ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (325-331), Month: April-June 2014, Available at: www.researchpublish.com

A Qualitative Comparative Study: Wormhole Attack Detection Techniques in WSN at Network Layer

Manisha[1], Gaurav Gupta[2], Nivedita Kashyap[3], Ruchika Chandel[4,], Vandana Sharma[5]

Department of Computer Science Engineering, Shoolini University, Solan, HP, India

Abstract: **Wireless Sensor Network platforms are less expensive and more powerful having tiny electronic devices called Motes (sensor nodes). Wireless sensor networks enhance its popularity in military and health centric research areas; now it is also popular in industrial area. Security is the main requirement of wireless sensor networks. This paper describes the network layer attacks which lead to subvert the network functionality. Amongst them, the wormhole attack is a severe threat to WSNs. This attack completely disrupts the network topology by altering the message, by relaying old and fake messages in the network. Researchers have developed and proposed many detection mechanisms to detect and prevent the wormhole attack. The aim of this paper is to elaborate the simulation results and also compare the performance of wormhole detection techniques (Transmission time based, Range based and MDS based) that are popular in WSNs.**

Keywords: **WSN, Wormhole, Motes, MDS, LCT and UDG methods.**

1. INTRODUCTION

Wireless sensor networks are heterogeneous systems that composed thousands of large and self-configurable sensor nodes (Motes) and few sink nodes have limited power supply and resource constraint, inexpensive and data storage [1,16]. These sensor nodes (passive nodes) communicate through wireless medium and since the data from the physical real world and send it to gateway/ sink node for further processing.WSN Nodes are following components [16]:

- Transceivers
- Battery
- Sensing unit
- Processing unit

Now days, WSNs are rapidly gaining interest as a research area in industry, academic and defense. WSNs are typically used in applications, such as, habitat monitoring, military surveillance, environment sensing and health monitoring.

WSNs are easily vulnerable to attacks. Providing secure routing in WSNs is a difficult task as many attackers attack on routing protocols. Hence, Security is the main concern in WSNs [17, 18]. Security attacks are classified according to OSI layered model. Generally, the security attacks are classified in two ways:

1.1 Active attack

In this attack, the intruder monitors and modifies the data stream on to communication channel and disrupts the network topology. These attacks are active in nature. Masquerade or fabrication, Message replay, Message modification and denial of service or interruption of availability are the four categories of active attack.

1.2 Passive attack

In this attack, the intruder monitors the communication channel and attempts to steal information by electronic eavesdropping (wiretapping). Passive attack is characterized by interception of data packets and messages but not modification. These attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords.

This paper focused on Network Layer Attacks such as sinkhole attack, black hole attack, selective forwarding Attack, false routing Information Attack and wormhole Attack. Due to distributed network Architecture and limited resource of sensors, Wormhole attack is one of the vital attacks available in WSNs. Wormhole Attack cannot be affected by any encryption and Cryptography Method, the malicious node captured the packets and tunnel these packets to other malicious nodes far away, it makes two nodes far away believe that they are neighbors in one hop.

The rest of paper is managed as: Section 2 represent the significance of wormhole attack. Section 3 represents the various detection techniques of wormhole attack in WSNs. Last section represents the conclusion and future work.

2. SIGNIFICANCE OF WORMHOLE ATTACK

Wormhole Attack in one of the severe network layer attack which is hard to defense against and detect in WSNs. Two Malicious Nodes can collaborate in setting up the low latency link (wormhole link), records the messages from one section, forward these messages through the wormhole link and release them to another section of the network [3,16]. The wormhole attack is illustrated in the "Fig.1" as:

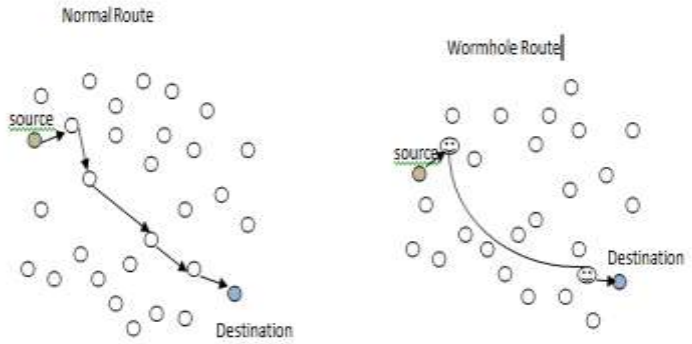

Fig. 1 Wormhole Attack

In simple words, wormhole attacker creates an illusion between nodes that they are very close to each other by generating the wormhole link. This allows an attacker to subvert the functionality of the routing protocols, by controlling the numerous routes in the network.

Since the Wormhole attackers have not any cryptographic keys, they can perform a wormhole attack on the routing protocols even if the communication is authenticated and secure. A wormhole attacker can also break any routing protocol that directly or indirectly relies on geographic proximity. As compared to wormhole attack with other routing attacks, it is convoluted and most popular attack in wireless sensor networks. Due to its passive in nature, wormhole attack gains much popularity in the research field [16].

3. WORMHOLE DETECTION TECHNIQUES IN WSNs

A significant research has been done to detect wormhole attacks in WSNs. Many algorithms and mechanisms have been implemented to detect the wormhole attack in routing protocols such that packet leashes which are presented in [4, 5, 6, 7]. This technique categorized in two ways: geographic leash and temporal leash. This technique used physical metric, such as time delay or geographic location to detect the wormhole attack. Wang [12, 7] implement an approach inspired by packet leashes, but their system is based on end-to-end location information, rather hop-by-hop leashes. Hu and Evans present a technique to wormhole attacks for ad hoc networks in which all nodes are equipped with directional antennas. SeRWA (Secure Route protocol against Wormhole Attack in sensor networks) has also been presented [13, 2]. This protocol didn't require any special hardware to detect wormhole attacks. Wang et al. [14, 7] propose a method named MDS-VOW [14, 7] that used multidimensional scaling to rebuild the network and detects the wormhole attack based on the distance of neighbors to a central server.

L. Lazes et al. [15, 7] propose another mechanism named LAGNs (Location –Aware 'Guard' Nodes) to prevent the wormhole attacks on wireless ad hoc networks based on the guard nodes. They acquire guard node to detect the message flow between nodes. A guard node can detect a wormhole attack using guard property and communication range constraint property during fractional key distribution. Design Dong [8] presented a distributed detection method which detects the wormhole attack based on topology. This method relies solely on network connectivity information.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (325-331), Month: April-June 2014, Available at: www.researchpublish.com

There are many detection mechanisms to detect the wormhole attack in WSNs. This paper presents the comparative study of mainly three wormhole detection mechanisms which are illustrated as:

3.1 Transmission Time based Detection in WSN (August 2012)

S.Sharmila and G.Umamaheswari proposed the wormhole attack detection mechanism "Transmission Time based detection" [9] which used transmission time and hop to detect the wormhole attack. This technique evolved three phases:

3.1.1 Grid formation phase: Every node is arranged in the virtual grid form and nodes are mobile. Each grid encompasses the base station to route discovery. The total terrain range is divided into a d*d square form. The location of node is identified (using equation 1):

$$LX = x/d \text{ and } LY = y/d \quad \text{- (1)}$$

3.1.2 Construction of neighbor list: This phase constructs the neighbor list by transmitting the REQ message and REP message as shown in "Fig.2". The time is formulated between REQ and REP messages of the neighbor nodes using this equation and saves it (using equation 2).

