ISSN:0975-9646

A Trust Based Scheme to Encourage Packet Forwarding in Mobile Ad-hoc Networks

Deepak Kumar Dixit, Praveen Kaushik

Department of Computer Science and Engineering, MANIT, Bhopal
MANIT, BHOPAL, INDIA

***Abstract*-- In a mobile ad hoc network (MANET), each node has to rely on intermediate nodes to relay its packets. Since most mobile nodes are constrained with resources such as bandwidth, power, and memory thus some nodes may choose not to cooperate while still using the network to forward their own packets. Most previous works focus on data forwarding. However, by choosing not to participate in the route discovery process by dropping Route Request (RREQ) is a better strategy for selfish node to avoid them from being asked to forward data packets. In this paper, we present a new mechanism to detect those selfish nodes. Each node is expected to contribute in the network and those which fails will undergo a test for their suspicious behaviour.**

***Keywords*-- Selfish Nodes, Mobile Ad-Hoc Networks (MANETs), Reputation, Direct Trust**

I. INTRODUCTION

Mobile Ad-hoc network (MANET) is infrastructure less, self organising network in which nodes which are participating has responsibility for creation, operation and maintenance. As the transmission range of the nodes in MANET is limited, so to transmit the information beyond their transmission range, node requires intermediate nodes to co-operate in routing and forwarding. In this multi hop communication, each node operates as both host and router. Routing protocol such as DSR [8], AODV [11] have been designed to handle such environments. The features such as minimal configuration, quick deployment, and no central governing authority make Ad hoc network suitable for emergency situations such as disasters, military conflicts and emergency medical situations [18]. When a node joins the network its task is to provide functions (such as routing and forwarding) to other nodes in the network and in turn newly joined node gets connectivity to the network. Such reciprocity principles are necessary for trust establishment among nodes. Adjacent nodes build up trust among them and distribute it across the network as reputation. However some nodes may easily follow these reciprocity principles in order to be connected to the
MANET but their intensions are bad such nodes are categorized as selfish nodes, malicious nodes, and hacker nodes. A selfish node may decide not to cooperate to save its resources while still using network to forward its own traffic. A malicious node tries to attack the network through various ways such as denial of service attack (DoS attack, such as sinkhole attack, flooding or sleep deprivation torture [17]), Sybil attack [13] to minimize network operations and minimize network throughput. Selfish node and malicious node misbehave and intentionally or unintentionally attack on the robustness of the MANET. A hacker node tries to capture information being transmitted between source node and destination node.

Selfish behaviour exhibited by a significant number of nodes may disrupt network operation and should be prevented; but because of the self-organising architecture of MANET prevention is only possible through creation of incentives for cooperative behaviour. In the last decade this issue has gained considerable attention, a rigorous game-theoretic approach (whereby cooperation should occur at equilibrium of a suitably designed inter-node game) is accompanied by various heuristic approaches, mostly in the form of reputation systems [4][15].

The rest of the paper is organised as follows. In Section II, we briefly describe the AODV (Ad-hoc on Demand Distance Vector Routing) protocol which is used for our proposed work. In Section III, we categorize types of misbehaviours in MANET. In Section IV, we summarize some of the existing solutions in order to motivate our approach. Section V, presents our ideas of mechanism for detection and cooperation enforcement. We conclude the work in Section VI.

II. AODV ROUTING PROTOCOL

Our proposed work is build upon AODV routing protocol with some modifications to the RREQ header. In the standard protocol when a source node S wants to communicate with a distant destination D which is outside source transmission range, node S starts a route discovery to find a route to destination D as depicted in Fig. 1.

