of attacks and makes the network vulnerable to the entire intruder. This paper focuses on one of network layer attack namely wormhole attack [2,5,6,19] and its detection and prevention techniques. It is kind of Denial of Service (DoS) attacks in the sensor-based network. Generally, DoS [1,3,10] is achieved by overflowing excessive request to the targeted machine or resource that overload the request to the system, as a result system denied to serve the legitimate requests. This type of attack is intended to interrupt, sabotage or destroy the network safety [12].

Among the various types of DoS attacks in the WSN, wormhole is one of the dangerous types as this attack has no crypto graphical breaks. In these attacks, more than one attacker is associated to each other through the channel that mostly sustained with high speed bandwidth that recognized as wormhole link [18]. Here, two attackers are engaged themselves in the network to constant observe the network and record the useful information of wireless network. In this attack malicious node may gain data packets at a one point and transfer the packets to another malicious node of the network using a separate route known as tunnel. This packet may be altered or tempered by the second malicious node and communicated further. This creates a fake impression to all other nodes that receive packets are broadcasted by the second malicious node are also a genuine node in that network. They unknowingly directed the packets to the previous malicious node or second malicious node as it seems to be neighbors with single-hop distance and also receiving the packets straightway from it. This paper focuses on the wormhole attack and its defensive measure to prevent wormhole attack.

A. Denial of Service (dos) Attacks

A Denial-of-Service (DoS) [1,9,15] attack can be considered as an attempt to stop a network services to its legitimate user by the attackers. It disrupts the network to provide authentic service to the users in time. DoS attacks can take place at various layers of the WSN protocol stack. Some kind of DoS attacks may disturb multiple layers of the network simultaneously or it attempt to exploit interactions between different layers. Network functionality gets disturbed due to the accidental failure of nodes or by the action of malicious node. Common DoS attack attempts to drain out the available resources of the sensor node by sending extra redundant packets and make it a victim node. Subsequently, the genuine users are prohibited to access the network services or resources to which they are authorised [11,19].

Manuscript published on 30 June 2019.
* Correspondence Author (s)
Moumita Pramanik*, Department of Computer Applications, Sikkim Manipal Institute of Technology, Sikkim Manipal University, Gangtok, Sikkim, India.
Samarjeet Borah, Department of Computer Applications, Sikkim Manipal Institute of Technology, Sikkim Manipal University, Gangtok, Sikkim, India.
Diksha Giri, Department of Computer Science, Inspiria Knowledge Campus, Siliguri, West Bengal, India.

B. Types of Wormhole Attack

Wormhole attack is an outbreak association where the attacker nodes communicate through a tunnel called a wormhole link.

The wormhole attack can be classified in various ways. Among these attacks, two very well-known wormhole attacks are in-band wormhole attack and out of band wormhole attacks. In the first type of attacks, invader builds an overlay channel over the existing sensor network. The nature of in-band attack is very destructive and it is one of the most favorite options for attacks to the invader. Whereas the out of band usages the divergent wireless network in order to achieve the attack in the network [19]. Other significant wormhole attacks are open wormhole attacks, half open wormhole attack and closed wormhole attack.

Open wormhole attack [19]: In this attack, attacker node sends route request packets in the network and the other nodes in the network assume that the request is from their direct neighbours nodes in presence of the malicious node. This way both the nodes reveal their uniqueness in the network.

Half open wormhole attack [19]: In this attack only one attacker nodes reveal its identity and another hides its identity in network. Hence, the packets alteration is carried out only in one side in the network.

Closed wormhole attack [19]: In this type, data packets are not tempered by the attacker nodes. Both of the nodes keep themselves hidden in the network. They skillfully observe to the movement of the packets in the network and display the direct path. When any source node finds its path using some system, then these unseen node response and source nodes trapped in this set-up.

