Performance Analysis of WSN under Wormhole Attack

Shailani[1] Dr. Sukhvir Singh[2]
[1]M.Tech [2]Associate Professor
[1,2]Department of Computer Science Engineering
[1,2]N.C. College of Engineering, Panipat

Abstract— In mobile ad hoc networks, data transmission is performed within an untrusted wireless environment. A Wireless Networks are more vulnerable to different types of attack than wired Network. Various kinds of attack have been identified and corresponding has been proposed. Wormhole attack is one of the serious are attacks which forms a serious threat in the networks, especially get against many ad hoc wireless routing protocols and location- based wireless security system. In which traffic is forwarded and replayed from one location to another through the wormhole tunnel without compromising any cryptographic techniques over the network. Thus, it is challenging to defend against this attack. The wormhole attack is very powerful and preventing the attack has proven to be difficult. We identify two types of wormhole attacks. In first type, malicious nodes do not take part in finding routes, meaning that, other nodes in the network does not know their existence. In second type, malicious nodes do create route advertisements and other nodes are aware of the existence of malicious nodes, but they do not know that these are the malicious nodes. Many researchers have proposed detection mechanisms for the first type. Existing some solutions to detect wormhole attacks require special hardware or strict synchronized clocks or long processing time. Moreover, some solutions cannot even locate the wormhole. This paper detects the wormhole attack using neighborhood information without using extra hardware or clock synchronizations. In it AODV routing protocol is used and all the simulations are done in ns2.35 simulator.

Key words: Manet, AODV, WSN, Processing Time

I. INTRODUCTION

Wireless network refers to any form of computer network that is not connected by cables of any kind. It is method by which homes, telecommunication networks and enterprises installations avoid the costly process of introducing cables into a building, or as a relationship between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio waves. This implementation takes place at the physical level of OSI model . A wireless sensor network (WSN) is formed by one or more base stations and a large number of sensor nodes to monitor the objects of interest. Modern networks are usually bi-directional, enabling us to control the activity of the sensor nodes.

The development of WSN was motivated by military applications such as battlefield surveillance and in today time such networks are used in many industrial and consumer application, such as habitat and ecosystem monitoring, seismic monitoring, industrial process monitoring and control, rapid emergency response, machine health monitoring, healthcare applications, monitoring groundwater contamination, home automation, automatic building climate control and traffic control.

A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or pre-determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

Many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited for the unique features and application requirements of sensor networks.

II. RELATED WORK

Vrutik Shah and Nilesh Modi proposed a technique to prevent wormhole attack in WSN named as an Anti-Worm protocol which is based on responsive parameters. This technique does not require as a significant amount of specialized equipment, trick clock synchronization, no GPS dependencies. The goal of Anti-worm is to find alternative route that does not go through the wormhole. The source will check the difference between the two routes and if the difference is greater than some value that is Responsive parameter then a wormhole is detected.

Xiaopei Lu et.al.; proposed a technique in which each node locally collects its neighborhood information and reconstructs the neighborhood sub graph using multidimensional scaling (MDS) . Potential Wormhole nodes are detected by validating the legality of the reconstruction. After that, refinement process is done which filter the suspect node and to remove false positives. This approach effectively identifies all wormhole nodes for a large class of network instances.

Damandeep Kaur proposed methodology work very efficiently in WSNs during wormhole attack . The method prevents the degradation of the wireless network and also helps in improving performance of wireless sensor network. In this method, the nodes which are not participating in multi-path routing generate an alarm message during delay and then isolate the malicious node from network.

Dhara Buch and Divesh Jinwala proposed approach which is based on the analysis of the two-hop neighbors forwarding Route Reply Packet. To check the validity of the sender, a unique key between the individual sensor node and the base station is required to be generated by suitable scheme. The RREP packet is forwarded only by checking the validity of the two-hop neighbor node that has forwarded the packet. Wormhole end is detected when the

identity of the two-hop neighbor is found illegal. Authenticity checking is carried out using a preloaded secret key. This approach focuses on the type of wormhole with out-of-band channel.

Huaiyu Wen and Guangchum Luo proposed algorithm named as Wormhole Detection based on Neighbor's Neighbor Scheme (WDNN) which is based on 2-hop neighbor in WSN. By using this algorithm, we enlarges the transmission range of the 2-hop neighbor, the faked network topology resulted by wormholes can be detected without using extra hardware or clock synchronization. By adjusting the transmission range of key node, the fake topology created by wormhole is detected. Another scheme called Random Walk Route is also proposed in which route is chosen without using the low latency link which is created by wormholes.

