Engineering Universe for Scientific Research and Management
(International Journal)
ISSN(ONLINE) : 2319-3069
Vol. 9 Issue 3
March 2017

Wormhole Attack Detection and Prevention over Sensor Network: A Review

Dilendra Kumar Bisen[1], Hansha Acharya[2], Anurag Jain[3]
Department of Computer Science & Engineering
Radharaman Institute of Technology and Science, Bhopal[1, 2, 3]
dbbharat.786@gmail.com[1]

Abstract
Wireless Sensor network is infrastructure-lessnetwork 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 Sensor Network is vulnerable to various security attacks. These attacks hinder the network performance. Sensor Network, security is considered as one of the critical issue. In this paper we 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 counteractive action we stream normal way node_id in the system.

Keywords: Wireless Network ; Sensor Network; Wormhole Attack; Network Venerability; Security; AODV; Path Zone.

1. Introduction

Wireless Sensor network is a collection of Sensor nodes that communicate among each other with the help of intermediate nodes. It is an infrastructure-less network hence prone to various types of attacks. Wireless Sensor network are used to monitor variation in physical phenomenon [1].Wireless sensor network is made up of number of sensor nodes randomly deployed. These sensors transmit data which is sensed by them to the BS (Base station) or sink [2].Security is one of the major factors that degrade the performance of Wireless Sensor network. One another issue in sensor network is energy efficiency [3]. The major cause of failure of node is having batteries which cannot be charged again so, energy is a significant part; to use energy efficiently is necessary in the sensor network.

Attack is an attempt to destroy or interrupt the normal functionality of the network and violate the basic security goals which are as: confidentiality, authentication, integrity, availability and non repudiation. Various security issues are present in Wireless Sensor network [2].Attacks are of two types depicted in the fig1: passive attack and active attacks.

a. **Passive Attack:** Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic. Passive attack violates confidentiality.

b. **Active Attack:** Active attacks are very severe attacks on the network that prevent message flow between the nodes These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. Active attack violates integrity. Active attacks are present in the network at different layers. Different types of attacks have been explained in [2]

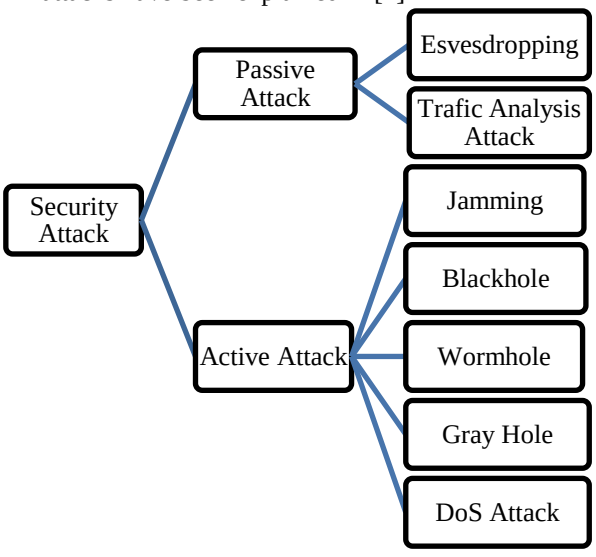

Fig1: Security Attack

2. Routing Protocols

Sensor network routing protocols are mainly classified into following classes; Proactive, reactive and hybrid protocols [3].

a. **Proactive Protocol:** It is also known as table-driven routing. Firstly route has to be determined and all nodes maintains the routing information about other nodes residing in the network and routing updates are broadcasted in the network whenever network topology changes. DSDV, CGSR, OLSR are proactive protocols.
b. **Reactive Protocols:** These are on demand routing protocols, a node only knows the routes it actually requires, find a route (route discovery) only when node wants to send data to a node. Maintains the route (route maintenances) only active routes are maintained. AODV, DSR are reactive protocols.
c. **Hybrid Protocols:** It is a Combination of both proactive and reactive routing protocols. ZRP is hybrid protocol**.**

3. AODV Routing Protocol

The AODV [4] routing protocol is an on demand routing protocol. Whenever there is need of path between source and destination then the route establishment is done. Once the route is established it remains till the time it is needed. Route discovery procedure is initiated to find the valid path between source and destination if any valid path is not available in the table. After route is established the data packet is forwarded to destination, only active paths are maintained in the table.

4. Wormhole Attack

Wormhole attack [5] is such type attack which comprises of two nodes known as the attacker nodes linked to one other via tunnel. The attacker node that resides at one side in the network occupies the packet from the authentic node and encapsulates the packet and with the help of tunnel transmits it to the other attacker node or malicious node present in the network. It consists of one or two malicious nodes and a tunnel between them. Wormhole nodes forge a route that is shorter than the actual path within the network means it create mirage for the legitimate node so that they believe the route is shorter than the actual one. However it is not compulsory that the route by the wormhole nodes might be shorter. Fig 2 represents example of wormhole [5].

