International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol 1 Issue 4 August 2015

Review of wormhole attacks in Wireless Sensor Network

Sapna Rajak[1], Prof. Sonal Choudhary[2]
[1] M.Tech Scholar, [2]Assistant Professor, CSE, ASCT Bhopal

ABSTRACT- The wireless sensor network is an emerging technology in the current scenario. There are number of devices are dependent on the approach of ad-hoc network. Sensors are also one of the important devices among them. In sensor network attack can possible due to loophole of the network. The wormhole attack is one of the types in this manner. This paper is a brief study of wireless sensor network and various types of attacks which can happen in this type network.

Keywords: Sensor, wormhole, Sybil, Sinkhole

I. INTRODUCTION

A sensor network is defined as a composition of a large number of low price, low power multi-functional sensor nodes which are highly distributed either inside the system or very close to it. Nodes which are very small in size consist of sensing, data processing and communicating constituents. The position of these minute nodes need not be absolute; this not only gives random placement but also means that protocols of sensor networks and its algorithms must possess self organizing abilities in unapproachable areas. Distributed or discrete sensor networks (DSNs) have recently emerged as an important research area. This progress has been spurred by advances in sensor technology and computer networking. It is economically feasible to implement DSNs, but there are various technical challenges that must be overcome before DSNs can be used for today's increasingly complex information gathering tasks.

Sensor networks are a promising new technology to enable economically viable solutions to a variety of applications, for example pollution sensing, operational integrity monitoring, and circulation monitoring. A huge subset of sensor network applications requires safety, especially if the sensor network protects or displays critical infrastructures. Security in sensor networks is convoluted by the broadcast nature of the wireless communication and the lack of tamper-resistant hardware (to keep per-node costs low). In addition, sensor nodes have limited storage and computational resources, rendering public key cryptography unpractical.

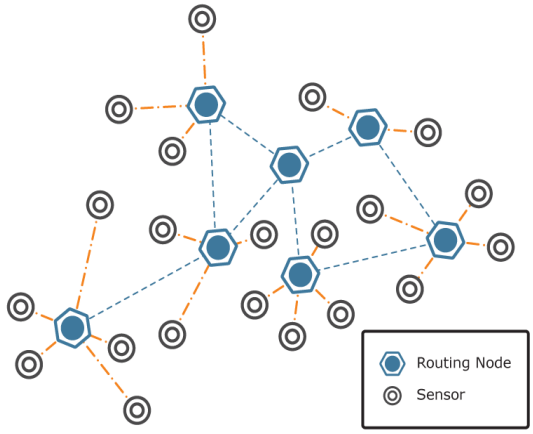

Figure 1. Example of sensor network

Most traffic in sensor networks can be classified into one of three categories:

1. Many-to-one: Multiple sensor nodes send sensor readings to a base station or aggregation point in the network.
2. One-to-many: A single node (typically a base station) multicasts or floods a query or control information to several sensor nodes.
3. Local communication: Neighboring nodes send localized messages to discover and coordinate with each other. A node may broadcast messages intended to be received by all neighboring nodes or unicast messages intended for a only single neighbor.
4. Sensor Network has several challenges. They include:-
5. **a) Power awareness:** Since the nodes in an Ad-hoc network typically run on batteries and are deployed in hostile terrains, they have stringent power supplies. appear minor, one significant attribute of cluster-based routing is that it can make a dynamic topology appear less dynamic. In order to implement a dynamic hybrid routing scheme, effective clustering algorithms need to be designed.
6. **b) Dynamic topology:** The nodes are mobile and hence the network is self-

organizing. Because of this, the topology of the network keeps changing over time.

7. **c) Quality of service (QoS)**: Providing constant QoS for different multimedia services in frequently changing environment.
8. **d) Multicast Routing:** Designing of multicast routing protocol for a constantly changing MANET environment.
9. **e) Security:** Security in an Ad-hoc network is extremely important in scenarios such as a battlefield. The five goals of security accessibility, privacy, integrity

II. ATTACKS IN SENSOR NETWORK

Most of the WSN's routing protocols are easy and straightforward. Because of this Spurpose they are vulnerable to attacks. There are different types of network layer attacks in WSNs which can be categorised as following:

1. Spoofed, altered, or replayed routing information
2. Selective forwarding
3. Sinkhole attacks
4. Sybil attacks
5. Wormholes
6. HELLO flood attacks
7. Acknowledgement spoofing

III. WORMHOLE ATTACK

In the wormhole attack [2], an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part 5. The simplest example of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks will more frequently involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker.

