International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 4 (April 2014), PP.29-34

Identification and Elimination of Selfish Nodes in Adhoc Network

Sheetal J. Nagar[1], Divan G. Raimagia[2], Pinaki A. Ghosh[3]
Department of Computer Engineering, Atmiya Institute of Technology and Science Rajkot, Gujarat, India

Abstract:- An Ad Hoc network is the network of self-configuring nodes without having fixed infrastructure. Each node acts as a system and router. Many of the routing protocols of Ad Hoc network are designed based on the assumption that every node forwards every packet but practically many of them act as selfish nodes, they use network and its service but don't cooperate with other nodes so as to save resources for themselves.

This report discusses the types of availability attack, malicious activity of selfish node, a Survey of techniques used to detect selfishness attack and some approach to detect selfishness attack. Here i have implemented the selfishness attack and analyze its effect on the Packet delivery ratio, End to End Delay and throughput. I have also implemented credit based algorithm to detect and overcome the activity of selfish nodes.

Keywords:- MANET, Selfish nodes, AODV, IDS, Watchdog

I. INTRODUCTION

An Ad Hoc network is the network of self-configuring nodes without having fixed infrastructure. Each node acts as a system and router.[1] Many of the routing protocols of Ad Hoc network are designed based on the assumption that every node forwards every packet but practically many of them act as selfish nodes, they use network and its service but don't cooperate with other nodes so as to save resources for themselves. This report discusses the types of availability attack, malicious activity of selfish node, a Survey of techniques used to detect selfishness attack and some approach to detect selfishness attack.

II. SECURITY REQUIREMENT IN MANET

To develop a reliable secure routing protocol that can work in the presence of Selfish nodes. To implement and analyze effect of availability attack on Ad hoc networks and implement detection methods. Develop a reliable trust based routing protocol which can detect the selfish nodes and prevents such nodes from disturbing the data transmission in AdHoc networks.

The purpose of this paper is to address the need of security in routing of wireless network. In AdHoc wireless networks due to lack of infrastructure and dynamic topology these networks are vulnerable for many attacks like Black hole, fabricated route, Resource consumption and Selfishness attacks. It is highly necessary to secure the routing of the Ad hoc network, which inspires to develop detection methods for Selfishness.

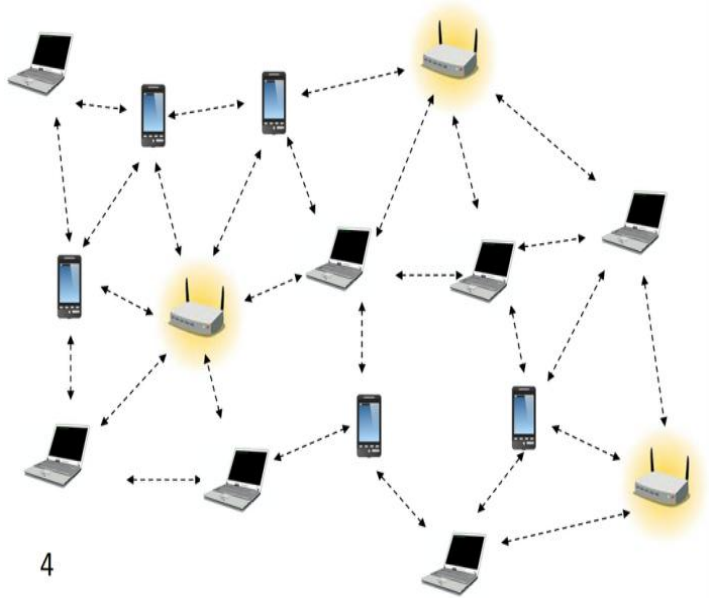

Fig. 1 Mobile Adhoc Network

III. ROUTING IN ADHOC NETWORK

Using limited recourses, routing helps to maintain routes between nodes in dynamic topology with preferably unidirectional links. Mobile Adhoc Network has multi-hop routes between nodes and may not use infrastructure. To find and maintain routes between nodes in a dynamic topology with possibly unidirectional links, using minimum resources. Routing in MANET can be divided into two parts: Table Driven Routing and On Demand Routing.

