International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 02, February 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK: A SURVEY

Poonam, Mrs. Meenu

[1,2] *CSE, Madan Mohan Malaviya University of Technology, (India)*

ABSTRACT

Wireless sensor networks passes a practical and Economically feasible alternative to manual data association in general and military scenarios, providing a means of surveillance of a region of field and providing warning of any threats. In common wormhole attack, the attacker receives packets in the network, forward them through a wired or wireless association with high-bandwidth low-latency bond in the network links, broadcast them to another point in the network. In these environments, security issues are intensely important since a successful attack can cause great damage, even portending human life. The main emphasis of this paper is to study wormhole attack & its detection method.

Keywords: WSN, Wormhole, Blackhole, Grayhole, Sinkhole.

I.INTRODUCTION

Wireless sensor networks (WSNs) are grow technology paradigm consisting of small, low-power devices that consist of limited computation, sensing along with radio communication capabilities. The technology has the ability to provide flexible infrastructures as numerous applications, industry automation, including healthcare, surveillance and defense. Most WSN applications are designed to achieve in trusted environments. However, security issues are a major concern when WSNs are deployed in untrusted environments. An attacker may damage a WSN by interfering with intra-network packet transmission by wormhole attacks ,Sybil attacks, jamming or packet injection attacks. In a typical wormhole attack, the attacker receives packets near to one point in the network, forwards them through a wireless or wired association with much less latency than the default links used by the network, and then broadcast them to another location in the network.

II.ARCHITECTURE OF WSN

A typical WSN consist of sensor nodes, base stations andthe server. Sensor nodes has some memory, processing power and battery power. These sensor nodes are connected to the neighboring sensor nodes or to the different base.stations and these all base stations are connected to the main server. All these nodes communicate through wireless medium. There are some protocols defined with help of which all sensors, base stations and main server can communicate. Following figure explains this all

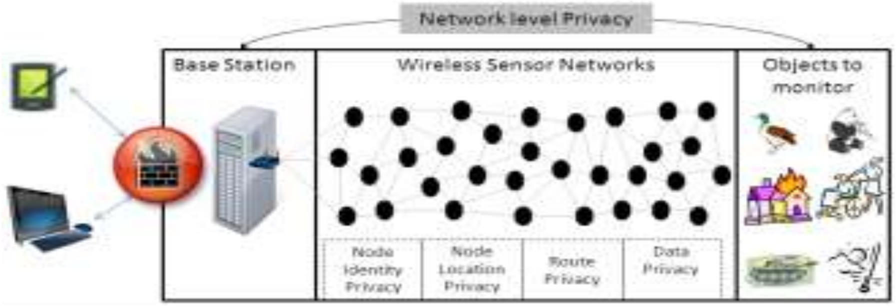

Fig. 1. A typical WSN scenario

III. WORMHOLE ATTACK

A.Security breach available to perform wormhole attack

- For secure communication there are some privacy primitives defined like sensor node identification privacy, sensor node location privacy, route privacy and data packet privacy. These privacy primitives help sensors to secure the data they have. But attacker can easily capture the packet and get this security information and hence can get access to sensor network.
- Also sensor nodes have limited resources these nodes need to replace after some time. These sensor nodes are also generally deployed in unattended environment . So in order to steal this sensitive information, attacker compromises any node in the network or he introduces his own node in the network without getting noticed. This node is then called as malicious node which is totallycontrolled by attacker. A typical wormhole attack needs two or more such malicious nodes to perform wormhole attack successfully needed that these nodes have larger resources than other nodes.

B. How wormhole attack is performed

As discussed earlier wormhole attack is done with the help of two or more malicious nodes having larger resources thanother sensors in the network. These malicious nodes createslow latency link (high bandwidth tunnel) between them. The tunnel can be established in many different ways, like through an out-of –band hidden channel (e.g., a wired link), packet encapsulation or high powered transmission. After establishing the tunnel, attacker promotes these tunnels as high-quality routes to the base station. Thus, neighboring sensor nodes adopt these tunnels into their communication paths, rendering their data under the scrutiny of the adversaries. Already the tunnel is established, the attackers collect data packets on one end of the tunnel, send them using the tunnel (wired or wireless link) and replay them at the other end. Wormhole attacks may result in serious damages in WSNs through interrupting or altering the information flow towards the base station.

