Reputation-Based Security Protocol for MANETs

Mohammed Mujeeb, Sudhakar K N, Jitendranath Mungara

Abstract: Mobile Ad-hoc Network is huge area for research with practical applications. It is a infrastructureless and self-organized network, vulnerable because of its characteristics such as open medium, distributed cooperation and it is difficult to predict the topology. In general, Routing security in MANETs appears to be a challenging task. In this article we study the routing security issues of MANETs, and analyze in detail — the "Blackhole" attack. We come with distributed reputation mechanism that improves security in MANETS. Some optimization to the current reputation scheme used in MANETs are one is Selective Deviation tests and second is Adaptive expiration timer that aims to deal with congestion and quick reputation convergence. Cryptographic mechanisms such as Digital signature and hashing technique are used for the authentication of the packets in network. We design and build our proposed protocol over existing AODV and test in Network Simulator-2 in the presence of variable active Black hole attack. By using proposed Secure AODV (RSAODV) protocol we achieve increased throughput by decreasing packet delivery delay and packet drop.

Keywords: MANET, RSAODV, Black hole, Routing, Digital Signature, Hashing

I. INTRODUCTION

Mobile Ad-hoc Network is composed of a multiple number of mobile nodes and is a self configuring infrastructure less network. In MANETs each node is a trans-receiver; it will accept the packets as well as forward it. Achieving secure routing in MANET is one of the challenging tasks because in such network, nodes are continuously moving and nodes are power constrained due to their limited battery resource. We incorporate our protocol within Existing Ad-Hoc On-demand Distance Vector (AODV) protocol. The aim is to find the secure route from source to destination.

The proposed protocol is named as Reputation based security protocols because, we are achieving secure routing by computing the reputation of each node. Reputation of a node is computed based on the number of authenticated packets it is going to forward in the network and how cooperatively it behaves in the network. Based on reputation of the node we are deciding whether to trust a particular node or not and this will help in choosing the nodes in routing secure path.

Revised Manuscript Received on 30 July 2012

***Correspondence Author(s)**

Mohammad Mujeeb*, M.Tech, Department of Computer Science and Engineering, CMRIT, Bangalore, India.

Mr. Sudhakar K N, Associate Professor, Department of CSE, CMRIT, Bangalore, India.

Dr. Jitendra Nath Mungara, Professor and Dean, Department of CSE and ISE, CMRIT, Bangalore, India.

A. Blackhole Attack:

A more aggressive attack where the malicious node is not only silently dropping the data packets and also actively reply to topology discovery requests and advertise itself as an attractive route to destination. This doesn't only cause the malicious nodes to intercept and drop the data packets but also to disrupt communication needed between other good nodes.

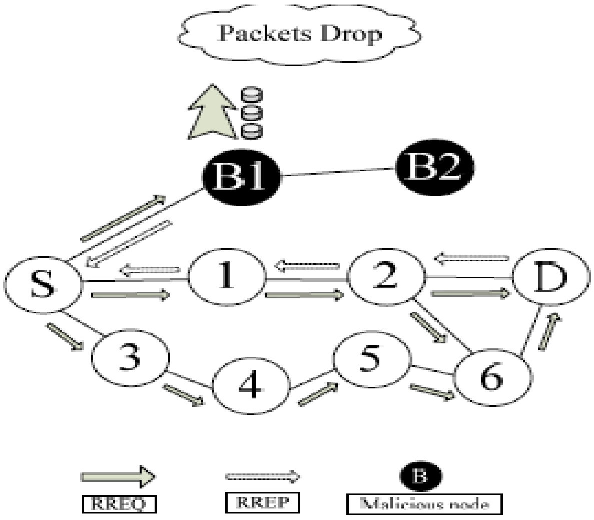


Figure 1 Blackhole attack in MANETs

Where 'S' is source, 'D' is destination, 'B1' and 'B2' are black hole nodes. When the source node broadcasts the RREQ message to all nodes ,the nodes which have the destination address in their routing table ,those send the RREP message to source and the nodes which doesn`t have the destination address will broadcast the RREQ further. When the blackhole node get the RREQ message it actively sends the RREP message to the source that it is having the shortest path to the destination, but actually it is not true and drops the packets which come to it.

