International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue:2 March-April 2017 p-ISSN: 2394-8280

IMPACT OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORKS: A SURVEY

Vikram Labana[1], Ankur Panot[2]
Research Scholar, Department of Computer Sc. & Engineering
vikramvicky58@gmail.com
Asst. Professor, Department of Computer Sc. & Engineering
ankur.panot@sait.ac.in

ABSTRACT: ***Wireless networks are playing important role for development and ease of use of human society. It also gets a lot of attention from research community towards the betterment of applications. A wide range of applications make it very popular and backbone of technology system i.e. GSM, Bluetooth, Wi-Fi etc. In order to categorization of applications, sensor networks give a unique range for monitoring and surveillance. WSNs may be ad-hoc is fixed natured use to deploy into remote areas for sensing and processing desire information.Due to distributed and open natured of wireless sensor networks, it is vulnerable and prone for attacked to intercept and hijack network communication. Its deployment in remote areas requires more concern of security issues. Open natured communication is a magnet for attacker to intercept and catch the sensed information. Numerous security threats can adversely affect its functioning & degrade network performance. The problem becomes more critical when it deploy for defense mission.***

Arbitrary network failure or node failure is the natural phenomena and may vary as per real life deployment, but intentional failure or compromising network may lead to leak the information. A various security threats like Work-hole attack, Black-hole Attack, Gray-hole attack, Sybil Attack etc. are used for packet dropping, capturing and degrading network performance. Security in sensor networks is a challenging task. Furthermore, low profile resources and security overhead create cumbersome situation for detection and prevention mechanism.The complete study observes that, security threats not only capture the packets but also degrade network performance. To overcome vulnerability problems, work considers wormhole attack as study target and will derive mechanism to identify and prevent sensor networks from security threat. A wormhole attack is very popular and applies on network layer by targeting vulnerabilities of routing protocols. The complete works consider Ad-hoc On Demand Routing protocol and identify several vulnerabilities.So far, very little research has been done in the development of secure routing protocols. The work investigate that attacker may deploy a high power transmission node to attract all neighboring node as shortest path. Such kind of attempt is known as high power transmission node wormhole attack. By the investigating transmission power work will investigate the wormhole attack. Work will also integrate security policy and algorithms into AODV routing protocol. The new secure routing protocol will be known as modified AODV. It will improve the throughput and packet delivery ratio and also reduce the energy consumption and improve the routing performance during security attack. At last work will compare the results between traditional AODV and proposed secure modified AODV.

International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue:2 March-April 2017 p-ISSN: 2394-8280

Keywords: Wireless Sensor Networks, Wormhole Attack, AODV

1. INTRODUCTION

A sensor network is a collection of functional transducers with a communications framework planned to supervise and record conditions at miscellaneous locations. Commonly supervised specifications are humidity, pressure, temperature, wind speed and its direction, intensity of vibration, pollutant levels and fundamental body functions. A sensor network contains many detection stations called sensor nodes, each of which is compact, portable and lightweight. Every sensor node integrates one or more sensors, a tiny microprocessor, a radio transceiver and a set of transducers, along with a small power source. The transducer accomplishes electrical signals on the basis of interpreted physical effects and phenomena developed. The microcomputer performs processing on the information and deposits the sensor output. The transceiver, which can be hard-wired or wireless, accepts the commands from a central computer and transports data to that computer. The power for each sensor node is put together from the electric function or from a battery. Major applications of sensor networks consist in the field of Automated and smart homes, Video surveillance, Traffic monitoring, Industrial automation etc… Sensor nodes are often deployed into hostile environment, where sensors are open and unprotected from physical attacks. Afterwards, there may be possibility of compromising the trusted nodes by adversary. Attack can occur from any direction on any node in a sensor network. It raises the need to implement a security policy into a WSN and, therefore security becomes the major cause.