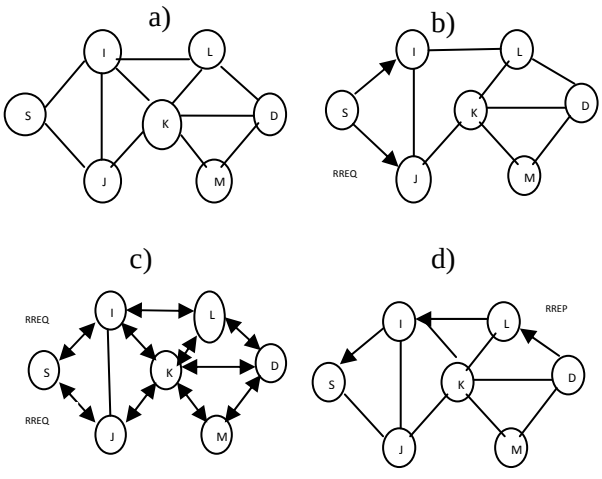

Fig. 1 AODV Operation; a) Network Topology, b) - d) Route Discovery

The process is started by broadcasting Route Request (RREQ) messages to the one hop neighbours, each node receiving such messages checks for the route in its local routing table to the requested destination D. If it does not contain the route then it forwards the packet to its direct

neighbours. If any one of them contains an appropriate route to the destination or is itself a destination, it returns a Route Reply (RREP) to node. All intermediate nodes forwarding this RREP message back to the source node update their local routing tables accordingly. In the end the source can get more than one route to the destination then it chooses the route which has minimum number of intermediate nodes.

III. NODE MISBEHAVIOURS IN WAN

In wireless Ad-hoc networks it is assumed that nodes are willing to cooperate in performing the networking tasks. This can only be guaranteed when all the nodes are under a central authority and having the same common objective. However that is not the case such as in civilian applications, some of the nodes may behave selfishly to increase their own profit. Providing services such as forwarding packets consumes resources such as battery, bandwidth, local CPU time, and memory which are limited in WAN nodes [7].

In general there are two types of node misbehaving: misleading and selfish. A misleading node is selective in choosing which packet it wants to respond. It behaves like an honest node; respond to all control packets during route discovery process. However, when the node receives a data packet it silently drops it. The reason behind dropping is that the size of the data packet is much larger than the control packets, thus it takes more resources to forward. This type of behaviour is also termed as "Gray Hole Attack" [1]. The second type of misbehaving node is selfish node. A selfish node discards all the packets (data and control packets) except those which are destined for it. By dropping control packets, the node escapes from routing and then be released from being requested to forward data packets. The similarity of these two types of misbehaving nodes is that they both use the network to forward their own packets but refuse to provide the service back. In this paper we present a mechanism to detect the selfish nodes and enforce them to cooperate to enhance packet forwarding in the network.

IV. RELATED WORKS

Several schemes have been proposed to identify selfish nodes in mobile ad hoc networks. These schemes can be classified into three categories: credit based schemes, reputation based schemes, and acknowledgement based systems. For credit based schemes [9][12] packet forwarding is considered as a service, so each node which performs the forwarding function correctly is rewarded with incentive. The node's contribution can be relaying other node's packets or paying credits, whereas node's benefit can be relaying its packets or earning credits. As these models incorporate virtual currency and colluding nodes can agree to forward their own packets to accumulate credits while dropping all other nodes packets, so to regulate the dealings they require temper proof hardware or a central authority as a virtual bank.

Reputation based schemes on the other hand uses reputation to forward packets through the most reliable path in the network. The reputation of a node can be defined as the perception of one node regarding the performance of another node during the execution of a network protocol [2]. The reputation of a node increases when it forwards the packets in right way without altering their fields. Some of the models also incorporate techniques which isolate the misbehaving nodes which are with low reputation value (RV). Reputation schemes are further subdivided into two subclasses. In first subclass each node observes its neighbouring nodes to take a routing decision and it does not exchange the RV's of its neighbour with other nodes, these models are known as first hand reputation models [6][10][16]. A monitoring method used by most of the systems in this category is Watchdog proposed by Marti et al. [16] to detect data packet non-forwarding by overhearing the transmission of the next node.

