Secure Routing using Detection Method in Wireless Ad Hoc network

Ghada Vaseem J[1] Prof. Sharada Valiveti[2]
[1]M.tech(ICT) Student, Department Of Computer Engineering
[2]Associate Professor , Department Of Computer Engineering
[1,2] Nirma University, Ahmadabad, Gujarat

Abstract— An Ad Hoc network is the collection of multiple nodes which can work together and they can send data over multiple hopes without any infrastructure like base station and antenna. 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 paper 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.

Index Terms — Ad Hoc networks, Availability attacks, IDS (credit based and reputation based techniques*)*.

I. INTRODUCTION

An Ad Hoc network [1] is an infrastructure less network in which many nodes are interacts with each other over multiple hops without base station or access point. Network topology is not maintained due to mobility of nodes. So process of managing route information is of much importance.

To enforce cooperation between nodes, trust is necessary. 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. Sometimes, the node is not forwarding the packet because they want to save their battery resources. Selfish node can perform many malicious activities like remain in sleep mode, does not forward route reply (RREP), does not forward data packet, does not unicast or broadcast route error (RERR), selectively drop packet etc.. Selfish node can be handled either by punishing that node or by rewarding that node which are not selfish. This paper presents the survey of various selfishness attack detection scheme and approaches for handling it.

II. 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 [2]. Availability means that the network should be in operational mode in the condition of attack.

These are availability attacks:

1) Black hole attack [3]

Black hole attack is a denial of service attack in which a malicious node can attract all the packets claiming a fresh enough route to the destination and dropping all the packets reaching at that node.

A black hole has two properties. (a) The node uses the Ad Hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination, even though the route is fake, with the purpose of intercepting packets. (b) The node consumes the intercepted packets. In an Ad Hoc network that uses the AODV protocol, a black hole node absorbs the network traffic and drops all packets.

2) *Selfishness attack [3]*

Cooperation among nodes in Ad-Hoc Networks is an important issue for communication. But some nodes do not cooperate in communication and saves their energy. These nodes are called Selfish nodes. Selfish and malicious nodes participate in route discovery stage properly to update their routing tables, but as soon as data forwarding stage begins, they discard data packets.

3) Resource consumption attack [3]

By sending unnecessary control messages, route request, stale information, route discovery message, the malicious node intentionally consumes the resources (Battery Power and Bandwidth). In this attack, The Malicious node also consumes Power and bandwidth by sending replication message. Hence lifetime of network gets reduced.

4) Fabricated route attack [3]

Fabrication attacks generate false routing messages. Such attacks can be difficult to confirm as invalid constructs, especially in the case of fabricated false messages that claim a neighbor cannot be contacted.

III. SELFISHNESS DETECTION

Basically there are two main techniques for preventing selfishness attacks. These techniques fall under the category of Trust based Routing. Selfish nodes are required to be handled through their property of selfishness only. Hence two methods are specified in literature:

1) *Credit Based Schemes [4]*

In this scheme for enforcing cooperation in performing the network function faithfully, credits are provided to the node. In the form of virtual currency based system is a node is getting some fixed amount of credit for forwarding the packet to next node and that node also pays some credit to its next node for cooperation. To implement this approach there are two models. 1. Packet Purse Model (PPM) and 2. Packet Trade Model (PTM). In PPM, the sender who is initiator pays some credit for getting packet forwarding service, this packet forwarding charge is distributed among

all forwarding nodes, initially the sender loads the packets with some credits which are enough to reach destination. At each intermediate node, packet should have some basic credit to get service. If it doesn't have enough credit then that packet is discarded. The main problem with this approach is to predict the total number of credits required for whole transmission of packet from source to destination. In PTM packet doesn't carry the credit but the packet are traded for credit by intermediate nodes. Each intermediate node takes some credits from previous node and pays it to next node. Total credit required for whole transmission is covered by destination. The problem of PPM is solved here; source node doesn't require predicting the total number of currency for service

2) Reputation Based Schemes [4]

In such schemes, reputation of each node of networks is measured and based on this, it is decided whether the node is malicious or not. After this the selfish node are discarded. There are two models for reputation based schemes.