$$T = Treq - Trep \quad \text{- (2)}$$

3.1.3 Detection Phase: After construction of neighbor list, the next phase is to detect the wormhole attack on the assumption of the time value. If the transmission time may considerably higher than other successive nodes and it is suspected that a wormhole link exists between the two nodes which lie in the routing path. The CACK packet is transmitted through suspected nodes and compares it's time value with the time value of successive nodes. If the time of the suspected nodes is higher than the time of successive nodes then it exist wormhole nodes (using equation 3 and 4)

$$Ta = Tsa(REP) - Tsa(REQ)$$
$$Tb = Tab(REP) - Tab(REQ)$$
$$Td = Tbd(REP) - Tbd(REQ)$$

The total time is formulated as:

$$TT = Ta + Tb + Td$$

$$Tsd = Tbd(Cack) - Tbd(REQ) \quad \text{- (3)}$$

The time of Ta, Tb, Td and Tsd depends up on the distance the transmission time (RT) is formulated as:

$$RT = (TH * TT) + (1 - TH) * Tsd \quad \text{- (4)}$$

If it lies in the range nearer to 1 then RT is same as T (Ta, Tb, and Td) and wormhole link doesn't exist. It lies in the range nearer to 0 than wormhole link exists due to delay in time in "Fig.2".

S	A
A	B
B	D
D	B
B	A
A	S

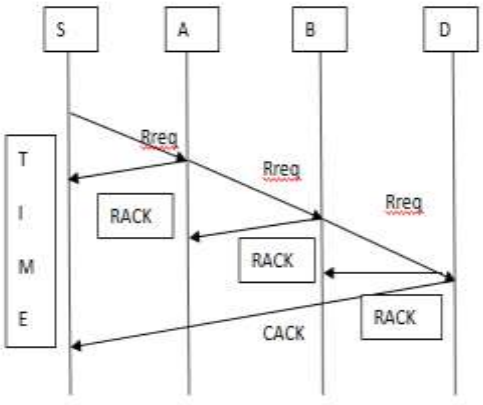

Fig.2. Transmission Time Based mechanism

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (325-331), Month: April-June 2014, Available at: www.researchpublish.com

3.1.2 Simulation Results

This simulation includes 50 mobile nodes deployed randomly in 1000 m * 1000 m terrain range using NS-2 simulator. This scheme is proposed on AODV routing protocol and uses radio propagation [9]. The transmission range is 250 meters and the packet size is 512 bytes. The randomly created wormhole nodes establish a tunnel between them and perform a wormhole attack in the routing protocol. Using this mechanism, the wormhole attack is detected in the AODV routing protocol. The detection rate is illustrated in "Fig. 3".