II. REVIEW OF LITERATURE

Distributed reputation has been used in both MANETs and P2P networks. "Collaborative Reputation" technique in MANET [4] proposed a watchdog for monitoring and isolating selfish nodes based on a subjective, indirect and functional reputation. This will consume more time for the identification of attacks. Existing system is concerned about the passive blackhole attack, where the malicious node is silently dropping the traffic into the network. This doesn`t only cause the wastage of network resources but decrease the life time of the networks.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

In the peer-to-Peer file-sharing, reputation is used to reflect the ratings of different users and distributed Eigen-Vector [7] has been proposed to calculate trust in a distributed Peer-to-Peer environment. Eigen Trust algorithm that assigned each peer a unique global trust value, based on the peer's history of uploads. Eigen Trust used 1 or -1 to represent user's satisfaction or dissatisfaction about the download transaction respectively. But in case of MANETs nodes are always mobile and we need to know each and every node`s reputation value to have decisions based on routing value. The existing system it is difficult to gather the reputation value of other nodes and have quick routing decisions.

III. PROPOSED WORK

In our proposed work we compute reputation of each node based on authenticated packets transmitted by a particular node and its cooperative behavior in network. There are two methods to collect reputation information, through direct observation of its neighbors (subjective observation) and gathers indirect (second hand) reputations from all other neighbor nodes. Based on the observations, our protocol uses reputation discounting to ensure that old reputations will fade away giving more chance for nodes to recover their reputation by consistently behaving cooperatively. We use secondary response to retaliate against any neighbor who originally had a bad reputation, if this neighbor shows early sign; then won`t consider that node while choosing the path. We employ deviation test and noise cancellation.

Proposed work is with Eigen vector centrality in order to elect the most influential nodes to assist in the role of helping other nodes to build their reputation into other less popular nodes in the network and act as community leaders. Nodes which have higher centrality have higher probability of getting in contact with many other nodes than nodes with low centrality. We identify the nodes that have both high centrality and good reputation as preferred sources for indirect reputation. This becomes even more important in high-mobility networks, as nodes often have few connections –if any- at any point in time, these connections are changing frequently which causes more uncertainty. In our system, we used the degree centrality to inform the reputation aggregation module to provide higher weights for highly reputed nodes. This has lead to fast reputation convergence due to the incorporation of high quality data from more central node and emphasizing on the importance of these node`s opinion about other nodes in the network. Nodes with higher centrality and higher reputation nodes are prime nodes to give highly trusted opinions about nodes in MANET in a self-organized manner.

Figure 2 shows an example of how we use Eigen-Vector reputation-based centrality to influence nodes decision about the reputation of other nodes and the importance of indirect-reputation exchanged between nodes. Node B is the observed node and each of its neighbors Node1 to Node 5 has a direct reputation measure for it as R1 to R5 respectively. Node A that is not directly connected to node B receives R1-R5 reputation observations about Node B. By applying the Eigen-Vector reputation-based centrality, , node A will have a centrality measure based on all Node B's neighboring nodes reputation evaluation of that node. Using this technique makes Node A immune against an attack where one node would collude with multiple other nodes to provide false indirect reputation about node B, as indirect reputation reported by

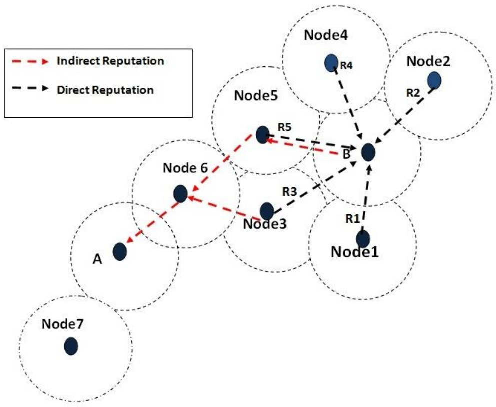
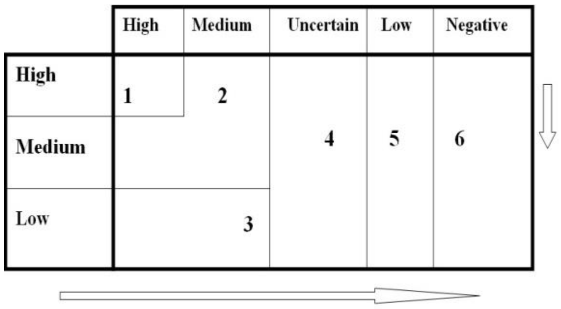


Figure 2 Eigen-Vector Reputation-Based Centrality.