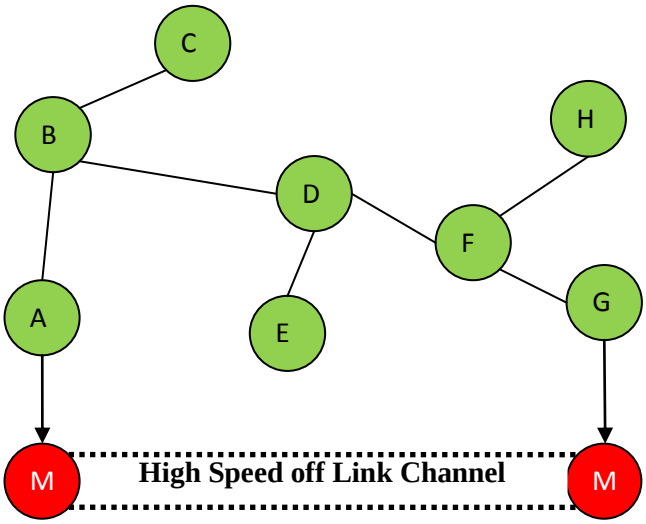

Fig 2: Wormhole attack

In given fig 2, here we have two malicious nodes M1 and M2 connected with each other with the aid of a link, known as tunnel, “the wormhole tunnel” by which malicious nodes transmits the packet to one other as well as the entire traffic follow this route via tunnel.In the fig 2, node A and node G are represented as source and destination respectively. So now the source node A will forward the packet to the legitimate neighbor i.e.; node C in this way intermediate nodes between node A and node G i.e., C, D, F will forward the packet from source to destination. In the absence of malicious nodes the legitimate path from node A to node G will be A-C-D-F-G so number of hops the packet travels is 3(three).Now when wormhole nodes are present as well as they are malicious nodes so now the nodes M1 and M2 will get activated making an illusion to source and destination of being immediate neighbors, capable of hearing one’s request so transmission take place among node A and node G via node M1 and node M2.

Wormhole attack have different variation on the basis of visibility, packet Transmission mode, Transmission Medium, Attacker type and victim node as shown in figure 3. Different types of wormhole attack are described in different literatures [5, 6].

Engineering Universe for Scientific Research and Management
(International Journal)
Vol. 9 Issue 3
March 2017

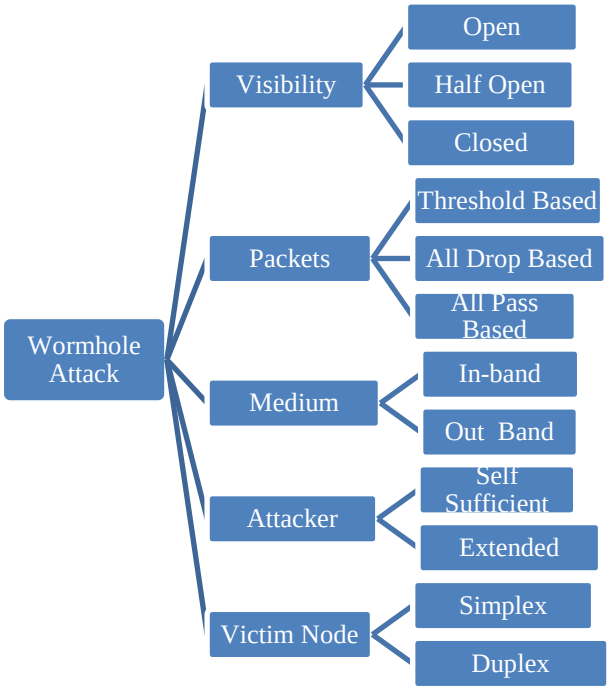

Fig 3: Types of Wormhole attack

Along with that wormhole attack comes with different mode on behalf of transmission ie Packet Encapsulation, Out Band Channel , High Power transmission, Protocal deviation, Packet Relay as shown in figure 4.The given fig.2 depicts the various modes of operations of wormhole attack. With the help of these modes wormhole attack is launched [2].

