International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-4 Issue-6 December-2012

Softening Misbehaviour of Nodes and Enforcing Cooperation in Mobile Ad Hoc Networks

Atul Kumar Purohit[1], Mukesh Kumar Baghel[2], Hitesh Gupta[3], Parmalik Kumar[4]
Department of Computer Science, Patel Collage of Science and Technology, Bhopal, (MP), India[1, 2, 3, 4]

Abstract

In Ad-Hoc Wireless network nodes have constraints of resources like CPU cycles, memory, battery power, software, because of which they are not always willing or able to forward others data over the network even if they have previously agreed to do so; also nodes owned by different entities can try to harm the network. These kinds of misbehavior of nodes can be categorized as broken, selfish and rational, overloaded or malicious. Misbehavior increases probability of dropping packets and route failure, which decreases networks performance drastically. We deal with misbehavior by proposing an approach (based on already existing Generous TIT-FOR-TATE algorithm) for forwarding the data packets of nodes, assuming nodes are self-interested and energy constrained. We modified the algorithm for best of our use. Results shows that our approach limits the effect of all kind of misbehavior to a particular class of nodes (classified on the basis energy) and rest of the network remain unaffected. Our approach also motivates nodes cooperate for receiving better service from network. Our approach is standalone to handle above all kind of misbehavior and to for the motivation of cooperation among nodes (that is no supports from other).

Keywords

False Accusation, GTFT, Nash Equilibrium, Optimality, Network Performance

1. Introduction

Ad hoc wireless network is a decentralized, autonomously self-organizing network with wireless connectivity, formed dynamically through the cooperation of an arbitrary set of independent nodes, sometimes mobile. The network is ad hoc because it does not rely on a pre-existing infrastructure. Instead, mobile nodes that are within radio range of each other communicates directly via wireless links, while those nodes that are far apart rely on other nodes to relay messages as routers or intermediate nodes. It typically refers to a set of networks where all devices have equal status and are free to associate with any other devices in radio range. In such networks nodes can be a laptop, mobile phone, sensor and similar kind of devices which have sufficient processing power, energy and memory units with wireless links, makes them enable to roam around until battery lasts. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts and also other handful applications scenarios ranging from home and car to office.

Wireless ad hoc network is emerging rapidly as the number of users is increasing with which expectations, applications are also increasing and so as the designing challenges. However above prospects made wireless ad hoc network an obvious choice, still there are some open issues and designing constrains which need to be addressed. Some of the major issues are

- Limited wireless transmission range many times leads to partitioned network
- Packet losses due to noise and mobility cause lower network performance
- Mobility induced route changes increases latency in the network
- Security related threats: Mobile wireless networks are generally prone to physical security threats. The increased possibility of eavesdropping, spoofing, and minimization of denial-of-service type attacks should be carefully considered.
- Dynamic Topologies: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable times.
- Nodes misbehavior or noncooperation of the nodes can cause lower throughput of the network
- Fairness of service provided by the nodes and service received by the node cannot be guaranteed.
- Many other issues are also hindering wireless ad hoc networks such as limited

bandwidth, node addressing issues, better Quality of Services (Qos) requirement

Many researchers are working on the various issues mentioned above separately. The scope of this work is limited to handle the misbehavior (non-cooperation) of the nodes. Cooperation or fair behavior of the node is considered as willingly and actively participating in the routing, by a node to route the data of other nodes.

Wireless Ad hoc Network is an interconnection of nodes with wireless links, are temporary in nature, can be mobile and have dynamic, distributed nature. In such networks, nodes can be a laptop, mobile phones or sensors with some limited amount of battery power, which enable nodes to roam around until batteries lasts. Nodes either transmit directly or through intermediate nodes, which can relay the data to the destination. But in reality nodes does not always cooperate and starts misbehaving. If most of the nodes deny to forward the data of other nodes then network will no longer exist or if exist then will have a poor performance. If more number of nodes not forward data packets, aggregate utilization of bandwidth decrease, shorter paths will not be available, probability of dropping of packet will increase and hence probability of route or network failure will increase, lead to poor performance of network [1], [2]. Nodes misbehave if they are (a) overloaded: if a node has memory, CPU cycles or bandwidth lesser than required. In such situation because of lack of resources node is not able to cooperate even if it wants to, (b) selfish: if a packet is not of interest of a node then it may be unwilling to spend its own battery memory space, and CPU cycle and deny for cooperation, (c) malicious: tries to harm a node or to harm the network by dropping packets, tampering packets, duplicating packets, analyzing packets, misleading about the identity of source or the route, or by collusion, (d) broken: might have a software fault which may cause misbehavior of node [1].

