Towards Improving Performance of Reputation based Dynamic Source Routing in MANET

Sonika
M. Tech (Student), Deptt. Of CSE, M.M University Mullana, Ambala, India

Sanjeev Rana
Professor, Principal M.M Group of Institution, Ramba Karnal, India

Rajneesh Gujral,Ph.D
Professor, Deptt. Of CSE, M.M University Mullana, Ambala, India

ABSTRACT
A mobile ad hoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure. Most existing approaches for secure route selection those are based on cryptography are resource constrained and high computational or increase communication overhead. Reputation based systems for mobile ad hoc networks concentrate on solving routing issues raised by misbehaving nodes using trust evaluation process for a node implies significant lower energy consumption, less processing for trust level calculation. Reputation based other solution do not follow the cache clearance mechanism , so every time when we check reputation value of the nodes in table, node with the high reputation value will be on top every time and other nodes will not get chance to participate into the communication. In this paper, we proposed a Security framework for DSR using reputation based scheme that not only improve the efficiency and reduce network overhead but also permit every node to participate into the route selection process for communication. The effectiveness of the proposed framework is analyzed using NS2 simulator.

Keywords
MANET, DSR, repDSR, Trust, Routing.

1. INTRODUCTION
A Mobile Ad Hoc Network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and service discovery without the help of an established infrastructure. An ad hoc network uses no centralized administration. This ensures that the network will not cease functioning just because one of the mobile nodes moves out of the range of the others. MANETs have several significant characteristics and challenges. MANETS is having dynamic topologies where each Node is free to move arbitrarily. Thus, the network topology may change randomly at unpredictable times, and may consist of both bidirectional and unidirectional links. Many routing protocols have been proposed for reliable information exchange in a network, In Pro-active protocols such as DSDV, TBRPF the host exchange routing information and construct the routing table in advance. In on-demand protocols such as DSR, ADODB the routing information is required and maintained only when it is needed. Unfortunately all these protocols have some limitations in the case of the performance and the throughput.

Mobile wireless networks are generally more prone to physical security threats than fixed-cable nets. The increased possibility of Modification, Impersonation, Fabrication, Eavesdropping, Replay, Denial of Service, and Malicious Software should be carefully considered. Several popular security approaches are provided to handle different kinds of attack. These approaches are categories as prevention, detection and reputation based schemes. Detection approaches, provides Watchdog and Path rater and intrusion detection techniques. Prevention approaches provides Message Authentication Primitives, Digital signature solutions but they may be of high computational or communication overhead (in case of cryptography and key management based solutions). Reputation Based Approach in MANET collects information about one entity's former behavior as experienced by others. Reputation Based approach provide solution based on trust evaluation process for a node implies significant lower energy consumption, less processing for trust level calculation. In this paper we proposed a Security framework for DSR using reputation based scheme that uses reputation with cache clearance process that not only improve the efficiency and reduce network overhead but also permit every node to participate into the route selection process for communication.

The rest of the paper is organized as follows, basic operation of dynamic source routing protocol is described in Section 2, Section 3 provide literature survey which deals with misbehaving nodes using reputation mechanisms, Section 4 explains our proposed framework and in Section 5, we present a preliminary evaluation of the performance of our protocol, and in Section 6, we present conclusions.

2. MOTIVATION
Dynamic Source Routing (DSR) uses source routing to deliver packets from one node in the network to some other node. The source node adds the full path to the destination in terms of intermediate nodes in every packet. This information is used by intermediate node to determine whether to accept the packet and to whom to forward it. DSR operates on two mechanisms, Route Discovery and Route Maintenance. Route Discovery is used when the sender does not know the path up to the destination. In this mechanism, the sender broadcasts a ROUTE REQUEST message which contains Source Address, Destination Address, and Identifier. Each intermediate node adds its address in ROUTE REQUEST message and rebroadcast it, unless it has not rebroadcast earlier.

The destination then sends a unicast ROUTE REPLY message in reverse direction whose information is obtained from list of intermediate nodes in ROUTE REQUEST message. When the ROUTE REPLY packet reaches the source, it records the route contained in it and saves in its cache for the specific destination. For better performance, intermediate nodes also record this route information from the two route messages. All nodes overhearing these packets add meaningful route entries in their caches. Finally, Route Maintenance Mechanism is used to notify source and potentially trigger new route discovery events when changes in the network topology invalidates a cached route. DSR have some security and performance issues like, it impersonating another node to spoof route message and Advertising a false route metric to misrepresent the topology. Node some time sends a route message with wrong sequence number to suppress other legitimate route messages.