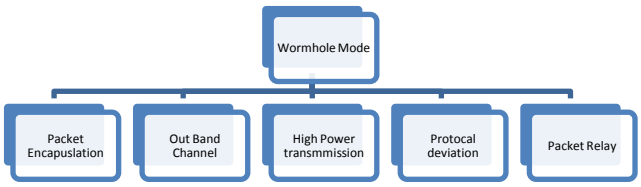

Fig 4: Modes of wormhole attack

5. Related Work

Biswas et al [7], this method is an enhancement to the existing "WAP" technique. The new proposed method is capable of detecting the false positive alarm known as WADP, (wormhole attack detection and prevention.). It provides the two way verification by collaborating WADP with node authentication in modified AODV. It is able of detecting both the hidden as well as exposed attack. Detection of hidden attack is done on basis of neighbor node list and timer. Detecting exposed is done by calculating the delay per hop. In this way both attacks are detected. For detecting false alarm in the reply packet adding two new fields ip address of intermediate node and a unique number. By this combination malicious nodes are detected and isolated from the network and resolves the issue of false alarm. Below are described the problems related to this approach.H. Lu et al. [8] proposed two SET protocols for CWSNs namely IBS scheme and the identity-based online/offline digital signature abbreviated as IBOOS scheme, known as SET-IBS and SET-IBOOS by utilizing the identity-based digital signature. The authors showed the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security issues and security analysis against various attacks. A. Liu et al. [9] formulated the secret-sharing-based multipath routing problem. In this technique, each packet is transformed into multiple shares to enhance the security of transmission. In this technique, the packets are transferred randomly and dispersively in the first two phases and then it was transmitted to the base station. The scheme is known as Security and Energy-efficient Disjoint Route abbreviated as SEDR. H. Alwan et al. [10] demonstrated the use of integrating codes and encryption scheme for providing Quality of service and secure data transmission in WSN. The K. Saleem et al. [11] presented BIOSARP routing protocol which used the test bed consisting of 10 sensor nodes. This routing protocol guarantees the reliability of data transfer and performs well and has the adaptability to the environmental changes. L. Mokdad et al. [12] presented a secure routing protocol considering the multi-paths between source and destination. S. Roy et al. [13] presented an attack-resilient computation algorithm which enables the computation of true aggregate by the base station. K. Saleem et al. [14] presented a WSN routing protocol defined as Biological inspired Self-Organized Secure Autonomous Routing Protocol abbreviated as BIOSARP enhances Secure Real- Time Load Distribution abbreviated as SRTLD with an independent routing mechanism. BIOSARP technique uses improved Ant Colony Optimization abbreviated as IACO for forwarding data packets. BIOSARP has been

designed to reduce the broadcast and packet overhead. W. Gu et al. [15] designed a secure protocol in randomly deployed WSNs. In this technique, different numbers of keys are distributed to different nodes to enhance the resilience communication paths and the techniques known as differentiated key predistribution. An energy-efficient secure routing protocol with a stationary base station for WSNs is proposed by H.W. Ferng et al. in [16]. By use of location information of the sink, the developed routing protocol makes the sink-oriented grids from the source to the sink to ensure the path availability. S. Ruj et al [17] have designed new pair wise key establishment schemes in WSN using deterministic predistribution techniques based on combinatorial designs. Combinatorial trades were applied for the first time for key predistribution in WSNs. Polynomial-based scheme is applied so that every three nodes indeed have a common (and unique) key. This technique is c-secure, where c is degree of polynomials used. A. Selcuk Uluagac et al. [18] presented the Secure Source- Based Loose Synchronization abbreviated as SOBAS protocol to securely synchronize the events in the network. In this technique, to encrypt each message nodes use their local time values as a onetime key. It provides an effective dynamic en-route filtering mechanism, where the harmful data is filtered from the network.Parmar Amish [19] proposed and implemented a wormhole detection and prevention mechanism to detect and prevent the wormhole attacks. In our technique, no special hardware is required. All we have done is calculated the round trip time (RTT) of every route to calculate threshold RTT. According to simulation results of various parameters like Average end to end delay, Packet delivery fraction and Average throughput it is proved that proposed mechanism performs better than wormhole affected AOMDV.

6. Problem Statement

Each node maintains the information of its neighbor node in a routing table. A node monitors the behaviour of its neighbors. Information related to path is also stored. This is time consuming and increases the overhead on nodes. A node can be treated as a malicious node. When radius of a node is small and node is mobile moves out of the transmission range of the other nodes for particular time duration and when it returns in the network that time the node can be treated as wormhole node. Packet can be modified. As for node authentication in the RREP packet two fields the IP address as well as unique number are used. When a node forwards a RREP packet to its neighbour node it verifies the combination as the authentic node knows this information. When passive attack is launched it cannot detect it as a result packet can be modified as the nodes are unable to collect the correct information. When any node forward a RREQ packet to its neighboring node it records the sending time of the packet and when the node overhears the RREQ packet after the set time the node which sends the RREQ packet is considered as a wormhole node.