When we resolve node's reputation as a function of its centrality characteristics, we classify the nodes as high, medium, low centrality and negative. Fig 3 below shows how we classify the observed nodes into zones based on their reputation and centrality. Nodes falling into zone 1 are highly trusted nodes that also have wider view of the network. Nodes which are classified as belonging to that zone have privileges such as higher watchdog expiration time and they are exempted from the deviation tests on their reported indirect-reputation, low or no discounting factor, and high Reputation-Record expiration time. On the other hand, nodes falling into zone 6 are classified as negative nodes called miss-behaving nodes, so their reported indirect-reputation is rejected. Nodes falling in zones between 1 and 6 would have different levels of acceptance and the different parameters would be adjusted to reflect their current zone. Nodes classification can change over time. This can be a result of a good reputation node that started to behave maliciously and hence become less trusted and fall to a less favorable zone.

Less Reliable



	High	Medium	Uncertain	Low	Negative
High	1	2	4	5	6
Medium					
Low		3			

Less reliable indirect reputation due to the node's bad reputation.

Figure 3. Self-Organized node selection for indirect-reputation information

Reputation is computed based on the number of authenticated packets that a node is going to forward and its cooperative nature in the network. The authenticated packets are identified by cryptographic techniques Digital signature and Hashing techniques [14].

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Advantages:

1) Our proposed work differ from the existing work and by using the Eigen trust and Degree centrality concepts we can have individual trust claims and take routing decisions easily with minimum time.
2) Our reputation based security protocol is concerned with the active black hole attack with cryptographic techniques like Digital signature and hashing techniques.
3) Avoids the wastage of network resources and increase the network life time.
4) The applications like eCommerce: eBay, Email: anti-spam techniques, Personal Reputation: PersonRatings.com, we can provide more security.

IV. REPUTATION SYSTEM ARCHITECTURE

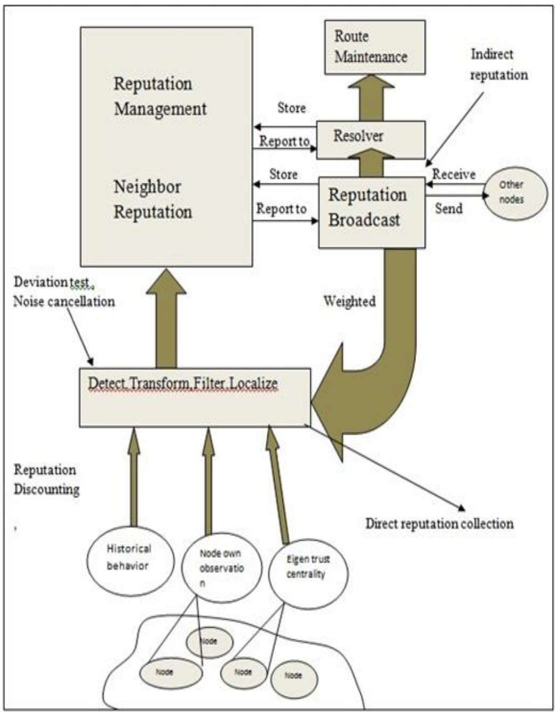


Figure 3 Reputation system model.

The architecture of reputation model in order to provide automatic and autonomous routing decisions to the under-laying routing protocol based on the available neighbors' reputations.

First entity is *Reputation Management that* is responsible for storing and retrieving all the node's neighbors' reputation records. It acts as the concentrating point for all the events taking place inside the system.

Second entity is *Neighbor Reputation* Record is the entity representing direct reputation or reputation observation for one of the neighbor. Each and every node holds M neighbor reputation records where M can be determined by the node's memory, power of CPU for maintenance to update these records.

Third entity is *Reputation Broadcast* is the entity responsible for receiving indirect reputation from neighbors. In Selective deviation Test, the observing node '*a'* attempts to calculate the reputation of its neighbor node '*j'*. Node '*a'* first checks the reputation of the reporting node (the sender of the reported reputation information) node 'i'. R_{ai} is the reputation held by node '*a'* about node 'i'. If the reputation R_{ai} > (threshold) then R_{ij} is trusted without further tests.

