DOI 10.4010/2016.1572
ISSN 2321 3361 © 2016 IJESC

Research Article Volume 6 Issue No. 6

A Survey on Detection of Wormhole Attack

T.Charanya[1], C.Bala Krishnan[2]
M.E Student[1], Associate Professor[2]
S.A Engineering College, Chennai, India
Charanyathiyagu93@gmail.com[1], kknbalki@gmail.com[2]

Abstract:
A Wireless Sensor Network (WSN) is a network made of numerous small independent sensor nodes.which is formed by detection of wormhole attack.communication among the sensor nodes has to established in a detection of wormhole attack and also to isolate them from the wireless network. Different detection of wormhole attack have been proposed for this purpose. In this paper, we summarize various detection of wormhole attack schemes which have been proposed for wireless sensor network to establish secure communication. These schemes are discussed elaborately and then a comparison based on their various types of detection features and capabilities are carried out.

Keywords: wireless network,wormhole attack,sensor nodes.

I. Introduction

Wireless sensor network sometimes called as wireless network and actuator sensor(WSAN).The sensor nodes, typically the size of a 35 mm, are self-contained units consisting of a battery, radio, sensors, and a minimal amount of on-board computing power. The nodes self-organize their networks, rather than having a pre-programmed network topology. Because of the limited electrical power available, nodes are built with power conservation in mind, and generally spend large amounts. WSNs (Wireless Sensor Networks) are spontaneous networks consist of nodes deployed in large numbers to collect and transmit data to one or more collection points,and this independently.

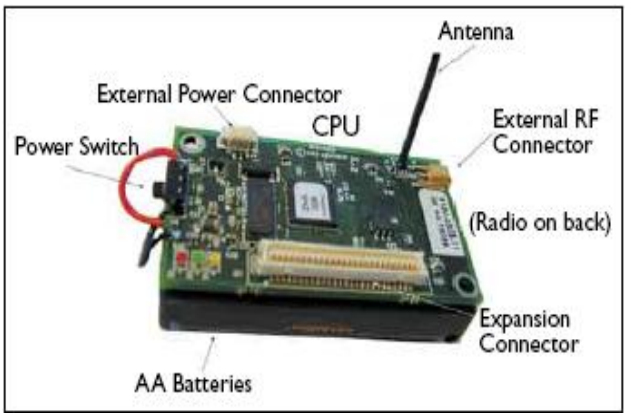

Fig 1.Sensor Nodes

As shown in fig 1.The sensor nodes usually have the network components of low computing power, memory and energy, access to the radio medium is the most expensive. And reduce this consumption(by reducing the number of packets flowing through the network)and prolong the lifetime of the network is an ongoing challenge for this type of network.

As shown in fig 2 the main task of a sensor node in a network of wireless sensors is the detection process and transmit data. It can participate in a WSN as sensing node or as a node like it is presented.

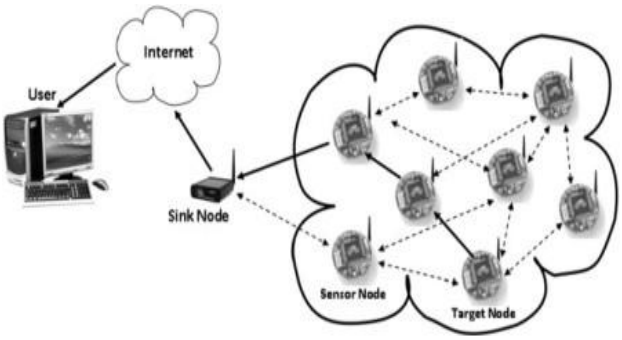

Fig 2.Wireless Sensor Network

2. Wormhole attack

Wormhole nodes fake a route that is shorter than the original one within the network. This can confuse routing mechanisms, which rely on the knowledge about distance between nodes. It has one or more malicious nodes and a tunnel between them. The attacking node captures the packet from one location and transmits them to other distant located node which distributes them locally.

