Different Approaches on Cooperation in Wireless Ad Hoc Networks

Raju Barskar
Student Of M-Tech CSE
MANIT, Bhopal (M.P) INDIA

Gulfishan Firdose Ahmed
Assistant Professor
MANIT, Bhopal (M.P) INDIA

ABSTRACT

Wireless Ad hoc Networks: is an interconnection of nodes which are mobile, have wireless links with temporary connections and without any centralized control. All this properties makes the network dynamic in nature. To communicate with each other over distance, nodes either can transmit directly or through intermediate nodes, which can relay the data to the destination, but such paths are contemporaneous in such networks. To improve the performance of such network, nodes must remain available to route and forward the data packets of other nodes. Since wireless nodes are energy constrained, it may not be in the best interest of a node to always accept relay requests. On the other hand, if all nodes decide not to expend energy in relaying, then network throughput will drop dramatically. Both these extreme scenarios (complete cooperation and complete noncooperation) are inimical to the interests of a user. Mobile ad-hoc networking works properly only if the par- participating nodes cooperate in routing and forwarding. How-ever, it may be advantageous for individual nodes not to cooperate. In this paper, we consider selfish node behavior in ad hoc networks and discuss trust and many reputation mechanisms that will stimulate cooperation between nodes. In this paper, we address the problem of service availability in mobile ad-hoc WANs. We present a secure mechanism to stimulate end users to keep their devices turned on, to refrain from overloading the network, and to thwart tampering aimed at converting the device into a "selfish" one.

General Terms

Security, virtual currency,Watchdog.

Keywords

Cooperation, reputation wireless ad hoc networks, fairness, robustness, trust.

1. INTRODUCTION

In today's world computational devices have enough processing power and memory such as cell phones, laptops, sensors, with sufficient amount of rechargeable batteries. Also the emergence of wireless communication makes possible for them to roam around and remain connected with each other. So from past decade a new kind of network is evolving namely Wireless Ad hoc Networks. *Wireless Ad hoc Networks:* is an interconnection of nodes which are mobile, have wireless links with temporary connections and without any centralized control. All this properties makes the network dynamic in nature. To communicate with each other over distance, nodes either can transmit directly or through intermediate nodes, which can relay the data to the destination, but such paths are contemporaneous in such networks. To improve the performance of such network, nodes must remain available to route and forward the data packets of other nodes. If more number of nodes remains available for routing the packets, aggregate utilization of bandwidth will increase, shorter paths will be available, probability of dropping of packet will decrease and hence probability of route or network failure will decrease, which will lead to better performance of network. When the nodes are owned by single authority such as military, sensor network deployed by any institution or organization, nodes will remain available to relay packets of other nodes. But when the nodes are owned by individuals for example laptops with wireless links owned by the students of an institute can constitute Wireless Ad hoc Network. They are able to take there own decisions. In such case either node, can behave rationally that is each node wants to maximize its own benefits with minimum efforts or due to lake of resources such as battery, memory space, and CPU cycle; dose not cooperate and so the network performance decreases. In Wireless Ad hoc Networks *Cooperation*: is to willingly participate in relaying of packets of other nodes by a node without considering any personal benefits or non cooperation is to deny for relaying packets of other nodes by a node. But in reality nodes dose not always cooperate since they are rational and starts misbehaving. There are some issues related to Cooperation:

2.COPERATION AS A PROBLEM

2.1 Resource Limitation: Consider a scenario of a campus where students having laptops, can constitute a Wireless Ad hoc Network over a particular area like cafeteria, library or class room. The laptops are having limited amount of power. Students wants there laptop to last not before day ends. To communicate they need to relay each others data (cooperative behavior), which will consume some energy. If they relay all the packets then they will run out of power. So they starts rejecting the relay request (non cooperative behavior), leads to degrade in network performance. Similar type of case will also happen with other resources like CPU and memory.

2.2 Security: In a wireless Ad hoc Network if the nodes are owned by single entity such as military then they works cooperatively but if node are owned by different entities link in above scenario then they may not cooperate or if cooperate they can be of malicious in nature. They can try to cause harm to network or a particular node by:

2.2.1 Denial of Service (Dropping the packets)
2.2.2 Integrity of Packets (Tampering the packets)
2.2.3 Confidentiality (revealing the identity of other nodes)
2.2.4 Authentication (changes the identity of sender)
2.2.5 Eavesdropping (Overhearing and analyzing others packet)
2.2.6 Diverting the flow of packets
2.2.7 Collusion.