A. PRO-ACTIVE (TABLE-DRIVEN) ROUTING PROTOCOLS

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network[2].

Respectively more amount of data for maintenance and slow reaction on restructuring and failures are main disadvantages of such algorithms.

Table-driven protocols are: Destination-Sequenced Distance Vector Routing Proto-col(DSDV),Wireless Routing Protocol(WRP),Global State Routing(GSR),Hierarchical State Routing(HSR),Zone-based Hierarchical Link State Routing Protocol(ZHLS) and Clusterhead Gateway Switch Routing Protocol(CGSR)[2].

B. REACTIVE (ON-DEMAND) ROUTING PROTOCOLS

This type of protocol creates on demand routes because this type of protocols finds a route on demand by over owing the network with route request packets[2]. The problems with such algorithms are high lead time in route handling and excessive over owing can lead to network jam.

On-demand Protocols are: Ad-Hoc On-Demand Distance Vector Routing (AODV), Cluster based Routing Protocol (CBRP), Dynamic Source Routing (DSR), Tempo-rally Ordered Routing Algorithm (TORA)[2].

IV. AODV ROUTING PROTOCOL

The Ad-hoc On-demand Distance Vector (AODV) routing protocol is a routing protocol used for dynamic wireless networks where nodes can enter and leave the network.The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for dynamic wireless networks[3]. As the name suggest AODV builds routes between nodes as per the wish of source code. AODV is capable of both unicast and multicast routing. These routes are maintained by the time it is required by source node.

The source node transmits a Route Request (RREQ) to its immediate neighbors to find route to a particular destination node. The neighbor replies back with Route Reply (RREP) if the neighbor has a route to the destination. Otherwise the neighbors in turn rebroadcast the request. This continues until the RREQ hits the final destination or a node with a route to the destination. At that point a chain of RREP messages is sent back and the original source node has a route to the destination.[3]

1) Advantages: Here routes are established on demand and the latest route to the destination is found based on sequence number. So the connection setup delay is lower.

2) Disadvantages:Here, if source code sequence number is very old, the intermediate nodes may follow inconsistent route and the intermediate nodes have higher but not the Latest sequence number leads to stale entries. Multiple Route Reply packets in response to a single Route Request packet can lead to heavy control overhead.

V. VULNERABILITIES AND ATTACKS ON ADHOC NETWORKS

Nodes of mobile ad hoc networks have limited ranges and because of that it requires multi hop communication. Ad hoc network runs on an assumption that once the node has promised to transmit the packet, it will not cheat but this does not holds true when nodes in the networks have contradictory goals. Due to this, neighbors of intermediate nodes can use the reputation of intermediate nodes to transmission. Node mobility leads to frequent change in network topology.

Use of wireless links into network increases the risk of link attacks and so results in relatively poor protection. Long life of network requires distributed architecture. Risk of Denial of Service (DoS) attacks due to lack of infrastructure is present and chances of link breakage and channel can be there in AdHoc networks.

Attacks on networks come in many varieties and they can be grouped based on different characteristics.

A. Availability Attacks

Availability is the most basic requirement of any network. If the networks connection ports are unreachable, or the data routing and forwarding mechanisms are out of order, the network would cease to exist

[4]. Availability attacks can be of the following types:

1) Packet Dropping or Black-hole Attack[4]:In mobile ad hoc networks (MANETs), nodes usually cooperate and forward each other's packets in order to enable out of range communication. However, in hostile environments, some nodes may deny to do so, either for saving their own resources or for intentionally disrupting regular communications. This type of misbehavior is generally referred to as packet dropping attack or black hole attack.

2) Fabricated route Attack [4]: Fabrication attacks generate false routing messages. Such attacks can be di cult to confirm as invalid constructs, especially in the case of fabricated false messages that claim a neighbor cannot be contacted.

3) Resource Consumption Attack [4]: In this attack, a malicious node intentionally tries to consume the resources (e.g. battery power, bandwidth etc) of other nodes in the network. The attack can be of various types like unnecessary route requests, route discovery, control messages, or by sending stale information.