A wormhole attack can easily be launched by the attacker without having knowledge of the network or compromising any legitimate nodes or cryptographic mechanisms. A wormhole is an out-of-band connection, controlled by the adversary, between two physical locations in the network a wormhole distorts the network topology and may have a profound effect on routing

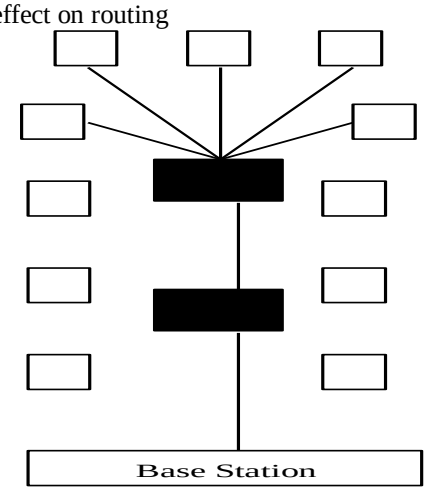

Fig 3.Wormhole Attack

As shown in fig 3 two powerful adversary nodes placed in two strategic locations. Advertise a low cost path to the sink. All nodes in the network are attracted to them looking for an optimal route. This is attack is usually applied in conjunction with selective forwarding or eavesdropping attack.

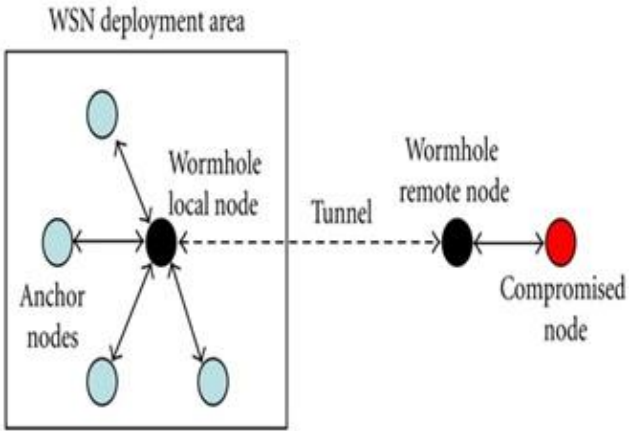

Fig 4.wormhole attack in wireless sensor network

As shown in fig 4 Hard to detect because communication medium between the two bad nodes are unknown. Control and verify hop count. This limits the self-organizing criteria of an ad-hoc network.Use protocol that is not based on hop count. In geographic routing, a route is based on coordinates of intermediate nodes. But if adversary nodes can mimic its location, this doesn't work.

II. Related Work

Communication among sensor nodes has to be establishing wormhole attack. This can be done by detecting the wormhole attack while transmitting the data from one sensor node to another sensor node. Some of the methods for detecting wormhole attacks are discussed in this section. Each scheme has its own pros and cons. Different detection patterns and cryptographic basis are used by each process. It can be selected for a particular network in order to establish detecting wormhole attack among wireless network .

A. Wormhole Attack Detection In Wireless Sensor Network

Zaw Tun et al [2] proposed a round trip time (RTT) for detecting wormhole attack in wireless ah-hoc network. This paper analyzes the nature of wormhole attack and existing methods of defending mechanism and then proposes round trip time(RTT) and neighbor numbers based wormhole detection mechanism. The consideration of proposed mechanism is the RTT between two successive nodes and those nodes' neighbor number which is needed to compare those values of other successive nodes. The proposed system is designed in ad hoc on-demand distance vector (AODV) routing protocol and analysis and simulations of the proposed system are performed in network simulator (ns-2).

In this scheme, directional antennas are used at the media access layer to defend against wormhole attacks, and packet leashes are used at a network layer. the new mechanism to defend the wormhole attack based on the RTT of the route message and number of neighbor nodes is proposed. The first consideration is the RTT between two successive nodes and in normal case all of the RTT between two successive nodes are nearly the same and the next fact is wormhole nodes may increase its number of neighbors. The significant feature of the propose mechanism is that it does not need any specific hardware to detect the wormhole attacks. This mechanism does not require more energy than normal and can extend to other routing protocols than current AODV protocols.