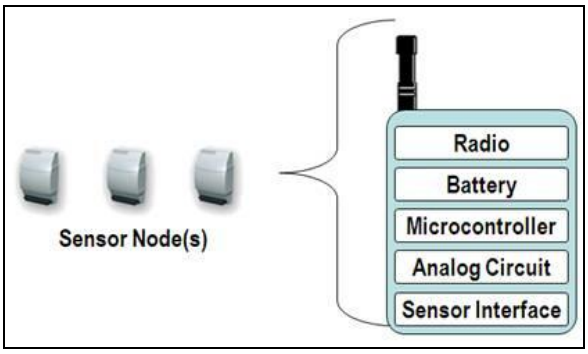

Figure 1: Sensor Node

Wireless Sensor Network (WSN) designates to an organization of spatially scattered and consecrate sensors for observing and recording the substantial conditions of the environment and coordinates the collected data at an intermediate location. WSNs calculate environmental conditions like sound, temperature, humidity, pollution levels, pressure, wind direction and speed, etc…WSNs were antecedently designed to promote military tasks but its application has since been expanded to the areas of health, traffic, and many other industrial and consumer product areas. A WSN may consist of few hundreds to thousands of sensor nodes. The sensor node accessory includes a microcontroller, a radio receiver by the side of antenna, an energy source, an electronic circuit, and a battery. The proportion of the sensor nodes can also vary from the dimension of a shoe box to as minute as the dimension of a fragment of dust. As such, their prices also range from a few rupees to hundreds of dollars

depending upon the objective of a sensor like energy utilization, bandwidth, memory and computational speed rate.

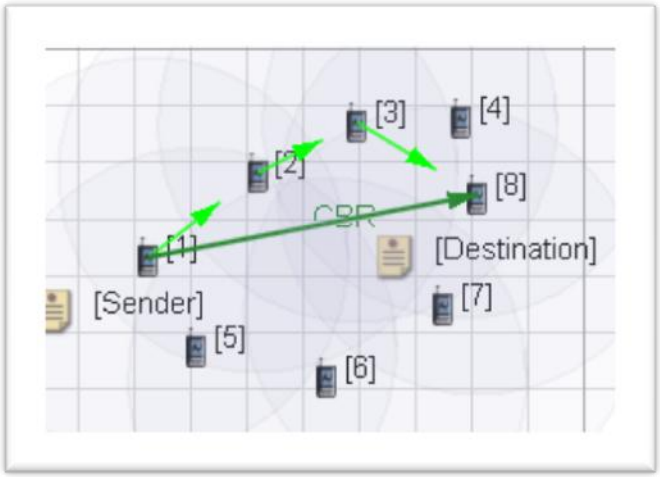

Figure 2: Wireless Sensor Network (WSN)

2. AODV

It is propagation technique which is using in routing or flooding between the hops of the network. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network The AODV Routing Protocol uses an on-demand approach for finding routes between source and destination nodes that is established by a source node for transmitting data packets only when it is required. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the WSNs.

In the AODV routing protocol, the source node broadcasts the RouteRequest packet (RREQ) in the network for establishing a route to the desired destination. It may obtain multiple routes to different destinations from a single RouteRequest. it uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination. A node updates its path information only if the DestSeqNum of the current packet received is greater or equal than the last DestSeqNum stored at the node with smaller hop count.

DestSeqNum indicates the current route that is accepted by the source. When an intermediate node receives a RouteRequest, it either prepares a RouteReply if it has a valid route to the destination or forwards it. The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the RouteRequest packet. All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send RouteReply packets to the source.

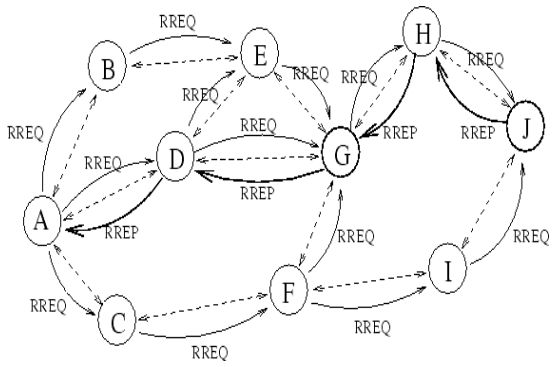

Figure 1.3: AODV message passing

In addition to traditional security issues like secure routing and secure data aggregation, security mechanisms deployed in WSNs also should involve collaborations among the nodes due to the decentralized nature of the networks and absence of any infrastructure. In real-world WSNs, the nodes cannot be assumed to be trustworthy apriority.

3. WORMHOLE ATTACK

A Wormhole attack is used to compromise the network by capturing or introducing better communication node then existing sensor nodes to degrade the performance. There are five methods to apply wormhole attack on AODV. The attacker uses high power transmission node or high bandwidth tunnel to create illusion of shortest path among nodes. Attacker uses these quality techniques to promote itself for route discovery or data packet communication.

