International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 2 (2014), pp. 173-182

http://www. irphouse.com /ijict.htm

Systematic Analysis of DoS Attacks in Wireless Sensor Networks with Wormhole Injection

Najma Farooq[1], Irwa Zahoor[2], Sandip Mandal[3] and Taabish Gulzar[4]

[1]Department Of Computer Science And Technology,Dehradun Institute of Technology, Mussourie Diversion Road Makkawala ,Dehradun, INDIA.
[2,3]Department Of Computer Science And Technology,Dehradun Institute of Technology, Mussourie Diversion Road Makkawala, Dehradun, INDIA.
[4]Department of Electronics and communication, Dehradun Institute of Technology, Mussourie Diversion Road Makkawala, Dehradun, INDIA.

Abstract

The Wireless Sensor Networks (WSNs) are emerging as one of the most reliable technologies for implementing ubiquitous computing ultimately leading to an all-pervasive paradigm of computing infrastructure that can be utilized for several interesting applications. There are number of attacks on wireless sensor networks like black hole attack, wormhole attack, sink hole attack, Sybil attack, selective forwarding attacks etc. In this paper, we assess the security issues of wireless sensor networks with respect to medical applications and find out the possibility of a scenario when a distributed denial of service (DDoS) attack may be injected in the system using wormhole attack. We also propose schemes for detecting such attacks and also provide solution for its mitigation.

Keywords: WSN, DDoS, Wormhole Attack, Detection techniques.

1. Introduction

Wireless Sensor Network have become interesting and promising area of research and development ,we can define wireless sensor network as a self-configuring network of small sensor nodes which communicate with each other via radio signals and deployed in quantity to sense, monitor and understand the physical world .WSN combines sensing, computation and communication in a single device called sensor node. Wireless sensor nodes are also called motes. Sensor nodes have capability to collect

sensed data and send that to the base station, a WSN generally consist of a base station that can communicate with a number of wireless sensors via radio link. WSN uses a wireless channel to communicate, so there are inevitably some issues such as message interception, tampering and other security [1]. Therefore, the security of networks has an important impact on the performance of monitoring, system availability, accuracy, and scalability, etc. The security of wireless sensor networks is an area that has been researched considerably over the past few years. The conventional security measures are not suitable to this wireless sensor networks due to resource constraints of both energy and memory. However, they are also highly susceptible to attacks, due to the open and distributed nature of the networks and the limited resources of the nodes. An adversary can compromise a sensor node, alter the integrity of the data, eavesdrop on messages, inject fake messages, and waste network resources. A common attack in WSN is DoS attack, and the objective of the attacker in DoS attack is to make target nodes inaccessible by [2] legitimate users. Many different kinds of DoS attacks against wireless sensor networks have been identified so far, e.g. selective forwarding attack, sinkhole attack, wormhole attack, black hole attack and hello flood attack, etc.

In this paper we will focus on wormhole attacks. The wormhole attack is a severe threat against packet routing in sensor networks that is particularly challenging to detect and prevent. In this attack, an adversary receives packets at one location in the network and tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network. An instance of a wormhole attack would involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel (defined by the wormhole Start Point and the End Point) available only to the attacker. Thus a false route would be established which would shorten the hop distance between any two non-malicious nodes. Wormhole attacks can cause Denial-of-Service through Data Traffic, Denial-of-Service through Routing Disruptions and Unauthorized Access. In Denial-of-Service through Data Traffic, the malicious node(s) can insinuate itself in a route and then drop data packets. Denial-of-Service through Routing Disruptions can prevent discovery of legitimate routes and Unauthorized Access could allow access to wireless control system that are based on physical proximity, e.g. wireless car keys.

