International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

Recovering from In-Band Wormhole Based Denial of Service in Wireless Sensor Networks

Najma Farooq[Á*], Irwa Zahoor[Á] and Sandip Mandal[Á]

[Á]Department Of Computer Science And Technology ,Dehradun Institute Of Technology, Mussourie Diversion Road, Makkwala Dehradun, India

Accepted 16 May 2014, Available online 01 June 2014, **Vol.4, No.3 (June 2014)**

Abstract

Wireless Sensor Networks (WSN) are composed of a large ,yet limited number of sensing devices called sensors, communicating over a wireless media. Wireless sensor networks find prospective applications in fields like environmental monitoring, healthcare, battlefield surveillance, and homeland security. A much broader spectrum of future applications is likely to follow. Deployment of WSN in hostile environments, unattended operation, openness of communication and resource constraints e.g. limited memory, energy and computational capabilities exposes WSN to a number of security attacks. The resource constrained nature of WSN makes conventional security mechanisms incongruous to apply. In this paper, an In-Band wormhole attack on a wireless sensor network is studied, in which an adversary creates a link between two regions of the network by using colluding network nodes. The impact of an In-Band wormhole attack on data transmission and energy consumption in the network is studied and a reactive recovery mechanism to detect and mitigate the Denial Of Service effect caused due to it is presented.

Keywords: *Wireless Sensor Networks, Wormhole, Denial of Service, Routing Attacks, In-Band Wormhole.*

1. Introduction

Typically Wireless Sensor Networks are formed of large number of multifunctional resource constrained devices with sensing, data processing and data forwarding capabilities. When compared to other wireless networks, for example, cellular systems and Mobile Adhoc networks, sensor networks are matchlessly characterized by certain features like Dense Node Deployment, application Specific nature, unattended operation, Many - to - One Traffic Pattern, data redundancy etc and are resource constrained with low energy, limited memory and computational capabilities. Due to such type of network characteristics, security objectives are hard and challenging to achieve in wireless sensor networks. Such network characteristics make wireless sensor networks susceptible to various types of security attacks which exploit the fundamental security requirements i.e. confidentiality, authenticity and availability.

This paper focuses on denial of service caused due to an In-Band wormhole attack in Wireless Sensor Networks. Wormhole attack is one of the most devastating routing attacks in WSN that is hard to detect and defend (Prasannajit B et.al 2010),(Karlof et.al, 2003). In this attack, a compromised node receives packets at one location of network and tunnels them to another location where the packets are replayed. This attack considerably tribulates a number of network protocols in terms of energy efficiency, routing, localization, service availability etc. The basic stark feature of wormhole attack lies in the fact that the attackers can easily launch an effective attack without understanding the protocols or cryptographic mechanisms used in the network. Based upon the technique which is used to launch the attack, Wormhole attacks can be classified (Khalil et.al 2007) as shown in the figure 1

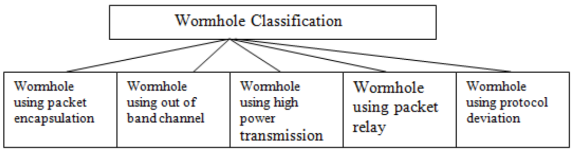
Wormhole Classification
Wormhole using packet encapsulation
Wormhole using out of band channel
Wormhole using high power transmission
Wormhole using packet relay
Wormhole using protocol deviation

Fig 1 shows the classification of wormhole attack based upon the technique used to launch the attack.

1.1 Wormhole using Packet Encapsulation

In encapsulation-based wormhole attack, each packet is routed via the legitimate path only, when received by the wormhole end data packets are encapsulated and forwarded via wormhole link ,The packet is brought into original form by the second wormhole end point

1.2 Wormhole using Out-of-Band Channel

In this attack the wormhole attack is propelled by having a high-quality, single-hop, out-of-band link between the malicious nodes. This type of attack needs specialized hardware capability. When an adversary creates a

*Corresponsing author: **Najma Farooq**

communication link between two end points of a network either by compromised or colluding network nodes, the wormhole is known as the in-band wormhole. Unlike out of band wormhole, the in band wormhole requires no specialised hardware capabilities

1.3 Wormhole using High Power Transmission

In this type of attack, a malicious node with high-power transmission capability replays packets in the network. It communicates with other regular nodes from a long distance. When a malicious node receives a route request it broadcasts the request with high-power level. Any node that receives the high-power broadcast rebroadcasts the route request packet to its neighbours

1.4 Wormhole using Packet Relay

In this type of attack, a mischievous node dispatches data packets of two distant sensor nodes to convince them that they are neighbours.Similar to the previous approach; only one malicious node is needed that replays packets between two far nodes and this way false neighbours are created.