Chen and et.al; proposed approach which not only detect the wormhole attack but also localize the attacker . This scheme detects the existence of wormhole attacks and accurately localizes the attackers for the system to eliminate them out of the network. The detection of attacker is done by using communication properties i.e packet uniqueness property and transmission constraint property. The main idea is to detect whether the communication between the mobile beacon and static beacon violates the communication properties. The location of the attacker is estimated as the center of its communication area by determining the intersection points of the chord's perpendicular bisector.

Poonam Dabas and Prateek Thakral proposed a novel technique in order to prevent the wormhole attack in WSN . A WSN is an infrastructure less self-configured collection of mobile nodes that arbitrarily change their location and hence the topology of the network keeps changing. Security has become the primary concern in order to provide the protected communication among the nodes. The absence of any central authority and shared wired media makes it more vulnerable to various attacks at different layers. The wormhole attack at network layer is the most attention seeking.

Jayesh Kataria et.al; they proposed a scheme to control flooding of Fake Route Request in Ad-hoc network [28]. Reactive routing protocols like AODV and DSR, flood the network with route requests whenever a new route is to be discovered. The technique of flooding can be easily misused by malicious nodes to disrupt the network. Generally all nodes have a limit beyond which requests cannot be sent. Malicious nodes can easily bypass this limit and send out large numbers of fabricated route requests in the network, flooding other nodes which ultimately waste all of their processing and battery power in forwarding them. As a result, genuine route requests get ignored and many routes do not get a chance to form.

Shi and et.al; they proposed a scheme named as Secure Neighbor Discovery (SND) [38]. The proposed scheme comprises of three phases- network controller broadcasting phase, response/authentication phase and network controller time analysis phase. In the broadcasting phase and response/authentication phase, local time information and antenna direction information is exchanged between the network controllers and legislate network node. In the network controller time analysis phase, the network controller can further detect the possible attack using the time-delay information from the network nodes.

Rakesh Matam et.al; they proposed a wormhole-resistant secure routing algorithm that detects the presence of wormhole during route discovery and prevents such routes from being established [39]. During route discovery, the proposed algorithm monitors for alternate paths for a cached RREQ and eliminate that RREQ which fails to meet the necessary and sufficient condition. This algorithm uses unit disk graph model to determine the necessary and sufficient condition for identifying a wormhole-free path.

III. Detection of Malicious Behavior

In AODV routing protocol a malicious nodes can easily disrupt the communication. A malicious node that is not part of any route may launch Denial of Service (DoS) Attack. Also once a route is formed, any node in the route may turn malicious and may cease forwarding packets, alter them before forwarding or may even forward to an incorrect intermediate node. Such malicious performance by a misbehaving node cannot be detected for in pure AODV protocol [33]. During the judgment process the neighbors send their conclusion about a node. When the node collects all conclusions of neighbors, it decides about honesty behaviour of reply's sender node. The decision is based on the following cases which are used to judge about honesty of a node facilities of AR2.

A. Steps to Judge an Honesty Node

CASE 1: If a node delivers many data packets to destinations, it is supposed as an honest node.
CASE 2: If a node receives many packets but do not sent same data packets, it is probable that the current node is a misbehavior node.
CASE 3: When the case 2 is correct about a node, if the current node has sent any Route REPLY packets; therefore surely the current node is misbehavior node.
CASE 4: When the case 2 is correct about a node, if the current node has not sent any Route REPLY packets; therefore the current node is a failed node.

B. Algorithm to Isolate Malicious Node

Given: Network N with node radius r, wormhole number c=0
While check every node m in N
do
Expand radius of m to R = 2r
For each node n in N (m) do
If there exists once d ϵ N (m) and d Ɇ N (m)
Then c+1
End for
End while

C. Explanation of Algorithm

Step 1: Source node sends the RREQ to the next neighbour node. If the route is found sends a RREP to the source node.
Step 2: If the route is established then source node sends data packet to the next node.
Step 3: If the intermediate node is a malicious node it will drop the packets which it receives from the neighbour node.

Step 4: The malicious node may send the fake RREQ to other nodes. So stop fake route request by ignoring the RREQ from the malicious node.

