Detection and Prevention of Wormhole Attack in Wireless Sensor Network: A Review

Rahul Jain, Varsha Namdev
RKDF Institute of Science & Technology, Bhopal (MP)
rahul.jain1300@gmail.com

ABSTRACT: Sensor networks 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 a serious threat to the security in multi-hop ad hoc networks. This paper gives a bird eye over sensor network and wormhole attack.

Keywords: Sensor Network, Multihop Routing, Ad-hoc Network, Wormhole Attack

I. INTRODUCTION

A Network is use to connect the devices for sending and receiving the data. To install any network there are three basic needs. These are 1) Computers 2) Connecting Media and 3) Protocol. As the network is a way to provide communication between two or more than two devices. Whether, wireless network uses radio waves to connect devices such as laptops to the Internet and to your business network and its applications. When you connect a laptop to a WiFi hotspot at a cafe, hotel, airport lounge, or other public place, you're connecting to that business's wireless network. Using this approach the wireless LAN can create to establish it in a required area.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance, a group of industry-set, promoting interoperability between 802.11 devices. 802.11 provide two ways to configure an ad hoc and wireless network infrastructure. Previously, there was a discussion of the wireless network may refer to a network, wherein all devices communicate without using a wired connection.

Wireless networks are usually applied with some information about the remote transmission system that uses electromagnetic waves, such as radio waves; for the carrier and this implementation usually takes place at the physical level or "layer" of the network.

An ad hoc network does not have a network infrastructure. This is a network which is spontaneously formed in order to meet the immediate need for communication between mobile nodes. Mobile ad-hoc network is operating in ad hoc manner.

A mobile ad hoc network is a set of nodes that are able to change their position randomly, but can communicate. Coordinate with other nodes there no centralized device available. These nodes are able to send and receive data on their own. They can also perform routing. And the Ad-hoc network is very popular due to unstructured network. Due to this assets, there are so many practical application used in this time. It can be used by the military.

The border is the most sensitive area that communication must take place 24 hours. But at some point it is necessary to establish a network of instant communication. Time for Ad-hoc network plays an effective role. At the time of natural disasters such as tsunamis, earth quack, tornadoes can destroy the infrastructure of the communication system together. Therefore, the rescue team can use the Ad-hoc network on the site. Mining is a dynamic sector that was changed after the mine each day. Therefore, the static grid can create problems in data communication. This is also an area in Ad-hoc network provides effective results.

Wireless sensor networks facilitate monitoring of physical environments from remote locations with greater accuracy. They have applications in a variety of areas such as environmental monitoring, military purposes and the gathering of sensitive information in inhospitable places. Sensor nodes have various energy and computational constraints because of their ad hoc nature and low cost method of implementation.

Above, the sensor arrays consists small number of sensor nodes that are connected to a central processing station. However, today, the focus is more on wireless nodes distributed detection. When the exact location of a particular phenomenon of distributed sensing can be placed closer to the phenomenon that a single sensor would be unknown.

Moreover, in many cases, several sensor nodes are needed to overcome obstacles such as environmental barriers, limited aim, etc. In most cases, the environment to be monitored does not have an existing infrastructure for power or communication. It is essential for sensor nodes to survive in small finite energy sources and communicate through a wireless communication channel. Applications of Sensor Network

Sensor networks have a variety of applications. Examples include environmental monitoring, which involves monitoring air soil and water, condition based maintenance, habitat monitoring (determination of the plant and animal populations of the species and behavior), seismic detection, military surveillance, inventory tracking, smart spaces, etc. in fact, due to the ubiquity of micro-sensors, sensor networks have the potential to revolutionize the way we understand and construct complex physical system.

II. WORMHOLE ATTACK

Wormhole attack is a type that occurs in the network layer. In worm-hole attack, a malicious node receives packets at one location in the network and tunnels to another location on the network where packets are sent over the network. This tunnel between two colluding attackers is considered a wormhole. This could be done via cable between two colluding attackers or a single wireless link without reaching. In this form of attack the attacker can create a wormhole even for packets not addressed to itself due to the broadcast nature

of the radio channel. The X and Y are malicious nodes that encapsulate data packets and tampered route length as shown in figure 1.

