Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 342 – 349

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad hoc Network

Mr. Nilesh N. Dangare[a], Mr. R. S. Mangrulkar[b]

[a]*M.Tech. (CSE), Bapurao Deshmukh College of Engg., Sewagram-442102, Wardha, India*
[b]*Head, Dept. of CE, Bapurao Deshmukh College of Engg., Sewagram-442102, Wardha, India*

Abstract

A Mobile ad hoc network (MANET) is self organizing, decentralized and infrastructure less wireless network. The successful transmission of data packet is depends on the cooperation of each node in the network. These types of network don't have permanent base station, so each node in the network acts as a router. Due to openness, decentralized, self organizing nature of MANET, it is vulnerable to various attacks. So security is the main concern in MANET. In this paper, we considered two attacks; Vampire and DDoS attacks. The Vampire attack is not any protocol specific. Single Vampire attack can increase the network-wide energy usage. DDoS attacks exhaust the resources available to a network. Both the attacks drain the energy of nodes. Here, we discuss method to mitigate these attacks.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: MANET; Vampire Attack; DDoS

1. Introduction

In Mobile Ad-hoc Network (MANET), the transmission of any data packets are totally depend on the cooperation of each node in the network, since packets are transmitted from hop to hop. Also each node has their own transmission range, so if any source node want to send the data packets to the final destination node, source node contact to its neighbour; that neighbour node again contact to another neighbour and so on, so that to reach the final destination node. As we know the wired networks need infrastructure and have centre administration. But in remote location such as mountain, valley, and some public location wired networks are hard to set up. Since MANETs are infrastructure-less, open and no central administration required, it become popular. Today MANETs are widely used in every area where wired networks can not reach. But due to the openness, infrastructure less and dynamic nature of MANET, it is highly sensible to various attacks. In MANET, routing is depends on various factors such as topology,

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.070

selection of route, route requests and responses etc. In MANET, if any attack is occurred, it will affect the whole performance of the network and may some secured information get stolen.

In MANET, to provide the security is the challenging work. Wireless links are more susceptible to various attacks. Malicious behaviour of any node, can disturb the smooth working of any network. To eavesdrop and gain the secrete information are become easy for malicious nodes. Since attackers are more and more intelligent and divers, it becomes hard to provide the security to MANET. Now a day many researchers give focus to develop the new techniques which provide the security to MANETs such as trust based technique.

Attacks can be categorised as Internal Attack and External Attack. External attacks are carried out by nodes which are not part of any network. Internal attacks are carried out by nodes which are in network and more sever and hard to detect as compared to the External attacks, such as Black hole attacks, Gray hole attack, DoS, DDoS, Vampire attack etc. In Passive attack, the attacker only listen the communication channel to know the confidential information is being transferred without altering or disrupts the operation of the network. In an Active attack, attacker can alters, drop or destroys the data being exchanged.

This paper is organized as follows: Section I includes introduction of MANET. Section II presents the Literature Survey, including the various techniques to mitigate various attacks. Section III introduces the types of attacks. In this paper, the vampire attack and DDoS attack are into consideration. Section IV presents the Propose Work. Section V presents Result analysis and Section VI presents Conclusion and Future scope.

2. Literature Survey

Sandeep A. Thorat and P. J. Kulkarni[2] compared trust based and cryptographic approaches for implementing security in MANET routing. Author discussed the design issues in trust based routing protocol for MANET in details. Paper has been presented a survey on trust based routing protocol and provide directions for future research in trust based routing protocol for MANET.

Ramya S. Pure et al[5] suggested proposed model which is designed over the ad-hoc On-demand distance vector routing protocol (AODV). The proposed routing algorithm adds a field to store the trust value or node's trust on its neighbor, so that the computational overhead can be reduced and trustworthiness of routing procedure can be generated. Based on the trust value of node, the routing information will be forwarded to the next node having highest trust value. Authors also worked on the some attacks such as Black hole attack, Gray hole attack and Wormhole attack. The proposed method helps to improve the throughput of the network.

Naveen Kumar Gupta and Kavita Pandey[7] proposed an algorithm which is based on Trust based AODV Routing Protocol for mobile ad-hoc network, and worked on the concept of honest value, which is calculated on the the concept of hop and trust to protect the network from affected nodes (malicious nodes). In proposed HAODV routing protocol, before forwarding the data through various routes, the routing paths have been evaluated according to the trust metrics by the nodes. This method is based on honest mechanism to secure the AODV routing protocol. The performance of the HAODV has been analyzed using three parameters namely the number of drop packets, throughput and Packet Delivery Ratio. The HAODV performs well in terms of throughput and number of dropped packets. The future work of this method is to implement the proposed scheme with more number of parameters while evaluating the path.

Naveen Kumar Gupta and Amit Garg[8] proposed a Trust based Management framework for securing AODV Routing Protocol. This worked on the concept of Trust factor and selection of most efficient route and using the Trust Value a routing path is evaluated, also during the route exchange process the route gets updated. The performance of the proposed system is calculated based on the Packet Delivery Ratio (PDR), number of drop packets and throughput. The identity information (Internet Protocol address and Trust Factor Value) has been used to prevent the attack by the malicious node. This identity information has been assigned to each node in the initialized phase or when the node has been configured. In future works, to optimize above mentioned scheme in terms of number of nodes and building the fast mechanism to detect and prevent the attacker nodes even when large number of nodes.

Sumathy Subramaniam et al.[11] proposed a framework for Opportunistic Routing help to improve the lifetime of