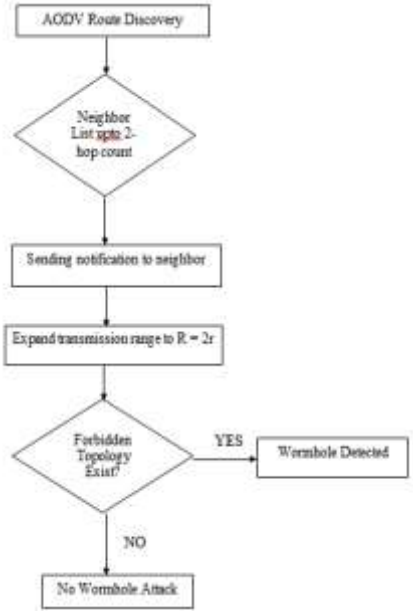

Fig. 1:

D. Simulation Setup

While simulating the MANET behavior I considered following network parameters and their values. Total number of nodes is 50. Ad-hoc on demand routing protocol is used for communication among nodes. The nodes are connected by wireless media.

Parameter	Value
Channel Type	Wireless Channel
Radio Propagation Model	Two way Propagation
Interface Queue Type	Queue
Maximum Packet in IFQ	50
Routing Protocol	AODV
Mac Type	Mac 802_11
No. of Nodes	50
Network Interface Type	Wireless
Antenna Type	Omni Antenna

Table 1: Network Parameter and their values used

IV. SIMULATION RESULT AND DISCUSSION

Here we described the simulation used for analyzing the performance of WSN under Wormhole attack in term of total packet sent, packet received, packet loss, PDF, energy consumption graph and detection rate graph.

A. Energy Consumption Graph:

In Figure 1 we took time on x-axis and energy consumed on y-axis while plotting the graph for energy consumption. As we saw in simulation data, the amount of energy consumption kept increasing with time. The straight upward line specifies the increasing rate of energy consumption in the network under wormhole attack.

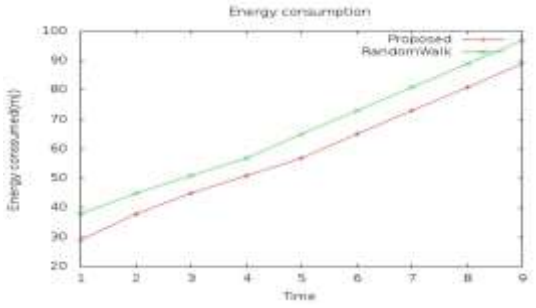

Fig. 2: Energy Consumption Graph

B. Detection Rate:

In Figure 2, we took time on x-axis and detection rate on y-axis and plotted the graph using GNUPLOT for a run of simulation. As we saw in simulation data, the detection rate kept increasing with time. The straight upward line specifies the increasing rate of detection of wormhole attack.

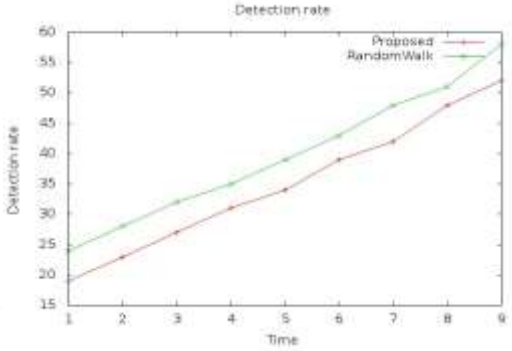

Fig. 3: Detection Rate Graph

V. CONCLUSION AND FUTURE SCOPE

In this paper, we studied about various types of wormhole detection algorithms in WSN and particularly we have proposed a new algorithm for detecting a malicious node and I studied about various types of attacks which WSN is prone to and considered the wormhole attack in particular to see its effect on WSN using AODV as routing protocol. In this type of attacks many solution have been suggested that can be used in network. All these solution have their own advantage and disadvantage. Disadvantage are in form of requirements (which can either be impractical, costly or else affecting other parameters of ad hoc network like mobility or decentralization) or their effect on overall performance (by increasing load on network).I used ns2.35 network simulator and we can draw following conclusion: Due to the mobility and open media nature of WSN these networks are more prone to security threats as compared to the wired network. I saw that the wormhole attack affects the network performance which can be analyzed using various network parameters like total packets sent, total packets received, throughput, packet delivery fraction by the help of simulation and graphs, etc. Consequently security needs are higher in WSN as compared to the traditional network. Hence I need a secure and reliable routing protocol that can be rapidly deployed and follows dynamic routing. AODV is prone to many attacks like spoofing, fabrication of error messages, source route tunneling, modification in sequence no. and hop count etc. Wormhole attack is real threat against AODV protocol in MANET. Malicious nodes usually target the routing control messages. Wormhole attack thus

prevents the routes other than wormhole from being discovered.

A. Future Work:

As currently there are many weak points in the system, which can be topic of concern for future research work. Some of them are listed below as the future aspects of this dissertation work:

1) In future, this work can also be applied for dense network also.
2) This work can also be applied on various network conditions such as the case that the network has frequent link breaks between nodes.