Fourth entity is *Reputation Detect, Filter, Transform and Localize:* The actual calculation of the direct reputations was inspired by the Eigen Trust algorithm [9] .Our algorithm calculates a global consistent reputation value at each node for all its neighbors and then resolves the reputation using direct and indirect (second hand) reputation information. The calculation is discussed in the Mathematical model.

Fifth entity is *Resolver* is responsible for doing the the calculation of the neighbor final reputation (called final resolved reputation (FRR)) by combining direct and indirect reputation (Error! Reference source not found.) and performs Reputation Noise Cancellation.

Last entity is Route Maintenance procedure, nodes keep an entry for each active route in their route table and periodically broadcast *hello* message to its neighbors in order to detect possible link failure. If a node detects a link failure, it would know that all active routes via this link would fail, so a Route Error message (RERR) is send to announce all relative source nodes. The source nodes then will decide whether to refresh the route or not. The RERR message contains the following items:

```
Basic AODV Routing
Source Node broadcasts RREQ
Source Node receives RREP
IF (RREP is from Destination Node or a reliable node) {
Route data packets (Secure Route)
 }
 ELSE {
 Do {
Send Further Request and Identity of the node of Intermediate Node to Next Hop Node
Receive Further Reply, Next Hop Node of the current Next Hop Node, Data Routing Information entry for
Next Hop Node's next hop, Data Routing Information entry for current Intermediate Node
IF (Next Hop Node is a reliable node) {
Check Intermediate Node for black hole using Data Routing Information entry
IF (Intermediate Node is not a black hole)
Route data packets (Secure Route)
ELSE {
Insecure Route
Intermediate Node is a black hole
All the nodes along the reverse path from Intermediate Node to the node
that generated Route reply are black holes
         }
      }
ELSE
Current Intermediate Node = Next Hop Node
   }
While (Intermediate Node is NOT a reliable node)
   }
```

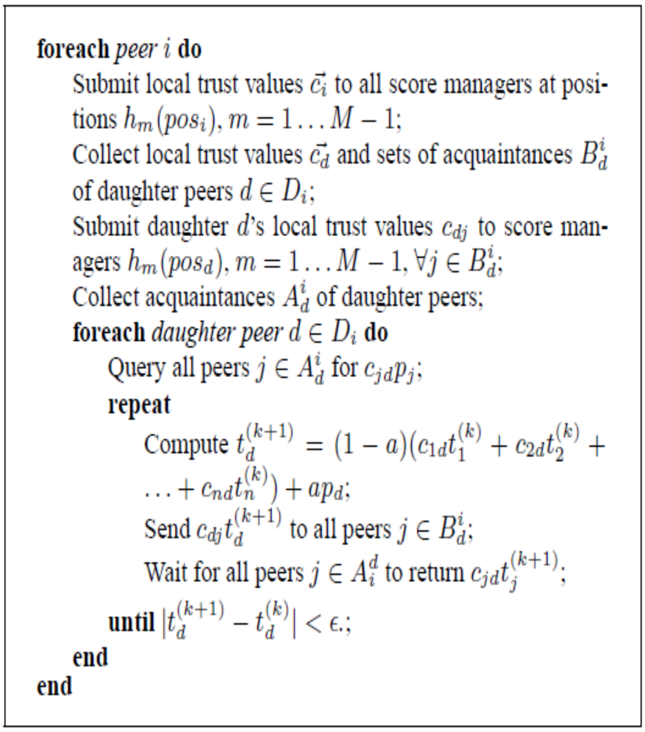
Eigen trust Algorithm:

Here we describe the Eigen trust algorithm to compute a global trust value. We use these definitions: Each peer has a number M of score managers, whose DHT (Distributed hashing table) coordinates are determined by applying set of one-way secure hash functions