1. Watchdog Model [4]
2. Path rater [4]

Watchdog:

Figure 1 shows watchdog Model. As shown in Figure 1, suppose a path exists from node S to node D through intermediate nodes A, B, and C. Here we can't send packet directly from node A to C. To send packet from S to D, A sends packet to B and then node B sends it to C. This way packet will reach to destination. Here each node maintains a buffer for recently sent packets to check the match. If the match is found, the packet is removed from buffer and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer time, the watchdog considers it as failure and increments a failure counter for the node responsible. If the tally exceeds a certain threshold bandwidth, it means that the node is selfish and about it the notification is sent to source node. The problems with watchdog are power limitation, collision at receiver, ambiguous collision and partial dropping.

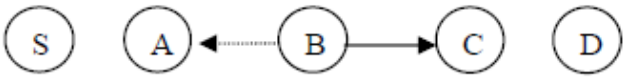

Figure -1 Watchdog scheme [4]

Path rater:

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. Table 1 shows the various methods for detecting selfish nodes in Ad Hoc networks

Scheme	**Description**	**Advantage**	**Disadvantage**
End-to-end Acknowledgments [5]	Monitoring the reliability of route by end to end acknowledgments	Avoid sending packets through unreliable route	Lack of Misbehaving detection
ABO(Activity based overhearing) [5]	Generalization of watchdog	Increase the number of observation and improve watch dog efficiency. It mitigate collision problem.	–
Two hop acknowledgments. [5]	It uses asymmetric cryptography	Mitigate power control technique usage problem of watchdog	–
Probing [5]	Combination of route and node monitoring	Probe packet for selected node to detect misbehavior	When selfish get probe packet, it choose to cooperate and forward packets for limited time.
CORE(collaborative reputation) [5]	It can be applied to both data and request packets forwarding function	Watchdog for monitoring both directed and broadcasted packets.	Watchdog's drawbacks are present.
CONFIDANT [5]	Cooperation of nodes and fairness in dynamic ad hoc network	Four components in each node. - Watchdog monitor -Trust	- Watchdog's problem - Reputation exchange process can cause overhead

		manager - Reputation system -Path manager	
Friends and foes [5]	Set of friends and foes	-it is used to secure control packet from dropping	-watchdog ‘s problem -More overhead -Mobile selfish node cannot detect
Ex-Watchdog [3]	- Maintaining table (source,dest,total no. of packets) -detection of malicious node which can partition network	Solve problem of watchdog	Fails when malicious node is on all path

Table -1 Study of Techniques for detection of selfish node

IV. PROPOSED APPROACH

Here we propose two approaches to enforce cooperation with Selfish Nodes:

A. Approach – I

In first approach we will use reputation based system to detect selfish node. This approach helps to detect selfish node, encourages and enforces the selfish node to cooperate. This approach works in three phases to detect selfishness. In Phase one, Monitoring and observing the behavior of one hop nodes is done by each node using its own watchdog module. And then it keeps the information about the number of packets sent and received by each node. After every specific time interval, watchdog upgrades the saved information. In second phase, a cooperation coefficient A is calculated which is same as the reputation of that node. This reputation coefficient of any node is measured by taking the proportion of Number of sent packets and Number of received packets. This coefficient is a number whose value may be between 0 and 1. The low coefficient value of node which is near to zero indicates that the node is selfish node and the high value of coefficient which is near to one indicates the high cooperation of that node. After calculating the reputation one new additional field is added to the header of routing protocol. Here each node has the table for maintaining the reputation. In phase three, priority of node for processing packets is decided. The node whose reputation value is high ,has the higher priority for getting network services like sending packets while the node which has low reputation value will get low priority for getting services.

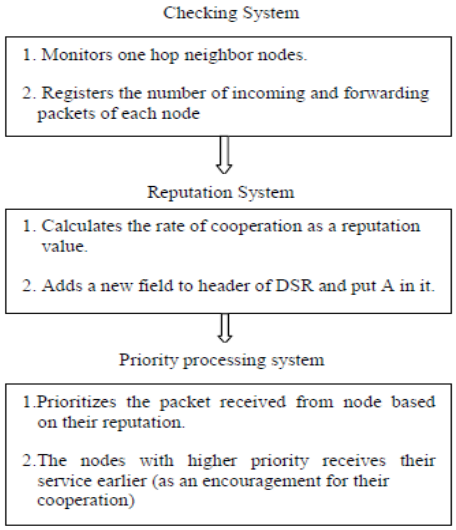

Figure-2. Flow diagram for reputation coefficient based mechanism.