2.3 Fairness: What ever may be the reason if there are nodes in wireless Ad hoc Network can be a) always drops others packet, b) occasionally drops others packet, c) never drops others packet, in all the cases services provided by a node is different from others, but the amount of service received by the nodes are same then it would be not fair to the nodes of type c.

If most of the nodes deny to cooperate then network will no longer exist or if exist then will have a poor performance. So to enforce the cooperation amongst node in Wireless Ad hoc Networks is a must. Nodes can misbehave if they are [1]:

2.4 Overloaded: When a node have 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.

.

2.5 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.

2.6 Malicious: tries to harm a node or to harm the network by dropping packets, tampering the packets, duplicating the packets, analyzing packets, or by misleading about the identity of source or the route.

2.7 Broken: might have a software fault which may cause non cooperation of node.
Thus this non cooperation or misbehave of the nodes will degrade the performance of the network so it is necessary to mitigate the problem of misbehaving nodes.

To stimulate the cooperation in Wireless Ad hoc Networks two things are required:

- **Mechanism for the detection of non cooperative nodes**
  - Watchdog [1]
  - Hop Acknowledgment [2] Context Aware Selfish Node Detection [3]
- **Cooperation enforcing mechanism for non cooperative nodes**
  - Incentive Based Schemes [4], [6], [7]
  - Punishment Based Schemes [5], [8], [9], [10]

3. MACHANISM FOR DETECTION OF NON-COOPERATIVE NODES

3.1 Watchdog

Assuming that all node works in promiscuous mode. Only a buffer is required to implement this mechanism. When a packet is send by a node, it also maintains a copy of it in buffer. By overhearing every packet and comparing every packet watchdog identifies selfish nodes. If a packet overheard, is in the buffer of the node then it is removed form buffer. If node remains in buffer for longer time than a certain timeout, watchdog increments a failure tally. When tally for a particular node exceeds a threshold value then it is considered as selfish.

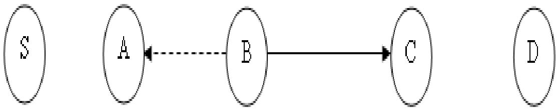

Figure: 1: Watchdog Mechanism

Consider the figure: 1: when A transmits a packet for B to forward it to C, A can tell by overhearing that B has forwarded the packet or not. But Watchdog has some limitations:

3.1. *1 Ambiguous Collision:* when two neighboring nodes simultaneously try to transmit.

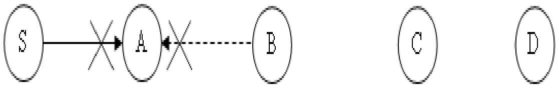

Figure 2: Ambiguous Collision

3.1.2 Receiver's Collision: when receiving of a node collide with the transmission of some other neighboring node.

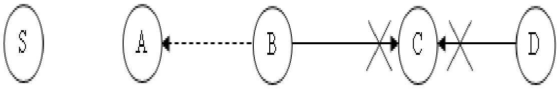

Figure 3: Receiver's Collision

3.1.3 Limited Transmission Power: when a node dose not receives a packet because of low transmission power but neighbors of sender overhears it as successful transmission.

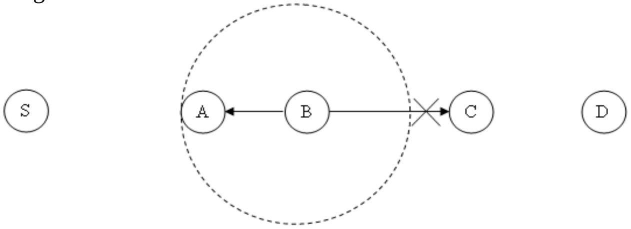

Figure 4: Limited Transmission Power

3.1.4 False misbehavior: when node doses not misbehave but still accused as misbehaving by other nodes.

3.1.5 Collusion: when more then one node misbehaves in cooperation.

3.2 Hop Acknowledgements:

Every node except destination is monitored by its predecessor in the source route for which it uses secret key encryption technique is used, to encrypt the acknowledgment. A buffer is maintained to keep record for packet send and received acknowledgment until timeouts. If acknowledgment dose not came before timeout then the rating of that node is recalculated and if crosses a threshold then considered as misbehaving node. This method resolve the a) and c) problems of watchdog. In this mechanism feedbacks travels two hop, consider figure 5; Node C acknowledge packet sent from A via B. Through this mechanism every node can keep an eye on its 1 hop neighbors and rate it as selfish. Use of security mechanism (hash functions) for sending feedback mitigates the problem of false acknowledgment.