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

$h_0, h_1, \ldots, h_{M-1}$ to

the peer's unique identifier. pos_i are the coordinates of peer **i** in the hash space. Since each peer also acts as a score manager, it is assigned a set of daughters Di - the set contains the indexes of the peers whose trust value computation is hold by the peer. As score manager, peer **i** also maintains the opinion vector c^i_d of its daughter peer d (where d € Di) at some point in the algorithm. Also, the peer **i** will learn $\mathbf{A^i_d}$ which is the set of peers which have downloaded files from its daughter peer **d** and it will receive trust assessments from these peers referring to its daughter peer d. At last peer **i** will get to know the set B^i_d, denotes the set of peers which its daughter peer d has downloaded files from: Upon kicking off a global trust value computation, its daughter peer **d** is supposed to give its trust assessments on other peers to its score manager with $\mathbf{B^i_d}$.



```
foreach peer $i$ do
    Submit local trust values $\vec{c_i}$ to all score managers at positions $h_m(pos_i), m = 1 \ldots M-1$;
    Collect local trust values $\vec{c_d}$ and sets of acquaintances $B^i_d$ of daughter peers $d \in D_i$;
    Submit daughter $d$'s local trust values $c_{dj}$ to score managers $h_m(pos_d), m = 1 \ldots M-1, \forall j \in B^i_d$;
    Collect acquaintances $A^i_d$ of daughter peers;
    foreach daughter peer $d \in D_i$ do
        Query all peers $j \in A^i_d$ for $c_{jd}p_j$;
        repeat
            Compute $t_d^{(k+1)} = (1-a)(c_{1d}t_1^{(k)} + c_{2d}t_2^{(k)} + \ldots + c_{nd}t_n^{(k)}) + ap_d$;
            Send $c_{dj}t_d^{(k+1)}$ to all peers $j \in B^i_d$;
            Wait for all peers $j \in A^d_i$ to return $c_{jd}t_j^{(k+1)}$;
        until $|t_d^{(k+1)} - t_d^{(k)}| < \epsilon$.;
    end
end
```

All the local trust values are gathered from each nodes. At each the following expressions are executed. Each node calculates the Eigenvector centrality of its neighbors in order to reflect on each neighbour reputation value and the level of confidence in this neighbor reported indirect reputation. In equation (1) x_i represents the score in the ith node. Let A_{ij} be the adjacency matrix of the network. A_{ij} is originally defined in Eigen-Vector Centrality as $A_{ij} = 1$ if the ith node is adjacent to the jth node, and $A_{ij} = 0$ otherwise. In our model, $A_{ij} = s$, where s is the wireless signal strength from the ith node to its neighbor jth node, and $A_{ij} = 0$ if the i and j are not neighbors. For the ith node, the centrality score is proportional to the summation of the scores of all nodes which are connected to it.

$$x_i = \frac{1}{\lambda}\sum_{j \in M(i)} x_j = \frac{1}{\lambda}\sum_{j=1}^{N} A_{i,j}x_j \qquad (1)$$

In equation (1), M(*i*) is the set of nodes that are connected to the ith node, N is the total number of nodes and λ is a constant. The connectivity of node takes place when the node either receives or requests a forward of a message from that neighbor. In our distributed network environment, each node marks its experience when it comes into contact (i.e. becomes connected) with another neighbor. Periodically, each node will evaluate its connectivity experience with each of its direct neighbors and gives it a rating and vice versa (2). Node *i* calculate the percentage of packets that are originating from *i* and that were forwarded by node *j* over the total number of packets offered to node *j*, *frwd(i,j)*, and the percentage of packets that were expired over the total number of packets offered to node *j, expr(i,j)*.

$$S_{ij} = \text{frwd}\ (i,j) - \text{expr}\ (i,j) \qquad (2)$$

Where S_{ij} denotes the recent satisfaction index for node *i* about node *j*. *Sij* would be then weighted (using (3) into the direct reputation of node *j*:

$$R_{ij} = R_{ij\text{-Prev}} * W_{\text{history}} + S_{ij} * (1 - W_{\text{history}}) \qquad (3)$$

$R_{ij\text{-}prev}$ is reputation value that node *i* had for node *j* before incorporating the most recent satisfaction index. $W_{history}$ is a constant that reflects the level of confidence that node *i* has in the past observed reputation for its neighbor *j (i.e.* whether the past reputation $R_{ij\text{-}prev}$ reflects a persistent behaviour). If no connectivity between *i* and *j*, R_{ij} is discounted instead using a constant value: $W_{discount.}$ We define max *t* to be the function that reports the maximum observation of R_{ij} over time. R_{ij} is normalized using (4).

$$R_{ij} = \frac{R_{ij}}{\text{Max}_t\ (R_{ij})} \qquad (4)$$

Adaptive Expiration Time is the time that a node waits for its direct neighbor to perform the requested function before a watchdog times-out and penalize that neighbor for its failure (i.e. forward the packet). Nodes are able to monitor their neighbors' behavior by utilizing the shared nature of the wireless medium and constantly overhearing its neighbors' traffic. We propose a per neighbor/adaptive expiration technique that allows a node to adjust the time depending on its neighbor reputation and network conditions. For trusted neighbors, the observation expiration time would be higher than for non-trusted neighbors.