B. Detecting Wormhole Attacks In Wireless Networksusing Connectivity Information

Ritesh Maheswari et al., [4] proposed a novel algorithm for detecting wormhole attacks in wireless multi-hop networks. This algorithm used only connectivity information in the connectivity graph. In this paper proposed a practical algorithm for wormhole detection. The algorithm is simple, localized, and is universal to node distributions and communication models. present simulation results for three different communication models and two different node distributions, Our algorithm provides very good results (no false alarms and 100% detection) when the network disconnection. Connectivity in the entire network is checked. The network is assumed disconnected if any two nodes do not have a path to each other

The wormhole detection algorithm is run to see whether there is a false positive. (At this time, there is no wormhole attack) A wormhole attack is established between two randomly chosen locations. The algorithm is run again to see whether it detects the wormhole. This algorithm is able to detect wormhole attacks with a 100% detection and 0% false alarm probabilities whenever the network is connected with high probability.

C. Wormhole Attack Detection Algorithm In Wireless Network Coding System

Shiyu ji et al. [3] proposed a DAWN algorithm for detecting wormhole attack. RLNC, when an innovative packet is sent from the source node, the nodes near the source node are more likely to receive the innovative packets earlier than the nodes that are far from the source node. In this scheme have demonstrated ETX is a proper metric to measure the distances between each node and the source node. Thus, the nodes with low ETXs can probably receive the innovative packets earlier.

The existence of worm- hole link intuitively changes the normal network topology since the innovative packets can be transmitted through the wormhole link directly and safely and thus the nodes around the remote side of the wormhole link can receive the novel packets earlier than expected. With a wormhole link, the order of the rank increments among the nodes will be significantly changed.

D. Prevention Of Wormhole Attack In Wireless Sensor Network

Dhara Buch et al. [1] presented here where each node forwarding Route Reply RREP packet checks the validity of the two-hop neighbor node forwarding that packet.To accomplish the presented technique, a unique key derived based on all the two-hop neighbors is p the techniques dealing with wormhole attack are investigated and an approach for wormhole prevention is proposed. Our approach is based on the analysis of the two-hop neighbors forwarding Route Reply packet. approach proposed here makes RREP packet forwarding conditional. By checking the validity of the two-hop neighbor node that has forwarded the packet, a node lets it to move further towards the source. Wormhole end is detected when the identity of the two-hop neighbor is found illegal.

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. rovided to each sensor node in the initial phase. By comparing the memory requirement for

various numbers of neighbors, it can be concluded that by spending more on setup cost, higher scalability can be achieved. The proposed scheme focuses on the type of wormhole with out-of-band channel.

Method & Algorithm	Protocol & technique	Authentication
Packet Leashes[7]	TIK	Not Present
WARRDP [12]	Hop count	Not Present
WAP [14]	DSR	Not Present
RRS & ANS [13]	BSR	Not Present
RRP [11]]	LEAP	Not Present
RRT [16]	AODV	Not Present
W-Delay [15]	OLSR	Not Present
WGDD [8]	Hop count	Not Present
DAWN[3]	RLNC	Not Present

Table 1: Comparison of different methods and protocols

E. Preventing Wormhole Attacks On Wireless Adhoc Networks: A Graph Theoretic Approach

L.Lazos et al. [5] presented a graph theoretic approach characterizing recently reported wormhole attacks on wireless ad hoc networks and also proposed a cryptography-based solution relying on local broadcast keys and provided a distributed mechanism for establishing them in randomly deployed networks. Graph theoretic model for characterizing the wormhole attack and derive the necessary and sufficient conditions for any candidate solution to prevent wormholes.

Analytically determined the level of security achieved by our scheme based on spatial statistics theory. Making use of geometric random graphs induced by the communication range constraint of the nodes, we present the necessary and sufficient conditions for detecting and defending against wormholes. Using our theory, also present a defense mechanism based on local broadcast keys. It is our claim that in the absence of location or distance bounding, we must use probabilistic techniques for dealing with wormholes.

F. Packet leashes:a defence against wormhole attacks in wireless networks

Yih-Chun Hu et al. [7] In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. In this paper, we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality.

In this paper introduce the notion of a packet leash as a general mechanism for detecting and thus defending against wormhole attacks. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. We distinguish between geographical leashes and temporal leashes.

