International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
*International Conference "*INTELINC 18*", 12th & 13th October 2018*

A Survey on Neighbor Discovery Threats for Cluster Based Nodes in 6LoWPAN Networks

B.Sudhakar
Asst.Professor, Dept. of ECE,
Annamalai University,Tamil Nadu
balrajsudhakar@gmail.com

Abhinaya.E.V
Ph.D Scholar, Dept. of ECE,
Annamalai University, Tamil Nadu
Abhinaya.e.v@gmail.com

Abstract- In 6LoWPAN (6 Low power Personal Area Networks), Internet Protocol 6 version (IPV6) is used in networks containing restricted processing facilities. In this network, the sensor devices are linked as a cluster and network connectivity is formed by reaching the edge router by connecting these clustered networks with the neighbor clusters. In 6LoWPAN Network, the major difficult task is discovering the neighbor and routing. Discovering the cluster path is susceptible to security threats because of the malicious nodes in the clusters. It is compulsory to carry out actions over the communication among the clusters. In existing, the authentication in node to node mutual communications is handled by the cryptographic strategies. They face security issues in excess of the mutual communication among clusters in the 6LoWPAN network. In this paper, a clear detailed survey has been done to find the details about the network and threats in the routing of data communication. It can be deal with through the simulation experiments done in the existing works of different categories of 6LoWPAN and MANET network.

Key Terms: Wireless Sensor Networks, 6LoWPAN Networks, clustered networks

I. INTRODUCTION

In Wireless Sensor Network, network formed by connecting the sensor devices for processing the sensed data. The sensor devices sense, assemble and send data to the sink when the processing is perform. Most important thing in the wireless sensor networks is to sensed data should be sent to the sink from time to time or when the data sensed by the devices.

In hostile environments [1] [2] such as forest and mountain area, the sensor devices are linked to the sink which is long distance from the sensor networks. The sensor nodes should be cost effective to balance the travel distance of sensed data from the environment to the sink. To optimize this type of networks, the low power capabilities of sensor devices are clustered to form to clusters. The aggregator node is essential to send data to the sink from the data gained from the cluster nodes consequently it is so called as cluster head.

The connected cluster nodes send the data to the sink if it is in close to the located area. For data processing, the low power capable sensor nodes are connected to the internet through the gateway and it needs more architecture system for the transmission of the data over the internet. Thus the network connection can be finished through gateway by means of Internet Version 6 Protocol so called 6LoWPAN Networks (6 Low power sensor networks over Wireless Personal Area Networks).

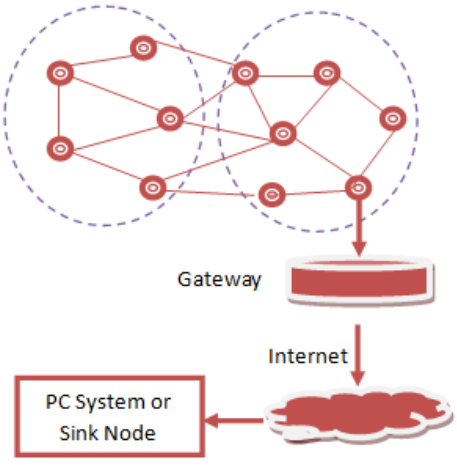

Fig.1.1 Architecture of 6LoWPAN Networks

That's the sensor nodes generate smart network world where all the machines network with each other automatically. The most crucial role is to gather massive amount of sensor data and the possibility of the far-off control will be a most incredible advantage that will support many application domains. 6LoWPAN is an IETF-standardized IPv6 adaptation layer that allows IP connectivity over the lossy and low power network links. It is frequently used in the Internet of Things applications as well as the industrial access control systems and smart cities.

The number of sensor node in the networks controlled by the Network Access control systems and that is size of the networks; steadfastness of the nodes should be increasable and expanding lifetime of node. Moreover, network admission control can also be used for the security.

The major contributions in this paper are too summarized as follows: 1. Construct a cluster based wireless sensor networks. 2. Assign cluster head connect it to the sink node. 3. To optimize the network admission control security using Elliptic Curve Cryptography when the neighbor discovery can be achieved.