Indirect or second hand reputation received by the observing node *i* is aggregated in equation (5) to a single value ARR_{ij} (Aggregated Reported Reputation).

$$ARR_{ij} = \frac{\sum (RR_{nj} * Dig_n * RR_{in})}{\sum (Dig(n) * RR_{in})} \qquad (5)$$

Where ARR_{ij} is aggregated reported reputation about node *j* as received and processed by node *i*), Dig(*n*) is the degree centrality of the reporting nodes(*n*).

Depending on the node's own knowledge about the medium quality reported by the node's physical layer, the node is able to adjust the threshold of acceptable silent error level from that neighbor. When the node experiences a packet loss from its neighbor below this threshold, it considers that packet loss as a noise and subsequently ignores it. If the losses is greater than noise threshold level, node will start reacting to these events accordingly. We call this approach "Reputation Noise Cancellation".

$$FRR_{ij} = W_{direct} * R_{ij} + (1 - W_{direct}) * ARR_{ij} \qquad (6)$$

Where FRR= Final Resolved Reputation.

In Route Maintenance procedure, nodes keep an entry for each active route in their route table and periodically broadcast *hello* message to its neighbors in order to detect possible link failure.

If a node detects a link failure, it would know that all active routes via this link would fail, so a Route Error message (RERR) is send to announce all relative source nodes. The source nodes then will decide whether to refresh the route or not.

SIMULATION RESULTS

We have performed experiments in MANETs where network experienced frequent neighborhood changes and lower route stability. We have integrated our reputation-based protocol with existing AODV and we named as RSAODV. Our simulation scenarios included 20 mobile nodes randomly moving around simulation area. Table1 shows a list of simulation setup parameters and other system configuration variables .Here we are varying two parameters i,e Number of attackers and simulation time keeping rest of the parameters as constant.

Parameter	Value
Area	750X750
Speed	20 m/s
Radio Range	250 m
Placement	Uniform
Movement	Random waypoint model
Routing Protocol	RSAODV
MAC	802.11
Sending capacity	4 kbps
Application	CBR
Packet size	512 B
Simulation time	500 s
$W_{discounting}$	0.9
Reputation Threshold	0
Publication timer	10s
Re-evaluation timer	10s
Fading timer	10s
$W_{history}$	0.70
W_{direct}	0.90
Deviation threshold	0.5

As per the parameters node speed is set to 20m/s and pause time is 1sec.There is 20% of blackholes used in the scenario.

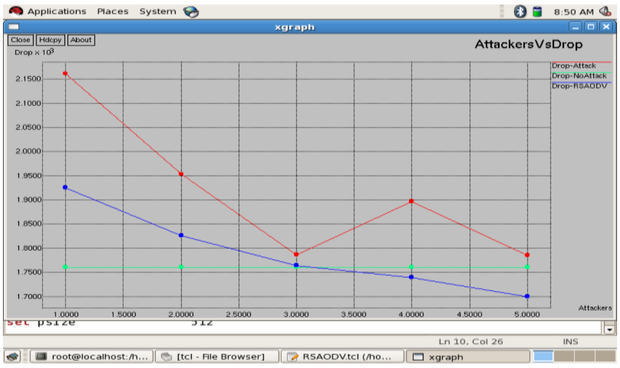


Figure (a) Attacker Vs Packet Drop

The fig (a) shows the comparison of Drop in case of there is No-attack, Attack and with the RSAODV protocol. From results we can justify in case of No-attack there will packet drop than in case of attack no packet drop and in case of presence of attacker there will be more packet drop and with that of the RSAODV protocol, we can reduce packet drop. The following fig (b) is the Time Vs packet here we can see the packet drop is reduced.