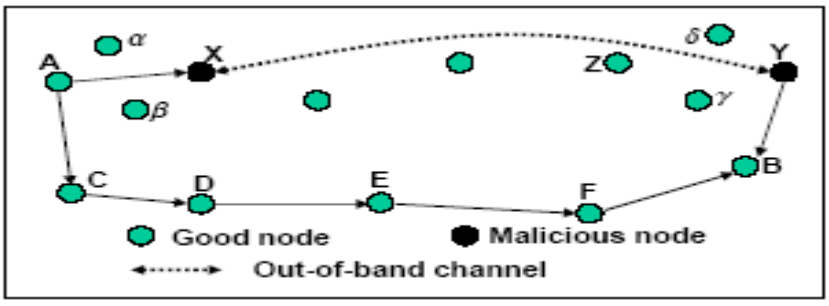

Fig. 1: Representing a Wormhole tunnel between nodes, X and Y of a Sensor Network.

The focus of this paper is to determine the impact that wormholes can have on node localization for isotropic wireless sensor networks where only a limited fraction of nodes have self-positioning capability and the node positions have been determined using the "DV-hop" propagation method. But before that, it is necessary that we have a look at most common types of DoS attacks and their defence mechanisms such that we may be better able to appreciate the novel approach that has been taken by the authors.

2. Types of Dos Attacks

Denial of Service attack defined as any event that diminishes or eliminates a network's capacity to perform its expected function [6], degrades network's intended service to its users, thus is considered one of the most general and dangerous attacks endangering network security.

2.1 Jamming

A malicious node may be able to set its radio to transmit continuously, or very frequently, such that it jams the radio receivers on its neighboring nodes. Since the neighboring nodes cannot receive intelligible messages, they will be unable to receive broadcasts

Defense- The most common defense against jamming attacks is the use of *spread-spectrum* communication [7]. In frequency hopping, a device transmits a signal on a frequency for a short period of time, changes to a different frequency and repeats. The transmitter and receiver must be coordinated. Direct-sequence spreads the signal over a wide band, using a pseudo-random bit stream. A receiver must know the spreading code to distinguish the signal from noise**.**

2.2 Exhaustion

Repeated collisions can also be used by an attacker to cause resource exhaustion. One solution to it could be the use of time division multiplexing. Another possible solution is to apply rate limits to the MAC admission control.

Defense- is to *rate-limit* response to even properly authenticated nodes. Excessive requests will be queued or ignored without sending expensive radio transmissions. The rate must be high enough to provide sufficient bandwidth and timeliness for authorized users.

2.3 Selective Forwarding Attacks

In selective forwarding attack a malicious node may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further [10]. A [11] special form of this attack known as black hole attack**.**

Defense-Two different countermeasures have been proposed against selective forwarding attack. One defence is to send data using multi path routing. Another one is detection of compromised nodes which are misbehaving in terms of selective forwarding and route. The data seeking an alternative path.

2.4 Sinkhole

In sinkhole attacks, adversary attracts the traffic to a compromised node. The simplest way of creating sinkhole is to place a malicious node where it can attract most of the traffic, possibly closer to the base station or malicious node itself deceiving as a base station. One reason for sinkhole attacks is to make selective forwarding possible to attract the traffic towards a compromised node. The nature of sensor networks where all the traffic flows towards one base station makes this type of attacks more susceptible [12].

Defense - is not as easy to attract routing to an One approach to avoiding sinkholes is to use routing algorithms that are ***resistant*** to arbitrary configurations, such as geographic forwarding [13][14]. Since each node makes an independent forwarding decision based on the location of its neighbors, it attacker.

2.5 Wormhole attack

An adversary can tunnel messages received in one part of the network over a low latency link and replay them in another part of the network. The simplest [15] instance of this attack is a single node situated between two other nodes forwarding messages between the two of them.

Defense- based on ***packet leashes***, where the distance that a message may travel in a single hop is limited [16]. Each message includes a timestamp and the location of the sender. The receiver compares these with its own location and time to determine if the maximum transmission range has been exceeded. The solution requires clock synchronization and accurate location verification, which may limit its applicability to WSNs.