A typical wormhole attack requires two or more attackers (malicious nodes) having better communication capability and resources than other sensor nodes. The attacker creates a low-latency link (high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighboring sensor nodes take up this tunnel for their communication. The strange factor is, all data packet moves from this tunnel and attacker may collect or drop data packet respectively.

3.1Wormhole Using Encapsulation

In encapsulation-based wormhole attacks, numerous nodes survive amid two malicious nodes and the data packets are encapsulated among the malicious nodes. Since encapsulated data packets are sent amid the malicious nodes, the definite hop count need not augment during the traversal. Therefore, routing protocols which use hop count for lane selection are chiefly vulnerable to encapsulation-based wormhole attacks.

3.2 Wormhole Using High-quality/Out-of-band Channel

In this mode, the wormhole attack is launched by having a high-quality, single-hop, out-of-band link (called tunnel) between the malicious nodes. This tunnel can be achieved, for instance, by using a straight wired link. This form of attack is harder to start on than the packet encapsulation method since it requests specialized hardware potential.

33 Wormhole Using High-power Transmission

In this kind of wormhole attack, simply one malicious node by means of high-power broadcast ability exists in the network and this node can correspond with other usual nodes

from an elongated space. When a malicious node receives an RREQ, it sends (broadcasts) the request at a elevated power level. Any node that receives the high-power broadcast rebroadcasts the RREQ towards the destination. By this method, the malicious node increases its probability to be in the routes recognized between the source and the objective even exclusive of the involvement of an additional malicious node. This attack can be mitigated if each sensor node is able to precisely measure the received signal strength.

3.4 Wormhole Using Protocol Distortion.

In this form of wormhole attack, a single malicious node tries to draw network traffic by distorting the routing protocol. Routing protocols that depend on the 'shortest delay' instead of the 'smallest hop count' is at the danger of wormhole attacks by means of protocol buckle.

3.5 Wormhole Using Packet Relay

Packet-relay-based wormhole attacks can be done by one or more malevolent nodes. In this attack type, a malicious node relays data packets of two distant sensor nodes to convince them that they are neighbors. This kind of attack is also called “replay-based attack” in the literature.

4. PROBLEM DOMAIN

Although, energy utilization and resource consumption are major problems with WSN, but security also becomes a key prerequisite for modern age applications. Weak security or absence of security may not only conciliate classified information but also makes them accessible for malicious attacks. In the WSNs, several anomalies can occur due to their lack of processing and communicating capability, limited storage capacity, range, bandwidth and energy. These networks are usually deployed in remote area and left unattended; they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc. Unfortunately, traditional security mechanisms with high overhead are not feasible for resource constrained sensor nodes.

One of the major issues with wireless sensor networks is to uphold confidentiality. A wireless sensor network should not leak out any of its credential even when sensors are read by their neighbor nodes. They use encryption algorithms for privacy conservation. Encryption mechanisms are very awkward in nature as they generate security overhead and enlarge packet size for that reason. They also increase energy utilization due to encryption and decryption procedures and network traffic. Finally, work concludes that, there is a necessity to find out different vibrant featured confidentiality approach based on network traffic condition and security level of current event and intermediate node for different applications.

The major security issue with wireless sensor network is insecure routing. Even though, a large amount of work has been done in this area but all the proposed techniques are based on stationary strategies. They do not consist of current network traffic, security factor of midway nodes and selected route. Further, the susceptibility of routing process gives opening to attackers for compromising sensor nodes or intermediate messages to misguide routing process or bring network into endless state. One of the major draw backs of insecure

routing is increased routing time, unnecessary energy utilization, resource consumption and restricted access conditions during communication.

Wireless Sensor Networks are vulnerable to various types of attacks. These attacks are mainly: Attacks on secrecy and authentication (outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets), Attacks on network availability (attacks on availability of WSN are often referred to as denial-of-service (DoS) attacks), Stealthy attack against service integrity (the goal of the attacker is to make the network accept a false data value).