The second hand reputation models [5][14][15] use similar monitoring scheme but then propagate collected information to nearby nodes and are susceptible to false praise and false accusation attacks. The last category is acknowledgement-based scheme which rely on the reception of an acknowledgement to verify that a packet has been forwarded. Liu et al. [3] proposed the 2ACK scheme where nodes explicitly send acknowledgement two hops upstream to verify cooperation. This scheme is susceptible to collusion of two or more consecutive nodes. Furthermore, colluding nodes can frame honest ones by claiming not to receive the acknowledgement.

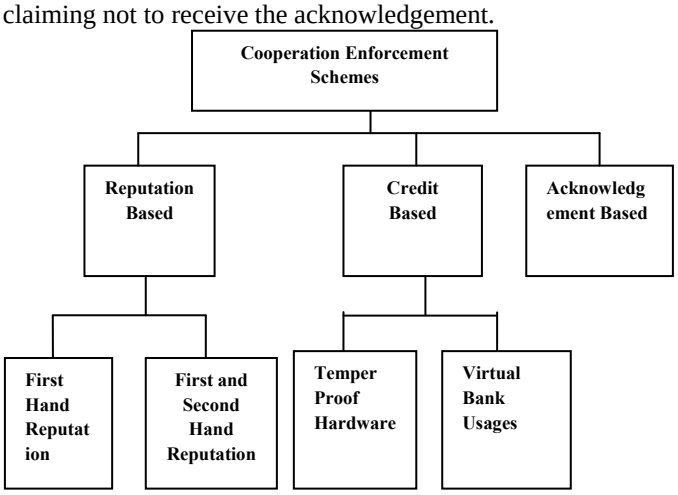

Fig. 2 The Taxonomy of the Cooperation Enforcement models proposed for MANET's

V. OUR PROPOSAL

We argue that if a node merely intends to save its own resources then it is easier for the node to become selfish node, discarding all the packets (data and control packets) that are not destined for it. The techniques which monitor data forwarding for identifying selfish nodes are not effective as a selfish node might choose not to participate in the route discovery phase by discarding Route Request (RREQ) messages and thus would not be used to forward data packets. Furthermore, some well behaved nodes in the network might not be required to forward data packets. Example of these nodes is the nodes located at the edge of the network. At that location, the node does not have any data packet to forward.

Our proposed works on Trust calculation and uses AODV routing protocol. The Trust mechanism performs two functions: (a) Identification of selfish nodes by monitoring control packets forwarding (b) Notifying the neighboring

nodes about selfish nodes. in our proposal we assume following:

- Each monitoring node operates in promiscuous mode, i.e., each node listens to RREQ packet transmitted by its neighbours even if the packet is not intended for it.
- A node may be selfish but not malicious. A node may be selfish in terms of saving its own resources but will not perform any function that could be more expensive in consuming resources than cooperating in packet forwarding.

In our scheme, all the nodes broadcast HELLO message to identify their neighboring nodes. Each node maintains a forwarding table which contains following fields:

- N_{id} :- It is the address of neighbouring node.
- P_s (*i, j*) :- Number of packets sent for route request by node *i* to node *j*.
- P_f (*i, j*) :- Actual number of packets of node *i* forwarded by node *j*.
- DT (*i, j*) :- Direct trust value of node *j* computed by node i.
- Flag (*i, j*) :- Boolean variable, when set shows that node *j* is selfish for node *i*.
- AC (*i, j*) :- Value of Alarm count for node *j* at node *i*.
-

Whenever a node S has a data packet to send to destination D, the source node S broadcasts RREQ message to all its neighbours, increment the $P_s(i, j)$ field of all the neighboring nodes and goes in the promiscuous mode to monitor neighboring nodes. when the neighboring nodes receives the RREQ message they search for the route in their local route table, if it exists then send Route Reply (RREP) message to the source or further broadcast RREQ to their neighbors. After monitoring the successful transmission of the RREQ the source node S increments the $P_f(i, j)$ field of the corresponding node. If the RREQ message is dropped by any of the node then $P_f(i, j)$ will not get incremented for that node. Thus all the nodes have a count for the number of times services demanded by a node and number of times services provided by the same node.

