Adhoc On-Demand Distance Vector Routing Reputation-Based (AODVRB) over MANET

Mr. Naveen. L[1], Dr. Balakrishna.R[2], Mr. Nandish U. G[3], Mr.Anand Kumar K. S[4]
[2.] Professor and HOD, [1, 3&4]Lecturer,
Department of Information Science and Engineering,
Rajarajeswari College of Engineering, Bangalore, India.

***Abstract*--** In this paper fully distributed reputation-based model is used to improve the security in MANETs. We design and build the prototype Adhoc On-Demand Distance Vector Routing Reputation-Based (AODVRB) over Adhoc On Demand Distance Vector Routing(AODV) and test it in our own simulator in the presence of variable black hole attacks in highly mobile and sparse networks. Our results show that we achieve increased throughput while delay is reduced and we focus on a single, multiple black hole attacks and also more aggressive black hole attacks, but our design principles and results are applicable to a wider range of attacks (gray hole attacks), so that efficiency is more and jitter is also decreased.

Keywords*— *MANETs, reputation, routing, AODV, AODVRB, Blackhole.

I INTRODUCTION

A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time; therefore, the limited wireless transmission range of each node gets extended by multi hop packet forwarding. This kind of network is well suited for the mission critical applications such as emergency relief, military operations, and terrorism response where no pre deployed infrastructure exits for communication. Due to its intrinsic nature of lacking of any centralized access control, secure boundaries (mobile nodes are free to join and leave and move inside the network) and limited resources mobile adhoc networks are vulnerable to several different types of passive and active attacks[1],[2]. Among these one of the most important security issues is the protection of the network layer from different active routing attacks. This paper is concerned with two types of routing attacks namely passive Black hole attack and active black hole attack which exhibits packet forwarding misbehaviour. In a black hole attack malicious node (called blackhole) replies to every route request by falsely claiming that it has a fresh enough route to the with the design, implementation and evaluation of a reputation-based self organized protocol that is specifically targeted for highly mobile and sparse environments. Here the proposed protocol follows distributed reputation guidelines given in [3] and considers two types of Centralities to improve on the reputation convergence and faster isolation of malicious nodes. We incorporate our protocol within AODV and perform extensive simulations a number of scenarios characterized by high node mobility (speed 20 m/s), and short pause time (1 second) in order to evaluate each of the design choices of our system. We focus on a single and multiple blackhole attacks [4] but our design principles and results are applicable to a wider range of attacks such as gray-hole attacks.

II. RELATED WORK

Distributed reputation has been used in both MANETs and P2P environments. CORE [6] was proposed for monitoring and isolating the selfish nodes based on subjective, direct and functional reputation. CONFIDENT [7] was proposed where node monitors their neighbourhood and detect several kinds of misbehaviour. SCAN [5] was proposed a network layer security protocol where here the decision is made to receive forward or discard a packet. This decision is based on ip address. In the peer-to-Peer file-sharing networks, reputation has been used to reflect the ratings of different users and distributed Eigen-Vector has been proposed to calculate trust in a distributed Peer-to-Peer environment [8], proposed 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. In our model, node's reputation is classified to not only good or bad but we classify nodes into multiple zone that enable higher details and better decision making depending on the required services such as packet forward or Topology discovery [9] proposed a solution to collaborative black hole attack using next hop information validation but showed no results or detailed analysis.

III. BLACKHOLE ATTACK.

A black hole is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. When the data packets routed by the source node reach the black hole node, it drops the packets rather than forwarding them to the destination node. Such malicious node also advertises itself as having shortest path to requested node. In *fig. 1*, node 1 wants to send data packets to node 4 and initiates the route

discovery process. We assume that node 3 is a malicious node and it claims that it has route to the destination whenever it receives RREQ packets, and immediately sends the response to node 1. If the response from the node 3 reaches first to node 1 then node 1 thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 3. As a result, all packets through the malicious node is consumed or lost.

