ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW ON VARIOUS TECHNIQUES FOR BLACK HOLE ATTACK DETECTION AND PREVENTION

E.r Mandeep Singh*, E.r Ashu Bansal
[*] Student M.Tech, CSE, BFCET, Bathinda, Punjab
Assistant Professor, CSE Department, BFCET, Bathinda, Punjab

ABSTRACT

In recent years mobile Adhoc network features a nice impact on wireless networks. In MANET, each node acts as a router to ascertain a route and transfer information by means that of multiple hops. Manet square measure a lot of susceptible to security problem. Once a node desires to transfer information to a different node, packets square measure transferred through the intermediate nodes, thus, searching and establishing a route from a supply node to a destination node is a vital task in MANETs. Routing is an important part in Manet and its many routing protocols. Circumstantial On-demand Distance Vector (AODV) is one in all the foremost appropriate routing protocol for the MANETs and it's a lot of susceptible to region attack by the malicious nodes. A malicious node that incorrectly sends the RREP (route reply) that it's a modern route with minimum hop count to destination so it drops all the receiving packets this is often referred to as as region attack within the case of multiple malicious nodes that employment in conjunction with cooperatively, the impact are a lot of this sort of attack is known as cooperative region attack. There square measure numerous efforts are created to defend against region attack, but none of the answer appearance most promising to defend against region attack. Thus during this paper, we've got surveyed and compared the present solutions to region attacks on AODV protocol.

KEYWORDS: Black Hole Attack, Gray Hole Attack, MANET Security. DSR, AODV.

INTRODUCTION

Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes . Nodes in these networks utilize the same random access wireless channel, cooperating in an intimate manner to engaging themselves in multihop forwarding The node in the network not only acts as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transferring packets; so there is need of a routing procedure. This is always ready to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

PROPERTIES OF AD-HOC ROUTING PROTOCOLS

The properties that are desirable in Ad-Hoc Routing protocols are :

i) Distributed operation: The protocol should be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The dissimilarity is that the nodes in an ad-hoc network can enter or leave the network very easily and because of mobility the network can be partitioned.

ii) Loop free: To improve the overall performance, the routing protocol should assurance that the routes supplied are loop free. This avoids any misuse of bandwidth or CPU consumption.

iii) Demand based operation: To minimize the control overhead in the network and thus not misuse the network resources the protocol should be reactive. This means that the protocol should react only when needed and should not periodically broadcast control information.

iv) Unidirectional link support: The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

v) Security: The radio environment is especially vulnerable to impersonation attacks so to ensure the wanted behavior of the routing protocol we need some sort of security measures. Authentication and encryption is the way to go and problem here lies within distributing the keys among the nodes in the ad-hoc network.

vi) Power conservation: The nodes in the ad-hoc network can be laptops and thin clients such as PDAs that are limited in battery power and therefore uses some standby mode to save the power. It is therefore very important that the routing protocol has support for these sleep modes.

vii) Multiple routes: To reduce the number of reactions to topological changes and congestion multiple routes can be used. If one route becomes invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure.

viii) Quality of Service Support: Some sort of Quality of service is necessary to incorporate into the routing protocol. This helps to find what these networks will be used for. It could be for instance real time traffic support.

Problems in routing with Mobile Ad hoc Networks

i) Asymmetric links: Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile and constantly changing their position within network

ii) Routing Overhead: In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

iii) Interference: This is the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

iv) Dynamic Topology: Since the topology is not constant; so the mobile node might move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted.

For example in a fixed network routing table updating takes place for every 30sec. This updating frequency might be very low for ad-hoc networks.

LITERATURE SURVEY

Prachee N. Patil , Ashish T. Bhole, Black Hole Attack Prevention in Mobile Ad Hoc Networks using Route Caching

The Dynamic Source Routing (DSR) algorithm makes use of caching concepts to store all newly constructed routing paths in mobile ad hoc networks. Route caching is aggressively used by DSR. By virtue of source routing, it is possible to cache every overhead route without causing loops. Basically the forwarding nodes are caching source route from the packet and forwards it for future use. Also, the destination replies to all requests. Thus the source learns many alternate routes to the destination that are cached.