II. BACKGROUND KNOWLEDGE

The main surroundings knowledge necessary for the discussion below is as follows: What is an attack? What are the kinds of attacks? What are the attacks which are unnatural in the layers of network? The attacks are occurred during the network nodes inside or outside the network. These attacks are making inferior in the network data transmission or in the network structure. The attacks are complete at the layers of the networks; it can be diverse based on their behavior.

In a dynamic mobile network [3] [4] it may consists of huge nodes, among which a malicious node might be present with an intention to attack an established network and provide false information.

Active Attack is an attack in which the attacker tries to enter the system by infecting it with false codes or may steel the information and reproduce it in different form which leads to improper functioning of the network. Active attack classified into external attack and internal attack. The external attack means intruder from the outside of the network will cause the damage to the network on the other side the internal attack means the node will act as malicious and represent itself as an entity of the internal network where it can be able to propagate the manipulated information.

Passive attack influences network traffic through the investigation of routing i.e. the communicating entities are identified, monitors the data transmission way among them, decrypt the affected probably encrypted data and detain authentication credentials such as private key , public key, passwords. From this identification, the inferences are taken by the attackers containing some privacy data and therefore high profile data's are stolen without the legitimate user information.

2.1 Network Layer Attacks

The network layer attacks and its detection methods are examined through the existing works proposed and experimented by the authority.

2.2 Black Hole Attacks

A black hole attack [3] [4] is one of the network layer attack where the malicious node under threat get the route with best sequence number and less hop count between the source and destination and then overhears or drops all data packets. The large usage of 6LoWPAN in hostile and other security relevant areas have made it a vital prerequisite for security requiring areas. The network will be destroyed as nodes participate in the routing process.

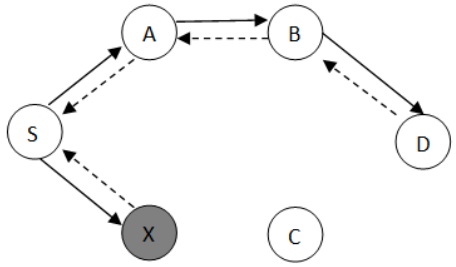

Fig. 2.1. Black Hole Attack Illustration

2.3 Warm Hole Attacks

Warm hole attacks [4] [5] [10] are as greatly like the kind of denial of service attacks in the packet transmission. This attack is most vulnerable and spontaneous in 6LoWPAN. In warm hole attack,

malicious node receives data packet from one part of the network and that it channeled to another malicious node. The wormhole referred as the channel exists between two or more malicious nodes.

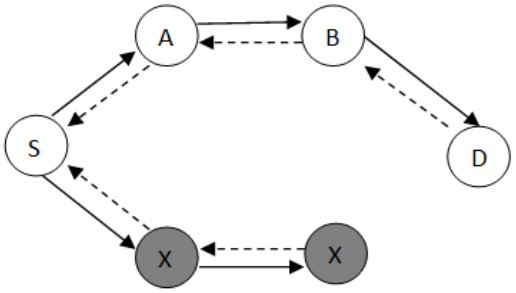

Fig. 3.1. Worm Hole Attack Illustration

Warm hole attacks are most vital threats to MANET routing protocols. To route many data in the nodes, attackers use wormholes in the network. When the attacker opt for worm hole attacks in DSR (Dynamic Source Routing) and AOD (Ad-hoc On Demand Routing), the attacker could avoid the discovery of any routes other than through the wormhole. If there is no security mechanism introduced in the network along with routing protocols, then the existing routing protocols will not be able to discover suitable routes.

III. PREVIOUS WORKS SURVEY

In [3], author surveys the detection of both black hole and gray hole attacks how its humiliates the act of the network data communication and the diverse defense mechanism that are offered to detect and diminish the black hole and gray hole attacks. In this work, they defined the both proactive and reactive routing methods and its design principles.

The Denial of Service attacks is the most susceptible attacks in the MANET, here to examine this attack, Alsumayt and Haggerty[6] surveys the attack vulnerability in the MANET and also its performance degradation. They proposed a perfect and new system to alleviate the DOS attacks and it also aids to plan a methodology to detect this attack with conviction in MANETs.