4) Selfishness Attack [4]: Selfish and malicious nodes participate in route discovery stage properly to update their routing table, but as soon as data forwarding stage begins, they discard data packets.

B. Confidentiality Attacks

Confidentiality describes the need to protect the data roaming in the network from being understood by unauthorized parties. Essential information is encrypted to achieve confidentiality by which, only the communicating nodes can analyze and understand it.

C. AuthenticityAttacks

Authenticity is crucial to keep eavesdroppers out of the network. With many services applicable in ad hoc networks, it is important to ensure that when communicating with a certain node, that node is really who/what we expect it to be (node authentication). Message authentication ensures that the contents of a message are valid.

D. IntegrityAttacks

Integrity of communication data helps to ensure that the information passed on between nodes has not been altered in any way. Data can be altered by two ways- intentionally and accidentally (for example through hardware glitches, or interference in the case of wireless connections).

E. Non-repudiation

Non-repudiation refers to the capability to guarantee that a party cannot deny the authenticity of their signature on a document or the sending of a message that they created.

VI. SELFISHNESS ATTACK

There are two types of uncooperativenodes[4]:

1. Malicious nodes and
2. selfish nodes.

Selfish nodes use the network but do not cooperate, saving battery life for their own communications. They do not intend to directly damage other nodes.

Malicious nodes aim at damaging other nodes by causing network outage by partitioning while saving battery life is not a priority.

A. Behaviours of Selfish Nodes

Selfish node can do the following possible actions in Ad hoc network:[5]

- Turn off its power when it does not have active communications with other nodes.
- Does not re-broadcast Route Request (RREQ) when it receives a RREQ.
- Re-broadcasts RREQ but does not forward Route Reply (RREP) on reverse route, therefore the source does not know a route to the destination and it has to rebroadcast a RREQ.
- Re-broadcasts RREQ, forward RREP on reverse route but does not forward data packets.
- Does not unicast/broadcast Route Error (RERR) packets when data packets are received but there is no route.
- Selectively drop data packets.

VII. IDS SCHEMES FOR SELFISHNESS ATTACKS

This IDS Schemes deal with problems of Selfishness on the packet forwarding in Mobile Adhoc Network.

A. End-to-end Acknowledgements[3]

This mechanism consists of monitoring the reliability of routes by acknowledging packets in an end-to-end manner, to render the routing protocol reliable. In this, the destination node gives acknowledgement of receipt of packets by sending a feedback to the source. This technique helps to avoid sending packets through unreliable routes and it can be combined with other technique. The problem with this is the lack of misbehaving node detection. This technique may detect routes containing misbehaving or malicious nodes and those which are broken, but without any further information regarding node causing packet loss.

B. Two-hop Acknowledgements[3]

This scheme uses asymmetric cryptography. It lessens Watchdog's problem related to power control technique usage.

C. Watchdog[7]

It aims to detect misbehaving nodes that don't forward packets, by monitoring neighbors in the promiscuous mode. The solution also includes pathrater component, that selects route based on the link reliability knowledge. The advantage of this scheme is it is able to detect misbehaving nodes in many cases, and requires no overhead when no node misbehaves. But it fails to detect misbehavior in cases of collisions, partial collusion and power control employment. It fails when two successive nodes collude to conceal the misbehavior of each other. It doesn't control detected misbehaving nodes.

D. Pathrater[7]

To check reliability of each path in the network, each node is preloaded with path rater. It gives the rate to path by averaging the reputation of each node of that path. If there are multiple paths to reach destination in network, the path which has highest rate is selected for transmission of packet.

E. Probing[4]

It is a combination of route and node monitoring. This approach consists of simply incorporating into data packets commands to acknowledge their receipt. These commands are called probes and intended for selected nodes. Probes are launched when a route that contains a misbehaving node is detected.

F. Friends and Foes[7]

In this, nodes are permitted to publicly claim that they are unwilling to forward packets to some nodes. Each node maintains basically three sets.