1.5 Wormhole using Protocol Deviation

Routing protocols that are based on the 'shortest delay' instead of the smallest hop count is at the risk of wormhole attacks by using protocol distortion. In this wormhole mode, a malicious node can create a wormhole by not forwarding Route requests without back-off. The purpose is to let the route request packet arrive first at the destination so that the malicious node makes a part of path to the destination (Sharma et.al 2013).

Due to capturing of data from one location of network and broadcasting it to the other, the overall count of sends and receives of the network will be intensificated, leading to a decrease in node energy as energy consumption in WSNs has a direct relationship with number of sends and receives. The depletion in node energy will make data packets immobile, leading to DoS (Denial of Service).

The purpose of this paper is to identify a Wormhole attack that can be injected in a vulnerable network thus measure and verify the DoS and propose a reactive mechanism that could measure it and counter it in case of declining network performance.

2. Related work

Certain criteria to identify and mitigate wormhole attacks have been followed by researchers. Some use approaches like finding dramatic changes in the certain arithmetical patterns and then infer the existence of wormhole in the network. Longer transmission can be another indication of wormhole presence. Also wormhole existence in a network can be determined by checking on parameters like transmission ranges, bandwidth, round trip time, received signal strength etc. Here are some of the approaches used by researchers since the last decade.

2.1 Location and Time based approach

A mechanism, called packet leashes (Hu et.al 2003), whose objective is to bound the distance which a packet travels in the network. They presented two approaches to attain this goal, the first one is called as geographical leashes, and a space based approach, which defines an upper bound on the distance a packet can travel. A node appends its current position and transmission time to a packet before sending it. The receiving node after receiving the packet, calculates the distance with respect to the sender and the time required by the packet to navigate through the path. The calculated distance information is used by the receiver to infer whether the received packet passed through a wormhole or not.

The second approach is a Time based approach known as Temporal Leashes. the sending node appends into the packet the time at which the packet was sent (Ts).The receiving node compares this value to the time at which the packet was received(Tr).The receiving node thus becomes able to identify if the packet travelled too far as per the claimed time of transmission and the speed of light.

2.2 Message Travelling time information based method

Round trip time (RTT) parameter is used to measure message travelling time information. In this mechanism, each node computes the RTT between itself and all its neighbours. As the RTT between two fake neighbours is greater than that between two real neighbours, a node can identify a malicious node pretending to be its neighbour. (Tran et al 2007),(J Zhen et.al 2003),can identify both the fake and real neighbours. No special hardware is required in this mechanism.

2.3 Multi-dimensional Scaling-Visualization-based Solutions

Adopted in(Wang et a 2004) to detect wormhole attacks in WSNs). The method is grounded on the observation that networks with malicious nodes have different visualization when compared to those with normal nodes. In this method, a layout of sensor nodes is constructed using multidimensional scaling (MDS). As per their approach, a wormhole attack can be identified by envisaging the inconsistencies introduced by the attack. Every sensor node in the network uses received signal strength to estimate the distance to its neighbours. This distance information is then sent to the base station (sink) and the physical topology of the network based on individual sensor distance dimensions is calculated. A roughly flat topology is expected in case of no wormholes in the network ,whereas a wormhole would be seen as a 'string' drawing different ends of the network together, the assembled network layout visualization will show some bent/distorted features.

2.4 Trust Based Methods

Trust information among sensor nodes can be used to detect Wormhole attacks(S.Ozdemir et al 2008). Sensor nodes can observe and rate their neighbouring nodes as per their activities. In such methods systems, each source node computes the most trustworthy path to its destination, based upon its trust information by bypassing intermediary malicious nodes. A wormhole in such a system **should** have the minimum trust level based upon the assumption that it drops all the packets and can be easily rejected. Likewise, a nearby node of a source node will have the utmost trust level if all the packets sent through it reach the destination.