In Wireless Ad hoc Networks Cooperation is to willingly participate in relaying of packets for other nodes by a node without considering any personal benefits. But in reality current approaches yields to failures as nodes are rational and starts misbehaving. Cooperation, along with misbehavior of nodes is considered as a major issue because it leads the network towards poor network performance. Some of the cooperation informant techniques are either incentive based (Watchdog [3], scheme based on 2-Hop Acknowledgment [4]) or reputation based (CORE [2], CONFIDENT [5], SPRITE [6], OCEAN [7]) but all are having some pros and cons. We studied and compared above schemes is done to know which one has an edge on other in different scenarios and on different parameters. All above techniques are having some of the drawbacks namely Latency Problem, Lower Throughput, False Misbehavior and False Accusation. A different approach from above schemes is used in this work.

In this paper we try to limit the misbehavior and effect of misbehavior on the network, simultaneously we try to encourage nodes to cooperate for forwarding data packets. We consider nodes as rational and self-interested. Nodes always try to get more service from the network and try to serve lesser to the network. Nodes can get maximum service from the network only when they adopt policy to serve the same amount of service to the network, which they get from the network with some generosity. Adopting this policy by many nodes, for forwarding data packets of other nodes, if some node misbehaves then they will not be served by the other nodes, but rest of the network will be served and hence the network performance will not be degraded drastically. Except broken nodes, all other types of misbehaving nodes will try to behave sincerely to get served from the network is such network.

Remaining of the paper contains the network model for the approach in section 2. In section 3 we explain the approach and the algorithm for forwarding data packets of other nodes. We consider misbehaving nodes and analyze the results in their presence in section 4 then we conclude in section 5.

2. Network Model

Consider some finite amount of nodes in the network with some energy associated with them. C Nodes can be classified on the basis of energy. Network randomly selects source and destination among all nodes for a particular connection. There can be any number of intermediate but less than total number of nodes in network. Source relays the data packets to destination via intermediate nodes. Intermediate nodes will either forward the data packets or drop it, in both cases they inform to source by acknowledgments either positive or negative. On getting negative acknowledgement source retransmits the packet. The amount of service node gets from the network is measured by the ratio of number of packets forwarded by intermediate nodes and total number of packets sends by the node to forward as a source. Similarly the service delivered by a node is the ratio of number of packets forwarded by the node as an intermediate node and total number of packet it gets from other nodes to forward them. Network can have nodes which misbehave as they can be broken, overloaded, selfish or malicious. We clearly states here that nodes which are malicious are due to only collusion, that is few nodes secretly agreed to serve each other and not to the network and all other types of maliciousness is beyond our scope.

The mathematical modelling of the network and behaviours of the node is done by system of nonlinear equations for finding the probabilities by which a node can forward the packets and by game theoretic approach for the behaviours of the nodes. The approach is based on past experiences of a node for all other nodes.

3. The Approach

Nodes are having limited energy so it will not be best of their interest to forward others packet. We assume that they will get one amount as payoff on forwarding a data packet, this can be realize by using some tamper proof incentive based system as used in many cooperation techniques [3],[4]. Node will always try to optimize their benefits, that is node will always try to maximize their payoff subject to the energy required to forward a packet must be less than or equal to average amount of energy particular class of node can have. There is a need to find the probability by which nodes can forward the data packets for nodes of different classes. This can be done by equating the subject to condition of optimization, based on the energy constrains of that particular class. Which can be calculated by summing over all possible combinations that a network can achieve weighted with the probability of acceptance. Generous TIT-FOR-TATE (GTFT) proposed in [8] for cooperation. We modified and used it in this work for forwarding data packets for the network to reaches to the Nash Equilibrium [9], [10] as proved in [8]. Nodes which behave sincerely will apply the algorithm for forwarding data packets. If a node (which is not a misbehaving node) gets a data packet to forward from a node of particular class, then it will do the following:

- If node has served more than the probability of providing service OR node has received lesser amount of service than it already served to the nodes of that particular class with some generosity; then drop the packet.
- Else forward the packet.

