Reputation based Dynamic Source Routing Protocol for MANET

Sangheetaa Sukumran
Research Scholar, Department of Information Technology, Anna Institute of Technology, Coimbatore, Tamilnadu, India

Venkatesh Jaganathan
Professor, School of Management Studies, Anna Institute of Technology, Coimbatore, Tamilnadu, India

Arun Korath,
Asst. Professor, Department of Management studies, Vedavyasa Institute of Technology, Kerala, India

ABSTRACT
With recent performance increase in the area of wireless mobile communications, mobile ad-hoc networks are playing a wide spread usage in the areas of military and other applications. But this mobile ad-hoc network does not have any centralized authorities like an access-point or a router as in case of wireless and wired networks to control and take care of routing. Thus routing has become a greater challenge to these types of networks. This paper proposes a new reputation based routing protocol based on DSR (Dynamic Source Routing) and through simulation results proves that the proposed method performs well compared to normal DSR.

General Terms
Routing protocol for Mobile Ad-hoc Networks.

Keywords
Reputation, routing protocol, MANETs.

1. INTRODUCTION
A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links, the union of which form an arbitrary topology. The emerging mobile ad-hoc networking technology seeks to provide users "anytime" and "anywhere" services in a potentially large infrastructure less wireless network, based on the collaboration among individual network nodes. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

The specific interest here is on the access to the network-layer functionalities like routing and packet forwarding. Access should be given only to well-behaving nodes and not to misbehaving nodes. A misbehaving node can be either a selfish or a malicious node. A selfish node may enjoy network services, e.g. receiving packets destined for itself but refuse to route or forward packets for others, therefore invalidating the basic collaboration premise in almost all current routing algorithms for mobile ad-hoc networks. A malicious node may seek to damage or disrupt normal network operations. Moreover, misbehaving node may act as a good network citizen for a certain time period or in certain places, but then starts to act selfishly or maliciously at other times or locations.

The main concentration of this paper is on the selfish nodes. This paper is organized in to following sections. Section 2 discusses some of the existing approaches in detail. Section 3 explains the proposed approach in detail. Section 4 gives the simulation results. Section 5 gives conclusion.

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

2.1 Reputation Based mechanism to isolate Selfish nodes
M. Tamer Refaei et al [1] proposed reputation-based mechanism as a means of building trust among nodes. Here a node autonomously evaluates its neighboring nodes based on completion of the requested service(s). The neighbors need not be monitored in promiscuous mode as in other reputation based methods. There is no need of exchanging of reputation information among nodes. Thus involves less overhead, and this approach does not rely on any routing protocol. This approach provides a distributed reputation evaluation scheme implemented autonomously at every node in an ad hoc network with the objective of identifying and isolating selfish neighbors. A reputation table is maintained by each node, where a reputation index is stored for each of the node's immediate neighbors. A node calculates reputation index of its neighbor based on successful delivery of packets forwarded through that neighbor. For each successfully delivered packet, each node along the route increases the reputation index of its next-hop neighbor that forwarded the packet and packet delivery failures result in a penalty applied to such neighbors by decreasing their reputation index. The indication of a success or failure is obtained from feedback received from the destination for e.g., using TCP acknowledgements. Selfish behavior is prevented and nodes are motivated to build up their reputation by determining whether to forward or drop a packet based on the reputation of the packet's previous hop. Once a node's reputation, as perceived by its neighbors, falls below a pre-determined threshold all packets forwarded through or originating at that node are discarded by those neighbors and the node is isolated.

2.2 CORE
PietroMichiardi and RefikMolva[2] proposed a Collaborative Reputation (CORE) mechanism that also has a watchdog component for monitoring. Here the reputation value is used to make decisions about cooperation or gradual isolation of a node. Reputation gives values are obtained by regarding nodes as requesters and providers, and comparing the expected result to the actually obtained result of a request. In

CORE the reputation value ranges from positive (+) through null (0) to negative (-). The advantage of this method is that having a positive to negative range allows good behavior to be rewarded and bad behavior to be punished. This method gives more importance to the past behavior and hence tolerable to sporadically bad behavior, e.g. battery failure. But the assumption that past behavior to be indicative of the future behavior may make the nodes to build up credit and then start behaving selfishly.