More network parameters can be considered for comparison of performance of various routing protocols under this attack.

REFERENCES

[1] Data communications and networking by Behrouz A. Forouzan.
[2] C.Siva Ram Murthy and B.S.Manoj, "Ad-Hoc wireless networks", Architecture and protocols, Pearson Education, Fourth Impresseion, 2009.
[3] Wireless Network - Wikipedia, Retrived March 4, 2015, from http://en.wikipedia.org/wiki/Wireless_network
[4] Debnath Bhattacharyya, et.al, "A Comparative Study of Wireless Sensor Networks and Their Routing Protocols", In MDPI -2010, Basel,Switzerland,Nov. 2010.
[5] Dr. G. Padmavathi and Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," In Proceeding of the International Journal of Computer Science and Information Security (IJCSIS), Vol. 4, No. 1 & 2, 2009.
[6] Wireless Sensor Network- Wikipedia, Retrived June 4, 2015, from http://en.wikipedia.org/wiki/Wireless_sensor_network.
[7] Abdul HadiAbd Rahman and Zuriati Ahmad Zukarnain,"Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks", European Joural of Scientific Research,pp.566-576,2009.
[8] Perkins, Charles E. and Bhagwat, Pravin (1994). Highly Dynamic Destination Sequenced Distance-Vector Routing (DSDV) for Mobile Computers (pdf). Retrieved 2006-10-20.
[9] MonisAkhlaq et. al.; Addressing Security Concerns of Data Exchange in AODV Protocol", World Academy of Science, Engineering and Technology 16, pp. 29-33, 2006.
[10] E.Perkins and E.M.Royer, "The Ad Hoc On-Demand Distance Vector Protocol (AODV)", In Ad Hoc Networking, C.E.Perkins (Ed.), pp.173-219, Addison Wesley, 2001.
[11] C.Perkins et.al.; Ad Hoc On-Demand Distance Vector (AODV) Routing," RFC 3561(Experimental), Jul.2003. [online].
[12] Piet Demeester, Jeroenhoebeke. An overview of Mobile Ad hoc Networks: Applications and Challenges http://cwi.unik.no/images/MANET_Overview.pdf.
[13] Mond Anuar Jaafar and Zuriati Ahmad Zukarnain, "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment", European Journal of Scientific Research,pp. 430-443,2009.
[14] Chakeres I, et.al., Dynamic MANET On-demand (DYMO) Routing", IETF, June 2006.
[15] I.Chakeres, S.Harnedy and R.Cole, "DYMO Manet Routing Protocol draft", IETF, Jan 2011.
[16] Vikas Kumar Upadhyay, Rajesh Shukla, " An Assessment of Security attack over Mobile Ad -Hoc Network" International Journal of Advanced Networking and Applications, Volume 5, Issue: 01, Pages: 1858-1866(2013), ISSN: 0975-0290
[17] Ankita Gupta, Sanjay Prakash Ranga, Various Routing Attacks in mobile ad-hoc networks", IJCCR, Volume 2, Issue 4, July 2012.
[18] Simulation study of Jellyfish Attack using AODV Routing Protocol http://www.ejournal.aessangli.in/ASEEJournals/CE71.pdf.
[19] Monis Akhlaq et.al., "Addressing Security Concerns of Data Exchange in AODV Protocol", World Academy of Science, Engineering and Technology16,pp.29-33, 2006.
[20] Laxmi Shrivastava, Sarita S. Bhadauria, G.S.Tomar, " Performance Evaluation of Routing Protocols in MANET with different traffic loads", International Conference on Communication System and Networks Technologies,2011.
[21] Bing Wu et.al., " A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer 2006,pp. 1-38.
[22] Shaishav Shah and Aanchal Jain, "Techniques For Detection & Avoidance Of Wormhole Attack In Wireless Ad Hoc Networks,"In Proceeding of the International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 10, December- 2012.
[23] Ali M, et al, "Mitigation of Wormhole Attack in Wireless Sensor Networks," In Proceeding of the Atlantis Press 2012.
[24] Majid M, et al.,"A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", In Proceeding of the IETE Technical Review, April.2011.
[25] Louazani Ahmed et.al.; "A Security Scheme against Wormhole Attack in MAC Layer for Delay Sensitive Wireless Sensor Networks", In I.J. Information Technology and Computer Science,2014
[26] Chao Gu, Qi Zhu, "A Cross-Layer Routing Protocol for Mobile Ad Hoc Networks Based On Minimum Interference Duration",In Proceedings of the 2nd International Conference on