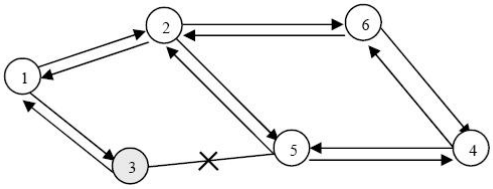

Figure 1: Black-hole attacks

IV.OUR REPUTATION-BASED FULLY DISTRIBUTED PROTOCOL FOR HIGHLY MOBILE AND SPARSE MANETS.

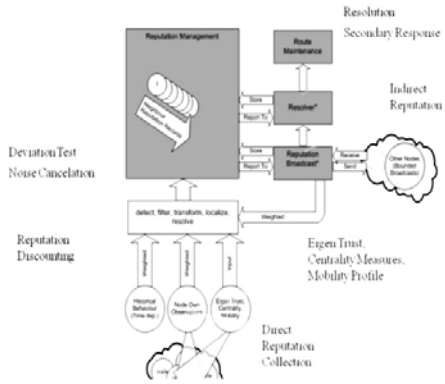

Figure 2: Reputation system model.

Reputation Management is the main entity responsible for storing and retrieving all the node's neighbours' reputation records. It orchestrates the operations of the other components and act as the concentration point for all the events taking place inside the system. **Neighbour Reputation** Record is the entity representing reputation observation for one of the neighbours. Each node holds N neighbour reputation records where N can be determined by the node's memory capacity, CPU power for maintenance to update these records and other resource constraints. Nodes with higher reputation and centrality should hold enough reputation records about other nodes in order to provide adequate coverage of the nodes in its own area. **Reputation Broadcast** is the entity responsible for receiving indirect reputation from neighbours. It performs a selective deviation test to ensure the unity of view with the receiving node point of view. In the early Deviation Test as presented in [1], requires each node to compare received indirect reputation with its own direct reputation for a given neighbour and reject any indirect reputation that deviate by a certain value Δ (the deviation threshold). In our Selective Deviation Test, the receiving node (a) attempts to calculate the reputation of its neighbour node (j). Node (a) first checks the reputation of the indirect reputation information source node (i). R_{ai} is the reputation held by node (a) about node (i). If the reputation R_{ai} > (threshold) then Rij is trusted without further tests. This enables fast reputation convergence which is critical in our challenged scenarios where nodes don't get enough time to observe the reputation of other nodes. At the same time, node (a) uncertainty with respect to node (j) decreases as a result of trusted node (i). **Reputation Detect, Filter, Transform and Localize:** The calculation of the direct reputations was inspired by the Eigen Trust algorithm presented in [8]. In our proposed reputation system model the prototype AODVRB is build over AODV and is tested in our own simulator in the presence of variable blackhole attacks. In the purpose of our reputation schema we use connectivity instead of transaction. This connectivity takes place when the node either receives or requests a forward of a message from that neighbour.The calculation of the direct and indirect reputations is done in this module by enhancing the existing Eigen trust algorithm to calculate a global consistent reputation value at each node for all its neighbours and then resolves the reputation using direct and indirect reputation information. Each node also calculates the Eigenvector centrality of its neighbours in order to reflect on each neighbor reputation and the level of confidence in this neighbor reported indirect reputation. The steps in the proposed algorithm is as follows: The enhanced eigen trust algorithm to calculate a global consistent reputation value at each node for all its neighbours and then resolves the reputation using direct and indirect reputation information.

Step: 1 Let $A_{i,j}$ be the adjacency matrix of the network. $A_{i,j}$ is originally defined in Eigen-Vector Centrality as $A_{i,j} = 1$ if the ith node is adjacent to the jth node, and $A_{i,j} = 0$ otherwise. In our model, $A_{i,j} = s$, where s is the wireless signal strength from the ith node to its neighbour j^{th} node, and $A_{i,j} = 0$ if the i and j are not neighbours. For the i^{th} node (the observed node), the centrality score is Proportional to the sum of the scores of all nodes which are connected to it. Hence:

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

Where M(i) is the set of nodes that are connected to the i^{th} node, N is the total number of nodes and λ is a constant.

