Generic Approaches for Node Co-operation in Ad-hoc Networks

Shabana Sultana
Dept. of Computer Science
The National Institute of Engineering,,Mysore-8, India
Shabnamkbn2k@yahoo.co.in

Dr. C. Vidya Raj
Dept. of Computer Science,
The National Institute of Engineering, Mysore-8, India
vidya_rajc@yahoo.com

***Abstract* :** In this paper, we review the approaches that uses the Generic methods to enforce cooperation in ad hoc routing. A very common assumption in the analysis and development of networking algorithms is the full co-operation of the participating nodes. However, the reality may differ considerably. The existence of multiple domains belonging to different authorities or even the selfishness of the nodes themselves could result in a performance that significantly deviates from the expected one. This review aims at providing the most popular Generic approaches to avoid selfishness in forwarding packets in ad hoc networks. This paper also discusses briefly the applications and issues in ad hoc wireless networks.

***Keywords*:** *Ad hoc Network, Selfish nodes, Nuglets, Watchdog, Pathrater*

*****

I. INTRODUCTION

Wireless networking is an emerging technology that allows user to access information and services electronically, regardless of their geographic position wireless networks can be classified into two types.

- *Infrastructure Networks*

Infrastructure network consist of a network with fixed and wired gateways. A mobile host communicates with a bridge in the network (called base station) with in its communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This is called handoff. In this approach the base stations are fixed.

- *Infrastructure less (Ad hoc networks)*

In ad hoc networks [1] all nodes are mobile and can be connected dynamically in an arbitrary manners. As the range of each host's wireless transmission is limited, so to communicate with hosts outside its transmission range, a host needs to enlist the aid of its nearby hosts in forwarding packets to the destination. So all nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. Ad hoc networks are very us full in emergency search- and- rescue operations, meetings or conventions in which persons wish to quickly share information and date acquisition operations in inhospitable terrain [2]..

II. APPLICATIONS OF AD-HOC NETWORKS

With the increase of portable of devices as well as progress in wireless communication, Ad-hoc network is gaining importance with the increasing number of wide spread applications. The following points show the importance of ad-hoc networks [3].

i. *Instant Infrastructure*: Unplanned meeting, spontaneous interpersonal communications etc., cannot rely on any infrastructure, it needs planning and administration. It would take too long to set up this kind of infrastructure; therefore ad hoc connectivity has to setup.

ii. *Disaster Relief*: Infrastructure typically breakdown in disaster areas. Hurricanes cut phone and power lines, floods destroy base stations, fires burn servers. No forward planning can be done, and the set-up must be externally fast and reliable. The same applies to many military activities, which are, to be honest, one of the major driving forces behind mobile ad-hoc networking research.

iii. *Effectiveness*: **Service** provided by existing infrastructure might be too expensive for certain application. If, for example only connection oriented cellular network exist, but an application sends only small status information every other minute, cheaper ad-hoc packet network might be a better solution. Registration procedure might take too long and communication overheads might be too high with existing networks. Tailored ad-hoc networks can offer a better solution.

iv. *Remote Areas*: Even if infrastructure could be planned ahead, it is sometimes too expensive to set up an infrastructure in sparsely populated areas. Depending on the communication pattern, so Ad-hoc networks or satellite infrastructure can be a solution.

v. *Other applications of wireless ad-hoc networking* are due to their quick and economically less demanding deployment, this network finds applications in several areas. Some of these include; military applications, collaborative and distributed computing, emergency operations, wireless mesh networks, wireless sensor networks, and hybrid wireless networks.

III. ISSUES IN ROUTING WITH MANET

The major problems [4] in ad-hoc networks are as follows

i. *Dynamic Topology*: The network topology in an ad-hoc wireless network is highly dynamic due to

mobility of nodes, hence an on-going session may suffer from frequently path breaking.

ii. *Limited Wireless Transmission Range*: In wireless network the radio band will be limited and hence data rates it can offer are much lesser than what a wired network can offer. This requires an optimal manner by keeping the overhead as low as possible.

iii. *Energy constrained operation*: Devices in mobile network may rely on batteries or other exhaustive means as their power sources. For these sources, the conservation and efficient use of energy may be most important system design criteria.

iv. *Routing overhead*: In wireless ad-hoc network, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

v. *Asymmetric links*: Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with Ad-hoc networks as the nodes are mobile and constantly changing their position within network.

In applications like battle field and rescue, all the nodes of the network belong to a single authority and have a common goal for this reason, the nodes are naturally motivated to cooperate.

Application for civilian scenarios are network of cars, provision of communication facilities in remote areas. In these applications, the nodes typically do not belong to a single authority and they do not persue a common goal. In addition, these networks could be much bigger and have a longer life time, and they could be completely self organized, meaning that the network would run solely by the operation of the end users. In such networks, there is no good reason to assume that the nodes cooperate and provide services to each other. Indeed, the contrary is true, service provision is not in the interest of the nodes, because it consumes energy and it does not have any direct advantages. Note that the nodes of mobile ad hoc, networks are after battery powered, and thus, energy is a precious resource that nodes may not want to waste for the benefit of other nodes.