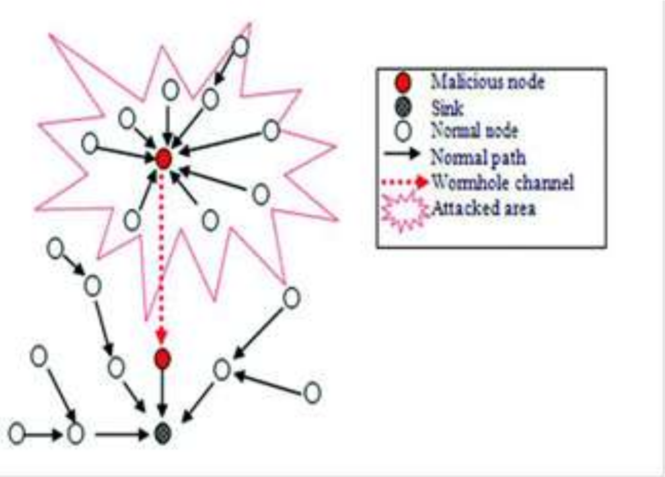

Fig. 2. Example of wormhole attack with two adversaries

IV. VARIANTS OF WORMHOLE ATTACK

There are three variants of wormhole attack Blackhole attack, Grayhole attack and Sinkhole attack. They are classified according to their severeness of stealing information and ease of detection in the network**.**

A. Blackhole attack

In this form of the wormhole attack attacker tries to collect most of the data and then use that data and then drops it without forwarding to other nodes . Because of its nature of dropping all available data it is known by Blackhole attack. This is the simplest and easiest form of wormhole attack. Drawback of this type of attack is that it can easily get identified by using data flow analysis and graph based techniques.

B. Grayhole attack

This is the second form of the wormhole attack and this form is more intelligent than Blackhole attack. In order to reduce the probability of detection, packet dropping in Grayhole attack is done selectively .Grayhole attack also exhibits random behavior in which packet dropping is done randomly while forwarding other packets thereby making it even more difficult to detect the malicious nodes. So it becomes more difficult to detect the Grayhole attack than Blackhole attack in the sensor network.

C. Sinkhole attack

This is the most dangerous and intelligent form of the wormhole attack. In this attack malicious nodes collect thedata and use it and after that it modifies the data and then replays it in the sensor network . In Sinkhole attacksometimes malicious nodes instead of forwarding data, drops the data. Because of this reason Sinkhole attack in the network is difficult to detect and prevent. Also because of modification of the data or dropping of the data Sinkhole attack reduces the performance of the network.

V. NEED TO PREVENT WORMHOLE ATTACK

There are two categories of routing protocols used in wireless network for communication between wireless devices. One is on-demand routing and other is proactive routing. A study shows that wormhole attack is successful inboth the type of routing protocol. Also presence of at least two wormholes in the network can divert nearly 50% of the traffic through the malicious node . Wormhole attack results in reduction of the performance of network and sometimes they may responsible for collapsing the entire network. Hence there is the need to detect and prevent the wormhole attack.

VI. DETECTION AND PREVENTION OF WORMHOLE ATTACK

WSN is spreading faster because of its various applications and hence the need of securing it also increasing. There are lot of algorithms for detection a prevention of the wormhole attack. Detection of wormhole attack is easier task as compare to prevention of wormhole attack. Loads of research is still going on for finding out efficient methods of detection and prevention. Some of the detection methods are mention in the following table.

TABLE:

S.NO.	Method [Year]	Requirements/Commentary
1.	LISP [2004]	Applicable only to static stationary networks ,Impractical
2.	Directional antennas [2004]	Directional antennas on all nodes; Good solutions for networks relying on directional antennas, but not directly applicable to other networks.
3.	Time of flight [2004]	Hardware enabling one-bit message and immediate replies

		without CPU involvement; Impractical; Likely to require MAC-layer Modifications
4.	Statistical analysis [2005]	This method works only with multi-path ondemand protocol
5.	LITEWORP [2005]	Static topology for network; Predistribution pair-wise key management protocol; not applicable for protocoldeviation mode.
6.	Connectivity-based Approaches [2006]	Require connectivity information Tightly synchronized clocks (ns),Impractical.
7.	End-to-end mechanism [2006]	Requires knowledge of location information,Loosely synchronized clocks; This mechanism uses geographic informationand authentication method to detect malicious neighbors
8.	True-link [2006]	Authentication mechanism; Time-based mechanism; Works only with standard IEEE 802.11 hardware with a minor backwards compatible firmware update.
9.	TTM [2007]	Cooperation of all nodes in the path; Transmission time-based mechanism.
10.	Radio fingerprinting [2007]	Require fingerprinting device; Chipcon 1000, 433 MHz radio was used.
11.	Connectivity graph [2007]	Connectivity information is required; To be independent to wireless communication models.
12.	Secure neighbor discovery [2008]	Secure neighbor discovery.
13.	CSB [2009]	No packet loss in the System,Conflicting-set-based resistant localization system.
14.	Secure localization [2010]	Conflicting-set-based resistant localization
15.	Local connectivity information [2011]	Centralized and distributed algorithm, 100% detection and 0% false alarm probabilities using proper parameter.
16.	MA WSN [2012]	Intensity of the transmission is scrutinized to discover the compromised node in the network; secures nodes from Sybil attack by 34%,Wormhole attack by 27.8% and Sinkhole attack by 29.8%.
17.	E2SIW [2012]	High detection rate, less overhead, and can consume less energy in less time, compared to the De Worm.
18.	Worm Planar [2013]	Graph theoretical method, exploits location free network

		planarization technique to perform connectivity-based wormhole detection**.**
19.	TPN model[2013]	Analytical results show that the secured version of CL-MAC can effectively.
20.	DAWN [2014]	Exploring the change of the flow directions of the innovative packets;good lower bound of successful detectionrate