C. Different classification of Wormhole Attack

Depending upon the packet encapsulation, channel used, transmission power and packet relay and protocol used, wormhole attacks are classified as follows:

- Attack through encapsulating packets.
- Attack by means of out-of-bound channel.
- Attacks through incorporating high-power transmission medium
- Attacks by manipulating packet relay
- Attack through distorting protocol itself

Submit your manuscript electronically for review.

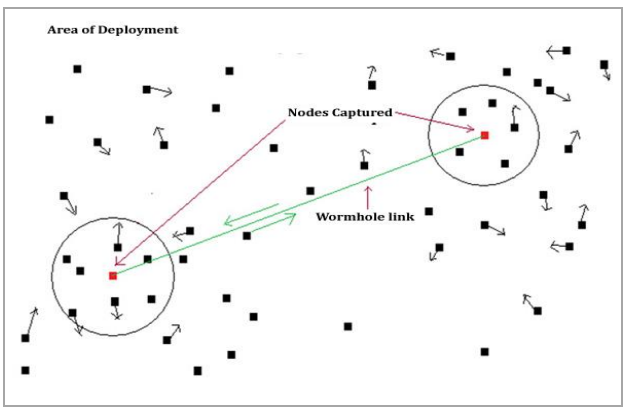

Fig 1. Wormhole Attack Scenario

Figure 1 shows wormhole outfits in a WSN where various nodes are positioned along with the two malicious nodes (here labelled by red colour) in the network. Usually, for any packet transmission, the data packets have to travel very long routes to reach its destination, but through a fabricated shortest path of the attacker nodes transmitted the packets very quickly. The wormhole linkage given in the Figure 1 represents the path through which attacker nodes tunnels the packets.

D. Techniques to mitigate Wormhole Attack

To mitigate the various wormhole attacks several precautionary measures are considered in the organisation of wireless sensor network. Many of them are discussed here. One of these methods is location and time based network approach [11]. In this network organisation, the position of current node with its neighbour node is analyzed before sending any packet or receiving any packet. It also estimates the distance from the sender node and receiving node and the approximate time required by the packets to traverse in the identified path.

Another approach is hardware based which uses a directional antenna [6]. In this approach one node send its packet in one direction and neighbour node can able to received packet from a specific direction only. Directional antenna confirms the neighbour nodes position so that it will able to receive the packets in the network in the right direction only.

In Graph based approach, graphical theory is used to mitigate the attack of wormhole. This protocol is aligned on the use of limited location-aware guard nodes (LAGNs) [11]. Here, the location and initiation of the nodes are well identified with the help of GPS receivers. It uses local broadcast keys to validate its authenticity, as it uses these keys only between one instant of hop neighbours. The difficulty for the wormhole attackers is to decrypt the packet which was encrypted with the pair-wise key at one end node in the network. During the key establishment, the use of hash massage from LAGNs helps to sense the wormhole in the network. If there are any wormhole exits, a node notice inconsistent in receiving messages from different LAGNs, otherwise node (guard) will not hear the same message twice.

Another wormhole detection tool is based on statistical analysis of multipath routing (MR) [17]. Multipath routing techniques decreases the adverse effect of variable wireless links and the frequently changing network topology. The feature assists to identity the intrusion especially in the network that follows the on- demand and multipath routing protocol. In Cluster Based Approach [7,8], wormhole is a controlled by the attacker, between two locations in the network. The main purpose of attacker is to impresses the clustering protocol. In this, malicious node are interfere the communication between cluster heads (CH) and able to attract the network traffic. Wormhole attacks identification is carried out based on clustering method where many clusters are formed randomly and also the cluster heads are picked dynamically. After the clustering and selection of cluster heads, its member has been identified.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Each node broadcast cluster head massage to its one-hop neighbour. Node must receive at least one massage with CH id; also massage must be received before other massage from neighbour to the requested node.

are continuing for searching the effective procedures to identification and prevention of the wormhole attacks. Many of the identification techniques are discussed in the following table.