Now for E.g., if a node S wants to communicate with destination node D and Route Reply (RREP) has come as S-A-B-C-D, where node A is the next hop to the source node S. now node S will send the data packet to the intermediate node A, here node A calculate the direct trust value of node S as follows:

$$DT(A, S) = P_f(A,S) / P_s(A, S)$$

Now if DT(A, S) > threshold value or DT(A, S) = threshold value then the data packet of the source node S is forwarded to the next intermediate node B. otherwise, if DT(A, S) < threshold value then the node A checks the Flag value corresponding to node S if it set to 1 then node A drops the data packet of node S, otherwise set the Flag corresponding to the node S and increments the AC(A, S) by one and checks the value of AC(A, S) if the AC(A, S) = number of neighboring nodes of S then the node S is declared as selfish and none of the neighbour of node S will forward the data packets of node S, or if AC(A, S) < number of neighboring nodes of S, then the node A broadcasts the AC(A, S) to all its neighbors, and the neighboring nodes replace the old value of AC(A, S) by the newly received value.

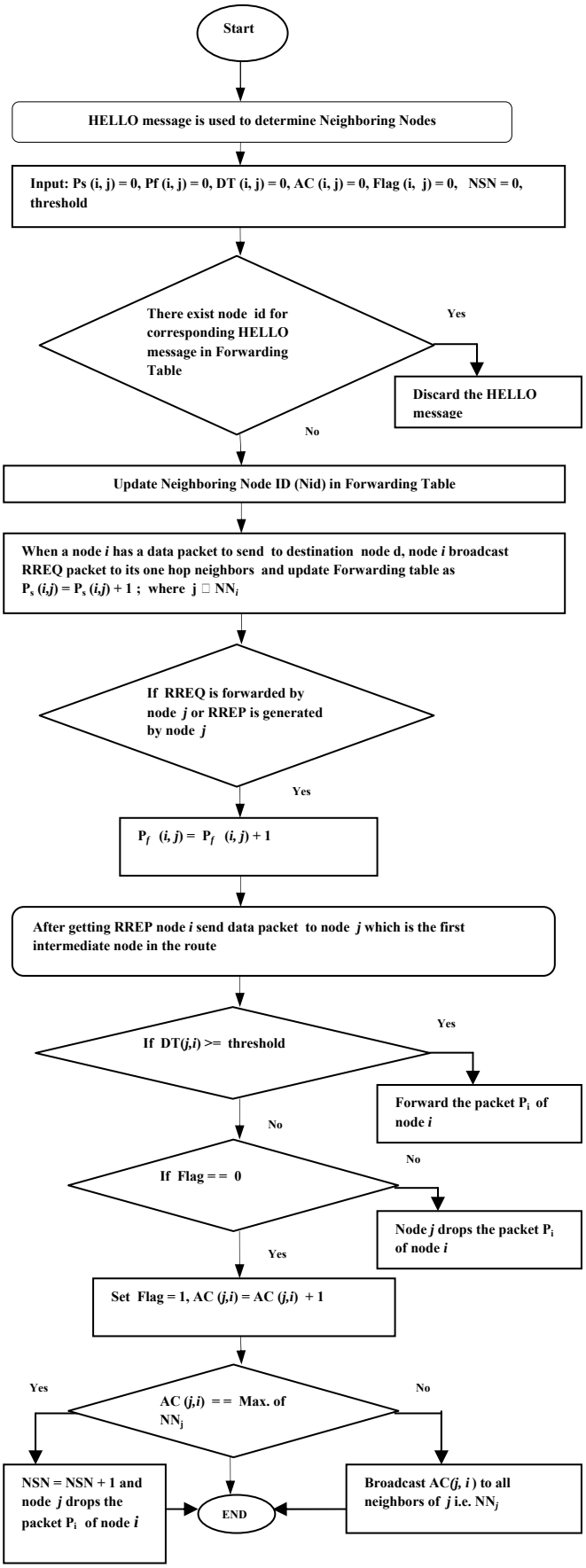

Fig. 3 Flow graph of proposed work

As the node S is not been able to communicate with the Destination D, and if it want to come into the network once again it has to participate in the route discovery process for other nodes by forwarding the RREQ of other nodes and increase its direct trust value at other nodes. In our scheme, each node considers its own personal decision for forwarding the packets.

VI. CONCLUSION

In this paper, we propose a new scheme to detect selfish nodes and encouraging them to packet forwarding and discipline selfish behaviour in non- cooperative ad hoc networks. Our scheme monitors the node behaviour during route discovery phase, thus more effective in identifying selfish nodes. If a node is mistakenly declared as selfish then it can easily increase its trust value by forwarding more control packets, thus the scheme provides second chance to the node to join the network make use of the network services once again.

REFERENCES

[1] G. Xiapeng and C. Wei, "A novel gray hole attack detection scheme for mobile ad-hoc networks," in IFIP International Conference on Network and Parallel Computing, pp. 209–214, September 2007.

[2] Hu, J., Burmester, M., "LARS: a locally aware reputation system for mobile ad-hoc networks", in 44th annual ACM Southeast Regional Conference, 2006.