TIK protocol implements temporal leashes and provides efficient instant authentication for broadcast communication in wireless networks. TIK stands for TESLA with Instant Key disclosure, and is an extension of the TESLA broadcast authentication protocol. A MAC layer protocol using TIK efficiently protects against replay, spoofing, and wormhole attacks, and ensures strong freshness.TIK is implementable with current technologies, and does not require significant additional processing overhead at the MAC layer, since the authentication of each packet can be performed on the host CPU.

Scheme	Synchronization	QOS
DELPHI[10]	No need	Delay
Geographic leash technique [19]	Low	Delay upto leash factor
Temporal leash technique [19]	Medium	Delay upto leash factor
HMTI [18]	No need	Jitter
WAP [14]	Only source node	Delay per hop
SECTOR[20]	No need	No delay

Table 2: Comparison of different detection methods and capabilities

G. Detecting Wormhole Attacks In Wireless Sensor Networks

Yurong Xu et al, [6] proposed a wormhole geographic distributed detection (WGDD) algorithm uses a hop counting technique as a probe procedure for detecting wormhole. After running the probe procedure, each network node collects the set of hop counts of its neighbor nodes that are within one/k hops from it. (The hop count is the minimum number of node-to-node transmissions to reach the node from a bootstrap node.) Next, the node runs Dijkstra's (or an equivalent) algorithm to obtain the shortest path for each pair of nodes, and reconstructs a local map using multidimensional scaling (MDS).

Finally, a diameter feature is used to detect wormholes by identifying distortions in local maps. This paper describes a distributed wormhole detection algorithm for wireless sensor networks, which detects wormholes based on the distortions they create in a network. Since wormhole attacks are passive in nature, the algorithm uses a hop counting technique as a probe procedure, reconstructs local maps in each node, and then uses a diameter feature to detect abnormalities caused by wormholes.

The wormhole geographic distributed detection (WGDD) algorithm presented in this paper employs a hop counting technique as a probe procedure for wormholes, reconstructs local maps using multidimensional scaling at each node, and uses a novel diameter feature to detect distortions produced by wormholes. Even in case of shorter wormholes that are less than three hops long, the algorithm has a detection rate of over 80% (with an FTR of less than 20%). Furthermore, the algorithm can be adjusted to produce extremely low false alarm rates (with an FDR of zero).

.

H. An Efficient Wormhole Attack Detection Method in Wireless Sensor Networks

Guowei xu et al. [9] In this paper introduce novel approaches for detecting wormhole attacks and propose an efficient wormhole detection algorithm, which is named Transmission Range based Method (TRM). With the existence of wormhole, the network topology is destructed and normal routes are misled.

Detecting wormholes in WSNs is essential since they can make the routing protocols malfunction. In this paper, a highly efficient wormhole detection method named TRM is developed, which uses the local neighborhood information to calculate the transmission range. Wormhole attack in WSNs has been drawing more and more attention since it can disrupt normal network routing protocols. However, in previous work of wormhole detection, most of them need either extra hardware or clock synchronizations and suffer from high complexity.

In this paper, an efficient wormhole detection method is proposed, which is based only on local neighborhood information In the detection procedure, the neighborhood information of each node is updated and exchanged periodically between neighbors along with the increment of the transmission range. A local topology that has a wormhole link finally reports a mismatch of the neighborhood information between nodes. According to the analysis, the algorithm gives O(n) for both of the time complexity and the space complexity.

III. Comparative Analysis

Different detection methods of wormhole discussed above are compared in this section. Each detection methods has its own algorithm as well as cryptographic basis. Comparative analysis of different detection methods are mentioned in the table 1 and 2. Table 1 gives a comparison of different methods, Algorithms, protocol and technique ,etc.

Table 2 gives a comparison of the capabilities like methods, algorithms, synchronization, quality of service (QOS) etc. of detection methods. Based on the requirements a suitable algorithms can be adopted in a wormhole detection methods. Hence, the comparative analysis shows the merits and demerits of a particular wormhole detection method in a well-structured manner.

IV. Conclusion

Detection method has to be established in a secure way. Algorithms is one among the security features of detecting wornhole attack. It helps in achieving secure communication among two sensor nodes. Hence, various detection methods are proposed. Each methods has its own security features, protocol, merits and demerits. In this paper, a survey of various detection methods are carried out. Security features of different algorithms and methods are analyzed and compared effectively.