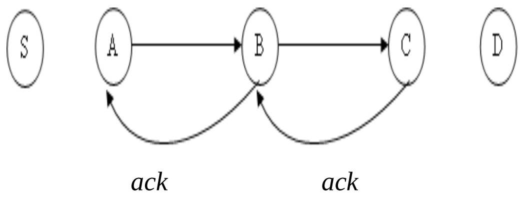

Figure 5: 2 Hop Acknowledgements

3.3 Context Aware Selfish Node Detection:

In this mechanism, route request messages and packets are hashed by sender (using unsigned hash chain), with its own identification, under destinations public key, every intermediate node has to do the same. At destination, node reverses the process. If any intermediate node has tried to tamper or dose not participated in forwarding, is detected. An acknowledgment is also sent to the sender about misbehaving of an intermediate node.

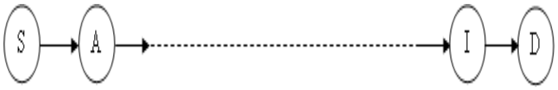

Figure 6: Context Aware Selfish Node Detection

Message send by sender S= $[S:D] \,||\, h(S:D ,r)$

Messages forwarded by intermediate node N = $[S:D] \,||\, N_{A,} \ldots\ldots\ldots N_{I} \,||\, h(\ldots\ldots\ldots(h(S:D ,r))\ldots\ldots\ldots)$

Table.1 Comparisons between non cooperative node mechanisms

Mechanisms Properties→ **↓**	**Watchdog**	**2 Hop Acknowledgments**	**Context Aware Selfish Node Detection**
Types of Misbehave Detected by the Mechanisms	Selfish	Selfish	Selfish and Malicious
Limitations	Ambiguous collision, Receiver's collision, Limited, transmission power, Collusion	Ambiguous collision, Collusion	Ambiguous collision, Receiver's collision, Limited, transmission power, Collusion
False Misbehavior	Not Detected	Detected	Detected
Packet Dropping Rate	Lower than DSR(when implemented with Path rater)	Lower then Watchdog	----
Latency	Higher than DSR	Higher then Watchdog	Higher then Watchdog
Energy Consumed	More than DSR	Approximately equal to watchdog	----

4. COOPERATION MECHANISM FOR NON COOPRETIVE NODES

4.1. Incentive Based Schemes*:*

* Virtual Currency:

To enforce cooperation incentive based scheme can be used. It deal with the selfish nodes, also discourages overloading. Nodes which are using service should be charged and nodes which are services provider should get some virtual currency call as *nuggets*. Since nodes are deployed with some limited amount of nuggets in the network so to avail services they have to earn nuggets and hence forced to cooperate and overloading will cause loss of nuggets so this will discourage overloading in the networks. There are two ways to use this scheme:

4.1.1 Packet Purse Model: sender while sending packets add some nuggets with it. All intermediate nodes takeoff there incentive from it and then forwards it to next hop thus it reaches to destination.

4.1.2 Packet Trade Model: each node purchases the packet from its neighbor for some nuggets and sells it to next node, thus the receiver is charged for receiving packet.

SPRITE [6] is based on the incentive based scheme.

*** Priority as Incentive:**

This scheme provides incentive is in form of priority and bandwidth to the nodes which forwards the packets of others [7]. A cooperation coefficient is calculated on the basis of feedback given by Watchdog. Cooperation coefficient of a node increases when it forwards a packet and decrease when sends its own packets. The nodes which are having higher cooperation coefficient will get the priority to use the bandwidth. But local flows are separated and have highest priority. In this way, the scheme also deals with fairness of bandwidth allocation policy.

Questions related to incentive based mechanism:

1) How to estimate nuggets required for the forwarding of a packet?
2) How to restrict a node to use same nugget twice?
3) How to ensure that a node will definitely forward a packet after grasping the nuggets?
4) Intermediary must be restricted from selling a packet twice in PTM.