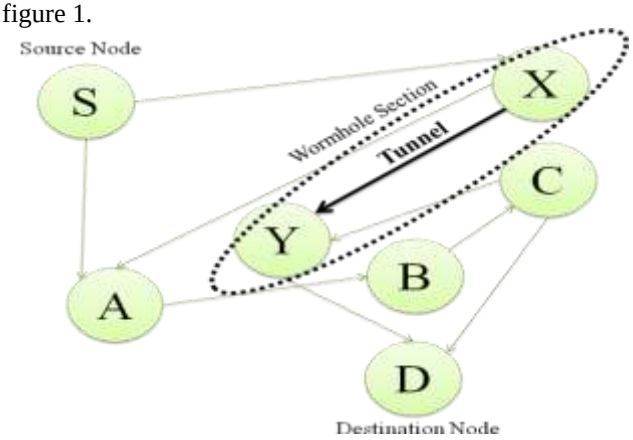

Figure 1: Wormhole Attack

There are many ways to send a data packet from the source S to D. but X and Y indicates the shortest path that does not exist. So wormhole occurs. Assume that node S wants to form a path to D and initiates the route discovery. When X receives the route request from S, X request encapsulates and tunnels direction Y through a network connection. When Y receives a request to route the encapsulated D, it will show that he only traveled {S -> X -> Y -> D}.

After the opening of the route, the destination finds two routes S unequal length, one 4 and one 3 If Y tunnels response way back to X, S would be wrong to consider the DX way better than the way, D via A. This type of attack prevents other channels instead of the vortex to be discovered.

III. Wormhole Attacks And Its Type

There are three types of wormhole attacks. These are classified on the basis of its Nodes. There are open wormhole attack, half open wormhole attack and closed wormhole as shown in figure 2.

Figure: 2 Types of Wormhole

- Open Wormhole Attack: In this type of attack both nodes in the network are available to complete the communication in the network. The two nodes can modify the data and show them self in the way of route discovery.
- Half Open Wormhole Attack: In this type of attack a node in the network is open to spoil data integrity.
- Closed Wormhole Attack: When the tunnel has formed then both node hide them self from the network but act for modifying the data. They show the shortest path to send the data.

The examples that include two malicious nodes consider M1 and M2, and represent the malicious nodes. S and D represent the good nodes as source and destination, and A, B etc. as the good nodes on the route. The nodes between the curly-braces ("{}") are the nodes which are on the path but invisible to S and D because they are in a wormhole.

In the wormhole attack, "closed," means "start from and include," and "open" means, "start from but not include". In figure 3, M1 and M2 tunnel the neighbour discovery beacons from S to D and vice versa, for this reason S and D assume that they are direct neighbours to each other.

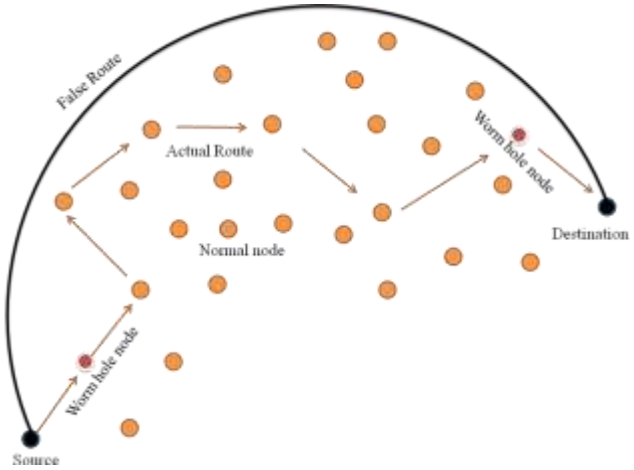

Figure 3: Closed Wormhole Attack

M1 is a neighbour of S and it tunnels its beacons through M2 to D, only one malicious node is visible to S and D, as shown in figure 4.