In [7], here the uniqueness of MANET with the challenges and the opportunities in attaining security models, such as confidentiality and integrity. They provide a large review of wormhole attack types and different detection methods and at last qualitative evaluation of wormhole detection methods.

In [8], the authors proposed a latest hybrid technique called WRHT: Wormhole Resistant Hybrid Technique, which is works like the techniques such as watchdog and Delphi schemes. Its most prominent feature of this proposed technique consists of is capability to protect against almost all categories of wormhole attacks independent on any accessories.

In Hash based Scheme, Wang W, Bhargava B and Linderman M [9], designed a hash based method to find out the behavior of the nodes including the data traffic information it contains while routing the path .In this scheme, an auditing technique is used for anticipating the packet drop attack. The audited node nn is required and to send the sequence numbers of selected packets to auditing node. A random number t0 is attached to every packet after source node sends out these packets. The intermediate node n1 joins the received packet and its own random number r1 to compute its value t1, and this operation is sustained within every intermediate node until nn receives the packet.

Goyal, P., Parmar, V., and Rishi, R [10] used weighted link to offer a misbehavior node detection algorithm using in a hierarchical 6LoWPAN Networks for cluster based sensor networks. Kejun Liu, Jing Deng [11] has proposed a network admission control solution for 6LoWPAN WSN that secures malicious nodes when it is unauthorized from using the sensor network to correspond with each other or to send data to the sink.

P. Rathiga, Dr. S. Sathappan [12] proposed a new framework with an authentication scheme for Mobile to Mobile communication in the 6LoWPAN Networks and the proposed scheme facilitates a 6LoWPAN device to strongly authenticate with the remote server with a session key recognized between them.

IV. CONCLUSION

In 6LoWPAN Networks, the network performance degradation is continuously protected by the attack detection and mitigation techniques and the growth can comes under the improvements in the performance of this separation of attacks. Here the network layer attacks such as Black Hole and Work Hole attacks are examined with the existing works. In

future, the new technique can be proposed and the results will also be evaluated with the existing results.

REFERENCES

[1] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao , "A survey of black hole attacks in wireless mobile ad hoc networks ", Human-centric Computing and Information Sciences 2011

[2] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges"

[3] Rajes Chowdari and Srinivas K, "A Survey on detection of Blackhole and Grayhole Attacks in Mobile Ad-hoc Networks", International Research Journal of Engineering and Technology, Vol. 04, Issue No.05, May 2017 pp. 1375-1378.

[4] Jain, S., & Hemrajani, N. 2013, "Detection and mitigation techniques of black hole attack in MANET: An Overview", International Journal of Science and Research (IJSR), India Online ISSN, 2319-7064.

[5] Divya R and Maheswari D, "Study of Various Security Attacks and in Network Layer and the Mitigation Techniques for MANET", International Journal of Advanced Research in Computer and Communication Engineering", Vol.5, Issue No.2, February 2016, pp.404-410.

[6] Alsumayt A and Haggerty J, "A Survey of the mitigation methods against DOS attacks on MANETs", Science and Information Conference, UK, August 2014

[7] Mudgal R and Gupta R, "Study of various wormhole attack detection techniques in mobile ad hoc networks", International Conference on Electrical, Electronics and Optimization Techniques, Published in IEEE, March 2016

[8] Rupinder, Jatinder and Ravinder Singh, "WRHT: AHybrid Technique for Detection of wormhole attacks in Wireless Sensor Networks", Research article on Mobile Information Systems, Vol.2016 – 13pps, Nov 2016.

[9] Wang W, Bhargava B, Linderman M, "Defending against Collaborative Packet Drop Attacks on MANET"

[10] Goyal, P., Parmar, V., & Rishi, R., "Manet: vulnerabilities, challenges, attacks, application", IJCEM International Journal of Computational Engineering & Management, 11(2011), 32-37.

[11] Kejun Liu, Jing Deng "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" IEEE transactions on mobile computing, vol. 6, no. 5, may 2007.

[12] P.Rathiga, Dr. S. Sathappan "Hybrid Detection of Black hole and Gray hole attacks in MANET", 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions, 2016