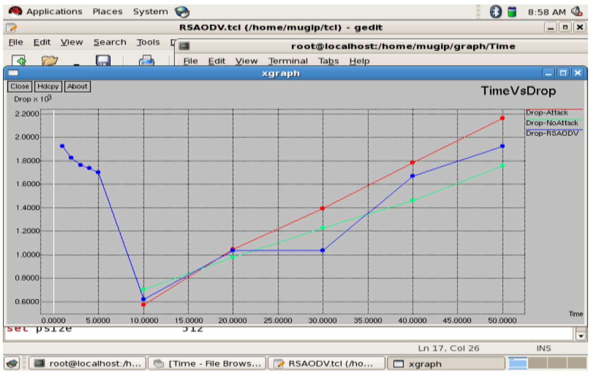
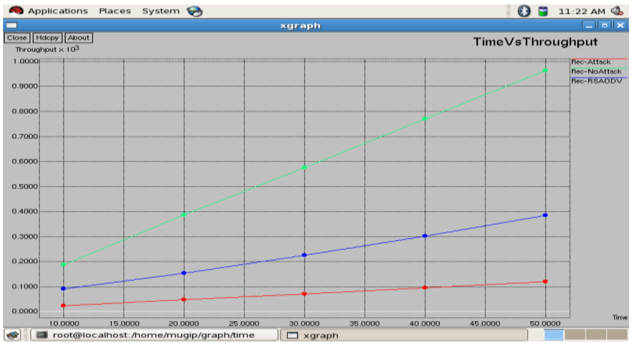


Fig (b) Time Vs Packet Drop

Fig (c) ensures that the throughput for RSAODV doesn`t decrease and it is better than that in case of Attack and simulator finishes its simulation with the specified simulation time.



Fig(c) Time versus Throughput

V. CONCLUSION AND FUTURE WORK

Reputation-based secure protocol framework relies on centrality and mobility as two key parameters to drive the system to a more stable state in Mobile Ad-hoc networks. We discuss how we integrate these two centrality in the proposedwork and propose the optimizations such as selective deviation test and adaptive expiration timer. For authentication of packets we use Digital signature and hashing techniques. Our subsequent work will focus on studying the impact of centrality and configuration parameters on the performance of protocol in relation to network throughput, network delay, packet drop and the protocol detection ratio or simulation time. We will investigate the results of the reputation-based protocol under the same parameters and high-mobility conditions, subject to collaborative blackhole and grayhole attacks.

REFERENCES

1. J. Ruiz, et al, "Black Hole Attack Injection in Ad hoc Networks," DSN2008, International Conference on Dependable Systems and Networks. Anchorage, Alaska, June 24-27 2008, pp. G34-G35.
2. Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes — Fairness In Dynamic Adhoc NeTworks. In *Proc. of IEEE/ACM MobiHOC*, 2002. IEEE.
3. A. Dadhich, "A Distributed Cooperative Approach To Improve Detection And Removal Of Misbehaving MANET Nodes", COMSWARE, 2008, pp728 – 735

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

4. P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", Proc. IFIP CMS, 2002.
5. S. Buchegger, and J.-Y. Le Boudec,“A Robust Reputation System for P2P and Mobile Ad-hoc Networks,” Proc. 2nd Workshop Economics of Peer-to- Peer Systems, 2004
6. H. Deng, W. Li, and D. P, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol 40, 2002.
7. M.T. Schlosser, "The EigenTrust Algorithm for Reputation Management in P2P Networks," ReCALL, 2003.
8. S. Ramaswamy et al., "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", ICWN’03, USA 2003.
9. S. Ramaswamy et al, "Simulation Study of Multiple Black Holes Attack on Mobile Ad Hoc Networks," ICWN'05, 2005, pp. 595-604.
10. F. Li, J. Wu, and B. Raton, "Mobility Reduces Uncertainty in MANETs", Proc. of IEEE INFOCOM, May 2007.
11. C.W. Yu, et al, Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks, Springer 2009.
12. E. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs" Source, 2007, pp. 32-40.
13. D. Feng and Y. Zhu, "Cooperative Incentive Mechanism Based on Game Theory in MANET" Simulation, 2009, pp. 201-204.
14. “Security enhancement over ad-hoc aodv routing protocol” By Zongwei Zhou,Department of Computer Science and Technology, Tsinghua University, Beijing, China.