Computer Science and Electronics Engineering (ICCSEE 2013).
[27] Poonam Dabas, Prateek Thakral, " A Novel Technique for the Prevention of Wormhole Attack", IJARCSSE, Volume 3, Issue 6, June 2013.
[28] Jayesh Kataria, P.S.Dhekne, Sugata Sanyal, "A Scheme to Control Flooding of Fake Route Requests in Ad-hoc Networks", International Conference on Computers and Devices for Communications, CODEC-06, December 18-20, 2006, Kolkata, India.
[29] Gagandeep, Aashima, Pawan Kumar, " Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, volume-1, Issue-5, June 2012.
[30] Yih-Chun Hu, Adrian Perrig and David B. Johnson, " Rushing attacks and defense in wireless adhoc network routing protocols", In Proceeding of the 2003 ACM Workshop on Wireless Security, pages 30-40, San Diego, CA, USA, 2003.
[31] Paul Meeneghan and Declan Delancey, " An Introduction to NS, NAM and OTcl scripting", April 2004.
[32] Mohammad Rafiqual Alam, " Detecting Wormhole and Byzantine Attacks in Mobile ad hoc Networks", International Journal of Computer Applications, May 2011.
[33] Devendra Singh Kushwaha et.al; "Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET", In International Journal of Computer Applications, Volume 62, No.7, January 2013.
[34] Damandeep Kaur and Parminder Singh, "Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack", In ACEEE Int. J. on Network Security , Vol. 5, No. 1, January 2014.
[35] Vrutik Shah and Nilesh Modi, " Responsive Parameter based an AntiWorm Approach to Prevent Wormhole Attack in Adhoc Network", In ACEEE Int. J. on Network Security, Vol. 5, No.1, January 2014.
[36] Xiaopei Lu et.al.; "MDS-BasedWormhole Detection Using Local Topology in Wireless Sensor Networks", In Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Volume 2012.
[37] Honglong Chen et.al.; "A Secure Localization Approach against Wormhole Attacks Using Distance Consistency", In EURASIP Journal on Wireless Communications and Networking, Volume 2010.
[38] ZHIGUO SHI et.al; "A Wormhole Attack Resistant Neighbor Discovery Scheme With RDMA Protocol for 60 GHz Directional Network", In IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, January 2014.
[39] Rakesh Matam and Somanath Tripathy, "WRSR: wormhole-resistant secure routing for wireless mesh networks", In EURASIP Journal on Wireless Communications and Networking 2013.
[40] Dhara Buch and Devesh Jinwala, "PREVENTION OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK", In International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.
[41] Mariano Garcia-Otero et.al; "Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques", International Journal of Distributed Sensor Networks,Volume 2012.
[42] Huaiyu Wen and Guangchun Luo, "Wormhole Attacks Detection and Prevention Based on 2-Hop Neighbor in Wireless Mesh Networks", In Journal of Information & Computational Science, September 2013.
[43] Zaw Tun and Aung Htein Maw, "Wormhole Attack Detection in Wireless Sensor Networks", In World Academy of Science, Engineering and Technology, 2008.
[44] Guoyuan Lv et.al; " A Detecting and Defending Method of Wormhole Attack Based on Time Ruler", In International Workshop on Cloud Computing and Information Security, 2013.
[45] Yanchao Niu et.al; "A Robust Localization in Wireless Sensor Networks against Wormhole Attack", In Journal of Networks, VOL. 7, NO. 1, January 2012.
[46] P. Hemalatha , " Detecting and Preventing Wormhole Attacks In Wireless Sensor Networks", In IOSR Journal of Computer Engineering, Volume 9, Issue 6, 2013.
[47] Ritesh Maheshwari et.al; "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information", In Journal of Networks, VOL. 8, NO. 1, January 2013.
[48] Dezun Dong et.al; "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks", In the National High Technology Research and Development Program of China, 2010.
[49] Hosny M. Ibrahim et.al.; " A Lightweight Technique to Prevent Wormhole Attacks in AODV", International Journal of Computer Application, Volume 104 – No.6, October 2014.
[50] Honglong Chen et.al; "Securing DV-Hop localization against wormhole attacks in wireless sensor networks", In Elsevier B.V., 2014.
[51] Dezun Dong et.al; "WormCircle: Connectivity-based Wormhole Detection in Wireless Ad Hoc and Sensor Networks", In 15th International Conference on Parallel and Distributed Systems, 2009.
[52] Yingpei Zeng et.al; "Secure localization and location verification in wireless sensor networks: a survey", In J Supercomput Springer, 2013.
[53] Shiyu Ji et.al; "DAWN: Defending Against Wormhole Attacks in Wireless Network Coding Systems", In IEEE Conference on Computer Communications, 2014