Short comes of Incentive Based Schemes:

- Tamper Resistant Security Module is required (for management of nuggets)
- Public Key Infrastructure is required (for Authentication of nodes)
- Performance degrades with the increase of dynamism in the network.
- It requires Omni directional Antennas, with Symmetric Links.
-

4.2 Punishment Based Schemes

Theme of this type of schemes is to *isolate those nodes which are non cooperative*. This scheme is evolved from 'The Selfish Gene'; [5] has explained the concept : "As explained in Richard Dawkins' 'The Selfish Gene' reciprocal altruism is beneficial for every biological system when favors are granted simultaneously, so there is an intrinsic motivation for cooperation due to instant gratification. The benefit of behaving well is not so obvious in the case of a delay between granting a favor and repayment, which is the case when, in mobile ad hoc networks, nodes forward for each other. A biological example used in 'The Selfish Gene' explains the survival chances (and thus gene selection) of birds grooming parasites off each other's head, which they cannot clean themselves. Dawkins divides birds into two types: 'suckers' which always help and 'cheats' which have other birds groom parasites off their head but fail to return the favor. In this system, clearly the cheats have an advantage over the suckers, but both are driven to extinction over time. Dawkins then introduces a third kind of bird, the 'grudger' which starts out being helpful to every bird, but bears a grudge against those birds that do not return the favor and subsequently no longer grooms their head. According to Dawkins, simulation has shown that when starting with a majority population of cheats and marginal groups of both suckers and grudgers, the grudgers win over time. Winning is defined as having the greatest benefit, assuming a cost for grooming another bird's head and a profit of having one's head groomed, a loss leading to extinction and profit leading to multiplication of the species. The rationale is as follows: The suckers help more than they get favors due to the large number of cheats, so the number of suckers decreases, while the number of cheats increases. The grudgers also suffer from some loss, but less than the suckers. Once the suckers are extinct, the grudgers grow rapidly at the expense of the cheats, because they don't help a cheat twice and cheats are also not helped by other cheats. After a while, the number of cheats decreases more slowly, because the probability of a first-help by a grudger increases with a higher population of grudgers. Over all, the population of the grudgers grows, whereas the other species become extinct."

Thus to stimulate isolation for non cooperative nodes, (from birds to network nodes) Grudge protocol [5] is developed by introducing following mechanisms to existing routing protocol (DSR):

4.2.1 Watchdog: Identifies the misbehaving nodes particularly selfish and partially malicious.

4.2.2 Trust Manager: Send and deal with received ALARM abut the misbehaving nodes.

4.2.3 Reputation System: Calculate and assign values (reputation values) to node based on direct observation and by received feedbacks from other nodes.

4.2.4 Path Rater: Rates the path based on reputation values, detect the path that contain misbehaving nodes, and act accordingly on receiving routing request.

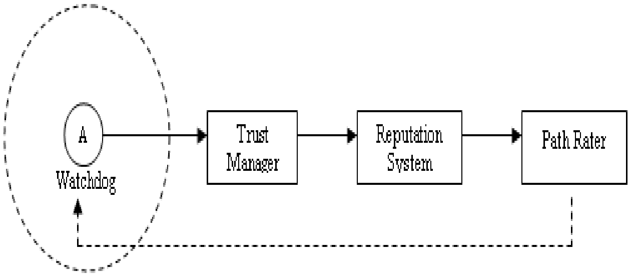

Figure 7: Punishment Based Schemes

Based on the above concept, some reputation based cooperation enforcing techniques are developed including *CONFIDENT* [8], *CORE* [9], *OCEAN* [10], *LARS* [11] uses negative experiences to rate the nodes. *CONFIDENT* and *CORE* uses global reputation i.e. rating from neighborhood as well as from other all nodes in the network is gathered to find the reputation of a node. While other two uses local rating i.e. rating from neighborhood is gathered to find the reputation of a node [12].

Questions related to punishment based mechanism:

1) How many numbers of selfish nodes can be tolerated by such mechanism?
2) How to overcome from problem related to watchdog?
3) Up to what extent we can scale such networks?
4) Can positive experiences of node be added?
5) How to decide thresholds for reputation values?