1. Set of friends-to which it is willing to provide services.
2. Set of foes-to which it is unwilling to provide services.
3. Set of nodes-known to act as if it is their foe(they don't provide service packets for it)named set of Selfish.

Advantages: It is used to secure control packet from dropping.
Disadvantages: Watchdog's problems remain same. It has more overhead.

G. Ex- Watchdog [4]

It is implemented with encryption mechanism and maintaining a table that stores entry of source, destination, and sum (Total number of packets+ the current node sends+ forwards or receives) and path. Its main feature is ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving.

Advantages: Solves problem of Watchdog.
Disadvantages: Fails when malicious node is on all paths from specific source and destination.

VIII. PROPOSED WORK

To detect the selfish nodes from the AdHoc Network, Watchdog mechanism can be used. A credit based approach for the nodes in Adhoc network is proposed. It works as follows.

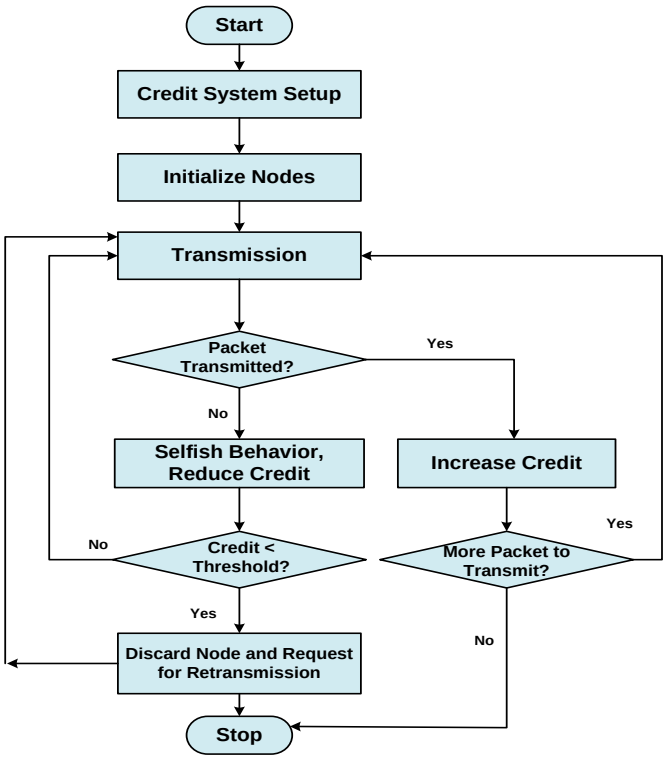

Fig. 2Flowchart for Credit Based Approach

In credit base system, all the nodes are initialized within the initial credit. Initially credit is same for all the nodes and all the nodes are treated equally. Then based on whether they are forwarding packets successfully or not, credit is increased or decreased. If a packet comes to a node and the node is transferring the packet successfully, then it's credit will be increased else the credit will be decreased, considering node's selfish behavior. The node will not be ignored just based on one unsuccessful transmission, but its behavior will be observed for some time, till its credit goes under threshold value. Once the credit will go under threshold value, that node will be ignored and next packets will not be given to it for forwarding.

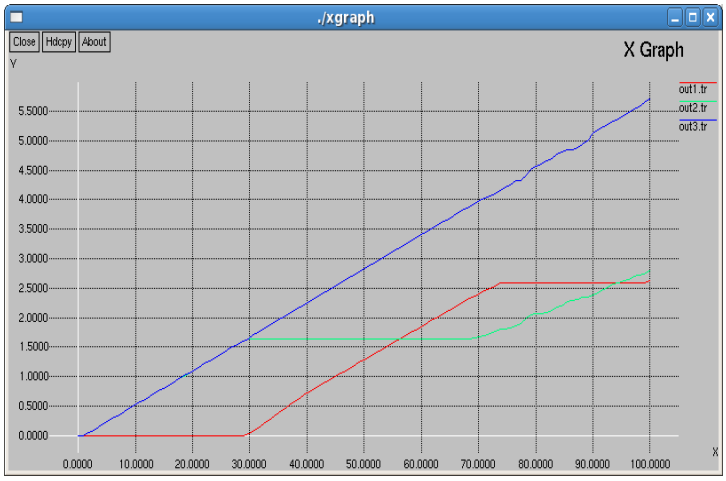

Fig. 3Result of Throughput in xgraph

After applying this approach, it is observed that PDR and throughput have increased and End to end Delay is decreased.