Table 1. Wormhole Parameters

Parameters	Normal AOMDV (45 nodes)	Wormhole AOMDV (45 nodes)	Proposed AOMDV (45 nodes)	EE-TS (Exist) (45 nodes)	EE-IDS-AODV (45 nodes)	EE-IDS-STR (45 nodes)	EE-IDS-OSTR (45 nodes)	Dabi et al. [6] (10 nodes)
Average Throughput	280.77	196.17	286.4	-	-	-	-	51
Average end to end delay	97.285	107.324	80.8036	189	179	174	173	1.4
Packet delivery fraction	0.8188	0.3247	0.7892	0.49	0.56	0.59	0.63	.34
Energy Consumption(J)	-	-	-	0.63	0.59	0.56	0.54	-

E. Identification and Prevention of Wormhole Attack

There are various identification and prevention techniques of wormhole attack. Identification of this attack is less difficult job as compare to anticipate the attack. Many research works

Table 2. Summary of Wormhole Attacks Identification Techniques

Method	Protocol	Approach	Advantages	Disadvantages
Sharma et al. [11]	AODV	Based on Location	Applicable in: • Hidden attack • Exposed attack.	Link failure causes more energy consumption
Parmar et al. [2]	AOMDV	Based on Location	• End to end delay • Less Cost	Node Mobility is the main concern
Maidamwar et al [14]	LEACH	Based on Clusters	Threshold based cluster-heads that changes for every round.	• Random selection of cluster-heads • Clusters are dynamic in nature
Khandare et al [13]	-	Encryption based – Public Key	• Secure communication • Encryption used	Higher energy consumption
Shahryar et al. [8]	M-LEACH	Cluster based approach	• Attack detection and localization prior sending data • Broadcasts packets • Independent of network data.	• Delay metric is not optimal • Partly cluster-formation overhead is higher • Detection time is somewhat more
Singh et al. 2014, [16]	-	Mixed Approach	Applicable for all types of wormhole attacks.	• The network must work on uninhibited mode • Each sensor node listens to the packets transferred by its own neighbour nodes

II. PROBLEM DEFINITION

In the wormhole attack, a malicious node bypasses the message received in one end and replays the message in another end in the network using a potential link. In this attacks, attacker form a wormhole link even for the packets that not addressed to itself as it can eavesdrop the packets in the wireless network and tunnel them at the opposite end node of wormhole link in the WSN. The wormhole tunnel can be structured in different forms using packet encapsulation, through a wired link (out of band hidden channel), or high powered transmission. The tunnel forms an impression that the two end points are very adjacent to each other. This is carried out by transmitting packets very faster with the help of less number of hops as related to the packets sent over standard routes. This allows an attacker to undermine the accurate operation of the routing protocol, by redirecting several routes in the network. The wormhole attack is a network layer attacks which is classified according to the network protocol stacks. Higher layers may not be stable in packets broadcast; however, the network layer tries to delivers its best service. In a large network, a message often has to travel many hops before reaching its destination. Packet delivery poorly affect by various reasons includes the broken down of dedicated link of a node with the next node and the inaccurate routing information of the neighbouring nodes; leads to one of the reason for wormholes attacks remain unnoticed. In the wireless sensor network, mobility of the nodes is a vital issue, sometime the hop count techniques are not able to provide the knowledge about the specific location of the node, and the invisible wormhole nodes take the advantage of this drawback to fulfil its intension. In Cluster based approach, clusters are formed dynamically where cluster heads (CH)s are not uniformly distributed as the cluster head is selected dynamically. Cluster head may be situated at the edges of the cluster; it is chosen random which does not consider the energy consumption. The difficult task in a WSN is to get the exact location of the nodes, so the detection of malicious nodes and prevent the attacks become a very difficult task.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Therefore, location based techniques help to get the particular location of the sensor nodes and help in hop counts in network. In Ad-hoc On-Demand Distance Vector (AODV) [2] routing the sender node broadcasts the route request packets to all the nearby neighbours and the transitional node that received the packet request check the request. If the destination of the packet request is matched with the intermediate node, it will reply with route reply message otherwise the request of the sender node is forwarded to other neighbour nodes for further enquiry.