Once a node is captured by an attacker, attacker collects all the credentials such as keys and identity etc. The attacker can re-program it and replicate the node in order to eavesdrop the transmitted messages or compromise the functionality of the network. Identity attackers lead to two types attack: clone and Sybil. In particularly a harmful attack against sensor networks where one or more node(s) illegitimately claims an identity as replicas is known as the Node Replication attack. The replication attack can be exceedingly injurious to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, etc.

Different kinds of holes can form in such network creating geographically correlated problem area such as coverage holes, routing holes, jamming holes, sink/black holes and worm holes, etc.

5. CONLUSION

The study of complete works concludes that wormhole attack is one of the severe security threats which not only compromised the information privacy but can also be able to fabricate the information. The bigger challenge with this attack is degradation of performance of network due to security threat. Continuous dropping of packet may also affect the Quality of service in WSN. The complete works end with the conclusion that there is strong need of mechanism which should be able to detect and prevent wormhole attack.

REFERENCES

[1] Gowrishankar.S , T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, "*Issues in Wireless sensor networks*" Proceedings of the World Congress on Engineering vol I, 2008.

[2] Pathan,A.S.K., Lee,H.W., Hong, C.S. "*Security in Wireless Sensor Networks: Issues and Challenges* " ICACT ISBN 89-5519-129-4, pp 1043-1048, 2006.

[3] Jaydip Sen "*A Survey on Wireless Sensor Networks Security*" In International Journal of Communication Networks and Information Security (IJCNIS) Vol.1, No. 2, August 2009, pp 55-74,

[4] Sangwan,A., Sindhu,D., Singh, K., "*A Review of various security protocols in Wireless Sensor Network*", IJCTA, ISSN:2229-6093, vol. 2 (4), july-august-2011, pp.790-797.

[5] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, Xiangke Liao "*Topological Detection on Wormhole in Wireless Ad Hoc and Sensor Networks*", IEEE/ACM Transaction on Networking, vol. 19, No. 6 December 2011, pp.1787-1796.

[6] Miss Morli Panday,Ashish Kr. Shriwastava, "*A Review on security Issues of AODV routing protocol for MANETs*", IOSR Journal of Computer Engineering(IOSR-JCE), e-ISSN:2278-0661, p-ISSN:2278-8727 vol. 14, Issue 5 (Sep. - Oct. 2013), pp.127-134.

[7] R.balakrishna, U.Rajeshwar Rao, N. Geetahanjali, "*Performance issues on AODV And AOMDV for MANETs*", International journal of Computer Science and Information (IJCSIT), vol. 1 (2), 2010,pp. 38-43.

[8] Babu, Sriramoju Ajay, and Namavaram Vijay. "Image Tag Ranking for Efficient Matching and Retrieval." (2016).

[9] Babu, Sriramoju Ajay, and Namavaram Vijay. "Design and Implementation of a Framework for Image Search Reranking." (2016).

[10] Babu, Sriramoju Ajay, and S. Shoban Babu. "International Journal of Research and Applications Jan-Mar© 2016 Transactions 3 (9): 422-426 eISSN: 2349–0020."

[11] Bhoyar, Mayur R., Suraj Chavhan, and Vaidehi Jaiswal. "Secure method of updating digital notice board through SMS with PC monitoring system." IOSR Journal of Computer Science (IOSRJCE), e-ISSN (2014): 2278-0661.

[12] Bhoyar, Mayur Ramkrushna. "Home automation system via internet using Android phone." InternationalJournal of Research in Science and Engineering. CSE Department, JDIET, Yavatmal: 6.

[13] Haridass, R., et al. "PERFORMANCE IMPROVEMENT OF POLLUTION CONTROL DEVICE USED IN SMALL SCALE FOUNDRY INDUSTRY." PERFORMANCE IMPROVEMENT 3.1 (2017).

[14] Bhoyar, Mayur Ramkrushna. "Home automation system via internet using Android phone." InternationalJournal of Research in Science and Engineering. CSE Department, JDIET, Yavatmal: 6.

[15] Maulana, Bagoes, and Robbi Rahim. "GO-BACK-N ARQ APPROACH FOR IDENTIFICATION AND REPAIRING FRAME IN TRANSMISSION DATA."

[16] Nofriansyah, Dicky, and Robbi Rahim. "COMBINATION OF PIXEL VALUE DIFFERENCING ALGORITHM WITH CAESAR ALGORITHM FOR STEGANOGRAPHY."