2.6 Flooding

Attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored

Defense -is to require the clients of services to commit significant resources before connections are established. ***Client puzzles*** are one such method, whereby servers dispense cryptographic puzzles that must be solved by brute-force before connection-related resources on the server are allocated [17] [18]. The difficulty of the puzzles is scalable, so the server can increase the requirements when it believes it is under attack. In a WSN, this could adversely affect the many legitimate sensor devices, each of which has limited resources to commit.

2.7 Proposed Detection Schemes in Literature

B.Yu [6] proposes a method to detect forwarding attacks based on checkpoints. Firstly choosing some nodes along the path randomly as the checkpoints node, then after receiving data packets, there will generate corresponding acknowledgments and then transmit them to the upper way. If any checkpoints node doesn’t get enough acknowledgments, it will generate warning messages to the source node, so that the detection of the selective forwarding attacks can be realized. But an apparent problem

exists in this process is that the nodes have to send acknowledgments continuously, which will greatly increase the cost of the network. By the way, this method can't judge whether there malicious tamper action exists.

Jiang [19] proposes a method to detect selective forwarding attacks, which is based on the level of trust and packet loss. After networking topology being established, when sensing data is transmitted on the path, the intermediate nodes detect and count the number of the packets they receive and send, and report the statistical results to the BS; According to these data, the BS calculates the trust level of nodes and evaluate the packet loss, so that it can determine whether this node is an active attacking node

Yu and Xiao in [20], proposed a scheme which uses a multi-hop acknowledgment scheme to launch alarms by obtaining responses from intermediate nodes. Each node in the forwarding path is incharge of detecting malicious nodes. If an intermediate node detects a node as malicious in its downstream/upstream, then it will send an alarm packet to the source node/base station through multi-hops

Sophia Kaplantzis et al [21] proposed a centralized intrusion detection scheme that uses only two features to detect selective forwarding and black hole based on Support Vector Machines (SVMs) and sliding windows. This intrusion detection is performed in the base station and hence the sensor nodes use no energy to support this added security feature. From this they conclude that the system can detect black hole attacks and selective forwarding attacks with high accuracy without depleting the nodes of their energy.

Brown and Xiaojiang [22] have proposed a scheme to detect selective forwarding using a Heterogeneous Sensor Network (HSN) model. The HSN consists of powerful high-end sensors (H-sensors) and large number of low-end sensors (L sensors). After deploying sensors, a cluster formation takes place with H-sensor as cluster head.

Xin, etal. Proposed [23] a light weight defense scheme against selective forwarding attack which uses neighbour nodes as monitor nodes. The neighbour nodes (monitoring nodes) monitor the transmission of packet drops and resend the dropped packets. They used a hexagonal WSN mesh topology.

Zurina Mohd Hanapi et al [24] proposed the dynamic window stateless routing protocol DWSIGF that is resilience to black hole, wormhole and selective forwarding attack caused by the CTS rushing attack. Even without inserting any security mechanism inside the routing protocol, the dynamic window secured implicit geographic forwarding (DWSIGF) still promise a good defense against black hole attack with good network performance.

Deng-yin ZHANG et.al [26] et.al proposed a method to detect selective forwarding attacks ba*sed* on digital watermarking technology. This method embeds watermark into the source data packets, which will be extracted at the base station (BS). The BS will judge whether there are malicious nodes in the transmission path by analyzing the packet loss rate from received data. Simulation results show that this method can effectively detect whether malicious nodes have discarded or tampered the contents of the packets.

3. DV-HOP Propagation Method

This scheme envisages determining the position of any node with respect to at least three nodes called *landmarks.* These landmark nodes are either GPS enhanced, or know their position by some other means and are present in the WSN grid. Thus, the landmark nodes supply a convenient anchor or referencing point in the grid.