2.5 Neighbor Discovery Approach

The neighbour discovery approach l (Modirkhazeni et.al 2010) is based upon the fact that a node receives data only from its actual neighbours i.e. which are only a single hop away, no matter which part of network the packets come from. If the receiving node is able to determine whether the received data came from an actual neighbour or not, it can easily detect a wormhole. In this approach a node constructs a neighbouring node list which is further used to detect where from the data arrived. Defensive measures are then followed to mitigate the malicious nodes.

3. Proposed System Model

3.1 Network Model

A wireless sensor network scenario with a large number of nodes is considered. We assume that any two nodes ‘A’ and ‘B’ can communicate with each other directly if they lie within each other’s transmission range. In order to accomplish the network’s operation data must flow in between source and destination nodes. A Source – Destination pair e.g (Sn,Dn) represents a link with ‘Sn’ as source node and ‘Dn’ as destination node, facilitating a flow of ‘n’ packets. It has been assumed that the source node maintains the packet flow at a persistent rate ‘r’. Any two nodes that do not lie within each other’s transmission range depend on multi-hop communication. Between two such nodes there exist a finite number of nodes. Since the sensor network topology undergoes changes due to sleep-wake cycles and nodes joining and leaving the network, multiple routes also exist between nodes relying upon multihop communication.

3.2 Attack model

Since the sensors are arrayed in an unattended environment, presence of mobile adversaries is natural, each adversary being capable of overhearing, copying and replaying eavesdropped packets including routing control messages. The adversary is able to determine the network topology by eavesdropping on routing control packets. The unattended nodes can also be physically captured by adversary. Once a node has been compromised, its cryptographic properties can also be extracted, enabling the adversary to substitute the captured node with a malicious node impersonating the captured node. Malicious nodes are governed by the adversary and are adept to conspire with other malicious nodes. One such attack is the wormhole attack. In a wormhole attack, a covert path (wormhole tunnel) that connects two distant nodes of the network is created by the adversary. This attack fakes the presence of a short path between two nodes, shortest-path routing protocols tend to route a large amount of the network traffic over the tunnel. The adversary can further control this transmission, selectively drop packets, increase delays, or create routing instability (Andrew et al 2013). The malicious nodes forming wormhole link can also eavesdrop packets at one location (at tunnel opening) and replay them at another location (at tunnel closing), in order to disrupt the network performance. The packet replay caused by the malicious nodes strongly increases the number of sends and receives in the network, consuming energy and wasting bandwidth to such an extent that after a point of time the network functionality tends to decline, leading to denial of service.

3.3 Detection and mitigation

The proposed approach analysis two inters related parameters: rate of packet flow and delay experienced by a packet while traversing a link. And finally deploys a counter-attack mechanism that helps to restore network performance. The goal of the adversary in launching a wormhole attack is to attract packet flow towards the wormhole tunnel. The packets travelling through an in-band wormhole experience a delay directly proportional to the number of nodes a wormhole tunnel is made from. The detection of the in-band wormhole is grounded on the probability that if a communication link experiences unexpectedly long delays and high flow rates, it is umpired to have a high likelihood of being a wormhole. If the delay experienced by a packet while transmitting through a link is greater than the expected delay. Also if some links in the network are observed to have high transmission rates than other links, transmissions going on between those links are seized by rendering the link end points obsolete (isolating the nodes). The Denial of Service injected due to presence of multiple wormhole tunnels in the network is shown by figure 2. Figure 2 represents how network performance declines due to increased unnecessary packet transmissions in the network.

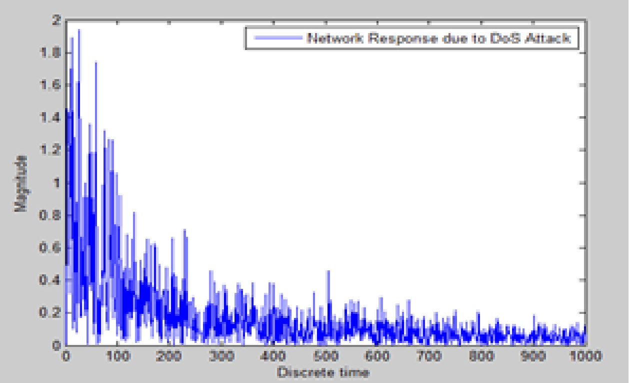

Fig 2 showing a decline in data flow due to wormhole attack.

