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

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DETECTION OF BLACK HOLE ATTACK USING CONTACT-BASED WATCHDOG

Prashantkumar Wagh*, Amutha Jayakumar
Department of Electrical Engineering ,Veermata Jijabai Technological Institute, Matunga, Mumbai, India.

DOI: 10.5281/zenodo.50380

ABSTRACT

MANET (Mobile Ad-hoc network) is group of mobile nodes interconnection .MANET depends on the nodes cooperation for working properly. MANET basically assumes that nodes participate honestly in packet forwarding. But some nodes may refuse to participate in the packet forwarding so that they can save their resources, leading to selfish behavior of the node. This affects the working of the network. Currently many are using watchdog for the detection of selfish nodes, but the detection by the watchdogs may lead to wrong result, generating false positive and false negative. Thus depending totally on watchdog may decrease the network performance. This paper proposes a method when two nodes come in contact with each other the information about selfish nodes is shared. This method will decrease the time and increase accuracy of detection.

KEYWORD: MANET, Black hole, AODV, Watchdog, Diffusion.

INTRODUCTION

Mobile ad hoc network is composition of mobile devices without any infrastructure connected via wireless links and forwards each other's packet. Mobile devices in MANET performs dual role of host as well router, they can enter and leave the network any time. The communication doesn't take place in centralized manner. MANET work on the assumption that every node honesty take part in packet forwarding that is if a node report of link break than that path is not used similarly if a node claims it can reach a certain node than it is trusted. MANET found their use in many areas like military, battlefield and emergency which require a wireless and infrastructure less network. Security is one of the important concerns in these areas.

As MANET depends on the honesty of the mobile nodes but there may be some nodes they may refuse to forward the packets. They may do so to save their resources or may be trying to disturb the network functioning intentionally. Such selfish node will affect the network performance drastically. An intruder can easily join the network and can utilize it for their benefit.

Cooperative networking has led to the development of wireless networks to effectively provide the services. These networks basically have contact based cooperation. The mobile nodes can communicate when they are within the communication range of each other.

The effect of selfish node is drastic and the studies shows that the packet delivery rate is highly degraded i.e. packet delivery rate drops to 30 percent from 80 percent when selfish node increases from 0 percent to 30 percent. Parameters like throughput, the number of packet dropped, average hop count and probability of reachability are highly affected by increase in no of selfish nodes. Therefore it is necessary to detect the selfish node quickly and accurately to maintain the network performance. Earlier work shows that watchdog is the mechanism for detection of selfishness and misbehaving of nodes.

1.1ATTACKS ON MANET

1.1.1 Flooding attack

Flooding attack is formed by sending multiple numbers of Route Request (RREQ) packets in a short span of time to a destination which doesn't exist in the network. The malicious node can create a flooding to exhaust the network resources like bandwidth and resources of node, such as battery, bandwidth and computational power or to interrupt the routing process to cause extreme degradation of performance of network. The network will be flooded with the RREQs sent by the malicious node as no node reply to route requests. This, results in consuming bandwidth of the network and draining of battery power of nodes. It could lead to the denial of service attack.

1.1.2 Routing Loop

In this the attacker creates false routing packets which consumes both bandwidth and the power on the network. This type of attack can be considered as one of the type of denial of service attack. By sending packets that did not have any destination, attacker can create a routing loop.

1.1.3 Grey Hole

Grey hole is a type of black hole attack. In this the attacker drops some of the packets received by it for e.g. it drops data packets and forwards routing packets.

1.1.4 Partitioning

In partitioning attack, the attacker analyse the network topology to partition between the set of nodes which makes the most harm to the system. The partition disconnects the communication between one set of node with another set of nodes.

1.1.5 Blackmail

Some Ad Hoc routing protocols tries to handle the security problems by keeping lists of possibly malicious nodes. Each node has a blacklist of, what it thinks, bad nodes and thereby avoiding using them when setting up routing paths. An attacker might try to blackmail a good node causing other good nodes to add this node to their blacklists and so avoid it.