This is the most basic scheme, and it comprises of three non-overlapping stages. First, it employs a classical distance vector exchange so that all nodes in the network get distances, in hops, to the landmarks. Each node maintains a table {*Xi, Yi, hi*} and exchanges updates only with its neighbors. In the second stage, a landmark, after it cumulates distances to other landmarks, it estimates an average size for one hop, which is then deployed as a correction to the nodes in its neighborhood. When receiving the correction, an arbitrary node may then have estimate distances to landmarks, in meters, which can be used to perform the triangulation, which constitutes the third phase of the method. The correction a landmark *(Xi, Yi)* computes is

$$c_i = \frac{\sum \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2}}{\sum h_i}, \quad i \neq j, \text{ all landmarks } j. \tag{1}$$

A regular node gets an update from one of the landmarks, and it is usually the closest one, depending on the deployment policy and the time the correction phase of APS starts at each landmark. Corrections are distributed by controlled flooding, meaning that once a node gets and forwards a correction, it will drop all the subsequent ones. This policy ensures that most nodes will receive only one correction, from the closest landmark. When networks are large, a method to reduce signaling would be to set a TTL field for propagation packets, which would limit the number of landmarks acquired by a node. Here, controlled flooding helps keeping the corrections localized in the neighborhood of the landmarks they were generated from, thus accounting for non-isotropies across the network. These correction factor values are then plugged into the triangulation procedure for a node to get an estimate position.

In DV-Hop based positioning, wormhole impacts would include incorrect calculation of the hop length between a landmark and a non-landmark node. Consequently, this would result in an incorrect calculation of the hop distance of a node from the landmark nodes, which in turn, would affect position accuracy of the nodes.

4. Proposed Detection Scheme

DDoS attacks can be detected by analyzing affected or degraded services as DDoS attacks are transmitted across the internet and directed towards the victim, but to launch a defense measurement against a DDoS attack near the victim is not a smart idea because the resources are already under heavy load and the victim cannot properly respond those measures. Therefore it is recommended to stop the attacks near the attack sources which are also helpful to save network resources and can reduce the congestion. However, DDoS attacks can’t be fully detected and filtered near the source.

The question is now, what is the ideal place to deploy the defense system against DDoS attack? A best solution for this is at the intermediate network. At this middle part of the propagation stream, we assume that DDoS attacks create more aggregation than the normal flow and consume more bandwidth as the attacks come more and more close to victim. However this congestion causes less congestion, making it hard to detect the attacks in single domain, therefore introducing shared information over several domains makes it possible to detect the DDoS attacks earlier.

There are two main stages in the proposed detection scheme. During first stage, each local node identifies the traffic anomalies using profile of normal traffic which is constructed using stream sampling algorithm.The next phase, we can improve the accuracy of detection of media by using gossip based multicast based on sharing information among different nodes. To improve the safety and reliability, our system is based on an overlay network which consists of local nodes such as routers with a DDoS attack detection and packet filtering function. An overlay network is a virtual network using the existing network. It consists of routers, and tunnels. Tunnels are paths in a database of network information and links on the top line. Each of the components, that are routers, can participate in more than one overlay at a time, or one of the coverage in several ways. As a result, it is a natural form of the network and can be an overlay network link. Multiple links can increase the flexibility of the network, and the more flexible the network is probably less vulnerable to attack.

Moreover, by building a comprehensive, self-organization and resilience overlay networks over the Internet, peer nodes in an overlay network can provide information about the attack in a fast and reliable way. Individual nodes are discovered at the exit routers and work as a separate system to collect all relevant information and identifying local DDoS attacks. The system then uses the overlay network to share information obtained from the detection by the use of gossip protocols based on epidemic algorithms over the Internet.