[3] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in manets," in IEEE Transactions on Mobile Computing, pp. 536–550, 2006.

[4] T. M. Refaei, V. Srivastava, L. Dasilva, and M. Eltoweissy, "A Reputation- based mechanism for isolating selfish nodes in ad hoc networks", Proc. 2nd Annual International Conf. on Mobile and Ubiquitous Systems: Networking and Services, San Diego, CA, USA, pp. 3-11, 2005.

[5] He Q, Wu D, Khosla P.,"SORI: a secure and objective reputation- based incentive scheme for ad-hoc networks," In Proceedings of IEEE WCNC2004, March 2004.

[6] Dewan P, Dasgupta P, Bhattacharya A., "On using reputations in ad hoc networks to counter malicious nodes," In Proceedings of QoS and Dynamic Systems, July 2004.

[7] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Communications, vol. 11, pp. 38–47, 2004.

[8] J. Broch, D. B. Johnson, and D. A. Maltz, "The dynamic source routing protocol for mobile ad hoc network," in IETF, internet Draft Version 08, February 2003.

[9] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in INFOCOM 2003, 2003.

[10] Bansal S, Baker M., "Observation-based cooperation enforcement in ad-hoc networks," Techical Report, Stanford University, 2003.

[11] C. Perkins, E. Belding-Royer, and S. Das, "Ad-hoc On-Demand Distance Vector (AODV) routing", http://tools.ietf.org/html/rfc3561, 2003.

[12] L. Buttyan and J. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," in Mobile Networks and Applications, vol. 8, no. 5, pp. 579–592, October 2003.

[13] Douceur J., "The sybil attack," In Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS02), March 2002.

[14] Michiardi P, Molva R., "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," In Proceedings of 6th IFIP Communication and Multimedia Security Conference, September 2002.

[15] S. Buchegger and J-Y. Le Boudec, "Performance analysis of the CONFIDANT Protocol: Cooperation Of Nodes – Fairness In Distributed Ad-hoc Networks", Proc. IEEE/ACM MobiHOC, Lausanne, Switzerland, pp. 226-236, 2002.

[16] Marti, S., Giuli, T. J., Lai, K., Baker, M., "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", in ACM MobiCom 2000 Conference, 2000.

[17] Stajano F, Anderson R., "The resurrecting duckling," In Proceedings of 7th International Workshop on Security Protocols, 1999.

[18] E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad-hoc mobile wireless network," IEEE Personal Communications, vol. 6, pp. 46–55, Apr 1999.