ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 3, June 2015

Detection and Prevention technique for mitigating Wormhole Attacks in Wireless Sensor Networks

Chaitrasree S
Post Graduation Student, Dept. of CSE, AIT Tumkur, India, chai.minchu@gmail.com
Rakesh S
Assistant professor Dept. of CSE, AIt, Tumkur, India, rakeshs.snb@gmil.com

INTRODUCTION

A Wireless Sensor Network (WSN) is a particular type of ad-hoc network. The participating nodes are smart sensors, typically the size of a coin, equipped with advanced sensing functionalities (thermal, pressure, acoustic, etc), a small processor, and a short-range wireless transceiver. The nodes exchange data in order to build a global view of the monitored region Figure 1.1. This data is typically made accessible to the user through one or more gateway nodes.

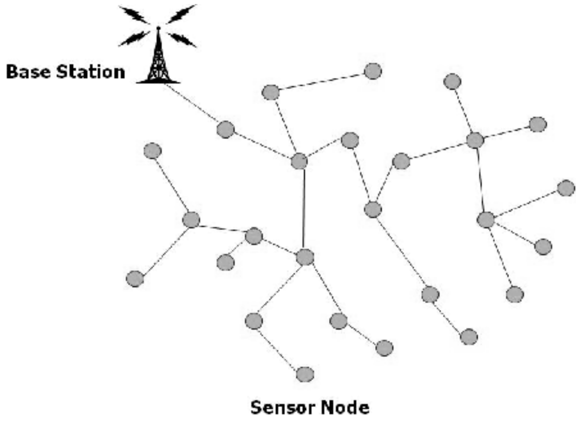

Fig.1.1 Sensor nodes exchange data to build a global view of the monitored region

WSNs have tremendous potential to provide very attractive, low cost solutions to a variety of real world problems. The application scenarios for WSNs are many, including military surveillance, commercial, environmental, medical, manufacturing and home automation, to name but a few. The past decade has witnessed an explosive growth in the use of wireless technologies. In particular, WSNs have become a very active area of research. There are many diverse and interesting aspects of this technology which demand further research to produce the innovative solutions needed to make WSNs a viable technology. Routing plays a central role in WSNs. In particular, owing to the inherent characteristics of WSNs, routing security is a hugely important area of research.

In order to maintain the availability of a WSN, resilience to node failure is very important. One of the ways that a WSN node could fail is through an attack. Although many WSN routing protocols have been proposed, none have been designed with security as a main goal. WSNs are vulnerable to a variety of security attacks due to the broadcast nature of the transmission medium and the fact that sensor nodes often operate in hostile environments. Security attacks in WSNs are often classified according the layers of the OSI model. The attacks which operate at the network layer are referred to as routing attacks.

Secure Routing For WSNS: Challenges

Providing secure routing in WSNs is a complicated and challenging task due to the constrained capabilities of sensor node hardware and the properties of their deployment. A brief outline of some of the major constraints present in WSNs is as follows:

- **Wireless Medium**: The wireless medium is inherently vulnerable due to its broadcast nature. It is relatively easy for an adversary to eavesdrop, intercept, and replay the transmitted data packets and inject malicious ones.
- **Hostile Environment**: WSN nodes are typically deployed in environments where they face the possibility of destruction or physical capture by attackers.
- **Limited Resources**: The extremely limited resources (power, bandwidth, CPU, memory) of sensor nodes are perhaps one of the biggest challenges in the design of robust and often resource-hungry security mechanisms. These constraints necessitate extremely efficient security algorithms.
- **Ad-Hoc Deployment**: The ad-hoc nature of sensor deployment means that the WSN topology is subject to regular changes. Any security mechanisms must be able to operate in such dynamic environments.
- **Immense Scale**: A typical WSN deployment could consist of hundreds of thousands of nodes. Any robust security mechanism needs to be able to scale to such large topologies.

Wormhole Attack

Wormholes are one of the most severe attacks on WSN routing. Two or more malicious nodes can collaborate in setting up a shortcut lower latency link between each other Figure 1 and through which they forward packets to each other and replay the packets there locally.

