Prevention of Wormhole Attack in WSN using Energy Optimized Scheme based on Hop

Yogesh Hassani[1] and Prof. Rakesh Shivhare[2]

1. M.Tech. Scholar, Radharaman Engineering College, Bhopal (MP)
2. Assistant Professor, Radharaman Engineering College, Bhopal (MP)

ABSTRACT

Sensor Network is infrastructure-less network in which communication takes place between mobile nodes, packet is transmitted with the help of intermediate nodes. Nodes are capable of moving free in the network, they can leave or join the network when it is needed. Hence with the dynamic changing nature of Sensor network is vulnerable to various security attacks. These attacks hinder the network performance Mobile ad hoc networks, security is considered as one of the critical issue. Sensor network are comprised of nodes that must cooperate to dynamically establish routes using wireless links. Routes may involve multiple hops with each node acting as a host and router. Since ad hoc networks typically work in an open entrusted environment with little physical security, they are subject to a number of unique security attacks like wormhole attack. The wormhole attack is considered to be a serious security attack in multi-hop ad hoc networks. Unlike many other attacks on ad-hoc routing, a wormhole attack cannot be prevented with cryptographic solutions because intruders neither generate new, nor modify existing, packets, but rather forward existing ones. In this paper work is concentrate on the noxious conduct of AODV under wormhole attack. On the premise of previous information check and zone data we identify wormhole and for counter active action we stream normal way node id in the system.

In this paper a simple technique to effectively detect wormhole attacks without the need for special hard ware and/or strict location or synchronization requirements is proposed. The proposed technique makes use of variance in routing information between neighbors to detect worm holes. The proposed approach have higher packet delivery ratio, lower routing overhead, lower energy consumption and higher throughput.

Keywords:-Wireless Network, Sensor Network, Wormhole Attack, Network Venerability, Security, AODV

1. INTRODUCTION

WSNs are one of the most advanced technologies in the present world. These networks have enabled many possibilities such as modern and satellite telecommunication, space communication, military systems, and underwater networks. This technology is also used in traffic monitoring, weather monitoring, fire detection, forest monitoring, smart homes, and the Internet of Things (IoT). Security is a major concern due to the decentralized nature of WSNs. These networks are prone to many security attacks based on node capture and node hacking, leading to the compromise of data and security.

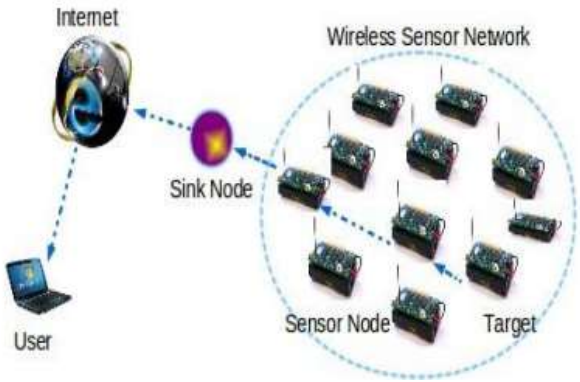

Figure 1: Illustration of wireless sensor network

The sensor nodes collect the data and send to the base station for processing and then it sent to the user via a wireless medium. A WSN has numerous applications in many fields. They are deployed in many places. A

WSN is used in these applications to monitor the maintenance, improve the productivity and enhance the security and safety. For wide deployment, it is required that the sensors should be made smaller and inexpensive. There are also many methods being proposed to secure the network from different kinds of attacks. Fig. 2 shows the applications of WSN's in numerous fields. They are deployed in many places and the sensors have a capability to give a warning at emergency situations.

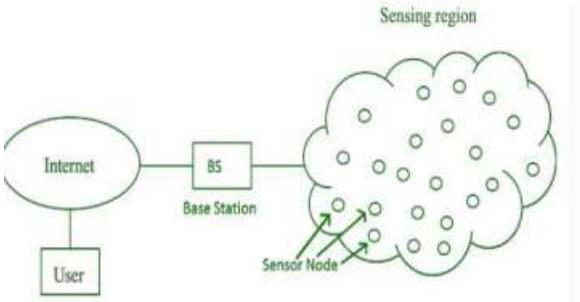

Figure 2: Actual image of a WSN with multi-hop communications

There are many types of attacks targets routing protocol in WSNs referred routing attack. The wormhole attack is a grave Attack. Fig. 3 shows two attackers locate themselves as two conniving sensor node tunnel control and data packets between each other with intention of creating shortcut in WSN. The first malicious sensor eavesdrops on first location to receive the control and tunnel packets to second malicious sensor, then second malicious sensor forwards the received packets to intended destination. They affect the network by changing or drop send packets or collecting packets with goal traffic examination/encryption breaking. The influence of system is powerless in discovering the routes that are longer than 2 hops thus the result in false network topology. This works contributes secure WSN against wormhole attack by proposing an energy preserving secure measure.