A. Analysis

In wireless sensor network several sensor nodes are spread over a wise area and the wormhole attack is one of the critical attacks where the malicious nodes form a tunnel or link between the each other. These attacks bend the path for packet transmission by sending fabricated routing data to the neighbour node in the network. The wormhole attack can be achieved various ways by disturbing the network, by controlling potential routes or controlling the routing protocols in the network. The attacker continuously analysis the traffic information of the packets over the network and prudently drops the sensitive data packets. To resistant the data packets, packets are shifted to the next nodes using some explicit modulating techniques. Sometime encryption technique is also used to protect the data packet for transmission and encrypted data packets are broadcasted in the multiple routes [14]. In cluster based network, specific sensor nodes are carefully chosen to form a cluster and each cluster comprise one or more cluster heads of its own. Typically, a cluster head (CH) is selected based on the factors like reliability, hop-distance, dependability. In clustered network, the adjacent group is formed with the nodes using any specific clustering process. The distance between the associate nodes and the cluster head usually one hop and the packets are sent sequentially via the cluster head to the base station. In this network, when any node needs to send data packets, it encrypts the packet with its own public key and sent the packet to the cluster head. On receiving the encrypted data packet cluster head broadcast the packets to the base station. Hence, if any wormhole node is exist in the path it unable to decrypt the packet. In case of cluster head expire, a substitute member node is chosen depending on the specific parameters so that it can help to prevent the wormhole attacks and give a secure data transmission over the network.

B. Solution Strategy

Here, an attempt has been made to counter the wormhole attacks in WSN environment using additional bits with RREP message. Various measures to protect the data transmission in WSN include secure broadcasting and multicasting of data packets, protecting the routing protocols, resisting the attacks against traffic analysis, protecting sensor nodes, detection of intrusion, protecting against physical attacks, secure data aggregation and trust management. To defend against wormhole attacks, an attempt has been made by implementing a secure algorithm in AODV. The RREQ (Route Request) message is sent by the source node to the destination node and a RREP (Route Reply) message is expected by the source from the destination. The RREP message includes the information of hop count of the route traversed from destination to the source. RREP sent by the destination is added with four extra bits with a specific integer. On receiving the RREP, the source node checks the signature and if signature is matched with the specific signature, source node sends encapsulated data packet through route where the destination address is mentioned. If some malicious activities found, the data packet is send via different safe route. The energy used to send the message is calculated, if the energy is not losing, the route may contain wormhole node. Thus the path is avoided. The data packet send to the destination is encapsulated so that secured communication is maintained. Hop count information is also maintains in the routing table of each nodes for further cross verification.

III. Proposed Methodology

Primarily the sensor nodes are organized randomly in a network area. The sensor nodes have little computational power which helps to sense the data in the network and send the data to the base station. Here ad-hoc on-demand distance vector routing protocol (AODV) is used to find out the path between the source node and destination node. AODV uses three main packets namely route request packet (RREQ), route reply packet (RREP) and route error packet (RRER) for the transmission.