The adversaries convince the neighbor nodes of these two end points that the two distant points at either end of the tunnel are actually very close to each other. An adversary situated close to a base station may be able to completely disrupt routing by convincing nodes that would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. In such a scenario, the attack is similar to the sinkhole as the adversary at the other side of the tunnel advertises a better route to the base station. Wormhole and sinkhole attacks are particularly difficult to defend against, especially when the two are combined. Wormholes are hard to detect because they use a private, out-of-bandchannel which is invisible to the WSN. Packets are forwarded between the malicious nodes by encapsulation and use of additional hardware such as a wired link or a directional antenna. Wormhole attacks are more likely be used in combination with selective forwarding or eavesdropping. The wormhole attack is especially difficult to detect in WSNs when using routing protocols in which routes are decided based on advertised information such as minimum hop count to base station.

A wormhole attack could be launched in two different modes: hidden-mode and participation mode. Defending against a hidden-mode attack is particularly difficult because it can be launched even if all routing messages are authenticated and encrypted. This is because the malicious node does not need to read or modify the packets, just forward them.

Although participation mode wormhole attacks are more difficult to launch (they require modification of routing packets), once launched, they are extremely difficult to detect since the malicious nodes can simply ignore the security mechanisms of the routing protocol.

1.1 Objective

The idea of the proposed system is derived from the work done by Jigalur et al., who has worked on attack mitigation techniques in wireless sensor network. Although, the concept is a superior idea as it presents a simple algorithm that is also cost effective, but the study is focused on wormhole attack only. In the area of wireless sensor network, various attacks exists e.g. Sybil attack, black hole attack, etc, which have different adversarial properties compared to wormhole attack. Hence, the applicability of in mitigating other attacks in WSN is still a question. Hence, the proposed system attempts to mitigate by addressing majority of the lethal attacks in WSN and will thereby act as a contributory in project work.

The aim of the proposed system is to design a framework for the purpose of mitigating the most lethal attacks in wireless sensor network using simple cryptography techniques. In order to accomplish the above mentioned, following objectives are met:

- To perform an literature survey to understand the existing techniques and their effectiveness in mitigating wormhole attacks.
- To design an adversarial module by considering the most potential and malicious behavior of sinkhole attack, Sybil attack, routing attack, and wormhole attack.
- To design a secure framework that can perform implementation of cost effective cryptographic to secure the routes against the adversarial attacks.
- To apply enhanced digital signature for surveillance the confidential data.

1.2 Problem Statement

In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multihop route, for example through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker.

It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.

1.3 Solution to the Problem

The design of the proposed project starts with developing a new adversarial model, which will extract all the potential attack characteristics of sinkhole attack, Sybil attack, routing attack, and wormhole attack. The considered attack at network layer is the most attention seeking attack in WSN. It consists of two malicious nodes and a tunnel between malicious nodes. Several methods have been proposed for detecting wormhole attacks in ad-hoc network. However, these methods usually require that some nodes in the network be equipped with special hardware.

The proposed model consists of building such a mechanism which would be helpful in prevention of wormhole attack in a clustered WSN using enhanced digital signatures. The complete network is divided into small clusters based on proximity of nodes. Each cluster has a Cluster Head (CH) which helps in maintaining the cluster and one or more Gateway (GW) nodes that form the communication links to different clusters. A node is selected to be a Cluster Head based on the number of nodes in its proximity (transmission range). Thus, every node in a cluster is one hop away from the CH. A Gateway Node can belong to only one cluster. Thus, for every interface between two clusters, two GW nodes participate, one from each cluster.