In this paper author propose a new approach for blackhole prevention in DSR based on route caching. In this approach, once the blackhole node is detected in MANET during the path construction, we pass the blackhole node id to path function of DSR. In this function, paths are ready to be added in route cache, however priory to add each path in route cache is decided by parsing these paths for presence of blackhole node id. This process makes use of normal time of caching process only. In this paper, authors propose the cache based blackhole prevention algorithm for DSR routing protocols in MANETs.

Dr.S.S.Dhenakaran, A.Parvathavarthini , An Overview of Routing Protocols in Mobile Ad-Hoc Network

This paper describes that Mobile Ad Hoc Networks (MANET)-a system of mobile nodes (laptops, sensors, etc.) interfacing without the assistance of centralized infrastructure (access points, bridges, etc.). There are different aspects which are taken for research like routing, synchronization, power consumption, bandwidth considerations etc. This paper concentrates on routing techniques which is the most challenging issue due to the dynamic topology of ad hoc networks. There are different strategies proposed for efficient routing which claimed to provide improved performance. There are different routing protocols proposed for MANETs which makes it quite difficult to determine which protocol is suitable for different network conditions .This paper provides an overview of different routing protocols proposed in literature and also provides a comparison between them.

G. Murali, D. Pavan, V.V. Rajesh Reddy, P. Bharath kumar, DYNAMIC ROUTING WITH SECURITY CONSIDERATIONS

In this paper algorithm is mainly proposed to improve the security and to overcome the limitations existing with the present cryptographic algorithms and protocols. Although some designs like IP security, Secure Socket Layer provide essential security, they unavoidably introduce substantial overheads in the Gateway/Host performance and effective network bandwidths.

This routing protocol is compatible with the Routing Information Protocol which uses hop-count as its Routing metric. So there will be a limited number of hops and data transmissions are done by selecting hops randomly in a network. This improves security as well as controls traffic in the network. So , the procedure also includes using the multipath routing to select the paths to be followed. It uses the randomization process for selecting the number of hops to be selected for transforming the data. The routing table in this algorithm is based on the well-known Bellman-Ford algorithm. So, this overcomes the problems with security and traffic occurred with increase in the number of networks in these days.

K.V.S.Mounika, Nanduri Jyothirmai, A.Rama Krishna ,Dynamic Routing With Security Considerations

In this paper author describes that one of the major issues for data communication over wired and wireless networks is the security. Different from the past works which includes the Cryptography algorithms and System Infrastructures, we are proposing a dynamic routing algorithm that could randomize the delivery of packets for data transmission as it is compatible and also easy to implement. It is compatible with some of the popular routing protocols such as the Routing Information Protocol which uses hop-count as its metric in the wired networks and Destination-Sequenced Distance Vector protocol in the wireless networks. In the RIP where the hop-count is considered only a limited number of hops are chosen and data transmission are done by selecting the hops randomly in a network. This improves security as well as controls traffic in a network. The routing table in this algorithm is based on the one of the Dynamic routing algorithms known as “Bellman-Ford algorithm” or “Ford Fulkerson Routing algorithm”. An analytical study on the proposed algorithm is presented and the results are verified to show the capability of the proposed algorithm.

EXISTING TECHNIQUES

DPRAODV (Detection, Prevention and Reactive AODV) scheme

In this paper authors proposed have proposed the method DPRAODV (A dynamic learning system against black hole attack in AODV based MANET) to prevent security of black hole by informing other nodes in the network. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. If its sequence number is higher than the one in routing table, this RREP packet is accepted. In this solution, it has an addition check whether the RREP sequence number is higher than the threshold value. If it is higher than the threshold value, then the node is considered to be malicious node and it adds to the black list. As the node detected as anomaly, it sends ALARM packet to its neighbors. The routing table for that malicious node is not updated, nor is the packet forwarded to another node. The threshold value is dynamically updated using the data collected in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The main advantage of this protocol is that the source node announces the black hole to its neighbors in order to be ignored and eliminated.

