Wormhole Attack and it's variants in Wireless Sensor Network: A Survey

Ruplesh Bhojusing Pawar
Department of Computer Engineering
AISSMS COE, Pune,
Pune, India

Pratik Uttam Patil
Department of Computer Engineering
AISSMS COE, Pune,
Pune, India

Gaurav Bombale
Department of Computer Engineering
AISSMS COE, Pune,
Pune, India

Arti Zalani
Department of Computer Engineering
AISSMS COE, Pune,
Pune, India

Abstract— Now a days, use of wireless sensor network (WSN) is spreading more rapidly across the globe. It's because WSN has found lots of applications in environment monitoring, military applications, health care monitoring, habitat monitoring, etc. Because of these applications WSN is carrying very sensitive information and hence is the target for hackers to get some sensitive stuff. Introducing the malicious node in the WSN achieves this for attacker and this is nothing but the wormhole attack. In order to perform the wormhole attack at least two such malicious nodes having better resources than the other sensor nodes are required. In this survey paper we are going to study the wormhole attack and its variants like Blackhole, Grayhole and Sinkhole and also their impact on the network. We also cover their detection and prevention measures.

Keywords—WSN, Wormhole, Blackhole, Grayhole, Sinkhole

IJERT

I. Introduction

The wireless sensor network (WSN) is the network of static or mobile sensors which are deployed at various places aiming at gathering the information from surrounding. The nodes of WSN sense the physical, chemical or mechanical change in the environment and send it to the base station where they can get analyze and then sent to main server. The different applications include environment monitoring, military applications, health care monitoring, habitat monitoring, industrial monitoring, etc. [1][9]. Because of these applications WSN is carrying very sensitive information which makes it more attractive to attacker. The sensors in WSN sense the data, collect it and send it to the base station or other sensor nodes. The sensor nodes in WSN have their own OS, memory and battery for performing different operations. These all resources of sensor nodes are in limited form. They hence need to replace after some time. These sensor nodes are generally located in unattended environment [13] so any one can physically access and change their setting or introduce their own programmed sensor node. Some major attacks on sensor network include jamming, tempering, flooding, spoofing, selective forwarding, replay attack, Denial of service (i.e. Dos) attack, wormhole attack, etc.[1][2][9].

II. Architecture of WSN

A typical WSN consist of sensor nodes, base stations and the 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.

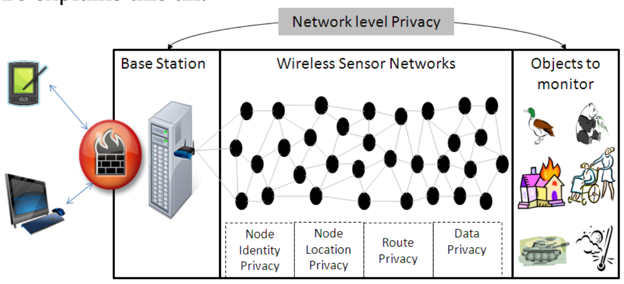

Fig. 1. A typical WSN scenario [1]

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 [1]. 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.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

- Also sensor nodes have limited resources these nodes need to replace after some time. These sensor nodes are also generally deployed in unattended environment [13]. 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 totally controlled 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 than other sensors in the network. These malicious nodes creates low latency link (high bandwidth tunnel) [2][13] between them. The tunnel can be established in many different ways, such as 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. Hence, neighboring sensor nodes adopt these tunnels into their communication paths, rendering their data under the scrutiny of the adversaries [11]. Once 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 by interrupting or altering the information flow towards the base station.

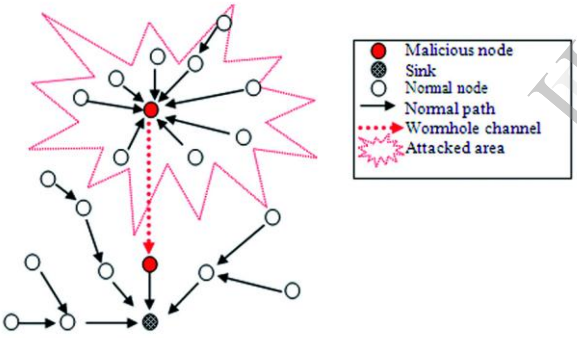

Fig. 2. Example of wormhole attack with two adversaries [2]

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.

C. 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 [9]. 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.

D. 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 [2]. Grayhole attack also exhibits random behavior [9] 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.