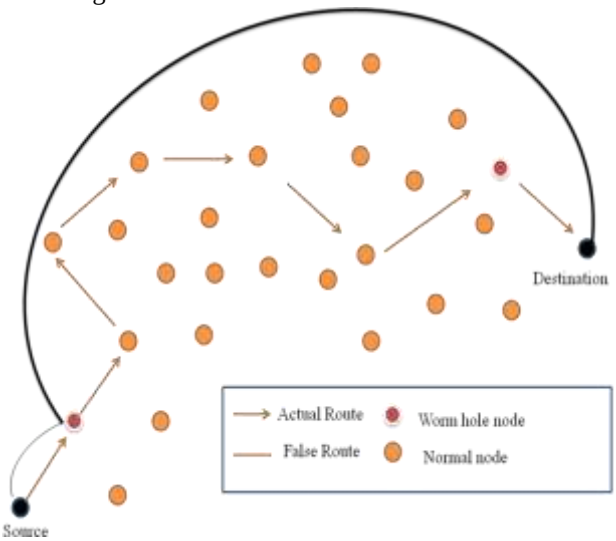

Figure 4: Half open wormhole attack

In an open wormhole, both attackers are visible to S and D as shown in figure 5. It is seen that the majority of previous approaches to detect wormhole shows performance and fell on the higher complexity.

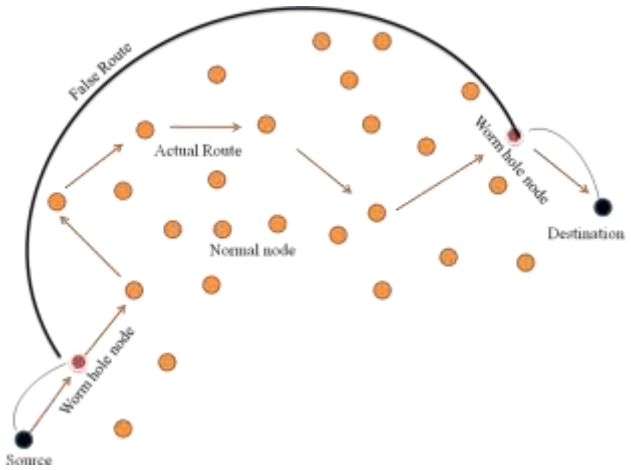

Figure 5: Open wormhole attack

As mobile nodes operate with limited battery power, so that the development of a technique that can successfully defend against the attacks of wormholes is very necessary, while maintaining low complexity. The objective of this work is to develop a new approach that can successfully defend themselves against attacks wormholes and consume less energy for longer survival of MANET and the battery sensor network.

IV. RELATED WORK

Nguyen et Al [20] 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.

The authors [20] 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.

Garcia et Al. [21] Wormhole attacks in ad-hoc networks have been attracting much attention over the years. They consist in two malicious nodes tunneling traffic from one end of the network to the other. Several approaches are proposed to detect these attacks but only few solutions exploit the information provided by multipath routing schemes. A new approach detecting wormhole attacks is presented in this paper. The Witness Integration Multipath protocol is based on the multipath DSR routing protocol and finds suspicious behavior related to wormhole attacks. It does not require any major protocol modification nor as much cryptographic processing as the previous solutions.

The results obtained in this paper shows that the WIM-DSR protocol is able to detect all strong open wormhole attacks with a very low rate of false positive alarms. This solution does not require any cryptographic processing by the intermediate nodes, if no attack takes place. In future works, the author will focus on relaxing the assumptions on which WIM-DSR relies. Specially, the author will investigate how to allow more malicious nodes.

Yifeng et al. [22] the paper shows the technique for detection of wormhole attacks based on distance verification for mobile ad hoc network (MANETs) applications. A node estimates its distances to a sender node based on the received signal strength (RSS) of received packets, and uses them to verify against the distances computed from the location information in the packets. The verification is formulated as a hypothesis testing problem and a Neyman-Pearson approach is used to decide whether the sender node is under wormhole attack or not. An implementation of the Optimized Link State Routing (OLSR) protocol is discussed.

A simple collaborative decision-making strategy is proposed to counter the limitations of distance verification by a single node. The proposed technique is computationally efficient. It is able to provide statistical performance measures for the detection results, an important component that has been missing in existing wormhole detection techniques. Finally, computer simulations are used to demonstrate the effectiveness and performance of the proposed technique.

Maulik et al [23] MANETs use wireless medium for communication, these are vulnerable to many security attacks. The proposed paper has done the comprehensive review on the very recent state of the art research results on wormhole attacks and relevant mitigation measures. 100% of the works reviewed here are published in last five years, out of which 80% are published in last three years. The simulation results in NS2 helps to quantify the comparative performances of the different solutions proposed.

Dhurandher, et al. [24] 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 the destination.

This protocol is capable of detecting wormhole attacks employing either hidden or participating malicious nodes. Simulations are conducted, showing that E2SIW 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.