Short Comes of Punishment Based Schemes:

1) It requires Omni directional Antennas, with Symmetric Links.
2) It requires more frequent exchange of messages to share the reputation of nodes.
3) Reputation System must have fairness, should provide second chance and should take care of false accusation.
4) With Reputation System which takes care of above parameters have degraded performance.
5) Performance degrades with the increase of dynamism in the network

5. CONCLUSIONS

In this paper, we comparisons between non-cooperative node mechanisms in Table-I and comparisons between non cooperative enforcement mechanisms in Table-II so we concluded that all the schemes either Incentive Based or Punishment based are not being able to fully solve the problem of cooperation enforcement. That is they are not being able to cover all the aspects of cooperation such as cooperation with fairness, security issues, pricing, and limitation of resources. Some tries to achieve all, but they have degraded performance in comparison of others, some requires hardware for security, while others require Public Key Infrastructure to authenticate the nodes. In Wireless Ad Hoc Network nodes are mobile with random individual speed some will have higher mobility than others, for some time a route will be there for other it will not, in such cases where network is highly dynamic, cooperation enforcement protocol dose not perform well. All the protocol (reputation based) assumes that antennas are omni directional and links are symmetric but in real scenario due to fading, multi path effects and mobility, links became asymmetric which leads to higher packet drops and degrades the performance of network. So no protocol has outperformed in real scenario yet.

6. REFERENCES

[1] S. 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, pp-255-265.

[2] Djamel Djenouri. CERIST, Basic Software Laboratory. Algiers, Algeria “New Approach *for* Selfish Nodes Detection in Mobile Ad hoc Networks”, Sept. 2005, pp-288-294.

[3] Paul, K. Westhoff, D. Sch. of Inf. Technol., Indian Inst. of Technol., Mumbai, India; “Context Aware Detection of Selfish Nodes in DSR Based Ad-hoc Networks”, vol.1, Nov. 2002,pp-178-182.

[4] L. 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, pp-87-96.

[5] 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, pp-403-410.

[6] 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, pp-1987-1997.

[7] Haijin Yan Lowenthal, D. Dept. of Comput. Sci., Georgia Univ., Athens, GA, USA; “Towards Cooperation Fairness in mobile Ad hoc Networks”,march-2005, pp-2143-2148.

[8] S. Buchegger and J.-Y. L. Boudec, “Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks,” in Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC). IEEE, June2002

[9] P. 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.

[10] S. Bansal and M. Baker, “Observation-based cooperation enforcement in ad hoc networks”, 2003.

[11] Jiangyi Hu. Computer Science Department. Florida StateUniversity.January11, 2005 “Cooperation in Mobile Ad Hoc Networks”.

[12] Binmore, Ken G; “Game Theory A Very Short Introduction” Oxford University Press 2007

[13] Baron. “Game Theory an Introduction”, A. J. Willy & Sons, Inc. publication, 2007.

[14] 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 March2005.

Table 2. Comparison between Cooperation Enforcing Mechanisms

Protocol → Properties ↓	***SPRITE[6]***	***CORE[8]***	***CONFIDENT[9]***	***OCEAN[10]***	***LARS[11]***
Scheme Used	Incentive Based	Punishment Based	Punishment Based	Punishment Based	Punishment Based
Monitor Mechanism	Tamper Resistant Security System	Watchdog	Watchdog	Watchdog	Watchdog
To Monitor	Increase or deduction of nuggets	Behavior of neighboring nodes	Behavior of neighboring nodes	Behavior of neighboring nodes	Behavior of neighboring nodes
Reputation Computation	----	Based on *global* information	Based on *global* information	Based on *local* information	Based on *local* information
Second Chance Mechanism	----	No	No	Yes	No
Routing Mechanism	DSR	DSR	DSR	DSR	DSR or AODV
Components	Credit Clearance Service, Payment Scheme	Watchdog, Reputation Table	Watchdog, Trust Manager, Reputation Table, Path Rater	Neighbor Watch, Rank-Based Routing, Malicious Traffic Rejection, Second Chance	Watchdog, Local Reputation Computation, Trace, Reaction to Non Cooperation
Achieved Network Throughput	----	Higher than DSR	Higher than DSR	Higher than global information based schemes	Higher than global information based schemes
False Accusation	----	Dose not allow a node to send negative ratings, restricts false rating	Negative ratings are propagated over network, leads to false rating	Only one hop neighbor shares information, so no chance of false rating	Only one hop neighbor shares information, so no chance of false rating