2.3 CONFIDANT

CONFIDANT was proposed by Buchegger et al [4]. Here evidence from direct experiences and recommendations is collected. Trust relationships are established between nodes based on collected evidence and trust decisions are made based on these relationships. There are four interdependent modules; (a) monitor, (b) reputation system, (c) path manager and (d) trust manager. Monitor collects evidence by monitoring the transmission of a neighbor after forwarding a packet to the neighbor. It then reports to the reputation system only if the collected evidence represents a malicious behavior. Reputation system changes the rating for a node if the evidence collected for malicious behavior exceeds the pre-defined threshold value. Then, path manager makes a decision to delete the malicious node from the path. Trust manager is responsible for forwarding and receiving recommendations to and from trustworthy nodes. But this approach does not talk much about isolating the misbehaving nodes from the network.

2.4 Reputation-based System for Encouraging the Cooperation of Nodes

TiranuchAnantvalee and Jie Wu [5] in their paper, introduces, a new type of node called as suspicious node besides cooperative nodes and selfish nodes, Some actions will be taken to encourage the suspicious nodes to cooperate properly after further investigation. They introduce the use of a state model to decide what to do or respond to nodes in each state. In addition to a timing period for controlling when the reputation should be updated, a timeout for each state is introduced.

2.5 Cooperative On Demand Secure Route

Cooperative On-demand Secure Route (COSR) proposed by FeiWang[6], is a novel secure source route protocol which takes action against malicious and selfish behaviors. COSR measures node reputation (NR) and route reputation (RR) by contribution, Capability of Forwarding (CoF) and RR is used to balance load and to avoid hot point. This paper addresses the problems like DoS attack, Black-hole attack, Rushing attack, Wormhole attack and also selfish nodes. In the COSR, node's reputation depends on the information from Physical layer, Media Access Control (MAC) layer, and Network layer, and it can be computed by node's CoF, history action, and recommendation.

The CoF is the new concept introduced in this paper. CoF denotes the capability of forwarding packets of a certain node. As the information of CoF is provided by its owner, malicious node might cheat others by false data. To avoid the emergence of such malicious behavior, COSR takes strategies like 1. Discounting where COSR uses node's reputation to discount those providing CoF data. 2. Punishment. Where once COSR finds that any node provided a false CoF, it will punish such node through reducing its reputation level. But the authors have not clearly specified how COSR will decide whether the advertised information is false or not.

2.6 Reputation based secure routing protocol

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.

2.7 Comparison of existing approaches

Table 2.1 gives a comparative analysis of existing approaches.

3. THE PROPOSED APPROACH

This section explains the proposed method in detail.

3.1 Reputation

Reputation is one node's opinion about another node. This reputation system can be used to make decisions about which nodes to include and which nodes to exclude from the network.

3.2 Dynamic Source Routing Using Reputation

The proposed approach is implemented over the existing on demand routing protocol DSR [8], Reputation value of node is used to classify a node as well behaving or misbehaving. Each node uses a monitoring mechanism like "watchdog" to monitor their neighbors. Monitoring the neighbors helps each node to calculate the reputation value of each of its neighbor. Reputation value is calculated using equation (3.1).Suppose there are 'N' nodes in the mobile ad-hoc network. Each node 'n_i' calculates the reputation ($R_{i,j}$)$_t$ for each of its neighbor 'j' at time t.