Internal node detection can be very complicated, but can be determined by checking on local traffic. Measuring the movement of local traffic is achieved by traffic measurement module. Further, this local identification mechanism uses this information to identify the local anomalies. On the same way, the information about the anomalies of the neighboring nodes is gathered and will be sent to the cooperative anomaly detection module, which makes use of global message diffusion module. Finally, the response units of any local module are informed about the actions to be taken to protect against the attacks.In our opinion, aggress routers are key elements necessary to identify the attack, and to provide the necessary information to respond these attacks, therefore these key routers have to coordinate with each other to carry out this task. This mechanism can improve the accuracy and speed of detection of DDoS attacks. The operations on these agress routers are described below:

- On the detection of an abnormality, each local node shares this information to its neighboring through gossip. If every node reports similar information, DDoS attack detection is declared after sharing this information with all nodes over the network.

- This information is compared with the local timestamp and discards the expired message after evaluating them with time stamp.
- On the confirmation of a DDoS attack, an effective counter defense is deployed to prevent the consequences of the attack.

We can make a combination of our proposed approach with justifying or rate limit technologies to get rid of anomalies before their execution. The curve below shows the performance of our algorithm (brown) compared to traditional techniques (blue)

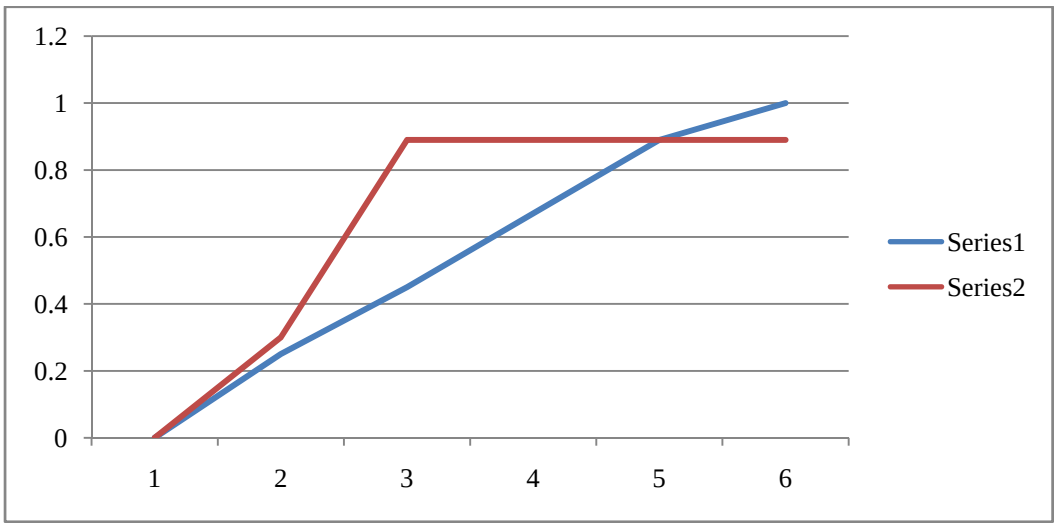

Fig. 2: Comparing performance of proposed technique with traditional ones.

5. Conclusion

Security and timely transmission of packets in wireless sensor network is its basic need of the network. The attack which affect this is the wormhole attack as in this attack malicious node drops the packet and make it unavailable to the destination. The detection of this type of attacks is important to meet the basic need of the network. Here is this paper we discuss few Dos attacks in wireless sensor networks and how they affecting the network and defense against them and we list up some detection techniques, which would help the user to know the techniques which have been proposed in recent year and in what way new techniques can be designed. Our new detection scheme at the intermediate result shows much promise as well. This analysis will help us to know the previous proposed schemes and will also be helpful to design new one in the future.

References

[1] Yuling Li, Feng Liu, and Luwei Ding “Research about Security Mechanism in Wireless Sensor Network” IEEE.

[2] Fengyun Li, Guiran Chang and Fuxiang Gao, Lan Yao" A Novel Cooperation Mechanism to Enforce Security in Wireless Sensor Networks" 2011 Fifth International Conference on Genetic and Evolutionary Computing. IEEE computer society .

[3] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. "Lightweight defense scheme against selective forwarding attacks in wireless sensor networks" pages 226 –232, oct. 2009.