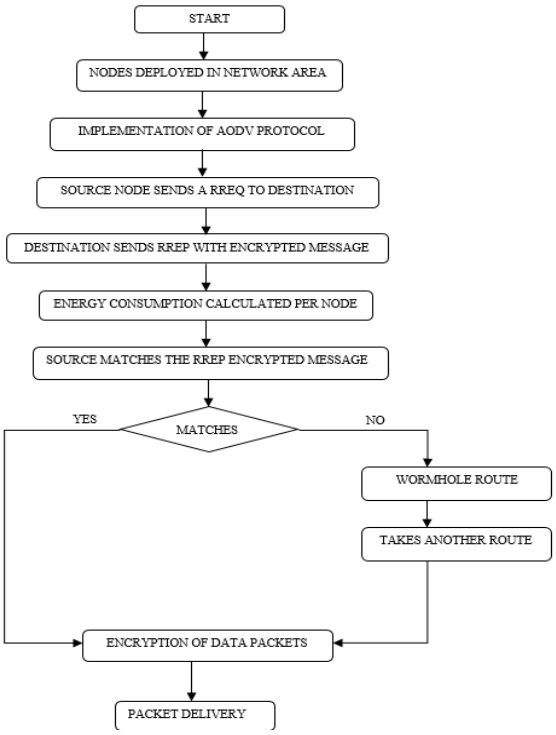

Fig 2. Proposed Wormhole detection model

In this process to sender node and receiver node checks the route information in the routing table before sending the packets to each other. If the route information is found in its local routing table it gives the path immediately otherwise it broadcast the RREQ information to the neighbour nodes. Each neighbour node checks the destination information and route information in its route table. Whenever the destination node receives the RREQ packets and on successfully matched with the required destination node information, it sends RREP packets to the source node with the same route through which RREQ packets has been reached.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

The routes are again stored in the local routing table at the source node.

In the approach the RREP packets send by the destination node is added with extra four bits of information with the packet of a particular integer that is known to the source node. On receiving the RREP packet at the destination node checks the added bits with its corresponding digits. If the bits are matched then it is assumed that the receiver node is not a malicious node and if bits are not matched then is considered that there may exist malicious node in that route. Once the source node aware of the existence of malicious node, it sends the encrypted data packet via a different safe route. The data packets are encrypted using strong encryption techniques to provide the secure communication of the data packets from source node to destination node.

Table 3. Algorithm of the proposed detection model

Start
Nodes are deployed using AODV Protocol.
Simulate AODV protocol using OMNeT.
Sender node broadcast REEQ packet to destination node via neighbour nodes.
Destination node sends RREP with data bits to the sender on receipt of REEQ packet.
The source node checks the signature of the RREP received.
IF (signature matched) Then
Source node of the RREP is a true destination node
Else
Malicious Node
End IF
Energy consumption for data transfer is checked
Encapsulation of data packet with a strong encapsulation mechanism
Encrypt with public key (n, e):
- r ←R [0, n-1]
- C0 ← re mod n
- W ← KDF(r)

Decrypt with private key (n, d)
- r ← C0d mod n
- W ← KDF(r)

IF (Malicious node present in the route) Then
Send data packet via different safe route
ELSE Send data packet via same route
END IF

IV. Results And Discussion

A. Simulation Area

To evaluate the effectiveness of above approach, we use the Castalia simulator as a simulation platform. We have setup a sensors network to simulate the transmission between a set of sensors nodes and a base station. Here, we segregated the network into few sectors and deploy the sensor nodes, which help to save the energy of sensor nodes in some extend. Table 4 represents the parameters of our model:

Table 4: Parameters of the Model

Parameters	Value
Simulator	OMNeT (Castalia framework)
Simulation Duration	10 sec
Area	30 meter X 30 meter
No. of Nodes	50
Routing Protocol	AODV
Channel Type	Wireless Channel
MAC Protocol Name	TunableMAC

B. Performance Analysis

In order to analysis of the performance of the above methodology in a wireless sensor network, we use the normal case and attack scenario. The sensor nodes have limited energy and sink which is considered to have a vast energy input. In this simulation, we undertake the sensor nodes and the sink are fixed. To check the correctness of the above structures, we plot a sensors network with 50 sensor nodes with simulation area of 30×30 meters and these sensor nodes are randomly distributed in the network. The performance of the network is analysed on the basis of consumption of energy and packet drop ratio.

Packet Drop Ratio

Packet drop ratio is the average of the number of packets produced by the networks and number of packets dropped by the network. Figure 3 shows that in case of wormhole attack, the number of packets dropped in the network is higher than in case of normal situations. Hence, it is determined that the packet dropped ratio in increased significantly in the presence of malicious nodes in the network.