1.1.6 Wormhole

In this attack an attacker uses a pair of nodes connected in some way. It can be a special private connection or the packets are tunneled over the Ad Hoc network. Every packet that one of the nodes sees is forwarded to the other node which in turn broadcast them out. This might create short circuits for the actual routing in the Ad Hoc network and thereby create some routing problems.

Also, all the data can be selectively forwarded or not using this attack thereby controlling the Ad Hoc network to a large extent. This kind of attack together with a partitioning attack can gain almost complete control over the network traffic.

1.1.7 Rushing Attack

Reactive routing protocols use sequence number for dominance of duplication at every node. An attacker can send multiple route requests with increasing sequence number so that it appear to be from different nodes. Due to which when actual request is sent out many nodes think it as a duplicate and interrupt actual route discovery process.

1.1.8 Resource Consumption

The Ad Hoc networks have limited resources such as bandwidth and battery power they are consumed for no reason by injecting extra data packets into it. More resources might be consumed by injecting extra control packets since these might lead to additional computation. Also, the other nodes might forward control information as it comes in resulting in even more resource consumption.

For devices that try to conserve battery power by only occasionally enabling their communication device a malicious attacker might communicate in an ordinary way but with the only intent to drain battery power.

1.1.9 Dropping Routing Traffic

In Ad Hoc network it is important that all nodes participate in the process of routing. However, in order to save energy, some nodes may act selfishly and process only routing information that are related to them. This behaviour of the selfish nodes can create network instability or even part the network.

1.1.10 Location disclosure

The Location disclosure attack let the malicious node know the address and exact location of the node and can get information about the structure of the network. Thus it also gets information about the neighbours of the destination node.

BLACK HOLE ATTACK PROBLEM

AODV protocol is a reactive protocol which generates path when demanded by the source node. A route discovery process is initiated by a node in the network when it wants to transmit some data packets. The node broadcasts a route request (RREQ) packet in the network. The packet sent to the neighbours, which is then forwarded to their neighbours, and this goes on until the destination node is not found. The intermediate node can reply to the RREQ packet if and only if it has a new route to the destination. As the RREQ packet reaches the destination node, the destination node (target) responds by unicasting the route reply (RREP) packet.

AODV protocol states that any intermediate node can give reply to the RREQ message if and only if it has new route, which is checked by the sequence number of destination contained in the RREQ packet. Thus malicious node easily gets into and can disrupt the routing process.

Black hole attack is shown in Figure 1 in this node S want to send data packets to the D. Thus the node S starts the route discovery process. The nodes N1 and N2 are the neighbours of the source node S and N11 and I are the next neighbours. In this the node I is the intruder (malicious) node. Node I will claim that it has shortest and active route to the destination (target) node as soon as it receives RREQ packets. The malicious node will reply to source node S with highest sequence number. When source node receives reply, it thinks that route to the destination is discovered. Node S will start routing data packets to the node I and will discard all other replies that came from the other neighbours. The malicious node I will drop all the packets sent to it thus increasing data packet loss, the destination node never receives data packet and source node thinks that the packets are safely received by destination .The malicious node formed a black hole in network, and it is called as black hole attack.

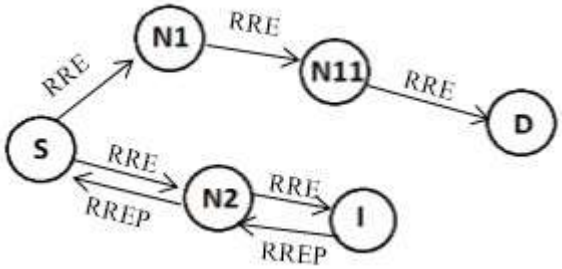

Figure 1: Black Hole Attack

RELATED WORK

Many methods have been proposed by researchers for detection of black hole attack in MANET:

Nidhi Tiwari and Raghav Yadav [1] proposed an approach in which the route request and reply messages are modified in order to discover the black hole node and the route to the destination. The idea is a normal node cannot find the route for invalid IP address but the malicious node will respond for an invalid IP address as it never search routing table for finding the route and sends reply without forwarding the packet. Thus in this method two destination IP address are specified in the route request message one is the valid IP address and the second one is invalid IP address for detecting the black hole nodes.