B. Approach – II

In second approach we will use credit based system. It will encourage and enforce the selfish nodes to cooperate. In this approach virtual currency system will be setup for node to perform networking operation faithfully. Here each intermediate node is paid for forwarding packets of another node and the originator have to pay them. In this approach, initially each node is preloaded with some fixed credit. For every communication a fixed amount of virtual currency would be deducted from the sender’s account and will be distributed evenly distributed among the intermediate nodes. Here the selfish node are not punished but the intermediate nodes are rewarded the currency for cooperation. The drawback of this approach is that the selfish node can attract more routes through it by flooding wrong message of strong routes and after this it can perform malicious activity on the packets.

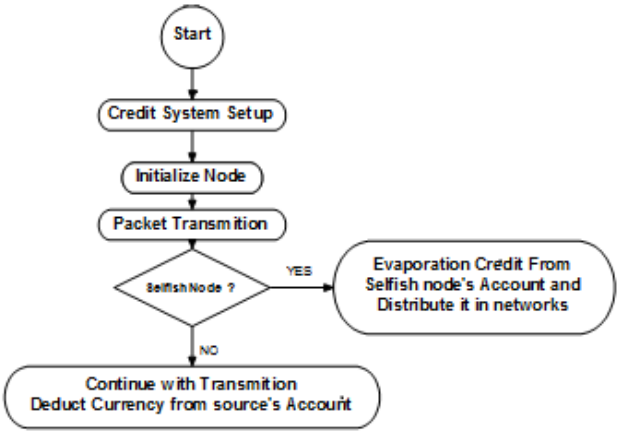

Figure-3 Flow Chart for Credit based mechanism.

V. PACKET DROPPING ATTACK

Step-1

Define a node as malicious node in tcl file
$ns- at 0.0 "[$node-(0) set ragent-] hacker"
$ns- at 0.0 "$node-(0) label \"Malicious Node\""

Step-2

Now check the index of malicious node and packets type weather it is same as tcl file or not and the packet is data packet or not. If the condition is satisfied than make the ttl (time to live) of data packets as zero and then drop the packets by calling drop () function and increase the drop index value by one. Now declare as selfish node when packet drop index value cross the some maximum threshold.

```
Static into d [5000];
Void forward ()
{   if (index==4 && ch→ptype()!=PT_AODV)
    { ih→ ttl=0;  }
    If (ih→ttl==o)
    {  d[index] = d[index] +1;
       Drop(p,DROP-RTR-TTL);
    }
    If (d[index] > 25)
    {
    Printf ("index= %d" is malicious node,index);
}   }
```

VI. SIMULATION & RESULT

PROPERTY	VALUE
Simulator	NS-2.34
Nodes	25
Simulation Time	600
Mobility Model	Random Way Point
Coverage area	1000m * 1000m
Mobility speed	10m/s
Pause time	2.0 sec
Connections	15
Traffic Types	Constant Bit Rate
Packet size	512 bytes