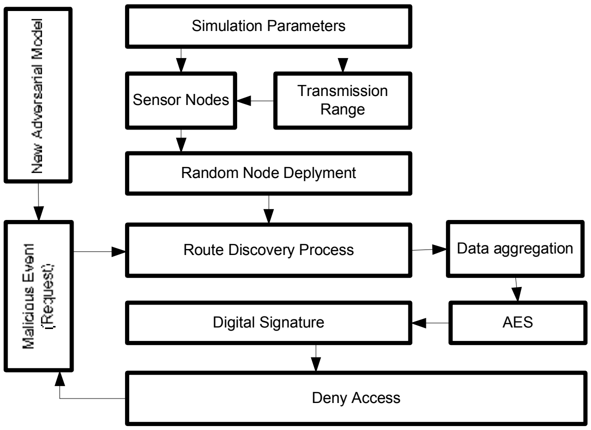

Figure 1.3 Tentative Architecture of Project

For a node to communicate with a node of another cluster, it must send the Route Request (RREQ) Packet to its CH which further sends the RREQ to other clusters (if needed) through GW nodes until the RREQ reaches the CH of the cluster to which the destination node belongs. The destination node then sends a Route Reply (RREP) packet to the source via the path that was discovered the earliest. Additionally, every CH broadcasts its Public Key to all the nodes within its cluster. GW nodes belonging to the two different clusters exchange the public keys of their respective CHs. Thus each GW node has two (or more) sets of Public Keys (one of its own CH and others of its neighbor's CH). The proposed algorithm will prevents nodes from routing data through the compromised routes as all communications take place through the CH and GW nodes, thereby, preventing a lethal attack.

When a source has to send a RREQ, it sends it to its CH. The CH uses its private key to digitally sign the packet. The CH checks if the destination is a member node. If yes, it sends the signed packet to the destination node. If not, it forwards the RREQ to all of its GW nodes (multicast). The GW node checks if the packet has come from its own CH by using the public key of the CH to verify the digital sign. The GW node then forwards the RREQ to its corresponding GW node. The communication is done through Gateway and Cluster Head further until the packet is reached to Destination.

On the other hand, the purposed technique is expected to work efficiently in all the scenarios. The system uses Java Simulation for simulating the network. The protocol succeeds in preventing a lethal attack as the compromised routes cannot successfully satisfy the security conditions imposed by the unique digital sign of each CH node. The proposed system will also use AES algorithm for preserving the data and to monitor the data in the network.

1.4Motivation

Wormhole attack is being reviewed from more than past decade but still the mitigation techniques are inefficient. This open issues motivates to select the topic to carry out project work.

LITERATURE SURVEY

Buch, Dhara Hitarth, and Devesh Jinwala. "Prevention of wormhole attack in wireless sensor network." arXiv preprint arXiv:1110.1928 (2011) [1].

This proposed here makes RREP packet forwarding conditional. By checking the validity of the two-hop neighbor node that has forwarded the packet, a node lets it to move further towards the source. Wormhole end is detected when the identity of the two-hop neighbor is found illegal. Authenticity checking of such two-hop neighbors is carried out using a preloaded secret key. By comparing the memory requirement for various numbers of neighbors, it can be concluded that by spending more on setup cost, higher scalability can be achieved. The proposed scheme focuses on the type of wormhole with out-of-band channel. It can be extended to detect other types of wormhole attacks also.

Sharif, Lukman, and Munir Ahmed. "The Wormhole Routing Attack in Wireless Sensor Networks (WSN)." JIPS 6, no. 2 (2010): 177-184 [2].

Thisexamined some of the most common routing attacks in WSNs. In particular, they focus on the wormhole routing attack in some detail. A variety of countermeasures have been proposed in the literature for such attacks. However, most of these countermeasures suffer from flaws that essentially render them ineffective for use in large scale WSN deployments. Due to the inherent constraints found in WSNs, there is a need for lightweight and robust security mechanisms. The examination of the wormhole routing attack and some of the proposed countermeasures makes it evident that it is extremely difficult to retrofit existing protocols with defenses against routing attacks. It is suggested that one of the ways to approach this rich field of research problems in WSNs could be to carefully design new routing protocols in which attacks such as wormholes can be rendered meaningless.

Tun, Zaw, and Aung Htein Maw. "Wormhole attack detection in wireless sensor networks." In proceedings of world Academy of Science, Engineering and Technology, vol. 36, pp. 549-554. 2008 [3].

This analyzed the nature of wormhole attack and existing methods of defending mechanism and then proposes round trip time (RTT) and neighbor numbers based wormhole detection mechanism. The consideration of proposed mechanism is the RTT between two successive nodes and those nodes' neighbor number which is needed to compare those values of other successive nodes. The identification of wormhole attacks is based on the two faces. The first consideration is that the transmission time between two wormhole attack affected nodes is considerable higher than that between two normal neighbor nodes. The second detection mechanism is based on the fact that by introducing new links into the network, the adversary increases the number of neighbors of the nodes within its radius.