E. Sinkhole attack

This is the most dangerous and intelligent form of the wormhole attack. In this attack malicious nodes collect the data and use it and after that it modifies the data and then replays it in the sensor network [2]. In Sinkhole attack sometimes 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 in both 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 [12]. 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 and 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 I. Existing Detection and Prevention Methods [2][6][7][8][9][10]

Method [Year]	Requirements/Commentary
Geographic and temporal leashes [2003]	GPS coordination of every node; Loosely synchronized clocks (ms); Robust, straightforward solution; Inheritance of general limitations of GPS technology
Packet leashes, end-to-end [2003]	GPS coordination of every node; Loosely synchronized clocks (ms); Inheritance of limitations of GPS technology
Network visualization [2004]	Centralized Controller; Works best on dense networks; Mobility is not studied; Varied terrains are not studied
Localization [2004]	Location-aware; use of ‘guard’ Nodes; Not readily applicable to mobile networks

IJERT

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

Method [Year]	Requirements/Commentary
LISP [2004]	Applicable only to static stationary networks; Impractical
Directional antennas [2004]	Directional antennas on all nodes; Good solutions for networks relying on directional antennas, but not directly applicable to other networks
Time of flight [2004]	Hardware enabling one-bit message and immediate replies without CPU involvement; Impractical; Likely to require MAC-layer Modifications
Statistical analysis [2005]	This method works only with multi-path on-demand protocols
LITEWORP [2005]	Static topology for network; Pre-distribution pair-wise key management protocol; not applicable for protocol deviation mode
Connectivity-based Approaches [2006]	Require connectivity information; Tightly synchronized clocks (ns); Impractical
End-to-end mechanism [2006]	Requires knowledge of location information; Loosely synchronized clocks; This mechanism uses geographic information and authentication method to detect malicious neighbors
True-link [2006]	Authentication mechanism; Time-based mechanism; Works only with standard IEEE 802.11 hardware with a minor backwards compatible firmware update
TTM [2007]	Cooperation of all nodes in the path; Transmission time-based mechanism
Radio fingerprinting [2007]	Require fingerprinting device; Chipcon 1000, 433 MHz radio was used
Connectivity graph [2007]	Connectivity information is required; To be independent to wireless communication models
TTBM [2008]	Time- and trust-based mechanism
MOBIWORP [2008]	Loosely synchronized clocks (ms); maximum limit on the number of nodes that an attacker can capture
Secure neighbor discovery [2008]	Secure neighbor discovery
GTA [2008]	Suitable for proactive protocols; Adjacency matrix of network and graph-based mechanism; impractical
Neighbor verification Protocol [2009]	Local geometric consistency tests; Secure neighbor discovery
CSB [2009]	No packet loss in the System; Conflicting-set-based resistant localization system
Secure localization [2010]	Conflicting-set-based resistant localization
RTT-TC [2010]	Based on RTT and topological comparison
Local connectivity information [2011]	Centralized and distributed algorithm, 100% detection and 0% false alarm probabilities using proper parameter
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%.
E2SIW [2012]	High detection rate, less overhead, and can consume less energy in less time, compared to the De Worm
Worm Planar [2013]	Graph theoretical method, exploits location free network planarization technique to perform connectivity-based wormhole detection.
TPN model[2013]	Analytical results show that the secured version of CL-MAC can effectively detect and avoid wormhole attack
DAWN [2014]	Exploring the change of the flow directions of the innovative packets; good lower bound of successful detection rate

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 [12]. 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.

Acknowledgment

We would like to thank authors, Majid Meghdadi, Suat Ozdemir and Inan Güler for their great research which inspired us to study in depth. We would also like to thank department of computer engineering AISSMS COE, Pune for their great support.

IJERT

References

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

[2] Majid Meghdadi, Suat Ozdemir and Inan Güler, "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," 12th IEEE International 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] Shiyu Ji, 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] Meenakshi Tripathi, 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), Procedia Computer Science 19 (2013), pp.1101 – 1107.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

[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] Pushpendra Niranjan, 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] Zaw Tun and Aung Htein Maw, “Wormhole Attack Detection in Wireless Sensor Networks,” World Academy of Science, Engineering and Technology 46, 2008.

[13] Robert G. Rittenhouse4 Junaid Ahsenali 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.

IJERT

(This work is licensed under a Creative Commons Attribution 4.0 International License.)