The above figure shows an increase in magnitude of packet transmission at early stages of wormhole operation. later on large energy consumption due to packet replay gradually results in decreased data flow.

After employing the proposed mitigation technique it is evident from figure 3 that a persistent network response is achieved, the network's early response (from figure 2) is compensated by a controlled response that prevents the network from suffering.

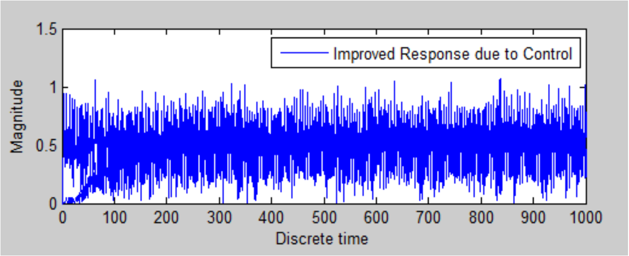

Fig 3 showing improvised network response after employing mitigation strategy.

4. Simulation Results

To assess efficiency of the proposed approach, simulation studies have been performed using MATLAB. Results in figure 3, 2 show the impact of an IN BAND Wormhole on network performance with and without applying the mitigation strategy respectively.

It can be observed from figure 2 that the network shows erratic behaviour upon being infected by a Wormhole. The packet transmission takes place with high magnitudes in the beginning and then network starts to disfunction due to exhaustion of resources. Figure 3 clearly shows how a steady transmission rate is achieved after applying the proposed control strategy on the wormhole infected wireless sensor network.

3. Conclusion and Future Work

In this paper, we considered the IN BAND wormhole attack on a wireless sensor network .wormhole attack can cause defilements of timing, delay and resource constraints in sensor networks. We presented a reactive mechanism for recovering the network from denial of service induced due to the wormhole attack. Future work is planned on detecting other forms of wormhole attack and presenting preventive and defensive approaches to counter such attacks.

References

Prasannajit B, Anupama, Vindhykumari, Subhashini, & Vinitha (2010) An Approach Towards Detection Of Wormhole Attack in Sensor Networks, *Integrated Intelligent Computing (ICIIC), 2010 First International Conference on,IEEE* , E-ISBN 978-0-7695-4152-5 pp 283-289

Karlof & Wanger(2003), Secure Routing in Wireless Sensor Network: Attacks and Countermeasures,*First IEEE International Workshop on Sensor Network Protocols and Applications*,SNPA 2003, pp 113-127

Khalil, Bagchi, & Shroff(2007), LiteWorp:Detection And Isolation Of The Wormhole Attack in Static Multihop Wireless Networks , *International Journal Of Computer AndT elecommunications Networking*,vol. 51(13),pp 3750-3772

Sharma, Pradeep kumar (2013) ,Localization Against Wormhole Attacks in wireless sensor networks

Y. C. Hu, A. Perrig and D. B. Johnson(2003), Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, *22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM),* pp. 1976-1986.

Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee and Heejo Lee(2007),TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks, *4th IEEE conference on Consumer Communications and Networking Conference*, pp. 593 - 598

J. Zhen and S. Srinivas(2003)., Preventing replay attacks for secure routing in ad hoc networks, *Proceedings of 2nd Ad Hoc Networks & Wireless (ADHOCNOW'03)*, pp. 140-150

W. Wang and B. Bhargava(2004). Visualization of wormholes in sensor networks, *WiSe, Proceedings of the 2004 ACM workshop on Wireless security. ACM Press*, pp. 51−60

S. Özdemir, M. Meghdadi, and Ý. Güler(2008). A time and trust based wormhole detection algorithm for wireless sensor networks,, *3rd Information Security and Cryptology Conference (ISC'08)*, pp. 139−4,

Ali Modirkhazeni, Saeedeh Aghamahmoodi, Arsalan Modirkhazeni, Naghmeh Niknejad(2011). Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks,*IEEE*,pp 122-128

Phillip Lee,Andrew Clark,Linda Bushnell1,and RadhaPoovendran(2013), A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems *.IEEE Transactions on Automatic Control, Special Issue On Control of Cyber Physical Systems*