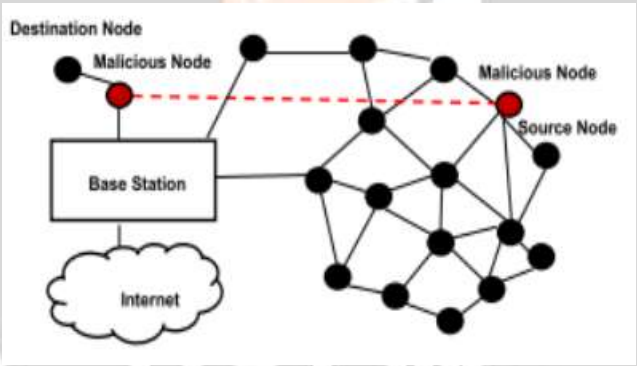

Figure 3: Wormhole attack in wireless sensor network.

2. LITERATURE SURVEY

The authors in [12] propose implementation of an attack fully functional worm hole in a £ 802.1 IPv6 network mobile wireless ad hoc (MANET) test bed running a routing protocol proactive. Using customized analysis tools the authors studied the traffic in the MANET at three different stages : i) regular operation, ii) a worm hole " Benin " joining distant parts of the network , and iii) stress the worm hole attackers who control a link in the MANET and drop packets at random. The focus of the authors was to detect anomalous behavior using timing analysis of routing traffic within the network. All authors first showed how to identify intruders based on the protocol irregularities that their presence creates once they begin to drop traffic. More importantly, the authors have continued to demonstrate that the mere existence of the worm hole itself can be identified, before the intruders begin the packet drop phase of the attack, by applying simple techniques of signal processing the arrival time of the routing management traffic. This is done by relying on a property of proactive routing protocols - that the stations must exchange management information on a specified periodic basis. This exchange creates identifiable traffic patterns and an intrinsic fingerprint "valid station" that can be used for intrusion detection.

In [15] Wormhole attacks in mobile ad hoc networks (MANET) have long been considered a serious threat to MANET‟s routing. Most of the existing proposals rely on GPS devices and require that the node's clocks are synchronized. Such constraints naturally lead to limitations of applicability since GPS does not operate well in obstructed areas, and clock synchronization in MANET is not always accurate. In this paper, the authors have proposed an efficient and simple way to detect wormhole attacks, using a technique called reference broadcast. GPS devices are not required, and clocks do not need to be synchronized. In fact, no particular assumption is made on the communication equipment. The authors have

shown that solution given in this work can be easily implemented; using either the well-known routing protocol OLSR or any neighbor discovery protocol. The proposed solution also exhibits a high degree of accuracy in detecting wormhole attacks

In [10] Wormhole attacks are considered as a severe security threat in multi-hop wireless ad hoc networks [11]. In this paper, the authors propose an Energy-Efficient Scheme Immune to Wormhole attacks (our so-called E2SIW). This protocol uses the location information of nodes to detect the presence of a wormhole, and in case a wormhole exists in the path, it finds alternate routes involving the nodes of the selected path so as to obtain a secure route to thedestination.Theprotocoliscapableofdetectingwormholeattacksemployingeither hidden or participating malicious nodes. Simulations are conducted, showing thatE2SIW can detect wormholes with a high detection rate, less overhead, and can consume less energy in less time, compared to the De Worm wormhole detection protocol, chosen as benchmark.

3. DESIGN AND IMPLEMENTATION

In proposed algorithm all decision will be taken on the basis of value of maximum hop distance i.e. maximum number of hop distance in alternate route between every pair of beacon node and detecting node is discover by AODV. If it's greater than maximum hop distance, then it's declared there is wormhole between beacon node and detecting node, elsewhere not.

To overcome this demerit proposed methodology combine the feature of neighbor node information scheme with beacon node scheme in order to overcome the demerit of both being alone. In proposed methodology for calculating maximum hop distance each and every node behave like beacon node and find the path having the largest number of node over the entire possible path between it and it's detecting node and consider average value highest hop distance of the entire node as maximum hop distance over the network.

4. EXPERIMENTAL RESULTS

- **Packet Delivery Ratio:** Packet delivery ratio of total number of packets successfully delivered during data transmission to total number of packet send. For any ideal wormhole detection technique it is required that it has higher Packet delivery ratio.

Table 1: Packet Delivery Ratio

Network Density	Hop	RTT
10	97	95
	95.12	93.45
30	93.79	91.98
40	89.56	87.56
50	85.96	83.95

- **Throughput**: -The fraction of the channel capacity for effective transmission (packets successfully delivered to the destination data) is given and is defined as the total number of packets received by the destination. It is in effect a measure of the efficiency of a routing protocol. In any sensor network it is required to have higher throughput i.e. need to increase rate of successful packet transmission.

