International Journal of Engineering Applied Science and Management
ISSN (Online): 2582-6948
Vol. 2 Issue 6, June 2021

A REVIEW ON SECURITY MECHANISM FOR DEFENDING BLACK-HOLE AND DOS ATTACKS IN MANET

A Kiran[1], Dr. Nandita Tiwari[2]
M.Tech Scholar, CSE Department, SRK University, M.P. India[1]
Asst. Professor, CSE Department, SRK University, M.P. India[2]

Abstract: *Security is a main anxiety for protected communication between mobile nodes in a hostile environment. The fact that mobile ad-hoc networks lack fixed infrastructure and use wireless link for communication makes them very susceptible to an adversary's malicious attacks. Black hole attack is one of the critical security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on-demand routing protocols such because AODV. Furthermore, DOS attack is a fairly new type of attack to cripple the availability of Internet services and resources. A DOS attack can originate from anywhere in the network and typically overwhelms the victim server by sending a huge number of packets. There are a number of attacks are deployed on mobile ad hoc network using routing protocols among them Black-hole and DOS attack is one of the critical attack in network. In this, Black-hole attack continuously drop the packets without forwarding them to neighbour node whereas in DOS, the attacker tries to jam the network using continuous flooding of false RREQ request to the target destination. That cases the loss in performance of network i.e. congestion, frequent energy loss, low packet delivery ratio and others. Therefore solution using node characteristics are proposed which detect and prevent both the attack, in this PDR threshold is estimated.*

Keyword: *AODV, Routing Protocol, Black-hole, DOS, Communication, Network Simulator*

1. Introduction

Network security is an essential part of study in both kinds of network i.e. wired and wireless network systems. Malicious attacks have caused tremendous loss by impairing the functionalities of the computer networks. Therefore, security is a main anxiety for protected communication between mobile nodes in a hostile environment. In unreceptive environments attackers can affect using active and passive attacks by manipulating routing control message and data packets [1]. Mobile ad hoc network (MANET) is single of the majority up-and-coming fields for investigate and review of wireless network. Necessary condition in MANET is security. In ad hoc network the communicating nodes sets new challenges for the security architecture since it doesn't essentially feed on fixed communications. The ad-hoc network is additional susceptible to denial of service attacks (DOS) and black-hole attack convincingly initiate during malevolent nodes or attacker.

1.1 Motivation

It is necessary to detect and prevent this unpredictable attack for improving the data transmission among mobile nodes. In this article, authors investigated the various proposed schemes for packet drop attack and present a remarkable comparison among them. Finally, Sumaiya Vhora et al. [3]have proposed a solution based on Rank Based Data Routing (RBDR) record to identify malicious behavior in network. The RBDR is created with field of routing details to analysis the behavior of network for detecting the malicious paths. The scheme is to identify the malicious paths for preventing the packet drop attack and also able to find the trusted multiple disjoint loop free routes for data delivery in MANET. The given concept will be implemented using AOMDV routing protocol through the NS2 network simulator.

1.2 Objectives

a. Study of Wireless Ad-hoc Networks and their Routing Techniques: In this phase the wireless ad-hoc network and their request in dissimilar

research areas are discussed. In adding up of that the dissimilar supporting routing protocols are moreover studied in this phase.

b. Investigation of Different Attacks based on the Routing and black-hole and DDOS attack: In this phase the different kinds of routing based attacks are studied additionally a detailed study on the Black-hole and DDOS attack is also summarized

c. Implementation of Proposed Work: In this stage, key issues based on the Black-hole and DDOS attack are addressed and their solution is prepared. Finally the prepared resolution is implemented with the help of NS2 simulation environment.

d. Performance Analysis of the Proposed Secure Technique: In this segment the performance estimation of the future security method is provided in adding up of that with the comparable network presentation parameters proportional study is moreover provided.