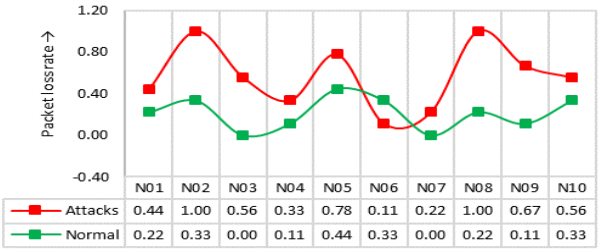

Fig 3. Packet Loss Rate

Packet Receive Rate

Packet receive rate is the average number of packets received by the nodes in the network. Figure 4 shows the number of packets received per node in the case of wormhole attack and in case normal situation (with the implantation of the above algorithms).

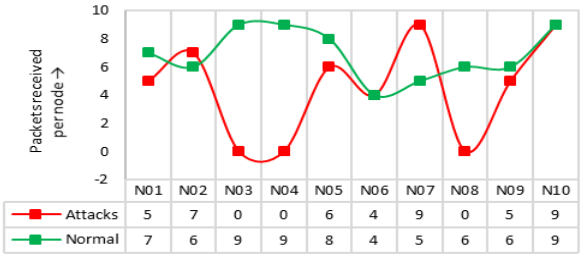

Fig 4. Packet received per node

Energy Consumption

The energy consumption (in Joules (J)) is analysed in Figure 5. It is observed that in the presence of wormhole attacks the energy consumption of the node is very high than that of a normal operation. It is noticed that the sensor node consume more energy in the presence of malicious node which leads to increase the overall energy consumption in the network for any data transaction. In other words, it can be said that in wormhole attack the performance of the nodes is reduced significantly which degrade the entire performance of the network in a large scale.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

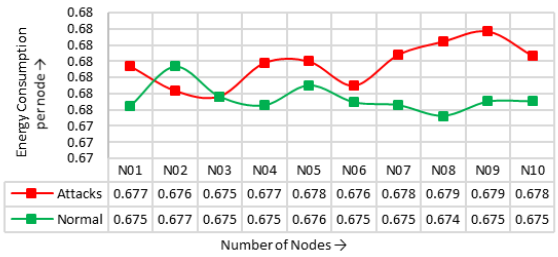

Fig 5. Energy consumption per node

Remaining Energy

Figure 6 shows the remaining energy of the nodes after transmission of packets. According to the figure it shows that due to an attack less amount of energy is remaining per node in the network.

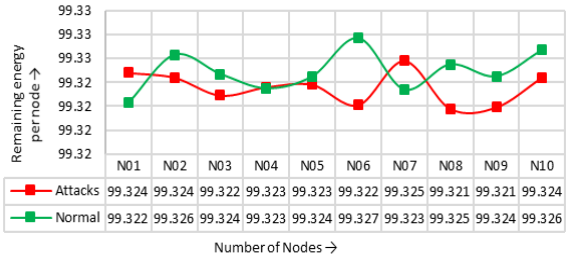

Fig 6. Remaining energy per node

Figure 7 shows the detailed list of parameters and output during the simulation. The setup is developed in OMNeT where the nodes deployed in the simulation area and a RREQ packets are sent by a source node.

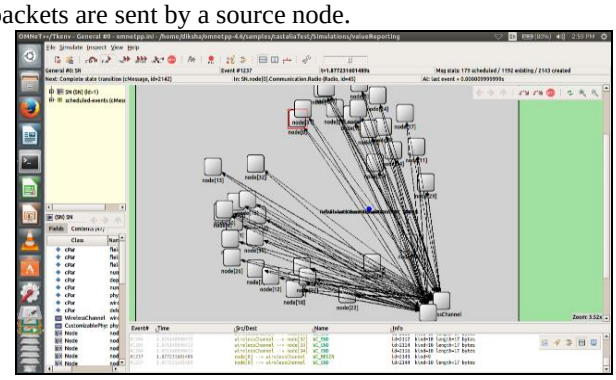

Fig 7. Scenario of AODV in OMNeT

The Figure 8 represents a simulation of nodes broadcasting of a RREQ message.