Table 2: Throughput

Network Density	HOP	RTT
10	1582.61	1055.07
20	1582.45	1054.97

30	1582.68	1055.07
40	1650.9	1100.68
50	1581.57	1054.43

- **Energy Consumption:** - Energy consumption means battery power used by any node for successful transmission. Higher energy consumption degrades the survival of network. And lower energy consumption maintains longer survival of network. For any ideal worm hole detection technique it is required that it has lower energy consumption, whereas existing approach by using RTT (Round Trip Time) Based On Ad hoc On demand Multipath Distance Vector routing Protocol have higher energy consumption as compare to proposed methodology by using Hop (Hop count)- Based on AODV routing Protocol as shown in Table3.

Table 3: Energy Consumption

Network Density	HOP	RTT
10	126.83	137.273
20	130.23	141.45
30	134.36	142.63
40	137.63	146.45
50	141.23	152.63

5. CONCLUSION

The wormhole is a major problem in the field of wireless network. To take this problem as a challenge this work has proposed an approach to detect and prevent the wormhole attack from the network. This is some kind of defensive mechanism. This is beacon neighbor node approach to defense wormholes in mobile ad-hoc network. The approach uses the two methods having their own limitation. This work uses the positive points of these approached and combined it. The results of the proposed approach are batter then the previous approaches in order to detect the worm hole in route suggested by routing protocol.

REFERENCES

[1]Wateen A.Aliady and Saad A.Al-Ahmadi, ‘‘Energy Preserving Secure measure against Wormhole attack in Wireless Sensor Networks”, IEEE Commun. Mag.,vol 7,July 2019

[2]Lijun Pei, Fanxin Wu, “Periodic solutions, chaos and bistability in the state-dependent delayed homogeneous Additive Increase and Multiplicative Decrease/Random Early Detection congestion control systems”, Mathematics and Computers in Simulation, Elsevier, 2020.

[3] Farkhana Muchtar, Abdul Hanan Abdullah , Mosleh AlAdhaileh ,Kamal Zuhairi Zamli, “Energy conservation strategies in Named Data Networking based MANET using congestion control: A review”, Journal of Network and Computer Applications Elsevier 2020

[4] Farkhana Muchtar, Abdul Hanan Abdullah , Mosleh AlAdhaileh ,Kamal Zuhairi Zamli, “Energy conservation strategies in Named Data Networking based MANET using congestion control: A review”, Journal of Network and Computer Applications Elsevier 2020.

[5]Z. Qian and Y.-J. Wang, ‘‘Internet of Things-oriented wireless sensor networks review,’’ J. Electron. Inf. Technol., vol. 35, no. 1, pp. 215– 227, 2014.

[6]Bharat Bhushan1 · Gadadhar Sahoo, "Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks",©Springer Science+Business Media, LLC 2017.

[7]K. Y. Ajay, T. Sachin, "QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs," Peer-to-Peer Networking and Applications, vol. 10, Pp. 897–909, 2017

[8] S. Zeadally E. Yaprak1 Y. Li X. Che , "A Survey of Network Performance Tools For Computer Networks Classes" ,Division of Engineering Technology, 2001

[9] Asha Ambaikar, H.R. Sharma, V. K. Mohabey , " Improved AODV for Solving Link Failure In Manet" , International Journal of Scientific & Engineering Research, Volume 3, Issue 10, Octob er-2012 1 ISSN 2229-5518 2012.

[10] Sunil Kumar and Pankaj Negi , "A Link Failure Solution in Mobile Adhoc Network through Backward AODV (B-AODV)", IJCEM International Journal of Computational Engineering & Management, Vo11,January 2011 ISSN (Online): 2230-7893, 2011

[11] Ravindra .E, VinayaDatt V Kohir and V. D Mytri , "A Local Route Repair Algorithm Based On Link Failure Prediction In Mobile Adhoc Network", World Journal of Science and Technology 2011, 1(8): 64-67 ISSN: 2231 – 2587, 2011.

[12] Srinath Perur, Abhilash P. and Sridhar Iyer , "Router Handoff: A Preemptive Route Repair Strategy for AODV" IEEE, 2003

[13] Donatas Sumyla, " Mobile Adhoc Networks" , IEEE Personal Communications Magazine, April 2003, pp. 46-55.

[14] Amandeep Singh Bhatia and Rupinder Kaur Cheema ,"Analysing and Implementing the Mobility over MANETS using Random Way Point Model" ,International Journal of Computer Applications (0975 – 8887) Volume 68– No.17, April 2013

[15] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester , " An overview of Mobile Adhoc Networks: Applications and challenges", Sint Pietersnieuwstraat 41, B-9000 Ghent, Belgium ,2005

[16] Priyanka Goyal, Vintra Parmar and Rahul Rishi , " MANET: Vulnerabilities, Challenges, Attacks, Application" , IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011