3. LITERATURE SURVEY

There are many solutions in the literature which deals with misbehaving nodes using reputation mechanisms. This section explains only some of them.

Santhosh Krishna B.V and Mrs.Vallikannu A.L [4] proposed a solution for single and multiple black hole attacks. They designed and build a prototype over DSR using reputation based approach and test the presence of variable active black hole attacks in highly mobile and sparse networks. In this work, they employ focus on black hole attacks where the malicious node is not only silently dropping the data packets, but also attacking the routing layer. They provided a protocol uses reputation discounting to ensure that old reputations will fade way giving more chance for nodes to reclaim their reputation by consistently behaving in a cooperative manner. For early signs misbehaver node they provided reputation discounting firing back process, this process increase computation process on a network and decrease the efficiency of the network.

Sameh R and Milena [7] in her paper proposed a reputation model based on eigen vector based degree centrality. Here each node collects information about its neighbor by direct monitoring as well as from other neighbors. Trust is built based on these centralities. Nodes with higher centrality have higher probability of getting in contact with other nodes. Second hand information is collected only from those neighbors with high centrality not from all the neighbors. They claim that their approach can be used in a highly dynamic environment and in a sparse network also.

Ceronmani Sharmila et al [11] proposed a fair non-repudiation protocol based on mobile agents and proxy certificates. Mobile DRMs need "time information" included in evidences for dispute resolutions. Users generate mobile agents which carry encrypted payment information to RIs. Mobile agent carries proxy certificate issued by its owner. But the disadvantage of this solution is according to binding mechanism of the proxy certificate and its corresponding subscriber certificate, mobile agent and its owner cannot repudiate their relationship and it takes more time and memory for computation work.

Sangheetaa Sukumran et al [15] proposed a solution for on-demand routing protocol using reputation mechanism. This approach calculates the reputation values of the nodes using simple formula. Any node is supposed to maintain a good reputation value in order to receive network services. When a node tries to identify a route, its route request will be forwarded by the neighboring nodes only if it reputation value is higher than the threshold value i.e. this node must be in the white list. Thus a node needs to maintain a good reputation value in order to enjoy network services. A misbehaving node which is isolated has no chance of rejoining the network until the entire network is reformed. This will decrease the efficiency and effectiveness of the network, low reputation value node is not allowed to participate in a network until network is reformed. We provided a solution that uses reputation with cache clearance process that not only improve the efficiency and reduce network overhead but also permit every node to participate into the route selection process for communication.

4. PROPOSED FRAMEWORK

In this paper, we proposed an approach for increasing the efficiency of Dynamic source routing protocol using trust based route selection process. Our solution is based on the concept of behavior trust, it also defines trust management in a network and updating trust value of nodes after some interval using cache clearance process. Cache clearance will decrease the overhead of the network and also neglect the dynamics of a scenario with highly mobile nodes where the chance to meet someone again is low. The recommendations improve the trust evaluation process for a node implies significant lower energy consumption, less processing for trust level calculation. In this Reputation value is calculated [15] using equation (4.1). Suppose there are N nodes in the mobile ad-hoc network. Each node ni calculates the reputation R (i, j) t for each of its neighbor "j" at time t.

$$R_{(i,j)t} = \frac{\sum_{pkts=0}^{\infty} F_{pkts}}{\sum_{pkts=0}^{\infty} S_{pkts}} \quad \ldots\ldots (4.1)$$

Where R(i, j)t is the reputation value calculated by monitoring the neighbor "j" directly at time "t" and Fpkts is the number of packets forwarded by node "j" and Spkts is the number of packets sent by node "j". Our proposed work will work on following basis:

- In reputation based system, DSR agent module continuously monitors the behavior of node. Each node maintains reputation values of its neighbors based on their packet forwarding activity. Reputation value assigned as numeric in order to make them objective and useful.
- Nodes first time meet the transmission will crate an entity for the node and assign reputation value 1.
- The nature of data flow, packet forwarding between any two nodes also depends on relative mobility A node, P, observes the packet forwarded by its neighbor, Q, and assigns a reputation value, r (P, Q), equal to the ratio of number of packets forwarded by Q to the number of packets sent to it. Each node stores these reputation values as a weighted average (∝) of old and new values using the following formula.
  R current (P, Q) = (1-∝) r old (P, Q) + ∝.r new(P,Q) ------- i)
- In situations where a node P, needs to form an opinion about a certain node Q, it requests reputation values from its neighbors. The formula suggested for computing the composite reputation value from the reputation values obtained from a neighbor, says R, is given as
  R composite (P, Q) = r (P, R). r (R, Q) + (1-r (P,R)) .r(P,Q) --------- ii)
- As a result, a node with the highest reputation will get the chance to participate in communication. After a fixed time period cache will get clear, this process refresh the reputation value of each node so that every node will get chance to participate in the communication it will increase performance and efficiency of the network.