Nishant Sharma, Upinderpal Singh, "A Location Based Approach to Prevent Wormhole Attack in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue. 1, 2014 [4].

This illustrated wormhole attack is a major problem that affects the wireless sensor network badly. In this paper, the proposed method has focused over the detection and long term prevention of wormhole attack in wireless sensor network. The proposed method is a robust and simple measure to wormhole attack. The proposed work clearly depicts the effect of detection and prevention using distinct implementation to isolate wormhole and further prevent it through Euclidean distance formula. The metrics used to validate the proposed work are throughput and packet lost over the network. And finally, the results through proposed work are quiet better in comparison to results in wormhole attack.

Saurabh Ughade, R.K. Kapoor, Ankur Pandey, " An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach", International Journal of Recent Development in Engineering and Technology, (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014) [5].

This illustrated implementing security techniques on wireless sensor network are of ample importance. This paper will help its readers in understanding of the attacks that WSN can be subjected to. The wormhole attack is a major setback of wireless sensor technology. Hence, there is an utmost significance of overcoming this problem. Few techniques have been mentioned which have been proved to be efficient against wormhole attacks.

Kaur, Gurpreet, and Er Sandeep Kaur Dhanda. "'Analysing the effect of Wormhole Attack on Routing Protocol in Wireless Sensor Network'." International Journal of Advanced Research in Computer and Communication Engineering 2, no. 8 (2013): 3217-3223 [6].

This present different routing protocol in wireless sensor network and how the attack named wormhole attack can affect the routing. The performance of different routing protocols can be evaluated on the basis of different parameters like throughput, end-to-end delay and energy consumption. Wireless sensor networks have an additional vulnerability because nodes are generally deployed in unprotected environment. Although there is no standard architecture of the communication protocol for wireless sensor network. The throughput of DSR routing protocol under wormhole threshold mode is more than other protocols as shown in fig.1.2. The ANODR protocol also performs well under threshold mode. The end-to-end delay of DSR protocol is also less as compared to others and ZRP protocol performs worst under wormhole threshold mode as shown in fig.1.3. The DSR protocol consumes less amount of energy both in energy consumed in transmit and receive mode as. The ANODR secure protocol also performs well for wireless sensor network under wormhole threshold mode.

Guowei Wu1, Xiaojie Chen1, Lin Yao1, Youngjun Lee2, and Kangbin Yim, "An Efficient Wormhole Attack Detection Method in Wireless Sensor Networks", Computer Science and Information Systems 11(3):1127–1141, , Retrived 2014 [7].

This illustrated a wormhole attack detection method is proposed based on the transmission range the exploits the local neighborhood information check without using extra hardware or clock synchronizations. Extensive simulations are conducted under different mobility models.

El Kaissi, Rouba Zakaria, Ayman Kayssi, Ali Chehab, and Zaher Dawy. "DAWWSEN: A defense mechanism against wormhole attacks in wireless sensor networks." PhD diss., American University of Beirut, Department of Electrical and Computer Engineering, 2005 [8].

This presented a new protocol called DAWWSEN that incorporates a detection and defense mechanism against the wormhole attack, a powerful attack that has serious consequences on sensor routing protocols. A great advantage of DAWWSEN is that it doesn't require any geographical information about the sensor nodes, and doesn't take the time stamp ofthe packet as an approach for detecting a wormhole attack, which is very important for the resource constrained nature of the sensor nodes. Finally, they have examined the performance of DAWWSEN through ns-2 simulations, and the results have shown that their routing protocol can efficiently defend against the wormhole attack and achieve low delay. In future work, they will try to introduce some modifications to their routing protocol in order to get a balanced tree where the load would be fairly distributed among the nodes since this will considerably help in reducing the value of Trefresh. They will also try to test their routing protocol in the case of 2 or more collaborating attackers.