ABM (Anti-Blackhole Mechanism) scheme

This paper attempts to detect and separate malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (Anti-Blackhole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS’s SN (suspicious node) table. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the suspicious node.

Honeypot based detection scheme

Authors propose a novel strategy by employing mobile honeypot agents that utilize their topological knowledge and detect such spurious route advertisements. They are deployed as roaming software agents that tour the network and lure attackers by sending route request advertisements. We collect valuable information on attacker's strategy from the intrusion logs gathered at a given honeypot.

ERDA (Enhance Route Discovery for AODV) scheme

Have designed an ERDA solution to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function a method called ERDA (Enhance Route Discovery for AODV). The proposed method is able to mitigate the a foresaid problem by introducing new conditions in the routing table update process and also by adding simple malicious node detection and isolation process to the AODV route discovery mechanism. The proposed method does not introduce any additional control message and moreover, it does not change the existing protocol scheme.

Cryptographic based technique

This paper focuses that many investigations have been done in order to improve the security in MANETs, most of which are relied on cryptographic based techniques in order to guarantee some properties such as data integrity and availability. These techniques cannot prevent a malicious node from dropping packets supposed to be relayed, there are basically three defense lines devised here to protect MANETs against the packet dropping attack. The first defense line (for prevention purposes) aims to forbid the malicious nodes from participating in packet forwarding function. Whenever the malicious node exceeds this barrier, a second defense line (for incentive purposes) is launched, which seeks to stimulate the cooperation among the router nodes via an economic model. Finally, once the two previous defense lines have been broken, a third on (for detection/reaction purposes) is launched aiming to reveal the identity of the malicious node and excludes it from the network.

CONCLUSION AND FUTURE SCOPE

A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. Since mobile nodes are not controlled by any other controlling entity, they have unrestricted mobility and connectivity to others. Routing and network management are done cooperatively by each other nodes. Due to its dynamic nature MANET has larger security issues than conventional networks. A black hole is a malicious node that falsely replies for any Route Request (RREQ) without having active route to specified destination and drops all the receiving packets. A mechanism is required to detect and remove the black nodes and regenerate the route and transfer the data to this new route. The system to be developed can be tested using simulation tools to check and compare the performances with the existing systems.

REFERENCES

[1] A.Parvathavarthini ,An Overview of Routing Protocols in Mobile Ad-Hoc Network.
[2] G. Murali, D. Pavan, V.V. Rajesh Reddy, P. Bharath kumar, DYNAMIC ROUTING WITH SECURITY CONSIDERATIONS
[3] K.V.S.Mounika, Nanduri Jyothirmai, A.Rama Krishna ,Dynamic Routing With Security Considerations.
[4] Navid Nikaein, Houda Labiod and Christian Bonnet ,DDR-Distributed Dynamic Routing Algorithm for Mobile Ad hoc Networks.
[5] Robinpreet Kaur & Mritunjay Kumar Rai, A Novel Review on Routing Protocols in MANETs.
[6] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma ,Review of Various Routing Protocols for MANETs.
[7] T.Manoj kumar, Dr. P.Harini, T.Maanasa , Dynamic Routing with Security Considerations.
[8] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao, A survey of black hole attacks in wireless mobile ad hoc networks
[9] Ravinder Kaur, Jyoti Kalra , A Review Paper on Detection and Prevention of Black hole in MANET
[10] Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi , Detection and Prevention of Blackhole Attack in MANET Using ACO
[11] Nitesh A. Funde, P. R. Pardhi , Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey
[12] Ramanpreet Kaur, Anantdeep Kaur , Blackhole Detection In Manets Using Artificial Neural Networks
[13] Chander Diwaker, Sunita Choudhary ,Detection Of Blackhole Attack In Dsr Based Manet

[14] Sarita Badiwal, VandnaVerma ,Survey of IDS in MANET against Black Hole Attack
[15] Poonam Rani , Neeraj Garg, Survey Paper On Blackhole Detection Schemes In Manet
[16] Govind Sharma, Manish Gupta, Black Hole Detection in MANET Using AODV Routing Protocol