A Review of Malicious Attack in Mobile Ad-Hoc Network Based On Power Constraints

Sanjay Yadav
M.Tech Scholar, Department CSE, TIEIT Bhopal, India
sanjayyadav787@gmail.com

Kaptan Singh
Department of CSE, TIEIT Bhopal, India
Kaptan2007@gmail.com

Abstract - The minimization of power in wireless sensor network is big issue. If the process of energy constraints is optimized increase the reliability and security of mobile ADHOC network. The management of ADHOC network is great challenge due to dynamic infrastructure and mobility of node. Due to mobility of node routing path of network and security of communication suffered. In the process of node mobility and path discovery of routing protocol take huge amount of power and decrease the life of network. For the improvement of power and secured communication various protocol are designed but all are limitation in terms of group communication in ADHOC network. A security constraint in mobile ADHOC network is very critical task. Some critical security issue such as black hole attack, wormhole attack, sinkhole attack, prevention and detection of attack is major challenge. For the detection of wormhole attack various authors used various technique such as clock synchronization, threshold based technique, nearest neighbor node selection method.

Keywords: - MANET, security threats, power management

I. INTRODUCTION

A collection of self-configuring mobile node without any communications network is called The Mobile Ad-hoc Network. In a Mobile ad-hoc network every nodes is connect by wireless radio interface using wireless links so every node can free to move without any connection and without any rhyme with capability of variable links with other devices again and again. Because of it is a multi-hop process, the partial communication range of energy constrained portable nodes and thus each tool in network topology acts as a router. With dynamic nature of network topology the routes changes very fast and frequent and so the efficient routing protocols plays important roles in handling it[1,2]. They should be capable to ensure the delivery of packets safely to their destinations. MANETs are also capable of handling topology changes and malfunctions in nodes through network reconfigurations. The wormhole attack is a serious threat for mobile ad-hoc network. And it cannot be detected easily. For detection of the wormhole attack in MANET a technique has been proposed[6]. In a wormhole attack, two attacker nodes join together. One attacker node receives packets at one point and "tunnels" them to another attacker node via a private network connection, and then replays them into the network [8]. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network. The wireless mobile network attack divided into two group one is active and another group is passive group. The passive group of network attack faced a problem of internal attack. And the active attack defines the process of external attack. The process of attack consumes more power during the process of involvement. The maximum power consumption decreases the life time of network. The life time of network is play a major role in wireless sensor network. The radio power management protocol divide all node group into three section one is sleep mode , transit mode and active mode of action of node. For the reduction of power consumption we modified the activation process of control message protocol according to sleep mode, transit state and active mode. The modified protocol acquired the process of thresholds priority Oder on the basic of neighbor's node. The selection of neighbor node deepens on the mode operation in three sections. According to order of state create cluster of priority of group. After creation of group calculate average threshold value and compare each group value with minimum threshold value and pass the control message for communication. Section-II gives the information of related work in mobile adhoc network. In section III discuss the security threats in mobile adhoc network. In section IV discuss problem formulation finally, in section-V conclusion and future scope.

II. RELATED WORK

In this section discuss the related work in the field of mobile adhoc network for the prevention of security attack and minimization of power consumption. The utilization of power is important factor in mobile adhoc network. The more consumption of power decreases the life time of network. Here some work discusses.

Mustafa Bani Khalaf and Ahmed Y.Al-Dubai etl. [1] Authors proposed a probability based algorithm for the selection of node for the transmission of data. The probability based method reduces also the consumption of power during the selection of transmission node. Author also describes the process of alternate node selection technique for communication.

Sandeep Gupta and Prof.Abhishek Mathur etl. [2] authors proposed a rebroadcasting technique for controlling the packet flooding in network and also control the traffic of wireless network. The proposed algorithm also reduces the Node discovery time for communication. The authors induced the location based protocol for the communication purpose.

Mozmin Ahmed and Md. Anwar Hussain etl. [3] Authors design the wormhole detection algorithm for mobile adhoc network. The proposed algorithm designed for independent component for collection of information of different node. The proposed algorithm also decides the communication range of inside node and outside node.

Zhimu Huang and Ryo Yamamoto etl. [4] authors describe the list based intrusion detection technique for wormhole detection. The list based technique designed in terms of normal list and abnormal list. The list of abnormal based on the concept of thresholding . the threshold based technique decide the selection process of malicious node.

Akshay Aggarwal and Savita Gandhi etl. [5] Authors describe the process of wormhole attack detection process based on digital signature. The digital signature process authenticates the source and destination node on the basis of key. Here also used trust value of key for the selection of node. The proposed digital signature based authentication process is good for prevention and detection of wormhole attack.

III. Security Threats in wireless sensor network

The wireless sensor network always threat by intruder and attacker. The attack scenario defines in two modes one is active mode and other is passive mode. The passive mode of attack defines in terms of data transmission during two nodes for communication. In this mode attack modify the content message and creates the replica of message and modify the content. In general the active attack is outside and external attack. The external attack such as jamming attack, denial of service attack and many more attack define in this section.

Eavesdropping:

Eavesdropping attacker read the message of content before the receiver. The attacker incepts the control message and changes the node receiver location and receives the data transmitted by the sender. The intruder and attacker induced the fake message in the network and crate the overhead. The major drawback of wireless sensor network is easily RF signal is decoded and intercepted.

Interference and Jamming:

The RF signal based wireless sensor network easily disturbed by the intruder using the concept of jamming and interference. The jamming attack induced the noise level equal to signal level and the receiver and transmitter and the process of communication is dead. The interference attack induced the small amount of noise value in level of signal for transmission.