3. HARDWARE & SOFTWARE REQUIREMENTS

The technical requirement specification of the project can be classified as:

3.1 Hardware Requirement Specification:

RAM: 4 GB

Processor: 2.20 GHz

Hard disk: Max 10 GB

Input: Standard Keyboard and Mouse

Output: High Resolution Monitor

3.2 Software Requirement Specification:

OS: Windows family

Programming language: Java

Programming tool:

4. INTRODUCTION ABOUT EXISTING SYSTEM

If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways. The attack can also still be performed even if the network communication provides confidentiality and authenticity, and even if the attacker has no cryptographic keys. Furthermore, the attacker is invisible at higher layers; unlike a malicious node in a routing protocol, which can often easily be named, the presence of the wormhole and the two colluding attackers at either endpoint of the wormhole are not visible in the route.

The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. For example, when used against an on-demand routing protocol such as DSR or AODV, a powerful application of the wormhole attack can be mounted by tunneling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination node's neighbors hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST and then discard without processing all other received ROUTE REQUEST packets originating from this same Route Discovery.

This attack thus prevents any routes other than through the wormhole from being discovered, and if the attacker is near the initiator of the Route Discovery, this attack can even prevent routes more than two hops long from being discovered. Possible ways for the attacker to then exploit the wormhole include discarding rather than forwarding all data packets, thereby creating a permanent Denial-of-Service attack (no other route to the destination can be discovered as long as the attacker maintains the wormhole for ROUTE REQUEST packets), or selectively discarding or modifying certain data packets.

The neighbor discovery mechanisms of periodic (proactive) routing rely heavily on the reception of broadcast packets as a means for neighbor detection, and are also extremely vulnerable to this attack. For example, OLSR and TBRPF use HELLO packets for neighbor detection, so if an attacker tunnels through a wormhole to a colluding attacker near node B all HELLO packets transmitted by node A, and likewise tunnels back to the first attacker all HELLO packets transmitted by B, then A and B will believe that they are neighbors, which would cause the routing protocol to fail to find routes when they are not actually neighbors.

5. ADVANTAGES AND DISADVANTAGES OF EXISTING SYSTEM

5.1 Advantages

- OLSR sense to sense the suspicious link and authenticate them in a simple step process.

5.2 Disadvantages

- False positive alarms problem gets negotiated.
- Both false positive and false negative alarms are considered
- Doesn’t extensively consider QoS parameters.

6. CONCLUSION

In this work, a new mechanism on designing a secure architecture for WSNs by using cryptographic actions with the help of digital signature is proposed and demonstrated. As compared to the conventional scheme the proposed scheme handles how monitoring of data is carried out by preserving privacy of data. The AES scheme by using secret key mechanism is considered such that until and unless he/she knows the secret key the data cannot be revealed by an attacker. This work much suits for preserving privacy of data in WSNs. The work is simulated in NetBeans environment which the results obtained are discussed using routing tables.

REFERENCES

[1] Buch, Dhara Hitarth, and Devesh Jinwala. "Prevention of wormhole attack in wireless sensor network." arXiv preprint arXiv:1110.1928 (2011).

[2] Sharif, Lukman, and Munir Ahmed. "The Wormhole Routing Attack in Wireless Sensor Networks (WSN)." JIPS 6, no. 2 (2010): 177-184.

[3] Tun, Zaw, and Aung Htein Maw. "Wormhole attack detection in wireless sensor networks." In proceedings of world Academy of Science, Engineering and Technology, vol. 36, pp. 549-554. 2008.

[4] Nishant Sharma, Upinderpal Singh, "A Location Based Approach to Prevent Wormhole Attack in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue. 1, 2014.

[5] Saurabh Ughade, R.K. Kapoor, Ankur Pandey, " An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach", International Journal of Recent Development in Engineering and Technology, (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

[6] Kaur, Gurpreet, and Er Sandeep Kaur Dhanda. "'Analysing the effect of Wormhole Attack on Routing Protocol in Wireless Sensor Network'." International Journal of Advanced Research in Computer and Communication Engineering 2, no. 8 (2013): 3217-3223.

[7] Guowei Wu1, Xiaojie Chen1, Lin Yao1, Youngjun Lee2, and Kangbin Yim, "An Efficient Wormhole Attack Detection Method inWireless Sensor Networks", Computer Science and Information Systems 11(3):1127–1141, , Retrived 2014