`It is seen that the majority of previous approaches to detect wormhole shows performance and fell on the higher complexity. As mobile nodes operate with limited battery power, so that the development of a technique that can successfully defend against the attacks of wormholes is very necessary, while maintaining low complexity. The objective of this work is to develop a new approach that can successfully defend themselves against attacks wormholes and consume less energy for longer survival of MANET and the battery sensor network.

V. CONCLUSION

This paper has focused on existing approach to detecting the wormhole and avoids the wormhole affected path as suggested by routing protocol but not to remove that wormhole. In existing work it seems that number of control packet has been increase because numerous of control packet has been send by beacon node to identify maximum hop distance in alternate path along with that there is also a need of calculating maximum hop distance that required various handshaking packet propagate over the network. So in future it needs to optimize the use of handshaking packet efficiently and try to minimized network over head. .

REFERENCES

[1] Z. Narmawala and S. Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks" in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2008.

[2] R. Sheikh, M. S. Chande and D. K. Mishra, "Security issues in MANET: A review", IEEE, pp 1-4, 2010.

[3] B. Kannhavong, et Al., "A survey of routing attacks in mobile ad hoc networks" IEEE, pp 85-91, 2007.

[4] M. K. Verma, S. Joshi, and N. V. Doohan, "A survey on: An analysis of secure routing of volatile nodes in MANET", IEEE, pp 1-3, 2012.

[5] A. Azer Mariannne, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE, pp 561-568, 2011.

[6] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks In Wireless Networks Using Connectivity Information," in Proc. of IEEE INFOCOM, 2007.

[7] Ali Modirkhazeni, et Al., "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", IEEE, pp 122-128, 2011.

[8] Ronggong Song, Peter C. Mason and Ming Li, "Enhancement of Frequency-based Wormhole Attack Detection", IEEE, pp 1139-1145, 2011.

[9] S. A. Razak, S. M. Furnell and P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols", School of Computing 2004.

[10] Xiangyang Li "Wireless Ad Hoc and Sensor Networks: Theory and Applications" Cambridge University Press, 978-0-521-86523-4

[11] K. Hoeper and G. Gong, "Pre-Authentication and Authentication Models in Ad Hoc Networks," Signals and Communication Technology, pp. 65-82, 2007.

[12] H D-Ferriere, M Grossglauser, and M Vetterli, "Age Matters: Efficient Route Discovery in Mobile Ad Hoc Networks Using Encounter Ages," 4th ACM International Symposium on MANET and Computing, 2003.

[13] S. Capkun, L. Buttya'n, and J. P. Hubaux, "Sector: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks" in Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003.

[14] P. Papadimitratos and Z. J. Haas, "Secure Routing For Mobile Ad Hoc Networks" in Proc. of CNDS, 2002.

[15] K. Sanzgiri, et Al. "A Secure Routing Protocol for Ad-Hoc Networks" in Proc. of IEEE, ICNP, 2002.

[16] C. E. Perkins, and E. M. Royer, "Ad-hoc on-demand distance vector routing," IEEE 1999, pp 25-26.

[17] S. Lee and K. Kim "An Effective Path Recovery Mechanism for AODV Using Candidate Node", Springerlink, Vol. 4331, 2006.

[18] A. Maria Gorlatova, et Al. "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis", IEEE

[19] Xu Su and Rajendra V. Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks" IEEE, pp 1136-1141, 2007.

[20] D. Q. Nguyen and L. Lamont "A Simple and Efficient Detection of Wormhole Attacks" IEEE, pp 1-5, 2008.

[21] L. F. Garcia and J. Robert, "Preventing Layer-3 Wormhole Attacks in Ad-hoc Networks with Multipath DSR", IEEE, pp 15-20, 2009.

[22] Y. Zhou and L. L. Li, "Wormhole Attack Detection Based on Distance Verification and the Use of Hypothesis Testing for Wireless Ad Hoc Networks" IEEE, pp 1-7, 2009.

[23] R. Maulik and N. Chaki, "A Comprehensive Review on Wormhole Attacks in MANET", IEEE, pp 233-238, 2010.

[24] S. K. Dhurandher, et Al. "E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks" IEEE, pp 472-477, 2012.

[25] F. Shi, et Al. "Time-based Detection and Location of Wormhole Attacks in Wireless Ad Hoc Networks" IEEE, pp 1721-1726, 2011.