To add generousness it is required that nodes will serve a little more as compare to what they gets from the network. Appling the above algorithm nodes can optimize their benefits and the network will converge to the Nash Equilibrium for serviced received by the nodes of particular class as it is the property of GTFT [5]. Only those classes will not converge which have misbehaving nodes. This will limit the effect of misbehaviour and network performance will not decrease drastically, also the incentives motivate the misbehaving nodes to forward others data packets when nodes are not broken. Results in following section support our arguments.

4. Simulation and Results

Considering 20 nodes in the network which are categorized in 5 classes according to their different energy levels they have, each class have exactly 4 nodes. The average energy of classes is 0.03, 0.025, 0.020, 0.015 and 0.010 respectively. There are maximum 18 relays in the network, network can be of smaller than or equal to 18 hops. Considering the network scenario, the probability of forwarding data packets is calculated.

	C-1	C-2	C-3	C-4	C-5
C-1	0.79	0.51	0.33	0.20	0.11
C-2	0.51	0.51	0.33	0.20	0.11
C-3	0.33	0.33	0.33	0.20	0.11
C-4	0.20	0.20	0.20	0.20	0.11
C-5	0.11	0.11	0.11	0.11	0.11

We show in table 1 the probabilities when there are exactly 18 relays. Where, C- 1 to C-5 represents the class number. Source of class i and intermediate node of class j, has the probability in row i, column j. When there is no misbehaving node the network converges to the above values, as shown in figure1.

In figures curve with empty Squares represents class 1, curves with solid squares, empty circles, solid circles and triangles represents curves of class 2, 3, 4 and 5 respectively. Now consider a scenario where 3 among 4 nodes of class 3, are broken then only class4 not converges as shown in figure 2, this shows that the effect of broken node are limited to nodes of class 3 only. Only class 2 not converges to the optimality.

Similarly figure 3 shows that if nodes of class 4 are overloaded then class 4 not converges to optimality. Next we considered that nodes of class 2 are selfish and never forward the data packets of other nodes. Figure 4 shows that this affects only to the class 2, but all other classes achieve convergence and this motivates them to conduct properly. Now in last scenario we consider that the nodes of class 3 are malicious (only collusion is considered) then the resulting graph indicates that again the nodes which misbehaves are not receiving optimal service from the network, but rest are so they are limited to affect the network.