Black hole attack:

The black hole attack is well knows attack in wireless sensor network. The black hole attacks changes the path of communication and divert the location of node. The new location of node receiver the information of destination node. The original destination node information is changed. And the process of PDR value is increased.

Rushing attack:

Rushing attack is a collective tunnel attack. The attacker creates the tunnel link to source node and block the information process of destination node. The block node cannot be accused the data during the communication. The rush attack sometimes called as denial of service attack.

Malicious code attacks:

The malicious code attack is basically application level attack. In this attack scenario attack induced the malicious code such as warm Trojan horse and some passive code. Also used sql injection attack on application level. The malicious attack creates the maximum traffic and reduced the bandwidth of network.

Denial of service:

Denial of service attack is very famous wireless sensor network attack. In denial of service attack, the attacker block the source and destination node for the communication. The denial of service attack also called bandwidth attack. Denial of service attack performed by TCP and UDP flooding attack. Basically this attack performed by packet flooding in mobile network.

IV. Problem Formulation and Our Approach

The wireless sensor network is basically based on battery power device and uses of network consumed more power during the searching of node and transmission of data. In this paper study of power reduction factor in wireless sensor network. For the reduction of power in wireless sensor network used different topology model and some standard protocol such as LEACH and Q-LEACH protocol.

- The distribution of wireless sensor node is depending on situation and geographical area for the purpose of data transmission and data actuation. If the node displacement area is more the sensor node take more power for searching of sensor node.
- In sensor network the distribution of node in the concept of base node and slave node. The slave node collects the information and sends to the base station node. The base stations node send the information to main node for the processing of data.
- The loss of energy and disputation of power is major factor in wireless network. The loss of power reduces the life cycle of network.
- The process of quality service estimation depends on the life cyclic of network. If the consumption of power is increases the life cyclic of network is decreased.
- The transmission mode plays an important role in MANETs. Nodes can take single-hop or multi-hop depending upon the type of network topology chosen for communicating or transmitting data to other nodes within the network.
- The sensor nodes can be mobile or static depending on the application. In surveillance applications, sensor nodes are placed in unattended areas so it should be self-organizing and self-creating.

V. Conclusion and Future Work

In this paper presents the review of security threats in mobile adhoc network. The mobile adhoc network is very versatile network in concern of malicious attack. The Malicious software degraded the performance of mobile adhoc network. The malicious software is collection of black hole attack, sink attack, jammer and many more attack. In this paper also discuss the management of power utilization in mobile adhoc network. During the security threats the consumption of power is increase and decades the performance of network lifetime. So in future used probabilistic based model for the minimization of power consumption and prevention of security attack in mobile attack network.

REFERENCES

[1] Mustafa Bani Khalaf, Ahmed Y.Al-Dubai and William Buchanan “A New Adaptive Broadcasting Approach for Mobile Ad hoc Networks” IEEE, 2010. Pp 1245-1251.

[2] Mr. Sandeep Gupta Prof.Abhishek Mathur “Enhanced Flooding Scheme for AODV Routing Protocol in Mobile Ad hoc Networks” 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.

[3] Mozmin Ahmed, Md. Anwar Hussain, “Performance of an IDS in an Adhoc Network under Black Hole and Gray Hole attacks” 2013, PP 567-571.

[4] Zhimu Huang, Ryo Yamamoto, Yoshiaki Tanaka, “A Multipath Energy-Efficient Probability Routing Protocol in Ad Hoc Networks” ICATE 2014.

[5] Akshay Aggarwal, Savita Gandhi, Nirbhay Chaubey, Keyurbhai A Jani “Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs”, 2014 Fourth International Conference on Advanced Computing & Communication Technologies.

[6] Jih-ching Chiu, Chun-Yao Zheng, Yao-Chin Huang and Kai-Ming Yang “Design and Implementation of Sequential Repair and Backup Routing Protocol for Wireless Mesh Network” IEEE, 2012, Pp 234-239.

[7] D. Sandhiya K. Sangeetha R.S. Latha, “Adaptive Acknowledgement Technique with Key Exchange Mechanism for MANET”

[8] Neha Shirke, Kishor Patil, Shriram Kulkarni, Shriram Markande, “Energy Efficient Cluster based Routing Protocol for Distributed Cognitive radio network” IEEE, 2014.

[9] Aarfa Khan Prof. Shweta Shrivastava, Prof. Vineet Richariya, “Normalized Worm-hole Local Intrusion Detection Algorithm (NWLIDA)” International Conference on Computer Communication and Informatics (ICCCI -2014).

[10] Jyoti Joshi, Vidhate Amarsinh, “Enhanced 2ACK Scheme to Prevent Routing Misbehavior Using OLSR Protocol.” 2014 International Conference on Computer Communication and Informatics, IEEE, 2014.

[11] Mallapur Veerayya, Vishal Sharma And Abhay Karandikar “Sq-Aodv: A Novel Energy-Aware Stability-Based Routing Protocol for Enhanced Qos In Wireless Ad-Hoc Networks” IEEE 2012.

[12] Seema Verma Pinki Nayak and Rekha Agarwal” Energy Efficient Routing in Mobile Adhoc Networks based on AODV Protocol “ in IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 2, November 2012

[13] Samir Das, Charles E. Perkins, Elizabeth M. Royer, and Mahesh K. Markina. Performance comparison of two on-demand routing protocols for ad hoc networks. IEEE Personal Communications, 2008.

[14] T. Brown, Q. Zhang, and H. Gabow. Maximum power life curve for a wireless ad hoc network, 2006.

[15] Jae-Hwan Chang and Leandros Tassiulas. Energy conserving routing in wireless ad-hoc networks. In INFOCOM 2000.