For each node,

$$R_{(i,j)t} = \frac{\sum_{pkts=0}^{\infty} F_{pkts}}{\sum_{pkts=0}^{\infty} S_{pkts}} \qquad \text{--------(3.1)}$$

Where $R_{(i,j)t}$ is the reputation value calculated by monitoring the neighbor 'j' directly at time 't' and $F_{pkts}$is the number of packets forwarded by node 'j' and S_{pkts} is the number of packets sent by node 'j'. This formula is used to calculate the reputation value of a node by directly monitoring the neighboring node's past behavior for some amount of time. It is also possible to pass this reputation value that is calculated directly by monitoring the neighbors, to the 1 or 2 hop neighbors. But the most reliable and quickest reputation values are those which are directly derived from personal experience.

Table 2.1 Comparison of existing approaches

Mechanism No	What is new?	Advantages	Disadvantages
2.1	Uses first hand information for calculating reputation value. Reputation table is maintained Acknowledgement based	Selfish nodes are identified and isolated No need for promiscuous monitoring of neighbors	Overhead in handling acknowledgements.
2.2	Watchdog, promiscuous monitoring	Identifies and isolated selfish nodes Simple mechanism	Depends on past history-nodes may build credit and start misbehave
2.3	Uses monitor, path manager and trust manager First hand and second hand information is used to calculate reputation.	Identifies selfish nodes	Does not isolate selfish nodes from network Does not deal with how to detect false alarm messages.
2.4	A new node called suspicious node and a state model is introduced.	Identifies and isolates misbehaving nodes or encourages suspicious nodes to cooperate.	False alarm messages are not handled well.
2.5	Node behaviour is determined from physical, data link and MAC layer information. Capability of forwarding and route reputation is calculated	Handles most of the attacks	No proper mechanism to detect false information from nodes.
2.6	Eigen vector based centrality First hand and second hand information	Applicable in sparse environment and highly dynamic network	Not dealing with routing attacks.

consists of nodes with lower reputation values. (e.g. less than 0.8). Gray list consists of nodes which are under suspect. Normally a node includes a node in the gray list if it receives an alert message from any one of its neighbor about misbehavior of that node.

Thus classifying a node into well behaving or misbehaving is done based on their reputation value calculated by direct observations. If a node receives an alert message about misbehavior of another node, it can be termed suspicious and kept in the gray list. A node in the gray list will be moved to black list if a node is found to be misbehaving by direct monitoring.

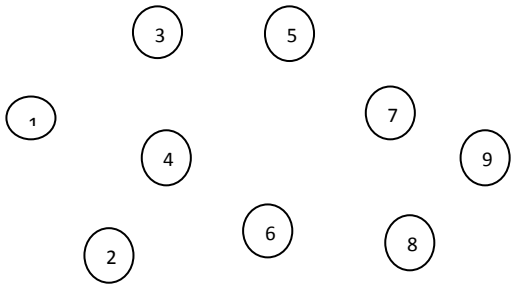

Fig 3.1 Example Scenario Source= 1, Destination = 9

In the first part of the protocol, a node (source node) which wants to communicate with another node (destination node) would search its cache to see whether route is available. If so it will use that route. Otherwise, the source node sends a route request to its neighbors. In normal DSR, route request (ROUTE REQUEST) packet will be sent as a broadcast to all the neighbors of the source node. But here, the source node checks the reputation table of its own and sends the ROUTE REQUEST packet to only those nodes with a higher reputation value i.e. to the nodes in white list.

In fig 3.1, node 1 wants to send packets to node 9. In route discovery phase, node 1 sends ROUTE REQUEST to node 3 and 2. Instead of sending ROUTE REQUEST as a broadcast, our approach sends the ROUTE REQUEST packet only to the neighbors with high reputation value. This reduces overhead in the network. On receiving ROUTE REQUEST from node 1, node 3 and 4 will check their corresponding reputation tables and send the ROUTE REQUEST to the next neighbor only if its reputation value is high. Thus finally the ROUTE REQUEST reaches node 9. As in DSR, the destination will give the RREP (route reply) packet to the source. This route will be a secure route since it avoids nodes with lower reputation. Reputation value decides how trustworthy a node is. Thus the route becomes trustworthy route. A threshold value of 0.8 is set (for simulation purpose) for deciding whether a node is of high reputation value. A node with greater than 0.8 reputation value will be classified as high reputation and kept in white list and below that as low reputation and will be kept in black list. The source node while the process of discovering the route sends the ROUTE REQUEST only to those neighbors with greater than 0.8 reputation value. If there's no such node in the table, then the source node will look for other options like sending the ROUTE REQUEST to nodes with greater than 0.6 and so on. Anyhow by sending the ROUTE REQUEST to only those nodes with high reputation value we can ensure that the ROUTE REQUESTs are not dropped or do not reach the misbehaving nodes.