VII. CONCLUSION

From this survey we conclude that WSN is spreading widely across the globe and thus becoming the main target for the attackers. Wormhole attack is such one of the serious threats for WSN. It reduces the performance of the sensor network. Presence of two wormholes can attract nearly 50% of the traffic .Although there are many algorithms and methods being developed from decade, not a single method.is able to detect and prevent the attack with considering the available sensor network parameters (like efficient use of memory, processing time, etc.) and without affecting other security measures. Hence there is still need to improve the performance of detection and prevention algorithms and efficient use of sensor memory.

REFERENCES

[1] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d Auriol, Heejo Lee, Sungyoung Lee and Young-Jae Song, Achieving Network LevelPrivacy in Wireless Sensor Networks,‖ Sensors 2010, *10*, pp.1447-1472

[2] MajidMeghdadi, SuatOzdemir and InanGüler, A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks,‖ IETE technical review, VOL 28, ISSUE 2, 2011

[3] Xiaopei Lu, Dezun Dong, Xiangke Liao, WormPlanar: Topological Planarization Based Wormhole Detection in Wireless Networks,42nd International Conference on Parallel Processing (ICPP), pp.498 –503

[4] Louazani A., Sekhri L., Kechar B., ―A time Petri net model for wormhole attack detection in wireless sensor networks,‖ International Conference on Smart Communications in Network Technologies(SaCoNeT), pp.1 – 6

[5] Alam M.R., Chan K.S., ―RTT-TC: A topological comparison based method to detect wormhole attacks in MANET,12thIEEEInternational Conference on Communication Technology (ICCT),2010, pp.991 – 994

[6] Ambika, N., Raju, G.T., ―MA WSN — Manifold authentication in wireless sensor network,‖ World Congress on Information and Communication Technologies (WICT), 2012, pp.572 – 576

[7] ShiyuJi, Tingting Chen, Sheng Zhong, Kak, S., DAWN: Defending against wormhole attacks in wireless network coding systems,INFOCOM, 2014 Proceedings IEEE, pp.664 – 672

[8] Dhurandher, S.K., Woungang, I., Gupta, A., Bhargava, B.K., E2SIW:An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks,‖ 26th International Conference on Advanced Information Networking and Applications Workshops, 2012, pp.472 –477

[9] MeenakshiTripathi, M.S.Gaur, V.Laxmi, ―Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN, The 8th International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN), ProcediaComputerScience 19 (2013), pp.1101 – 1107

[10] D.Sheela, Srividhya.V.R, Vrushali, Amrithavarshini and Jayashubha J ―A Mobile Agent Based Security System of Wireless Sensor Networks against Cloning and Sink Hole Attacks, International Conference on Computational Techniques and Artificial Intelligence (ICCTAI'2012) Penang, Malaysia

[11] PushpendraNiranjan, Manish Shrivastava, Rajpal Singh Khainwar,Enhancement of Routes Performance in MANET, International Journal of Computer Applications (0975-8887) Vol.42–No.12, March 2012

[12] ZawTun and AungHtein Maw, ―Wormhole Attack Detection in Wireless Sensor Networks,‖ World Academy of Science, Engineering and Technology 46, 2008.

[13] Robert G. Rittenhouse4 Junaid[17] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks.*IEEE Communications Magazine*, 40(8):102–114, August 2002Ahsenali Chaudhry1, Usman Tariq2, Mohammed Arif Amin3, ―Dealing with Sinkhole Attacks in Wireless Sensor Networks,‖ Advanced Science and Technology Letters Vol.29 (SecTech 2013), pp.7 – 12.

[14] D. R. Raymond and S. F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. In *IEEE Pervasive Computing*, volume 7, pages 74–81, 2008

[15] I. Khalil, S. Bagchi, and N. B. Shroff. Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks. *Comput.Netw.*, 51(13):3750– 3772, 2007

[16] John PaulWalters, ZhengqiangLiang,Weisong Shi and VipinChaudhary. Wireless sensor network security: A survey. *Security in Distributed, Grid, and Pervasive Computing*, 2006

[17] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci.A survey on sensor networks.*IEEE Communications Magazine*, 40(8):102–114, August 2002

[18] E. Shi and A. Perrig, "Designing Secure Sensor Networks," *Wireless Commun. Mag.*, vol. 11, no. 6, Dec. 2004 pp. 38–43

[19] Z. Tanveer and Z. Albert. Security issues in wireless sensor networks. In *ICSNC '06: Proceedings of the International Conference on Systems and Networks Communication*, page 40, Washington, DC, USA, 2006. IEEE Computer Society

[20] H. Chan and A. Perrig, "Security and Privacy in Sensor Network IEEE Communications Surveys & Tutorials • 2nd Quarter 2006