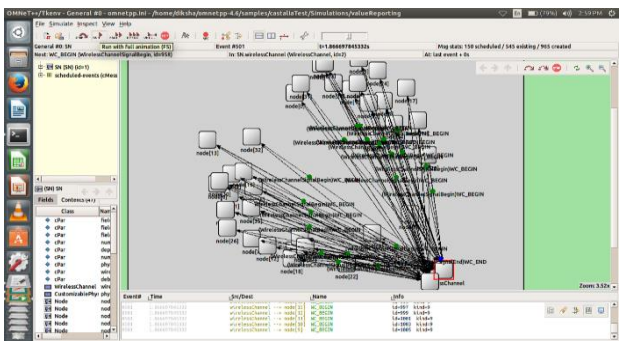

Fig 8. Scenario of RREQ Broadcasting

Our offered solution strategy focused on the security of the data packet transmission in a wireless sensor network and also provides an effective security solution to preserve the overall performance of the network. This paper provides a thorough and broad revision on the wormhole attacks in wireless sensor networks with different management techniques.

Here, we discussed many efficient wormhole detection and prevention techniques along with the advantages and disadvantages in wireless sensor network that suggested by various researchers time to time. There are exists many other techniques to identify wormhole attacks, and we use the above solution strategies to detect the wormhole attacks and provide a secure data transmission technique over a wireless sensor network

V. Conclusion

Wormhole attack is difficult to detect and found to be a challenging work. This attack results in route discovery as well route discovery errors, in addition to the degradation of the communication between the nodes of the network. The proposed method is based on wormhole attack prevention. However, detection of wormhole node is difficult but prevention methods are being implemented. In this work, malicious nodes are implanted in the network and results are examined through simulation. However, implementing this methods or algorithm in a real scenario or a sensor network is more difficult due to limitation of resources.

The proposed algorithm can be improved to detect wormhole attack. The RREP packet sent by the destination can be encapsulated with a code where all the route node information can be given. Also the data packet can be further fragmented into small packets and transmitted via multiple paths to the destination. At the destination, the received packets (through various routes) can be put together to get a valid information. This may allow a secure communication. Additionally, the malicious nodes may not be able to assemble the packets into a valid information as it transmits through different routes. The broken links can be avoided with the help of acknowledgement messages sent by the destination node. The proposed approach presents a decent solution for secure exchange of information while taking into consideration the constraints and limitations imposed by this environment.

REFERENCES

1. A. D. Wood, J. A. Stankovic, Denial of Service in sensor Networks, Computer, Vol. 35(10), 2002, pp. 54-62.
2. Amish, Parmar, and V. B. Vaghela. "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol." Procedia computer science 79 (2016): 700-707.
3. Annie Jenniefer, John Raybin Jose, Techniques for Identifying Denial of Service Attack in Wireless Sensor Network: A Survey, Intl J. of Advanced Research in Computer and Communication Engineering, Vol. 3(6), 2014.
4. Dargie, Waltenegus, and Christian Poellabauer. Fundamentals of wireless sensor networks: theory and practice. John Wiley & Sons, 2010.
5. Diksha Giri, Samarjeet Borah, Ratika Pradhan, Approaches and Measures to Detect Wormhole Attack in Wireless Sensor Networks: A Survey, Advances in Communication, Devices and Networking, Springer LNEE, Vol. 462, 20198, pp. 855-864