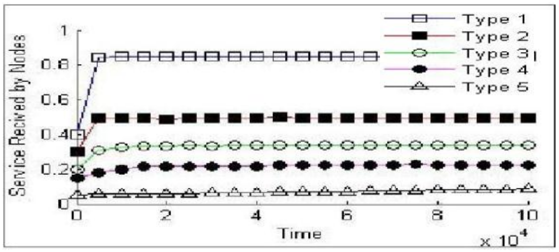

Figure 1: Convergence Graph

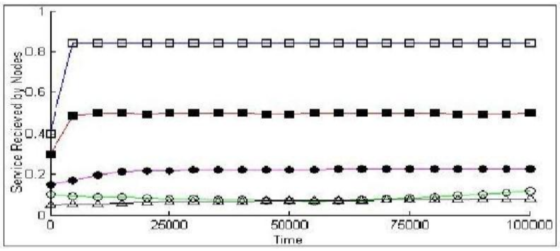

Figure 2: Convergence when nodes are broken

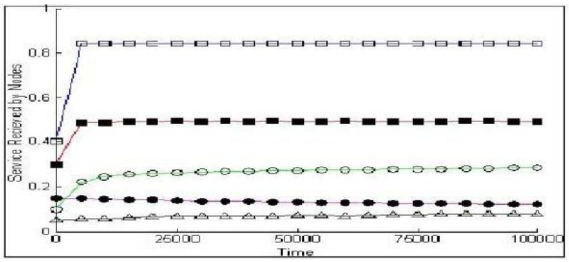

Figure 3: Graph when nodes are overloaded

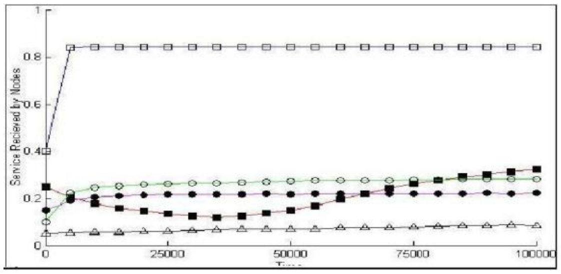

Figure 4: when nodes of class 2 are selfish

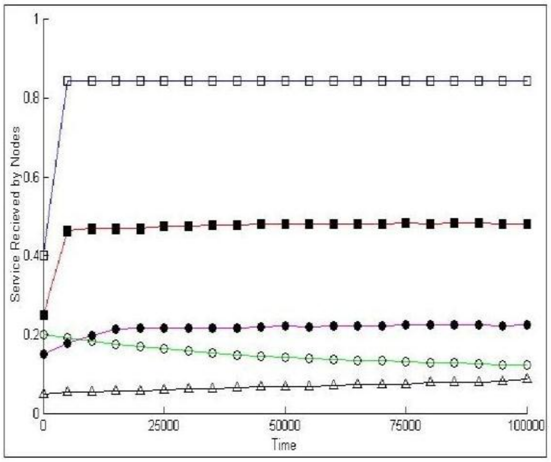

Figure 5: Graph when nodes are malicious

Figure 5 shows the results of the scenario where the curve with empty circles fails to attain optimality and receives lesser from the network as they are not serving the network sincerely. The analysis of the results shows that this feature is adopted by the approach because the algorithm uses for each node uses the past values for it experienced earlier and behave same with some generosity.

5. Conclusion and Future Work

Ad-Hoc Wireless network has valuable contribution in the area of Wireless communication as in most of the cases nodes is mobile, however not evolved fully yet. Misbehaver of the nodes is a definite problem with this kind of network. We addressed the problem in this work and able to limit the effect of broken, overloaded, selfish and malicious (collusion) nodes by applying the above approach. If such nodes relay less data than they has to be then they get lesser service from network. Our results shows that we can limit the effect of misbehaviours to certain nodes and remaining of the network can reach to its optimal performance. Our approach involves both isolation and incentives which motivates all the nodes in the network to behave sincerely that is nodes cooperates in forwarding other nodes data packets. This will lead to the better performance of networks.

This work is a complete framework to address the problem of misbehaviour and cooperation, but still there is a need to address issues related to the implementations such as propagation of information amongst nodes, protocol designing related issues. Security related issues that are all other type of maliciousness are required to be addressed. An assumption which is made in our work related to acknowledgements is left to be addressed. A deeper comparison with all other types of incentive based and reputation based schemes with respect to the pros and cons of them are required to be complete. We hope that all these future work accomplishment will make our work for realization in the real world.

References

[1] Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," in Proceedings of The Sixth International Conference on Mobile Computing and Networking 2000, Boston, MA, Aug. 2000.

[2] S. Buchegger and J.-Y. L. Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," in 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, 2002.

[3] Buttyan and J. P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs," Proc. of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Boston, MA, USA, August 2000.

[4] Sheng Zhong, Jiang Chen, and Yang Richard Yang, Sprite: A simple, Cheat proof, Credit-based System for Mobile Ad Hoc Networks, in Proceedings of IEEE Infocom '03, San Francisco, CA, April 2003.

[5] Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol" in Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC). IEEE, June2002.

[6] Michiardi and R. Molva. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In IFIP Communication and Multimedia Security Conference 2002, Aug 2002.

[7] Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks", 2003 available at: www.citeseer.ist.psu.edu.

[8] V Srinivasan, P Nuggehalli, C.F. Chiasserini, "An Analytical Approach to the Study of Cooperation in Wireless Ad Hoc Networks". IEEE Transactions on Wireless Communications March 2005.

[9] Binmore, Ken G; "Game Theory A Very Short Introduction" Oxford University Press 2007.

[10] Baron, "Game Theory an Introduction", A. J. Willy & Sons, Inc. publication, 2007.