Vol. 2, Issue IV, April 2014
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

SURVEY PAPER ON BLACKHOLE DETECTION SCHEMES IN MANET

Poonam Rani[1] , Neeraj Garg[2]

[1] M.Tech Scholar , Dept.of CSE, Haryana Engineering College Jagadhri, India
poonamsaini222@gmail.com
[2]Professor CSE, Haryana Engineering College, Jagadhri, India
neerajgarg01@gmail.com

Abstract: In manet the mobility and resource constraints of nodes may lead to network partitioning. Each node in manet acts as router and communicate with other nodes. However some nodes may cooperate partially or selfishly. The selfish node could reduce the overall performance of the network. Routing protocols play an important role in mobile network communication. In manet detection of misbehaving nodes is very important. The main objective of this research paper is to study various blackhole detection and prevention techniques.

Keywords: *MANET, BLACKHOLE DETECTION, ROUTING, AD HOC.*

1. INTRODUCTION

Mobile Ad hoc Networks (MANET) are the extension of the wireless networks. They plays important role in real life applications such as military applications, home applications etc. Mobile Ad hoc networks are threatened by a lot of security attacks such as Modification, Denial of service attack and Fabrication attack etc. Black hole attack (also called Selfish node attack) is a hazardous active attack on the mobile Ad hoc Networks (MANET). In this research paper a well-organized approach for the detection and removal of the Black hole attack in the Mobile Ad Hoc Networks (MANET) is described. The algorithm is implemented on AODV (Ad hoc on demand Distance Vector) Routing protocol. The algorithm can detects both the single Black hole attack and the Supportive Black hole attack. The benefit of the algorithm described in this paper is that it not only detects the black hole nodes in case when the node is not idle but it can also detect the Black hole nodes in case when a node is idle as well.

1.1.1 Table Driven Routing Protocols

In Table Driven routing protocols each node maintains one or more routing tables containing routing information about all other node in the network. All nodes keep on changing these tables to maintain latest view of the network. Some popular proactive protocols are: DSDV, WRP etc.

1.1.2 On Demand Routing Protocols

In On Demand routing protocols, the nodes don't maintain any routing table but they have a route cache. Routes are discover dynamically only when a node want to communicate with another node with the help of the route discovery process which is invoked by the source node. DSR and AODV are the example of on demand routing protocols.

1.1.3 Hybrid Routing Protocols

This type of protocols merges the best features of table driven and on demand routing protocols. In case of the intra-domain routing, these protocols uses the table driven approach, while in case of inter-domain routing these protocols uses the on demand approach. Such as Zone Routing Protocol (ZRP) etc.

1.2 AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

The Ad hoc On-Demand Distance Vector (AODV) protocol is one of the most well-liked reactive routing protocols. It is pure on demand routing protocol. This protocol enables dynamic, self-starting, multi hop routing among the mobile nodes in the mobile ad hoc networks. AODV allows mobile nodes to react to link breakages and changes in network topology in a timely manner. The best thing about the AODV is that AODV provides the loop-free route and also by using the link state routing technique it eliminates the "counting to infinity" problem and provides quick

convergence when the ad hoc network topology changes.

1.3 BLACKHOLE ATTACK

Black hole attack is hazardous active attacks on the Mobile Ad hoc Networks. A black hole attack is performed by a single node or combination of nodes as shown in figure 1. This attacker node is also called selfish node. In Black hole attack an attacker node sends a fake Route reply (RREP) message to the source node which initiates the route discovery procedure order to find the route to the destination node. When the source node received numerous RREP, it selects the greatest one as the most up to date routing information and selects the route contained in that RREP packet.[1]

2. LITERATURE REVIEW

Neelam Khemariya et. al. [1] In this research paper an well-organized approach for the detection and removal of the Black hole attack in the Mobile Ad Hoc Networks (MANET) is explained. The algorithm is implemented on AODV (Ad hoc on demand Distance Vector) Routing protocol. The algorithm can detects both the single Black hole attack and the Cooperative Black hole attack. The beauty of the algorithm described is that it not only detects the black hole nodes in case when the node is not idle but it can also detect the Black hole nodes in case when a node is idle as well.