In some cases, an adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convert nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole.

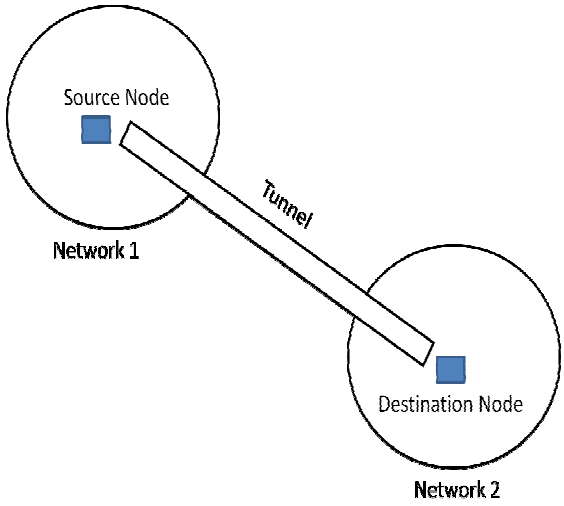

Figure 2. Wormhole Attack

This may generate a sinkhole: due to the potential attractiveness of the route created by the wormhole, those nodes neighboring the adversary on the other side of the wormhole may choose to forward packets destined for a base station through her and then propagate knowledge of this route to their neighbors and attract more traffic. Figure 6 shows an example of a wormhole being used to create a sinkhole.

Wormholes may also be used purely to convince two distant nodes that they are neighbors by relaying packets between the two of them. Wormhole attacks would likely be used in combination with selective forwarding or eavesdropping. Recognition is potentially hard when used in conjunction with the Sybil attack.

One node in the network (sender) sends a message to the another node in the network (receiver node).Then the receiving node attempts to send the message to its neighbors. The nearby nodes think the message was sent from the sender node(which is usually out of the range), so they attempt to send the message to the creating node, but it never reaches since it is too far away. Wormhole attack is an important threat to wireless sensor networks, because, this type of attack does not require compromising a sensor in the network rather, it could be performed even at the primary phase when the sensors start to discover neighboring information. Wormhole attacks are hard to counter

because routing information supplied by a node is difficult to verify

Table1: Attacks on Various Layer

Attack	Layer
Denial of Service	Physical, Data Link, Network & Transport
Wormhole	Data Link, Network
Sybil	Network, Application
Sink hole	Data Link, Network
Hello flood	Network

IV. WSN ROUTING PROTOCOL

Routing in sensor networks involves finding a path from the source to the destination, and delivering packets to the destination nodes while nodes in the network are moving freely [8]. Due to node mobility, a path established by a source may not exist after a short interval of time. To manage with node mobility nodes need to maintain routes in the network. Depending on how nodes create and maintain paths, routing protocols for ad-hoc networks broadly fall into pro-active, responsive, hybrid, and location-based categories.

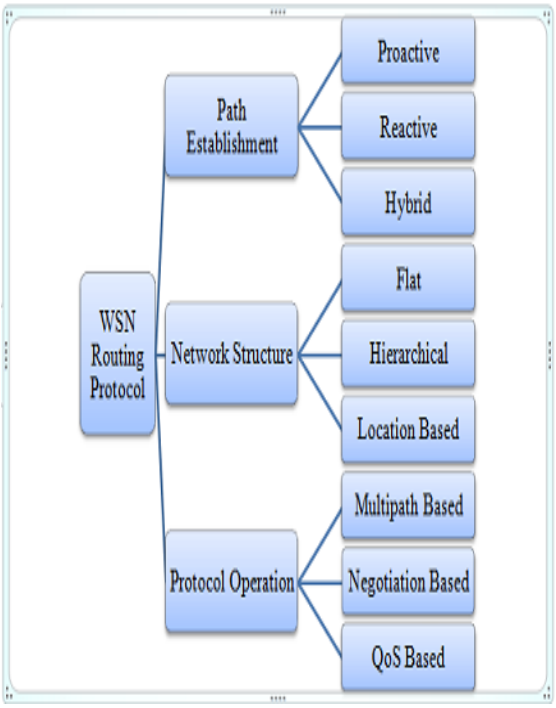

Figure 3. Classification of WSN protocols

Challenges in WSN

There are number of challenges have to be face in wireless sensor network but some of them has been discussed here:

- Limitations of the Sensor Network
  - packet loss due to transmission errors
  - variable capacity links
  - frequent disconnections/partitions
  - limited communication bandwidth
  - Broadcast nature of the communications
- Limitations Imposed by Mobility
  - dynamically changing topologies/routes
  - lack of mobility awareness by system/applications
- Limitations of the Mobile Computer
  - short battery lifetime
  - limited capacities

V. RELATED WORK

Thanassis Giannetsos [5] has highlighting in this article how the system can be used for defending against wormhole attackers. The author has presented their work on intrusion detection. They also has introduced the LIDeA which is a lightweight IDS framework. This frame work has specially designed for wireless sensor networks. lightweight IDS framework is based on a distributed architecture. In this architecture the nodes may be overhear their neighboring nodes. The conclusion of this approach is teams up with each other for successfully detect the intrusions of the network.

Bayrem TRIKI [6] has studied the number of solutions proposed by the various author and collect it in the literature in order to detect wormhole attacks in the environment of wireless sensor networks (WSN). It seems to be that the most of researchers haven't took an interest in problem of digital investigation. In this work the author has proposed a solution for digital investigation in order to investigate the wormhole attacks in Wireless Sensor Network. The work has based on the forwarding the data packet in the securing manner. The indication will be collecting the nature of the sensor node. To observe the activity of sensor network node there are some special node call the observers

Amar Rasheed [7] presents the threat posed in wireless sensor networks with the help of mobile sinks using wormhole attacks. Here the new approach has been proposed to defense the wormhole attack that involves leveraging channel diversity. This is like a security methodology for wireless sensor network. This scheme improves the flexibility to detect the wormhole attack in the sensor network. Here the property of threshold has been used which has used to calculate the probability of attacker. In this method the polynomial pool-based key pre-distribution scheme has used. There is a availability of multiple channel on the sensor network.

In this paper, [8] the author has proposed a simple and effective time-based scheme to prevent wormhole attacks in wireless ad hoc networks. Our scheme consists of two phase which are detection phase and location phase. They has uses the first phase in order to identify wormhole attacks exist or not in the network. The author has used the second phase in order to find the wormhole attackers. The proposed scheme of author no need to any additional hardware, e.g., GPS device, or synchronization, which is the main limitation of the other suggestions. The analysis of performance simulation approves the availability and efficiency of our scheme.

VI. CONCLUSION

This paper is gives the detail about sensor network. It also throws some light on the security constraints of sensor network. This paper presented and discussed various security issues, attack and threats sensor network. It also describes selfish node behaviors along with wormhole attack. It look like to be that the worm hole attack very harmful so there is huge need to identify the warm hole in the network. In future we plan to continue our work in field of secure routing over sensor networks & wormhole detection and prevention technique which are present in the network in order to enhance the security of sensor networks.

REFERENCES

[1]. G. S. Sara and D. Sridharan "Routing in mobile wireless sensor network: A survey", IEEE 2013

[2]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayiric "Wireless sensor networks: A survey", IEEE 2000., vol. 38, no. 4, pp.393 -422

[3]. P. Ferrari, A. Flammini, D. Marioli and A. Taroni "IEEE802.11 sensor networking", IEEE 2006., vol. 55, no. 2, pp.615 -619

[4]. N. Jain and D. P. Agrawal "Current trends in wireless sensor network design", Int. J. Distrib. Sensor Netw., vol. 1, no. 1, pp.101 -122 2005

[5]. Thanassis Giannetsos, Tassos Dimitriou, Neeli R. Prasad, “State of the Art on Defenses against Wormhole Attacks in Wireless Sensor Networks”, IEEE 2009, pp 313-318

[6]. Bayrem Triki, Slim Rekhis, and Noureddine Boudriga, “Digital Investigation of Wormhole Attacks in Wireless Sensor Networks” IEEE 2009, pp 199-186

[7]. Amar Rasheed and Rabi Mahapatra, “Mobile Sink Using Multiple Channels to Defend Against Wormhole Attacks in Wireless Sensor Networks”, IEEE 2009, pp 216-222

[8]. Fei Shi, Dongxu Jin, Weijie Liu, JooSeok Song, “Time-based Detection and Location of Wormhole Attacks in Wireless Ad Hoc Networks”, IEEE 2011, pp 1721-1726

[9]. P. Papadimitratos and Z. J. Haas, “Secure Routing For Mobile Ad Hoc Networks” in Proc. of CNDS, 2002.