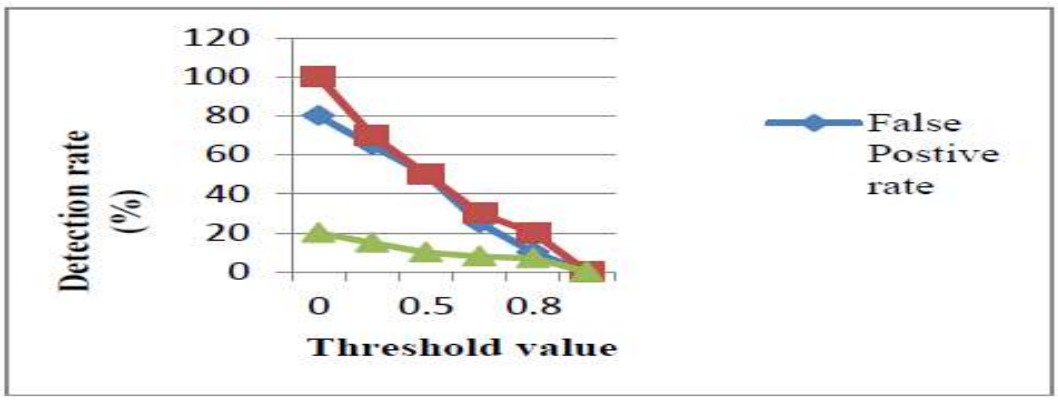

Fig3. Detection Rate

3.2 A ranging based Detection Mechanism (June 2012)

TIAN Bin, LI Qi, YANG Yi-Xian, LI Dong, XIN Yang propose ranging based detection mechanism to detect the wormhole attack in WSN. The topology of the network is static and nodes are randomly deployed. This scheme analyzed the time overhead from the node broadcast a message to the node receive from its neighbor echo the message and fake neighbor nodes. This technique used k-means cluster analysis to detect the wormhole attack detection that relies on the distance correlation in the physical location of nodes. The nodes are characterized in two clusters, say, legal nodes and illegal nodes [10].

3.2.1 Simulation results

This simulation includes 100 sensor nodes deployed randomly in 100 * 100 m2 square regions. The radio range is set to 15m and also modified the application layer code to report packet sending and receiving time at the network layer [10]. The fig4 shows the discovery packet that contains delay time as shown in "Fig.5".

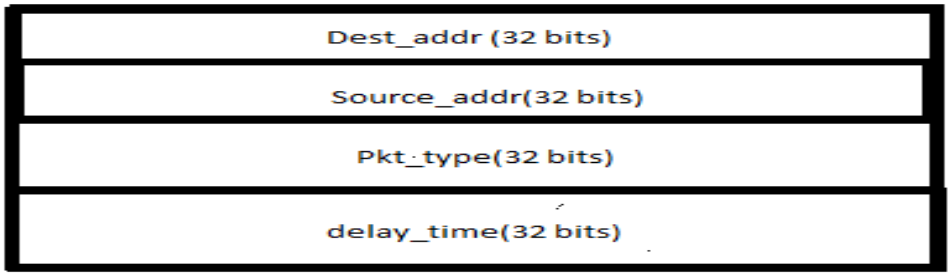

Fig4. Neighbor discovery packet format

This simulation result shows that the wormhole is detected more in the configuration where this attack is launched over a longer hop count. Since the packets are encapsulated repeatedly through the wormhole link which causes more delay transmission in "Fig.6".

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (325-331), Month: April-June 2014, Available at: www.researchpublish.com

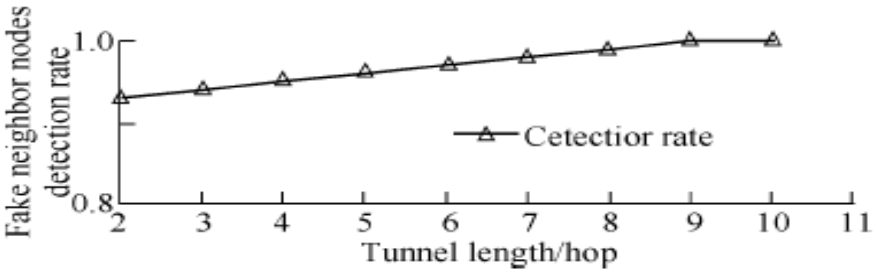

Fig5. Fake Nodes detection Rate

3.3 MDS-based Wormhole Detection Using Local topology in WSN (November 2012)

Xiaopei Lu, Dezun Dong, and Xiangke Liao propose MDS (multidimensional scaling- based detection mechanism which detects the wormhole attack by only topology information. This detection scheme mainly involves two components: 1. Performing local MDS-based reconstruction: It acquires a number of suspect wormhole nodes. 2. Performing refinement process: It refines the suspect nodes and presents the final detection results.
In this approach, the algorithm is described to detect the wormhole attack based on several parameters that influence the performance of this algorithm discussed as:

Influence of k.:- k is the constant term set to 2 means twofold. First small k introduces the communication overhead of each node. Second, if ^{v} is the wormhole node, its 2-hop neighbors would cover all wormhole nodes [11].

Influence of λ_{th}: This approach will be on the aggressive side and select a relatively lower threshold which impact on the detection accuracy.