R. Sudha et. al. [2] There are many routing protocols have been proposed for mobile ad hoc networks & well-known among them are DSR, AODV and TORA However, the maximum of these MANET secure routing protocols did not give a complete solution for all the MANETs' attacks & assumed that any node contributing in the MANET is not selfish and that it will cooperate to support different network functionalities Much work is going on to provide security to the network.This paper discusses Temporal table based schemes that can be applied to ARAN to detect selfish node and improve the performance.

Isaac Woungang et. al.[3] A blackhole is a malicious node that can falsely reply for any route requests without having an active route to a specified destination & drops all the receiving data packets. In this paper, a novel scheme for finding Blackhole Attacks in MANETs (so-called DBA-DSR) is introduced. The BDA-DSR protocol detects & avoids the blackhole problem before the actual routing method is started by using fake RREQ packets to catch the malicious nodes. Simulation results are proposed, showing that the proposed DBA-DSR scheme outperforms DSR in terms of packet delivery ratio and network throughput, chosen as performance metrics, when selfish nodes are present in the network.

Prashant Dewan et. al.[4] The reputations of the nodes, based on their history of relaying packets, can be used by their neighbors to make sure that the packet will be relayed by the node. This paper introduces a reputation method for ad hoc networks. Instead of choosing the minimum distance path to the destination, the source node selects a path whose next hop node has the highest reputation. This policy, when used again and again, in the presence of 40% malicious nodes, changes in best way the throughput of the system to 65%, from 22% throughput provided by AODV. This improvement is achieved at the cost of a higher number of route discoveries with a minimal increase in the average hop length.

Abdul-Fatau Adam et. al. [5] Nodes in mobile ad hoc networks communicate with one another by the use of packet radios on wireless multihop links. Because of moving the nodes and power limitations, the network topology changes fastly. Routing protocols therefore play an significant role in mobile multihop network communications. A recent trend in ad hoc network routing is the reactive on-demand philosophy where routes are established only when required. Maximum of the protocols in this category, however, use one route and do not utilize many alternate paths. In this paper, propose a scheme to improve existing on-demand routing protocols by creating a mesh and providing multiple alternate routes.

V. Giri Babu et. al. [6] Each node in a MANET acts as a router, and communicates with each other. In a manet (mobile ad hoc network), the mobility & resource constraints of mobile nodes may lead to network partitioning or performance degradation. Many data replication techniques have been proposed to minimize performance degradation. Maximum of them assume that all mobile nodes collaborate fully in terms of sharing their memory space. In reality, however, many nodes may selfishly decide only to cooperate selfishly, or not at all, with other nodes. These selfish nodes could then decrease the overall data accessibility in the network. In this paper, examine the impact of selfish nodes in a mobile ad hoc network from the perspective of replica allocation. The term this selfish replica allocation

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

R. Gomathi et. al. [7] Mobile Ad hoc Networks (MANETs) are very popular because of their widespread usage. In MANET, each node has to co-operate with each other to complete functions in the network. However some nodes do not contribute in routing and forwarding packets which are not destined to them, in order to save their energy. Such misbehaving nodes which try to get benefitted from other nodes but refusing to forward other nodes packets can severely degrade the performance of the whole network. In MANETs, detection of these selfish nodes is very important. In this survey, a detailed study of selfish nodes, their characteristics and their effects in various layers of the network are discussed.

3. CONCLUSION

In this survey detail study of selfish nodes, their effect in various layers of network are discussed. Various detection schemes are also suryed for performance analysis in terms of packet delivery ratio and network throughtput as performance metrics when black hole nodes are present in network.

REFERENCES

[1] Neelam Khemariya and Ajay Khuntetha, " An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs," March 2013

[2]R. Sudha and Dr. D. Sivakumar, "A Temporal table Authenticated Routing Protocol for Adhoc Networks," 2011 IEEE

[3]Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, and Mohammad S. Obaidat, "Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks," 2012 IEEE

[4]Prashant Dewan, Partha Dasgupta and Amiya Bhattacharya, "On Using Reputations in Ad hoc Networks to Counter Malicious Nodes," 2004

[5]Abdul- Fatau Adam, "Performance enhancement of AODV over DSR on demand routing protocols - aspect of packet salvaging in ADOV," 2011 IEEE

[6]V. Giri Babu and T. Sreenivasulu, " Detection of Selfish Node and Replica Allocation Over MANETs," September, 2013

[7]R. Gomati, Sony Jose and J. Govindarajan , " A Survey on Detection Schemes of Misbehaving Nodes in MANETs," September,2013