4. SIMULATION RESULTS

Ns2 [9] is used for simulation. Ns2 is a discrete event simulator, which is widely used for simulation of both wired and wireless networks.

4.1 Simulation Setup

The simulated network consists of 50 wireless nodes deployed in a field of 1200 x 1200 square meters. The random waypoint is chosen as a mobility model. Each node is first randomly placed in the field, waits for the pause time (10 second in our simulation), then moves to another random position with a speed chosen between 1 to 15 m/s. Every 10 seconds during the simulation, ten new source and destination pairs are randomly selected, therefore, every node has chances to be both a source and a destination. The Constant Bit Rate (CBR) traffic is selected as the traffic model. Each simulation is run for 900 seconds.

4.2 The Network Model

Following are the assumptions and network model used in this approach.

1. Each node is identified by a unique, persistent ID.
2. Each node runs a "Watchdog" mechanism to monitor other nodes
3. Network is dense enough to establish communications.
4. Links are bidirectional, i.e. If communication between A to B is possible, then communication between B to A is also possible.
5. Nodes are selfish, not malicious.
6. A node which agrees to forward in routing packets will not drop data packets. This ensures that if a trust worthy route is established between source and destination, then chances of intermediate nodes dropping the packets is less.

The reputation based DSR (R-DSR) is compared with Dynamic Source Routing protocol. The parameters used for performance analysis are 1.Overhead in the network when number of route requests increases 2. Reliability of the route in a network with misbehaving nodes.

Fig 4.1 gives the overhead in the network when the number of route requests increases. As the traffic increases, the overhead increases in DSR protocol. But in reputation based DSR, it manages to be less compared to DSR. This is because, DSR send the Route Request packets to all nodes in the network, where as R-DSR transmits Route Request packets only to the nodes with higher reputation value.

Fig 4.2 shows, that even when the number of selfish nodes are increased, the R-DSR is able to provide reliable communication. This is because R-DSR 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 R-DSR provides better performance compared to DSR

4. 3 Isolating Misbehaving Nodes

This approach not only identifies misbehaving nodes but also isolates them from enjoying 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 makes sure that the misbehaving nodes are punished for their behavior, and once punished it is very difficult for them to re-associate themselves with the network. Hence all the nodes are supposed to cooperate.