2. Literature Review

1. Wormhole Attack: In wormhole attack a malicious device receives packets at one place in the network to a different location in the network, anywhere these packets are retransmitted to the network. This channel between two secret consensus attackers is referred to as a wormhole. It could be conventional during wired links among two secret consensus attackers or using a single long-range wireless association. In this type of attack the attacker may construct a wormhole for packets not addressed to itself, for the inspiration that the transmit possessions of the radio channel [22]. Assume that node S wants to create a route to D and initiate route discovery. When X receives a route application from S, X summarizes the route application and tunnels it to Y over an accessible route, in this condition {X □ A □ B □ C □ Y}. When Y receives the summarize route request for D then it will make obvious that it had only negotiate {S □ X □ Y □ D}. Neither X nor Y update the packet header. Behind route discovery, the purpose finds two different routes of unequal length from S: one is about 4 and another is about 3. If Y channels the route reply to X, S would falsely consider the pathway to D via X is better than the pathway to D via A. Thus, tunnelling can prevent honest intermediary devices from properly increasing the metric used to calculate path lengths. The wormhole attack is principally unsecure for various ad hoc network routing techniques by which the device that listen a packet transmission openly from some node consider themselves to be in the range of (and thus a neighbour of) that node. As an instance, while used next to an on-demand routing protocol such as DSR [23],

2. Black hole Attack: In Black whole attack, using routing protocol to an attacker promotes itself as the shortest path to the objective device [24]. An attacker watches the routes appeal in an overflow based routing protocol. When the attacker receives an application for a route to the purpose node, it forms a react connecting of actually short route. If the naughty respond reaches the initiate node previous to the reply from the authentic node, a false route gets formed. Once the malicious device joins the network itself among the converse nodes, it is forceful to do the whole thing during the packets passing through them. It can crash the packets between them to implement a denial-of-service attack, or on the beforehand use its situation over the route is the first step of man-in-the-middle attack [25].

3. Byzantine Attack: In Byzantine attack, a compromised intermediary device or a set of devices are involved to deploy attack like producing routing loops, forwarding packets on non-ideal paths and carefully drop packets [27] which results in interruption or ruin of the routing activities. It is hard to detect Byzantine failures.

4. Information Disclosure: Any classified in sequence exchange must be protected through the communication process. Also, the significant data stored on nodes must be protected from not legalized entrance. In ad hoc networks, such information may enclose anything, e.g., the exact status details of a device, the position of the nodes, passwords, private keys or secret keys, and so on. From time to time the control data are more critical for security than the traffic data. For occurrence, the routing orders in packet headers like the distinctiveness or location of the devices can be more respected than the application-level messages. A conciliation node may leak top secret or significant in sequence to unauthorized nodes present in the network. Such data may contain in sequence about the network topology, geographic location of apparatus or best routes to authorized device over network [28].

5. Resource Consumption Attack: In Resource Consumption attack, an attacker tries to consume resources of other nodes obtainable in the network. The

incomes that are aimed are bandwidth, battery power, and computational power, which are only limitedly nearby in ad hoc wireless networks. The attacks could be in the form of out of work needs for routes, very regular production of beacon packets, or forward of rotting packets to nodes. Continuously flooding packets to that device consumes supplementary power results as a sleep deprivation attack [29].

6. Routing Attacks: There are some attacks which can be mounted on the routing protocols and may disturb the appropriate process of the network. Pithy descriptions of such attacks are known below:

7. Routing Table Overflow: In routing table overflow attacker produces routes to imaginary nodes. The aim is to construct plenty routes to preserve fresh routes from being formed or to overwhelm the protocol performance. In the case of practical routing algorithms we require to determine routing in sequence even previous to it is necessary, while in the case of reactive algorithms require locating a path only while it is requisite. Thus the main goal of such an attack is to create flood over routing tables, which would in turn avoid the configuration of records equivalent to fresh routes to authorized devices.

8. Routing Table Poisoning: In routing table poisoning attack attacker nodes present in the networks and alter open route update packets referred to other accepted nodes. Routing table poisoning may effect in sub-optimal routing, overcrowding in portions of the network, or yet compose various parts of the network unapproachable.

9. Packet Replication: In packet replication, an attacker replicates rotten packets. This exploit supplementary bandwidth and battery power available to the devices and also causes unnecessary misperception in the routing process.

10.Route Cache Poisoning: In the case of on-demand routing protocols (such as the AODV protocol), each node preserves a route cache that holds data concerning routes that have become recognized to the device in past. Related to routing table poisoning, a resistance can in addition exterminate the route cache to achieve similar objectives.