Payal N. Raj and Prashant B. Swdesh [2] proposed a solution against black hole attack. In this approach authors checks the sequence no in RREP packet. If the sequence no in RREP has the higher value as compared to the sequence number in the routing table of sender then the RREP packet is acceptable. For comparing authors has defined a threshold value. After comparison if the value of the sequence no is also higher than the threshold value then the sender of RREP is consider as malicious and an ALARM message is send to the neighbours by the source node.
Seryvuth Tan and Keecheon Kim [5] proposed a new protocol SRD-AODV (Secure Route Discovery for AODV-based MANET) for detecting the black hole nodes. In this the authors defined three thresholds for classifying malicious and normal node in three different environments- small, medium and large environments. In this approach the sequence number of each response is compared with threshold value. If the sequence no is greater than the node is black hole node otherwise normal node.

Hongmei Deng, Wei Li and Dharma P. Agarwal [7], they proposed two solutions for the black hole problem. First one is confining the ability of intermediate nodes replying to a message, so all reply should come only from the destination node. In this method the intermediate node cannot reply. Disadvantage of this solution is increased time delay and malicious node can fabricate a reply message on behalf of destination node.

Mistry N,Jinwala DC and Zaveri M[8] proposed a method that uses Watchdog and Pathrater for detecting black hole attacks. The watchdog enables neighbour nodes to detect malicious nodes. If a node repeatedly discards packets then it is said to be malicious node. The pathrater assigns a default value to each node and then observes the transmitting behavior of each node. After a period of time, if the value for a node is below a certain threshold, the node will be added to the list of black hole nodes. This method cannot handle cooperative attacks.

B. Sun, Y.Guan, J.Chen and U.W. Pooch. [9] presented a neighborhood approach for detecting the black hole attack. As the root discovery process initiated by the source is over, the source node sends a special control packet to request the destination to send its current neighbor set. If the two neighbor sets received by the source at the same time are different enough, it can be considered that they are generated by two different nodes. Thus the difference between the two neighbor set is compared with threshold value. If the difference is larger source node assumes that this network has thee black hole node. But this approach is unable to count the number of black hole nodes present in the current ad hoc network.

PROPOSED SOLUTION

This system proposes a new scheme for detection of selfish nodes. The detection is based on combination of diffusion of information on network and the information we get from local watchdog. The diffusion information consists of information about status of nodes whether it is selfish or not, this information is transmitted to other nodes when contact occurs. A selfish node does not take part in packet forwarding to save its resources. Generally local watchdog is used for detection of selfish nodes. The selfish node neither routes nor relays the packet.

Contact-based watchdog is combination of local watchdog and diffusion of information during contacts between nodes. A contact is an opportunity for two nodes to have enough time to communicate with each other.

Consider a scenario having 4 mobile nodes A, B, C and D and a selfish node S. Suppose that node A has detected the node S positive. When node B comes in contact with node A the node A will transmit the information about node S to node B. Now node B also has the status of node S as positive. Node C does not have any information about the S node, if node S makes its impression as negative node in front of node C then it will mark it as negative i.e. not a selfish node. Now node A and B has marked node S as positive i.e. selfish and node C marked it as negative i.e. not selfish. Node D do not have any information about the node S, it have several possibilities: if comes in contact with S node it may be able to detect it, if it contacts the node A and B it will mark it as positive but it comes in contact with node C it will mark it as negative i.e. a false negative.

Figure 2 shows the architecture of Contact-Based watchdog. The architecture has three main functions: Local Watchdog, Diffusion and Information update function. The local watchdog function is responsible for detection of new contacts and detection of selfish contacts.