5. PERFORMANCE ANALYSIS OF PERPOSED FRAMEWORK

5.1 Simulation Parameter

This section describes the parameters used in the simulations. The performance simulation environment used is based on NS 2, a network simulator that provides support for simulating multi-hop wireless networks complete with physical and IEEE 802.11 MAC layer models. Experimental Setup and Performance Metrics are shown below. In our entire node movement pattern, the node choose a destination and move in a straight line towards the destination at uniformly speed. This is the random waypoint model. Once the destination is reached, another random destination is targeted after a pause.

Table 1: General Experimental Setup Parameters

Parameter	*Value*
Number of Nodes	50
Application	Constant Bit Rate (CBR)
Node Speed	0-10 m/s
Traffic Model	Generated Randomly
Packet Time	Variable
MAC Protocol	MAC 802.11
Routing Protocol	DSR
Mobility Pattern	Random Waypoint Model
Antenna Type	Omni Antenna
Work Area (x,y)	(800,800)
Interface queue type	Queue/Drop Tail
Network Interface	Phy/ Wireless Phy

The maximum speeds used were chosen from between 0 m/s to 10 m/s. The node communication using, Constant Bit Rate (CBR) node to node connection. CBR is chosen to avoid potential peculiarities associated with more complex protocol such as TCP. The simulated environment consists of 50 wireless mobile nodes roaming in 800 meters*800 meters.

5.2 Simulation Results

Packet delivery Ratio

It is the ratio of the number of packets actually delivered without duplicates to the destinations versus the number of data packets supposed to be received.

PDR= Total Number of packets Received /Total Number of packets Sent

Trace are the special object in NS-2 that are used to store information about each packet that is send, dropped and received during runtime. The graph below shows the packet delivery ratio comparison of DSR and repDSR depend upon the reputation value of nodes. Total number of packets is 420. Graph shows the number of packet delivered to the destination by using standard DSR and repDSR. Standard packet delivery ratio is 64 % but after using the reputation method delivery ratio increase by 31 %, it became 95 %. repDSR is able to provide reliable communication. This is because repDSR selects the best route based on the reputation value. But, normal DSR collapses when number of selfish nodes is increased. Thus from the results it is proved that repDSR provides better performance compared to DSR.

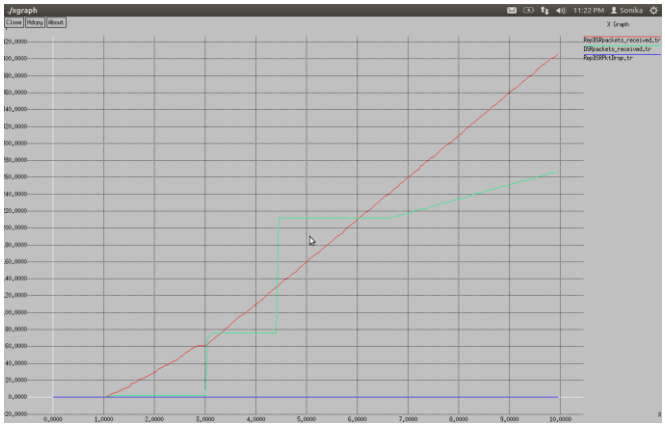

Figure: 1 Packet delivery Ratio Comparison DSR and repDSR

Packet Drop

Dropped packets are pieces of data that are disregarded by network sensors when they are overwhelmed. A dropped packet affects quality of service for network. In DSR protocol with the increase in pause time we can't reduce the data drop that is done by the malicious nodes but after the implication of the proposed method it can be constantly reduced in repDSR. In our work standard DSR packet drop ratio is 46 % and in repDSR packet drop ratio is 5%.

Dropped Packet = Packets Sent-Received Packet.