11. Rushing Attack: On-demand routing protocols that use replacement defeat through the routing discovery method are disposed to this attack. An attacker who accepts a RREQ packet from the starting node floods the packet rapidly throughout the network, before other nodes which also accept the same RREQ packet can act in response. Nodes that accept the legitimate RREQ packets suppose persons packets to be replacement of the packet before received. Hence take away those packets. Any route observe by the source node would contain the attacker as one of the centre nodes. Consequently, the resource node would not be conversant to conclude secure routes, that is, routes that do not have the attacker. It is actually difficult to observe such attacks in ad hoc wireless networks [30].

3. Conclusions

Perhaps the most widespread notion of a mobile ad hoc network is a network formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. Since the nodes in a network of this kind can serve as routers and hosts, they can forward packets on behalf of other nodes and run user applications. . Due to diver's nature of connectivity the network is becomes very valuable for various application areas. On the other hand some of the issues are exist such as high performance losses, limited connectivity, energy sources, frequently changing topology, and low secure communication are the major issues in the network. Due to this most of the responsibilities are made on the routing protocols. Most of the attackers are targeting the routing algorithms to deploy the attack. Among them the Black-hole and DOS is a one of the most critical attack in network.

In this presented work the Black hole and DOS flooding attack is targeted for the investigation and study. In black hole attack attacker node capture the packets and drop without forwarding them and in DOS attacker node frequently floods the RREQ (request) packets to the designation. Due to this the other network nodes making further request to the known host, this causes the network resources consumption in terms of energy, packet delivery ratio and routing overhead. Consequently, the entire network performance is affected. Therefore a node characteristics analysis based technique is proposed for implementing with routing protocol for enhancing the detection rate of malicious attackers.

4. FUTURE SCOPE

The proposed work is intended to identify the malicious nodes in network by which the security and performance of the network both can be obtainable. The required security solution is developed successfully and their performance is estimated under the attack conditions. The results show the effectiveness of the proposed solution. In near future the work is enhanced more with adding more

parameters to distinguish more or different kinds of network attacks. The solution is based on iterations so consumption of time is also a scope for future work. The whole research work can be extended in the future in other protocol rather than AODV.

5. REFERENCES

[1] PriyankaGoyal, SahilBatra and Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, Volume 9– No.12, November 2010.

[2] KhushbooSawant and Dr. M.K Rawat, "Survey of DOS Flooding Attacks over MANET Environment", International Journal of Engineering Research and Applications, Volume 4, Issue 5, Version 6, PP.110-115, May 2014.

[3] SumaiyaVhora, Rajan Patel and Nimisha Patel, "Rank Base Data Routing (RBDR) Scheme using AOMDV: A Proposed Scheme for Packet Drop Attack Detection and Prevention in MANET", 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), PP. 1 – 5, Coimbatore, 5-7 March 2015.

[4] Pradip M. Jawandhiya and Mangesh M. Ghonge, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), PP. 4063-4071, 2010.

[5] Indrani Das and D. K Lobiyal, "Effect of Mobility Models on the Performance of Multipath Routing Protocol in MANET", Computer Science & Information Technology (CS & IT) Computer Science Conference Proceedings (CSCP), PP. 149–155, 2014

[6] Vaibhav, "Mobility Models and traffic Pattern Generation Based Optimization of Reactive Protocols", International Journal Intelligence Engineering Informatics, 2012.

[7] Y. Z.a and W. Lee, "Intrusion Detection in Wireless Ad-Hoc networks," presented at the 6th annual international conference on Mobile computing and networking, PP. 275-283, 2000.

[8] Ali Dorri and Seyed Reza Kamel, "Security Challenges in Mobile Ad Hoc Networks: A Survey", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015.

[9] M. Frodigh, P. Johansson, and P. Larsson.―Wireless ad hoc networking: the art of networking without a network,‖ Ericsson Review,No.4, 2000, pp. 248-263.

[10] HaoYang, Haiyun& Fan Ye, "Security in mobile ad-hoc networks: Challenges and solutions", Pg. 38-47, Volume 11, issue 1, Feb 2004.

[11] Luis Bernardo, Rodolfo Oliveira, Sérgio Gaspar, David Paulino and Paulo Pinto A Telephony Application for MANETs: Voice over a MANET-Extended JXTA Virtual Overlay Network.