The Local watchdog generates three events: PEvent when the watchdog detects a selfish node, NEvent when the watch dog detects that the node is node selfish and NoEvent when the node does not enough information about a node, this may happen if the contact time is less. New contact is based on watchdog detection i.e. by overhearing the neighbourhood packets.

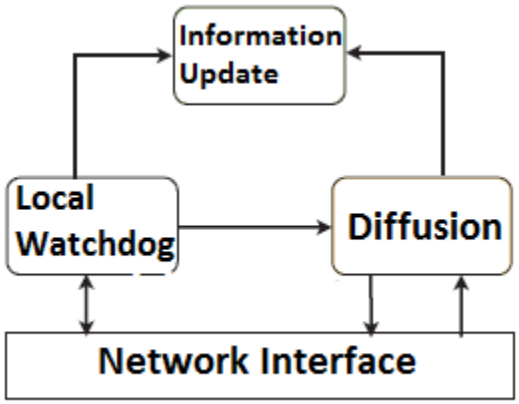

Figure 2: Architecture

The Diffusion module has two functions, the transmission and reception of both positive and negative detections. As a network has less number of selfish of nodes as compared to the legitimate users the positive detection is always transmitted with low overhead. But transmission of only positive detection may generate false positives thus the negative detections are also transmitted. A low value of negative detection factor is sufficient to neutralise the effect of positive detection. This information is transmitted to the new detection made by the local watchdog.

Information Update module consolidates and updates the information about the positive and negative detection. The state is updated when a PEvent or NEvent events are received from the diffusion and local watchdog module. These events update the reputation values. For a positive event the reputation value is increased by a factor and for a negative event it is decreased by the same value. We have a threshold value if the value of reputation is greater than the threshold value its status is changed to positive and if its value is smaller the status is changed to negative.

The threshold helps us to reduce the fast diffusion of false positive and false negative. The status is set to positive and negative has an expiration time and is updated if out of contact. That is the decision about a node is taken on the basis of most recent information.

CONCLUSION

This paper proposes a Contact-Based watchdog to improve the effectiveness for detection of selfish nodes. It also reduces the time required for detection of selfish nodes. Contact-based watchdog is based on diffusion of information when a contact with other node takes place, during this the information about known positive and negative is diffused which reduces the harmful effects of false positive, false negative and malicious nodes.

REFERENCES

[1] Nidhi Tiwari and Raghav Yadav, Detection of Black Hole Attack using Control Packets in AODV Protocol for Manet, International Journal of Computer Applications ,Vol. 118-No.24,May 2015
[2] Payal N. Raj and Prashant B. Swdesh, DPROADV: A dynamic leaning system against black hole attack in AODV based MANE, International Journal of Computer Science Issues (IJSI), Vol 2, 2009
[3] CoCoWa:A Collaborative Contact Based Watchdog for Detecting Selfish Nodes, IEEE transactions on mobile computing, Vol.14,No.6,2015

[4] Soufiene Djahel, Farid Nait-abdesselam and Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks:Proposals and Challenges,IEEE Communications surveys and tutorials Vol.13,No.4,2011
[5] Seryvuth Tan and Keecheon Kim, Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs, IEEE International Conference on High Performance Computing and Communications & IEEE International Conference on Embedded and Ubiquitous Computing, 2013
[6] Wang W, Bhargava B, Linderman M Defending against Collaborative Packet Drop Attacks on MANETs. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009).
[7] Deng Hougmei, Li Wei and P. Aggrawal Dharma, Routing Security in Wireless Ad Hoc Networks, University of Cincinnati,IEEE, 2009
[8] Mistry N, Jinwala DC, IAENG and Zaveri M, Improving AODV Protocol against Black hole Attacks, the International Multi Conference of Engineers and Computer Scientists, Hong Kong,2010
[9] B. Sun, Y. Guan, J. Chen and U.W. Pooch , Detecting black-hole attack in mobile ad hoc networks, presented at 5th European Personal Mobile Communications Conference, Apr. 2003, 490