Average End to End Delay

It is the average time from the transmission of a data packet at a source node until packet delivery to a destination which includes all possible delays caused by buffering during route discovery process, retransmission delays, queuing at the interface queue, propagation and transfer times of data packets. repDSR is able to provide reliable communication and decrease the overhead in the network because repDSR transmits Route Request packets only to the nodes with higher reputation value

$\sum$ (arrival time- send time)/ $\sum$ number of connections

Below diagram represents the difference between DSR and repDSR end to end delay.

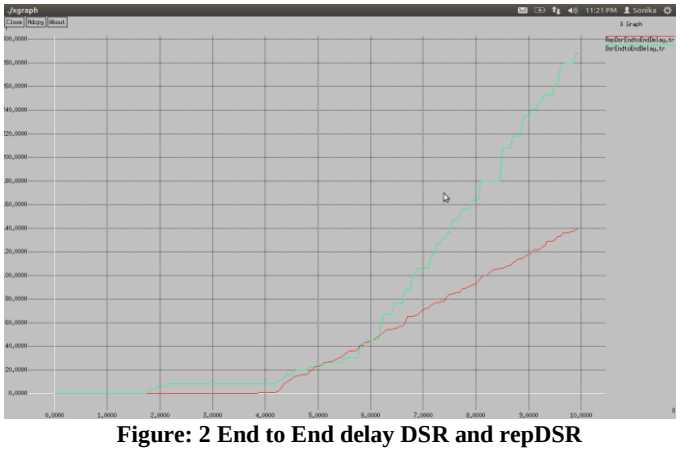

Figure: 2 End to End delay DSR and repDSR

6. CONCLUSION

This work explained about the on-demand routing protocol using reputation mechanism. Any node is supposed to maintain a good reputation value in order to receive network services. As a result of our studies, in repDSR cache clearance process not only improve the efficiency and reduce network overhead but also permit every node to participate into the

route selection process for communication, we concluded that repDSR exhibits a better performance in terms of packet delivery fraction and throughput, end to end delay with number of mobile as compared to other cryptography based solutions those consume more memory and computation process time.

7. REFERENCES

[1] Gagandeep, Aashima, Pawan Kumar "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" in International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[2] D. Ganesh and M. Sirisha "Reputation and Trust Evaluation in MANETs Using Eigen Trust Algorithm" in VSRD- IJCSIT, Vol. 2 (3), 2012, 175-189.

[3] Zaiba Ishrat "Security issues, challenges & solution in MANET" in IJCST Vol. 2, Issue 4, Oct. - Dec. 2011.

[4] Santhosh Krishna B.V, Mrs.Vallikannu A.L "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism" in International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010 1ISSN 2229-5518.

[5] R.Balakrishna, U.Rajeswar Rao, G.A.Ramachandra, M.S.Bhagyashekar "Trust-based Routing Security in MANETS" in International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 547-553.

[6] Sofiane Boukli Hacene, Ahmed Lehireche "Coherent Route Cache In Dynamic Source Routing For Ad Hoc Networks" in Computer Science Journal of Moldova, vol.19, no.3(57), 2011.

[7] Sameh R. Zakhary, Milena Radenkovic "Reputation-Based Security Protocol for MANETs in Highly Mobile Disconnection-Prone Environments".

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks."

[9] R. Balakrishna, U. Rajeswar Rao , G.A. Ramachandra ,M.S.Bhagyashekar "Trust-based Routing Security in MANETS" in R. Balakrishna et al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 547-553.

[10] David B. Johnson and David A. Maltz "Dynamic source routing in ad hoc wireless networks,"

[11] Ceronmani Sharmila , Komala Valli "Enhanced Security through Agent Based Non-Repudiation Protocol for Mobile Agents" in International Journal of Power Control Signal and Computation (IJPCSC) Vol3. No1. Jan-Mar 2012.

[12] Kulbir Nain, Poonam Kumari, Roshan Lal Hiranwal "Improved DSR Protocol using Repudiation Based" in Journal of Computer Networking, Wireless and Mobile Communications (JCNWMC) Vol.2, Issue 1 Sep 2012 7-15.

[13] Ernesto Damiani, Sabrina De Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati, Fabio Violante "A Reputation Based Approach for Choosing Reliable Resources in Peer to Peer Networks".

[14] Yogendra Kumar Jain, Nikesh Kumar Sharma "Secure Trust Based Dynamic Source Routing in MANETs" in International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 1 ISSN 2229-5518.

[15] Sangheetaa Sukumran, Venkatesh Jaganathan, Arun Korath "Reputation based Dynamic Source Routing Protocol for MANET" in International Journal of Computer Applications (0975 – 888) Volume 47– No.4, June 2012