IX. LIMITATIONS

In this approach the selfish nodes are detected and eliminated from the network but they are not reintroduced in the network. An efficient MANET requires not only detection and elimination of such malicious nodes but it also requires mechanism to reintroduce the same.

X. CONCLUSION

Due to Mobility of node network topology cannot be maintained. The proposed approach enforces the nodes to cooperate. In the credit based approach the selfish nodes are punished for their malicious activity the non-malicious node are rewarded for their cooperation in network functionality. In presence of selfish node in routing, PDR and Throughput will be reduced and End to End Delay will be increased. For detection and prevention of the selfishness attack we have proposed the approach. After implementing the approach, PDR and Throughput will increase. Thus, Mobile Ad Hoc Network can be more efficient and secure after implementation of credit based approach.

REFERENCES

[1] RubanaTarannum, YogadharPandey, "Detection and Deletion of Selfish MANET Nodes-A Distributed Approach" IEEE 2012

[2] D.S.NishantChaurasia, Sanjay Sharma, "Review study of routing proto-cols and versatile challenges of manet",vol.1

[3] SandhyaKhurana, Neelima Gupta, NagenderAneja, "Reliable Ad-hoc On-demand Distance Vector Routing Protocol", IEEE, Jan 2003

[4] Niyati Shah, SharadaValiveti, "Intrusion Detection System for the Avail-ability Attacks in Ad-Hoc Networks", IJECSE,2011.

[5] Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog", IEEE, MAY 2012

[6] SangheethaaSukumaran, Venkatesh. J, Arunkorath, "A survey of method to mitigate selshness in MANET", IJICT Vol-1 No.2, June 2011

[7] DipaliKoshti, SupriyaKamoji, "Comparative Study of Techniques used for Detection of Selfish Nodes in MANET", IJCSE Vol-1 Issues-4,Sept-2011

[8] D.S.NishantChaurasia, Sanjay Sharma, "Review study of routing proto-cols and versatile challenges of manet",vol.1

[9] A novel approach for selsh node detection in MANETs: proposel and petri nets based modeling,8th IEEE internation conference on telecom-munication,2005

[10] AleksandarLazarevic, Vipin Kumar, JaideepSrivastava, "INTRUSION DETECTION: A SURVEY", Computer Science Department, University of Minnesota

[11] NiyatiShah,"Trust based Routing using IDS in Ad-hoc networks, Thesis report, May-2012

[12] PreetiNagrath,AshishKumar,ShikhaBhardwaj, "Authenticated Routing Protocol based on Reputation System For Adhoc Net-works",International Journal on Computer Science and Engineer-ing(IJCSE),Vol.2: 3095-3099,2010

[13] S.Tamilarasan,Dr.Aramudan, "A performance and Analysis of Misbe-having node in MANET using IDS",International Journal on Computer Science and Network Security(IJCSNS),Vol.11, May 2011

[14] SADIA HAMID KAZI, "Congestion control inMobile Ad-Hoc Net-works(MANETs)", BRAC UNIVERSITY, April 2011

[15] RubanaTarannum, YogadharPandey, "Detection and Deletion of Selfish MANET Nodes-A Distributed Approach" IEEE 2012

[16] Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog", IEEE 2013

[17] Sisily Sibichen1, Sreela Sreedhar2 "An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks", IEEE 2013

[18] Chee-Wah Tan, Sanjay Kumar Bose. "Modifying AODV for Efficient Power-Aware Routing in MANETs", IEEE 2007

[19] RakeshMatam, SomanathTripathy, "THWMP: Trust Based Secure Routing for Wireless Mesh Networks" ICCCS 2011

[20] Wenjing Lou, Wei Liu, Yanchao Zhang, YuguangFang , "SPREAD: Improving network security by multipath routing in mobile ad hoc networks" Springer 2007.