3.3.1 Simulation Results

The network set up 1600 nodes deployed over a square region. This simulation presents up = 2 for perturbed grid model, and ρ = 0.75 for quasi-UDG model. The average node degree varies from 4 to 13. The wormhole nodes are arranged diagonally in the network and the average number of wormhole nodes is 15. The simulation result takes 100 runs with random network generation and describes the average results. The results are illustrated in the "Fig. 7". The first four sets of simulations indicates that the false positive rate decrease and also detecting the multiple wormholes. When the distance between two different wormholes is long enough, they will not affect each other. Thus, this mechanism can well detect all wormhole nodes [11]. Otherwise, if multiple wormholes are close, they may interfere with each other, which make the detection more difficult.

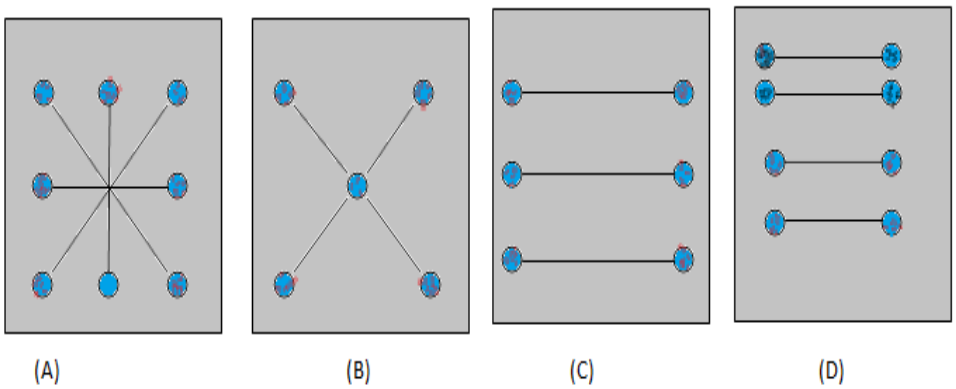

Fig.6 Detection results for multiple wormholes. 900 nodes are deployed over a square region. Perturbed grid deployment with p = 1.5 and quasi-UDG with ρ = 0.75 are adopted to generate the networks. The average node degree is 7.5. Multiple wormholes are placed at different positions in the network.

This table describes the qualitative comparison of wormhole detection mechanism in WSNs by evaluating simulation results.

Table1. A Qualitative comparison of wormhole detection mechanisms in wireless sensor networks

Parameters	**Range based mechanism**	**Transmission time based mechanism**	**MDS-based using local topology mechanism**
Nodes	Up to 50 Randomly deployed	50 Randomly deployed	1600 (p = 2 → perturbed grid Model ρ = 0.75 → quasi-UDG model)
Methods	Using Local topology	Using transmission time	Using UDG and LCT method
Arrangement of Nodes	Grid	Grid	Diagonal
Terrain region (sq. meters)	100 *100	1000*1000	$[x- pd, x + pd]\times[y- pd, y +pd]$
Packet Size(bits)	32	512	-
Detection Time(ms)	100	590	100
Energy Consumption	Small Energy Consumption	More energy consumption	Not Analyzed
Memory Overhead	-	48 bytes	-
Detection Rate	Relatively Low	100% When the threshold value is zero	Relatively low
False Positive Rate False Negative Rate	-	80% 20%	Few false positive rate and false negative rate
Additional Hardware	No	No	No

4. CONCLUSION AND FUTURE WORK

Wireless sensor networks have gained much popularity over the past few years. Due to its operating nature and openness in a wireless channel, security is the most challenging aspects.

Among the various attacks of different layers, wormhole attack, combination of others attacks, is the most popular attack because of its complex nature and hard to detect. Wormhole attacks can significantly degrade the network performance and threaten network security [16]. Various countermeasures have been done for the detection of wormhole attacks as above explained.