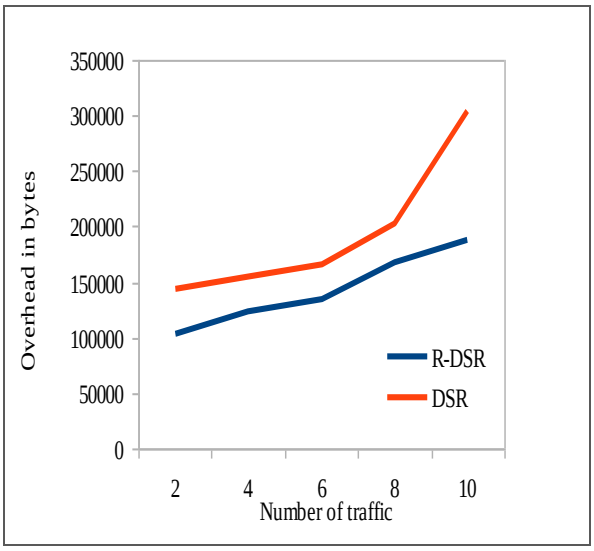

Fig 4.1 Overhead Vs. Number of traffics

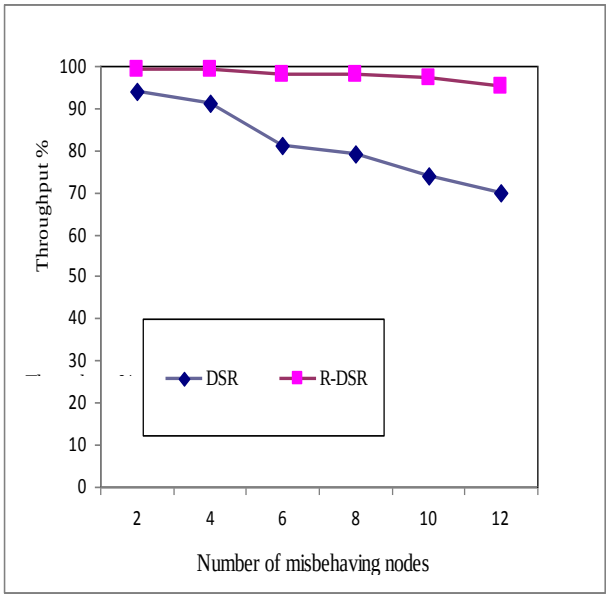

Fig 4.2 Throughput Vs. Number of misbehaving nodes.

5. CONCLUSION

Thus this paper explained about the on-demand routing protocol using reputation mechanism. Our 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. Only by forwarding other nodes' packets a node can maintain a high reputation value. Thus behaving selfish will not help them. This encourages nodes to be cooperative. Here no node is malicious. The aim of

misbehaving nodes is just to conserve energy. But conserving energy for the sake of self-transmission is not possible due to the implementation of reputation mechanism over the routing protocol.

This approach has the clear advantage of simplicity, ability to get a trustworthy route etc. But this approach does not consider the malicious nodes. Malicious nodes may disturb the communication by redirecting the route requests or simply dropping the route requests, or dropping or misdirecting the data packets etc. Since the main concentration of the paper is on the selfish nodes, malicious nodes are not considered.

5. REFERENCES

[1]. Animesh Kr Trivedi1, Rishi Kapoor1, Rajan Arora1, Sudip Sanyal1 and SugataSanyal , " RISM - Reputation Based Intrusion Detection System for Mobile Adhoc Networks" Available from link profile.iiita.ac.in/aktrivedi_b03/rism.pdf.

[2]. M. Tamer Refaei, VivekSrivastava, LuizDaSilva, Mohamed Eltoweissy, " A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks", Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05) , 2005

[3]. PietroMichiardi and RefikMolva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia, 2002.

[4]. Buchegger, Sonja ; Le Boudec, Jean-Yves, "Performance A nalysis of CONFIDANT Protocol: Cooperation of Nodes - Fairness in Dynamic Ad-Hoc Networks," Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC). IEEE, June 2002.

[5]. TiranuchAnantvalee, Jie Wu: Reputation-Based System for Encouraging the Cooperation of Nodes in Mobile Ad Hoc Networks", Proceedings of International conference of Communications, pp 3383-3388, 2007.

[6]. Fei Wang. Furong Wang, Benxiong Huang, Laurence T. Yang,"COSR: a reputation-based secure route protocol in MANET "in Journal EURASIP Journal on Wireless Communications and Networking - Special issue on multimedia communications over next generation wireless networks archive Volume 2010, pp. 1-11, January 2010.

[7]. Sameh R. Zakhary and Milena Radenkovic ,"Reputation-based security protocol for MANETs in highly mobile disconnection-prone environments" in International conference on Wireless On-demand Network Systems and Services (WONS), PP. 161 – 167, Feb. 2010.

[8]. David B. Johnson, David A. Maltz, v "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", draft-ietf-manet-dsr-09.txt, 2003.

[9]. Ns2 - www.isi.edu/nsnam/ns/ns-tutorial/tutorial-02.