Step: 2 Node i calculate the percentage of packets originating from i 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 (i.e. packets that were originating or forwarded by node i to node j but they were not subsequently forwarded by node j) over the total

number of packets offered to node j, expr(i,j). Where S_{ij} is the recent satisfaction index for node i about node j.
S_{ij} = frwd(i,j) – expr(i,j)

Step: 3 S_{ij} would be then weighted using step 3 into the direct reputation of node j; R_{ij}-prev is reputation value that 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 neighbour j
$R_{ij} = R_{ij\text{-}prev} * W_{history} + S_{ij} * (1\text{-}W_{history})$

Step: 4 If no connectivity between *i* and *j* takes place, R_{ij} is discounted instead using a constant value: $W_{discounting}$. Then it is defined that max $_t$ to be the maximum observation of R_{ij} over time. R_{ij} is normalized using step 4 as:
$R_{ij} = R_{ij} / \max_t (R_{ij})$

Step: 5 Second hand reputation received by the observing node i is aggregated (step 5) to a single value ARR_{ij} (Aggregated Reported Reputation about node j as received and processed by node i. Hence ARR_{ij} is given by:
$ARR_{ij}=\sum(RR_{nj}*Dig_n*RR_{in})/\sum(Dig(n)*RR_{in})$
Where Dig(n) is the degree centrality of the reporting nodes(n)

Resolver is responsible for doing the actual calculation of the neighbour final reputation (called resolved reputation) by combining direct and indirect reputation and performing Reputation Noise Cancellation. As packets might get dropped accidently by nodes due to other network conditions such as congestion, interference which doesn't constitute malicious behaviour, we have included an adaptive threshold measure that is adjusted depending on the neighbour node movement profile and the link quality between the observing node and its neighbours. If the node experiences a packet loss from its neighbour below this threshold, it considers that loss as a noise and subsequently ignores the lost packets. If the losses were above the noise threshold level, the node will start reacting to these events accordingly. **Route Maintenance** is being called when the Resolver detect that a certain neighbour reputation has fallen below a certain threshold. The "Route Maintenance" entity is responsible for breaking all the routes going through this neighbour and initiates a new replacement route search as needed. In our implementation using AODV, the "Route Maintenance" entity sets the route to a special mode called "Local Route Repair" as described in [10]. This special route mode would enable queuing packets going out on the route until an alternative route is established if possible, else all the packet queued are dropped and a route error (RERR) message is sent to the neighbour nodes.

V.RESULTS

Initially the simulator is made run by the simulator control as shown below in figure 3

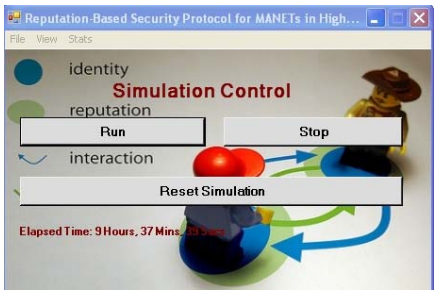

Figure 3: simulator form

Once the simulator form is created run the simulation and view the network once when the network is viewed the network is as shown in following figure 4 where the nodes are created and the transmission is seen with both direct and indirect reputation.

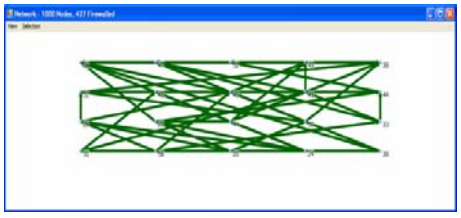

Figure 4: creation of nodes and its transmission

After the creation of nodes and its transmission the each nodes reputation value, throughput, its capacity, time,delay and nodes collisions occurred during transmission from source to destination is viewed as shown in the below figure 5.

Figure 5: Each node reputation value & throughput

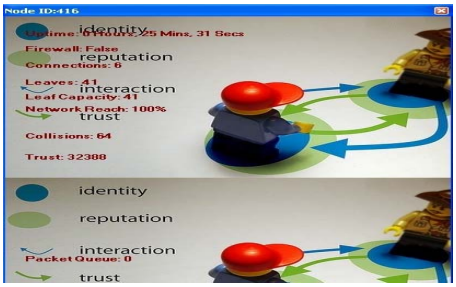

Figure 6: Number of collisions and black-hole detected

Therefore, the number of collisions will be identified when there is more collision and active transmission is taken place

and through which the black hole attack is identified this is as shown in below figure 6.