6. Honglong Chen, Wendong Chen, Zhibo Wang, Zhi Wang, Yanjun Li, Mobile Beacon based Wormhole Attackers Detection and Positioning in Wireless Sensor Networks, Intl. J. of Distributed Sensor Networks, 2014, ISSN 1550-1329.
7. Kehkasa Mirza, Vaidehi Shah, Using Cluster based Approach Wormhole Attack Detection in Wireless Sensor Network: A Survey, Intl. J. of Innovative Research in Science, Engineering and Technology, Vol. 4(12), 2015.
8. Maliheh Shahryari, Hamid Reza Naj, A cluster based approach for wormhole attack detection in wireless sensor networks", J. of Advanced Computer Science & Technology, Vol. 4(1) (2015), pp. 95-102.
9. Monika Malik, Yudhvir Singh, A Review: DoS and DDoS Attacks, Intl. J. of Computer Science and Mobile Computing, Vol. 4(6), June 2015, pp. 260-265.
10. Nagarathna C. R., Chinnaswamy C. N., Technique to detect and avoid the Denial of Service Attacks in Wireless Sensor Networks, Intl. J. of Research in Engineering and Technology, Vol. 3(5), 2014.
11. Nishant Sharma, Upinderpal Singh, A Location Based Approach to Prevent Wormhole Attack in Wireless Sensor Networks, Intl. J. of Advanced Research in Computer Science and Software Engineering, Vol. 4(1), 2014.
12. Poonam Rolla, Manpreet Kaur, Review of Prevention Techniques for Denial of Service (DOS) Attacks in Wireless Sensor Network, Intl. J. of Scientific & Technology Research, Vol. 5(7), 2016.
13. Pravin Khandare, N. P. Kulkarni, Public Key Encryption and 2Ack Based Approach to Defend Wormhole Attack, Intl. J. of Computer Trends and Technology, Vol. 4(3), 2013, pp. 247-252.
14. Priya Maidamwar and Nekita Chavhan, Research on Qualitative Analysis of LEACH with Wormhole attack in Wireless Sensor Network, Intl. J. of Advanced Computer Research, Vol. 3(1), 2013.
15. Raymond, David R., and Scott F. Midkiff. "Denial-of-service in wireless sensor networks: Attacks and defenses." IEEE Pervasive Computing 1 (2008): 74-81.
16. Rupinder Singh, Jatinder Singh, and Ravinder Singh, WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks, Mobile Information Systems, Volume 2016, Article ID 8354930, http://dx.doi.org/10.1155/2016/8354930, pp. 1-13.
17. Saswati Mukherjee et al., Wormhole Detection Based on Ordinal MDS Using RTT in Wireless Sensor Network, Journal of Computer Networks and Communications, Vol.1 2016, ISSN 2090-7141.
18. Shiyu Ji, Tingting Chen, Sheng Zhong, Subhash Kak, DAWN: Defending against wormhole attacks in wireless network coding systems", INFOCOM 2014 Proceedings, IEEE, pp. 664-672, 2014.
19. Ughade, Saurabh, R. K. Kapoor, and Ankur Pandey. "An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach." International Journal of Recent Development in Engineering and Technology 2.4 (2014): 102-109.

AUTHORS PROFILE

Moumita Pramanik holds her Bachelor degree in Software Systems from North Bengal University and Master Degree in Computer Science & Engineering from Sikkim Manipal Institute of Technology (SMIT) in the year 2014. Her interest area includes Network Security, Wireless Sensor Network and Image Processing. She is currently working as an Assistant Professor in department of Computer Applications, SMIT

Samarjeet Borah received his Master's degree in Information Technology from Tezpur University, in the year 2006 and PhD degree in Engineering from Sikkim Manipal University, India, 2010. He is currently working as Professor at Department of Computer Applications, Sikkim Manipal University (SMU), Sikkim, India. Dr. Borah handles various academics, research and administrative activities at SMU. He is involved with various funded projects sponsored by AICTE (Govt. of India), DST-CSRI (Govt. of India) and Dr. TMA Pai Endowment Fund, India. He is also associated with IEEE, ACM (CSTA), IAENG and IACSIT. Dr. Borah is involved with various journals of repute in the capacity of Editor/Guest Editor such as IJSE, IJHISI, IJGHPC, IJIM, IJVCSN, JISys, IJIPT and IJDS.

Diksha Giri pursued her Bachelor and Master degree from Sikkim Manipal Institute of Technology (SMIT) in 2015 and 2017 respectively. Her interest area includes Wireless Sensor network and Routing Protocols. She is currently working as Assistant Professor in Inspiria Knowledge Campus, Siliguri.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)