Table -2 Simulation Parameters

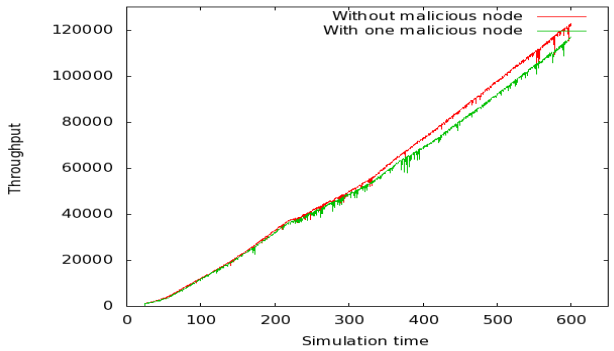

Figure -4 Throughput Comparisons

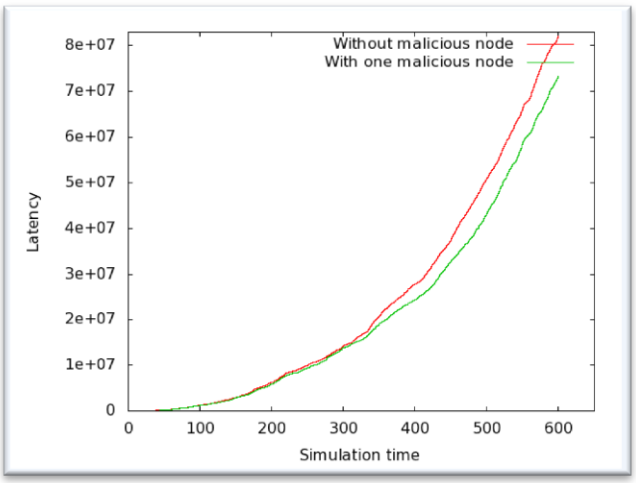

Figure-5 Latency Comparison

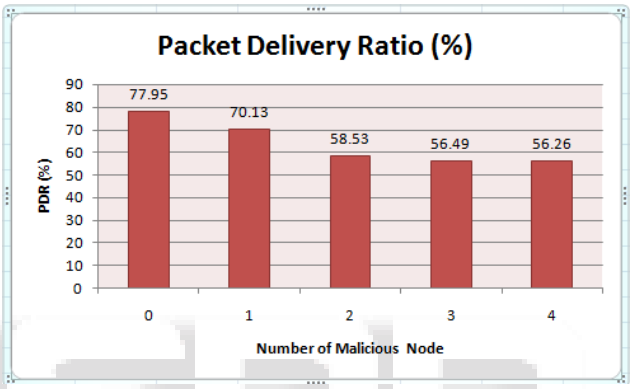

Figure -6 PDR Comparisons

VII. CONCLUSION

In this paper we have discussed types of availability attack in wireless Ad Hoc network. This paper presents the role and malicious activity of selfish node in network and a survey of intrusion detection system for selfishness attack in Ad Hoc network. Here Reputation and Credit based, two main detection techniques and their module are discussed in detail. In addition two algorithms for selfishness detection are proposed, one of them credit based and another one is reputation based system. In reputation based approach the selfish nodes are punished for their malicious activity and other nodes are getting batter priority for their reputation where in credit based approach instead of punishing the malicious node, the non-malicious node are rewarded for their cooperation in network functionality. Here from the result we can conclude that in the presence of malicious node Packet Delivery Ratio and Throughput decrease. With the help of the proposed approach we can improve that both the factor.

REFRENCES

[1] A.P. Yih-chun Hu, David B. Johnson, "Sead: Secure efficient distance vector routing for mobile wireless Ad Hoc, networks,"2003.
[2] A.Burg," Ad hoc network specific attacks,"2003.
[3] Niyati Shah, Sharada Valiveti,"Intrusion Detection System for the Availability Attacks in Ad-Hoc Networks,"2011.

[4] Djamel Djenouri, Nadjib Badache,"MANET: Selfish Behavior on Packet Forwarding", Encyclopedia of wireless and Mobile communication, 2008
[5] Marti,Giuli,Lai,Baker,"Mitigating routing misbehavior in mobile adhoc networks",ACM conference on mobile computing and networking,2000
[6] Kargl,Klenk,Weber,Schlott,"Advance detection of selfish or malicious node in adhoc networks", 1st European workshop on security in adhoc and sensor networks,2004.
[7] Djenouri, Badache," A novel approach for selfish node detection in MANETs: proposel and petri nets based modeling",8th IEEE internation conference on telecommunication,2005
[8] Awerbuch,Holmer,Nita,Rubens,"An on demand secure routing protocol resilient to byzantine failure",ACM workshop on wireless security,2002
[9] Michiardi, Molva, "CORE: collaborative reputation mechanism to enforce node cooperation in MANET", 6th IFIP communication and multimedia security conference, 2002