References

[1] Dhara Buch et al., "Prevention Of Wormhole Attack In Wireless Sensor Network", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011

[2] Zaw Tun et al., "Wormhole Attack Detection In Wireless Sensor Network" World Academy of Science, Engineering and Technology 46 2008

[3] Shiyu ji et al., " Wormhole Attack Detection Algorithm In Wireless Network Coding System" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 3, MARCH 2015

[4] Ritesh Maheswari et al.," Detecting Wormhole Attacks In Wireless Networks using Connectivity Information" CNS-0519734, OISE- 0423460, CNS-0308631 and a grant from the Sensor CAT center.

[5] L.Lazos et al., "Preventing Wormhole Attacks On Wireless Adhoc Networks: A Graph Theoretic Approach" https://www.ee.washington.edu/research/nsl/papers/WCNC-05.pdf.

[6] Yurong Xu et al., "Detecting Wormhole Attacks In Wireless Sensor Networks" Critical Infrastructure Protection,Chapter 14.

[7] Y .C. Hu, A. Perrigand D.B. Johnson, "Packet Leashes:A Defense against Wormhole Attacks in WirelessNetworks",in 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM),pp.1976-1986,2003

[8] V a n Tran,LeXuanHung, Young-KooLee, SungyoungLee and HeejoLee, "TTM: An Efficient Mechanism to Detect Wormhole AttacksinWirelessAd-hocNetworks",in4th IEEE conference on Consum r Communications and Networking Conference,pp. 593-598,2007.

[9] Guowei xu et al., "An Efficient Wormhole Attack Detection Method in Wireless Sensor Networks" Computer Science and Information Systems 11(3):1127–1141 DOI: 10.2298/CSIS130921068W, February 27, 2014.

[10]Hon sun chiu et al., "DelPHI: wormhole detection mechanism for ad hoc wireless networks",http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=10746,jan 2006.

[11] Saurabh Upadhyayand Brijesh Kumar Chaurasia, "Impact of Wormhole Attacks on MANETs", in International Jo u r n a l of Computer Science and Emerging Technologies (E-ISSN:2044-6004), vol.2,issue.1,pp.77-82,February2011

[12] Saurabh Gupta, SubratKar and S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", in International Conference of Innovations in Information Technology, pp. 226 to 231, 2011

[13] E.Poornima, C.Shobha Bindu and SK.Munwar, "Detection andPreventionofLayer-3Wormhole Attacks on Boundary State Routing in AdHoc Networks", in International Conference on Advances in Computer Engineering,pp.48-53,2010

[14] Sun Choi, Doo-youn g Kim, Do-hyeon Lee and Jae-ilJung, "WAP: Wormhole Attack Prevention Algorithmin Mobile Ad Hoc Networks", in IEEE International Conferenceon Sensor Networks, Ubiquitous, and Trustworthy Computing,pp.343-348, 2008

[15] Honglong Chen,WeiLou ,Xice Sunandand Zhi Wang, "A Secure Localization Approach against Wormhole Attacks Using Distance Consistency", in Hindawi Publishing Corporation EURASIPJournal on Wireless Communications and Networking, vol.2010,11pages,2010

[16] I F Akyildiz, W Su and Y Sankara subramaniam, E Cayirci, "Wireless Sensor Networks: asurvey," in Elsevier Scienc eB.V.,Computer Networks, vol.38(4) ,pp.394-422, March 2002

[17] P. Papadimitratos and Z. Haas, Secure routing for mobile ad hoc networks, Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, 2002.

[18] M.A. Gorlatova, P.C. Mason, L. Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis". In IEEE Military Communications Conference, 2006.

[19] Yih-Chun Hu et al., "Packet Leashes: A Defens'e against Wormhole Attacks in Wireless Ad Hoc Networks" Rice University Department of Computer Science Technical Report TR01-384 December 17, 2001 Revised: September 25, 2002.

[20] S.Capkun, L. Butty_an and J. Hubaux, SECTOR: Secure tracking of node encounters in multi-hop wireless networks, Proceedings of the First ACM
Workshop on Security of Ad Hoc and Sensor Networks, pp. 21{32, 2003.