[4] C. Intanagonwirat, R. Govindan and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in 6th Annual Conf. on Mobile Computing and Networking, Aug. 2000, pp. 56-67.

[5] B. Karp and H. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in 6th Annual Conf. on Mobile Computing and Networking, Aug. 2000, pp. 243-254.

[6] B Yu, B Xiao. "Detecting selective forwarding attacks in wireless sensor networks". In: Proe. of the 20th International Parallel and Distributed Processing Symposium, RhodesIsland, Greeee, 2006,1218 1230

[7] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein. Theory of spread spectrum communications.a tutorial. *IEEE Transactions on Communications*,20(5):855.884May1982.

[8] Ross Anderson,Markus Khun "Tamper resistance . a cautionary note." In proceedings of 2nd USENIX Workshop on Electronic Commerce, Pages 1.11,Oakland,california,Nov. 1996

[9] David r.raymond and scott f.midkiff "Denial of service in wireless sensor nerworks: attacks and defences" published by IEEEcs temparing

[10] Prabhudutta mohanty , sangram panigrahi,nityananda sarma and sidhartha sanker satapathy "Security issues in wireless sensor networks data gathering protocols : a survey" journal of theoretical and applied information technology.

[11] Jihan rehana "Security of wireless sensor networks" TKKT -110.5190 Seminar on inter networking.

[12] Ritu Sharma, Yogish chaba,Yudhvir singh "Analysis of security protocols in wireless sensor networks" Int j Advance networking and applications volume :02 , issues:03

[13] G.G. Finn. Routing and addressing problems in large metropolitian-scale internetworks.Technical report ISI/RR-87-180, ISI, March 1987

[14] Chris Karlof and David Wanger. Secure Routing in wireless sensor networks : attacks and countermeasures .In First IEEE InternationalWorkshop on Sensor Network Protocols and Applications, 2003.

[15] Anthony d.wood , john a.stankovic "denial of service in sensor networks" 2002 IEEE.

[16] Yih-Chun Hu,Adrian Perrig and David B.johnson. Packet leashes: A defense aginst wormhole attacks in wireless networks. In Proceedings of IEEE Infocom 2003, April 2003.

[17] Ari Juels and John Brainard. Client puzzles : A cryptographic defence aginst connection depletion attacks.In S.Kent,editor,Proceedings of NDSS ’99 (Networks and Distributed Security systems), pages 151.165,1999

[18] Tuomas Aura,Pekka Nikander,and Jussipekka Leiwo. DOS-resistant authentication with client puzzles.*Lecture Notes in Computer Science*, 2133:170.177, 2001.

[19] Jiang changyong, Zhang jianming. “The selective forwarding attacks detection in WSNs”. Computer Engineering, 2009, 35(21):140-143

[20] Bo Yu and Bin Xiao. Detecting selective forwarding attacks in wireless sensor networks. In Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International, page 8 pp., 2006.

[21] Sophia Kaplantzis , Alistair Shilton , Nallasamy Mani , Y. Ahmet S¸ekercio glu ,” Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines”, intelligent sensors, sensor networks and information ,3rd international conference ,pg 335 – 340,ISSNIP 2007 .

[22] Jeremy Brown and Xiaojiang Du. Detection of selective forwarding attacks in heterogeneous sensor networks. In ICC, pages 1583–1587, 2008

[23] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. pages 226 –232, oct. 2009

[24] Zurina Mohd Hanapi, Mahmod Ismail and Kasmiran Jumari, Priority and Random Selection for Dynamic Window Secured Implicit Geographic Routing in Wireless Sensor Network”, American Journal of Engineering and Applied Sciences 2 (2): 494- 500, 2009.

[25] 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, 1447-1472; doi:10.3390/s100301447

[26] Deng-yin ZHANGa, Chao Xub, Lin Siyuan “Detecting Selective Forwarding attacks in WSNs using Watermark.