As previous wormhole detection techniques are not able to detect wormhole attack accurately. The research work done earlier has some problems such as memory overhead, energy consumption. Hence, the future research work is to propose a new detection technique based on frequency to detect the wormhole attack in wireless sensor network.

REFERENCES

[1] Kashyap Patel, Mrs.T.Manoranjitham (May – 2013), Detection of Wormhole Attack In Wireless Sensor Network, *International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 5*, ISSN: 2278-0181.

[2] Lukman Sharif and Munir Ahmed (June 2010), The Wormhole Routing Attack in Wireless Sensor Networks, *Journal of Information Processing Systems, Vol.6, No.2*.

[3] Padmavathi, G., & Shanmugapriya, D. (2009), A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security (IJCSIS): Vol.4, No.1 & 2*.

[4] Y.-C. Hu, A. Perrig, D. B. Johnson (2006), Wormhole Attacks in Wireless Networks, *Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2*, pp. 370- 380.

[5] Y. Hu, A. Perrig, and D. Johnson (2004), Packet Leashes: a Defense against Wormhole Attacks in Wireless AdHoc Networks. in proceedings *of INFOCOM*.

[6] W. Weichao, B. Bharat, Y. Lu, X. Wu, Wiley Interscience (2006), Defending against Wormhole Attacks in Mobile Ad Hoc Networks. *Wireless Communication and Mobile Computing.*

[7] Zaw Tun and Aung Htein Maw (2008), Wormhole Attack Detection in Wireless Sensor Networks, *World Academy of Science, Engineering and Technology Vol: 22 2008-10-22*.

[8] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li and Xiangke Liao(2011), "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks, *IEEE/ACM Trans. Networking, vol. 19*, pp. 1787-1796.

[9] S.Sharmila, G.Umamaheswari(August 2012), Transmission Time based Detection of Wormhole Attack in Wireless Sensor Networks, *Special Issue of International Journal of Computer Applications (0975 – 8887) on Information Processing and Remote Computing – IPRC.*

[10] TIAN Bin, LI Qi, YANG Yi-xian, LI Dong, and XIN Yang (June 2012), A ranging based scheme for detecting the wormhole attack in wireless sensor networks, *www.sciencedirect.com/science/journal/10058885, 19(Suppl.1):6-10.*

[11] Xiaopei Lu, Dezun Dong, and Xiangke Liao(November 2012), MDS-Based Wormhole Detection Using Local Topology in Wireless Sensor Networks, *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2012, Article ID 145702*, 9 pages doi:10.1155/2012/145702.

[12] W. Wang, B. Bhargava, Y. Lu and X. Wu(June 2006), Defending Against Wormhole Attacks in Mobile Ad Hoc Networks, *Wireless Communication and Mobile Computing, Volume 6, Issue:4*, pp.483-503.

[13] Wood, A. & Stankovic, J. (2002), Denial of service in sensor networks, *In Computer. Vol 35, (p 54 –62).*

[14] W. Wang and B. Bhargava (2004), Visualization of Wormholes in Sensor Networks, *In Proceedings of the ACM workshop on Wireless security (Wise'04), pp. 51-60*

[15] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L.W. Chang(March 2005), Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach, *In Proceedings of Wireless Communictions and Networking Conference, IEEE, pp.1193-1199.*

[16] Manisha, Gaurav Gupta (September 2013), Attacks on Wireless Sensor Networks: A Survey. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Volume 3, Issue 4,* (Impact Factor – 2.080)

[17] Gaurav Gupta, Deepika Gupta (September 2013), Intrusion Detection against DoSA in MANET Environment". *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Volume 3, Issue 4,* (Impact Factor – 2.080)

[18] Gaurav Gupta, Deepika Goel Gupta (July 2012), Security in Location Based Services, *International Journal of Scientific and Engineering Research (IJSER) - (ISSN 2229-5518). IJSER Volume 3, Issue 7, [Paper ID: I016382]*