7. 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 Sensor network. Wormhole attack severely degrades network performances. Finding out this attack in network is difficult. This paper has focused on detecting the wormhole and avoids the wormhole affected path as suggested by routing protocol but not to remove that wormhole. Future work includes developing a technique for removal of the wormhole or black list that malicious node ie responsible to generate wormhole attack over the network after detected with the help of this proposed approach.

Reference

[1] Parmar, M.K. ; Jethva, H.B.” Analyse impact of malicious behavior of AODV under performance parameters”, in International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 2014.
[2] Priyanka Sharma, Dr. H.P Sinha, Er. Abhay Bindal, “ A Review on Prevention of Wormhole Attack in Mobile Ad-hoc Network “, International Journal of Research in Information Technology, volume 2, issue 3, March 2014
[3] Aarti, Dr. S. S. Tyagi, “Study of MANET: Characteristics, Challenges, Application and Security Attacks” International Journal of

Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[4] Abdelaziz, A.K. ; Mehdi, N. ; Salim, G.” Analysis of security attacks in AODV”, in International Conference on Multimedia Computing and Systems(ICMCS), 2014.

[5] Saurabh Upadhyay, Brijesh Kumar Chaurasia,” Impact of wormhole attacks on MANETs “, International Journal of computer science & Emerging Technologies (E-ISSN: 2044-6004) volume 2, issue 1, February 2011.

[6] R. Maulik and N. Chaki,” A comprehensive Review on Wormhole Attacks in MANET”, in proceeding of 9th International Conference on Computer Information Systems and Industrial Management Applications, (**2010**), pp. 233-238.

[7] Juhi Biswas, Ajay Gupta, Dayashankar Singh,” WADP: A Wormhole Attack Detection and Prevention Technique in MANET using Modified AODV routing Protocol”, 9th International Conference on Industrial and Information Systems (ICIIS), 2014

[8] H. Lu, J. Li and M. Guizani, “Secure and Efficient Data Transmissionfor Cluster-Based Wireless Sensor Networks”, IEEE Transactions onParallel and Distributed Systems, vol. 25, no. 3, pp. 750-761, March2014.

[9] A. Liu, Z. Zheng, C. Zhang and Z Chen, “Secure and Energy-Efficient Disjoint Multipath Routing for WSNs”, IEEE Transactionson Vechicular Technology, vol . 61, no. 7, p. 3255-3265, September2012.

[10] H. Alwan and A. Agarwal , “A Secure Mechanism for Qos Routing inWireless Sensor Networks”, IEEE Conference on Electrical andComputer Engineering (CCECE), 2012 25th IEEE CanadianConference, Montreal ,QC, pp. 1-4, May 2012.

[11] K. Saleem, N. Fisal and M.V. Baharudin, “A Real-Time EmpiricalStudy of BIOSARP based Wireless Sensor Network Testbed”,sensors IEEE, Taipie, pp. 1-4, October 2012.

[12] L. Mokdad and J. Ben-Othman, “Performance evaluation of securityrouting strategies to avoid DoS attacks in WSN”, IEEE on Globalcommunications conference,Anaheim,CA, pp. 2859-2863, December2012.

[13] S. Roy, M. Conti, S. Setia and S. Jajodia, “Secure Data Aggregationin Wireless Sensor Networks: Filtering out the Attacker’s Impact “,IEEE Transactions on Information Forences and Security, vol. 9, no.4, pp. 681-694, April 2014.

[14] K. Saleem, N. Fisal and J. Al-Muhtadi, “Empirical Studies of BioinspiredSelf-Organized Secure Autonomous Routing Protocol “ ,Sensors journal, IEEE, vol.14, no.7, pp. 2232-2239, July 2014.

[15] W. Gu, N. Dutta, S. Chellappan and X. Bai, “Providing End-to-EndSecure Communications in Wireless Sensor Networks“, IEEETransaction on Network and Service Management, vol. 8, no. 3, pp.205-218, September 2011.

[16] H.W. Ferng and D. Rachmarini , “A Secure Routing Protocol forWireless SensorNetworks with Consideration of Energy Efficiency”,IEEE on Network Operation and management symposium (NMOS),pp. 105-112, April 2012.

[17] S. Ruj, A. Nayak and I. Stojmenovic, “Pairwise and Triple KeyDistribution in Wireless Sensor Networks with Applications”, IEEETransactions on Computers, vol. 62, no. 11, pp. 2224-2237,November 2013.

[18] A. Selcuk Uluagac, R.A Beyah and J.A Copeland, “Secure SOurceBAsed Loose Synchronization (SOBAS) for Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 4, pp. 803-813, April 2013.

[19] Parmar Amish, V.B. Vaghela, Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol, Procedia Computer Science, Volume 79, 2016, Pages 700-707.