VI.CONCLUSION AND FUTURE WORK

Here we have considered the problem of black hole attacks in MANETS and proposed our AODVRB using reputation based protocol for security in MANETS. Our results confirm that active black hole attacks can be detected easily and efficiently than previously existing approaches in identifying the blackhole. Our early prototype implementation over AODV confirms and extends the results published in [3][4][5]. The results presented in this paper show that the throughput remains above 70% in the presence of the increasing number of black-hole nodes, while the jitter and delay decrease and are below AODV. We also discuss the impact the distribution of centrality and reputation of our nodes has on the time needed to isolate malicious nodes. Our subsequent work will focus on studying the impact of centrality and configuration parameters on the protocol performance in relation to network throughput, network delay, network jitter and the protocol detection ratio. We will investigate the response of the reputation protocol under the same high-mobility conditions and subject to collaborative black-hole and gray-hole attacks.

ACKNOWLEDGEMENTS

The authors are thankful for the encouragement and strong support received throughout this research work to Principal & Management, RRCE, Bangalore

REFERENCES

[1] Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru, Herbert Rubens “Mitigating Byzantine Attacks in Ad Hoc
Wireless Networks”, ACM MobiCom, Aug-2000.

[2] Charles E.Perkins and Elizabeth M. Royer,“Ad hoc on demand distance vector (AODV) routing (Internet-Draft)”, Aug- 1998.

[3]S. Buchegger, "Reputation Systems for Self-Organized Networks: Lessons Learned," In IEEE Technology and Society Magazine, Toward Fourth Generation Wireless, March 2008., pp. 1-10.

[4]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.

[5]H. Yang, et al, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE Network, vol. 24, 2006, pp. 1-13.

[6]P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", Proc. IFIP CMS, 2002.

[7]S. Buchegger and J.L. Boudec, "A robust reputation system for peer-to-peer and mobile ad-hoc networks", proc. of P2PEcon, 2004..

[8]M.T. Schlosser, "The EigenTrust Algorithm for Reputation Management in P2P Networks," ReCALL, 2003.

[9]S. Ramaswamy et al., "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", ICWN’03, USA 2003..

[10]C.E. Perkins and E.M. Royer, "Ad-hoc on-demand distance vector routing,", In proc. of 2nd IEEE Workshop on Mobile Wireless Networks, 1999.

[11] Janne Lundberg, Helsinki University of technology,"Routing Security in Ad Hoc Networks" http://citeseer.nj.nec.com/400961.html.

Authors Biography

Mr.Naveen.L, Obtained his M.Tech. Degree from East Point College of Engineering and Technology, Bangalore, Affiliated to isvesvaraya Technological University, Karnataka. Working as Lecturer in Department of Information Science and Engineering, Rajarajeswari College of Engineering, Bangalore, India. His Research interests are in the field of cloud computing,Image Processing and Computer Networks.

Dr.R.Balakrishna, working as a Professor and HOD, Rajarajeswari college of engineering, Bangalore, India. His research interests are in the field of wireless adhoc network, Sensor Network, Artificial Neural Networks, Data Mining, Operating System and Security. He has published over 35 National and International journals and Conferences various papers across
India and other Countries. He is the Life member of Indian Society for Technical Education and IAENG
.

Mr.Nandish U. G, Obtained his M.Tech. Degree from East West Institute of Technology, Bangalore, Affiliated to Visvesvaraya Technological University, Karnataka. Working as Lecturer in Dept of Information Science and Engineering, Rajarajeswari College of Engineering,Bangalore,India. His Research
interests are in the field of cloud computing, Image Processing and Computer Networks.

Mr.Anand Kumar K.S, Obtained his M.Tech Degree from R.V. Collegeof Engineering, Bangalore, Affiliated to Visvesvaraya Technological University, Karnataka. Working as Lecturer in Department of Information Science and Engineering, Rajarajeswari College of Engineering, Bangalore, India. His Research interests are in the field of Data Mining, Bioinformatics and Computer Networks.