The need of mechanisms for stimulate cooperation became evident as ad hoc network started to be studied for uses different than the military one. The general approach followed was proposing a mechanism or a protocol and to study the behavior of the proposed mechanism. In this paper, we present the General approaches to stimulate cooperation among the nodes in the network for forwarding the packets in ad hoc networks. Also the first half of the paper deals with applications and issues in wireless ad hoc networks

IV. GENERIC APPROACHES

A Watchdog and Pathrater

In this work[5] the authors explore an approach, and install extra facilities in the network to detect and mitigate routing misbehavior. In this way, they can make only minimal changes to the underlying routing algorithm. They introduced two extensions to the Dynamic Source Routing algorithm to mitigate the effects of routing misbehavior the watchdog and the pathrater. The watchdog identifies misbehaving nodes, while the parhrater avoids routing packets through these nodes. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is misbehaving, the pathrater uses this knowledge of misbehaving nodes to choose the network path that is most likely to deliver packets.

- Watchdog

The watchdog method detected misbehaving nodes. how the watchdog works is given here. Suppose there exists a path from node S to D through intermediate nodes A, B, and C. Node A cannot transmit all the way to node C, but it can listen in on node B's traffic., Thus, when A transmits a packet for B to forward to C, A can often tell if B transmits the packet. If encryption is not performed separately for each link, which can be expensive, then A can also tell if B has tampered with the payload or the header.

They implemented the watchdog by maintaining a buffer of recently sent packets and comparing each overhead packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotton by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node.

The watchdog technique has advantage and weaknesses. DSR with the watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior, 5) collusion, and 6) partial dropping.

- Pathrater

The pathrater, run by each node in the network, combines knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. They choose this metric because it gives a comparison of the overall reliability of different paths and allows pathrater to emulate the shortest length path algorithm when no reliability information has been collected. As explained below. If there are multiple paths to the same destination, it chooses the path with the highest metric. Not that this differs from standard DSR, which chooses the shortest path in the route cache. Further note that since the pathrater depends on knowing the exact path a packet has traversed, it must be implemented on top of a source routing protocol.

The pathrater assigns ratings to nodes according to the following algorithm. When a node in the network

becomes known to the pathrater (through route discovery), the pathrather assigns it a "neutral" rating of 0.5. A node always rates itself with a 1.0. This ensures that when calculating path rates, if all other nodes are neutral nodes (rather than suspected misbehaving nodes), the pathrater picks the shortest length path. The pathrater increments the ratings of nodes on all actively used paths by 0.01 at periodic intervals of 200 ms. An actively used path is one on which the node has sent a packet within the previous rate increment interval. The maximum value a neutral node can attain is 0.8, They decrement a node's rating by 0.05 when they detect a link break during packet forwarding and the node becomes unreachable. The lower bound rating of a "neutral" node is 0.0. The pathrater does not modify the ratings of nodes that are not currently in active use.

B Reputation Mechanism

The authors attempted to analyze the CORE[6] protocol by means of game theory analysis tools. CORE is a reputation based co-operation enforcement mechanism. Every node monitors its neighbor's behavior and rates it. Only nodes whose reputation is greater than a predefined threshold are served, while the other nodes are gradually isolated unless they alter their behavior and start co-operating. This section presents the CORE scheme with the definition of the components that participate to the collaborative reputation mechanism. The network entity corresponds to a mobile node. Each entity *si* is enriched with a set of Reputation Tables (RT) and a watchdog mechanism (WD). The RT and the WD together constitute the basis of the collaborative reputation mechanism presented in this paper. These two components allow each entity to observe and classify each other entity that gets involved in a request/reply process, reflecting the cooperative behavior of the involved parts. The classification of the entities based on their behavior is then used to enforce the strong binding between the cooperative behavior of a subject and the utilization of the common resources made available by all the other entities of the network. They use the notation *requestor* when referring to a network entity asking for the execution of a function *f* and the notation *provider* when referring to any entity supposed to correctly execute *f*. They also use the notation *trusted entity* when referring to a network entity with a positive value of reputation.

- Reputation Table is a table stored in each network entity. Each row of the table includes the reputation data pertaining to a node. Each row consists of four entries: the unique identifier of the entity, a collection of recent subjective observations made on that entity's behavior, a list of the recent indirect reputation values provided by other entities and the value of the reputation evaluated for a predefined function. Each network entity has one RT for each function that has to be monitored.

- The Watchdog mechanism implements the validation phase and it is used to detect misbehaving nodes. Every time a network entity (*si,m*, monitoring entity) needs to monitor the correct execution of a function implemented in a neighboring entity (*sj,o*, observed entity), it triggers a WD specific to that function (*f*). The WD stores the expected result *er(f)* in a temporary buffer in *si,m* and verifies if the observed result *or(f)* and *er(f)* match. If the monitored function is executed properly then the WD removes from the buffer the entry corresponding to the *sj,o*, *er(f)* couple and enters in an idle status, waiting for the next function to observe. On the other hand, if the function is not correctly executed or if the couple *sj,o*, *er(f)* remains in the buffer for more than a certain time out, a negative value to the observation rating factor is reported to the entry corresponding to *sj,o* in the RT and a new reputation value for that entity is calculated.

C. Nuglets- A virtual Currency

The authors present two important issues[7] targeted specifically at the ad hoc networking environment: first, end-users must be given some incentive to cooperate to the network operation (especially to relay packets belonging to other nodes); second, end users must be discouraged from overloading the network. T he solution presented in their paper consist in the introduction of a virtual currency (that they call Nuglets) used in every transaction. Two different models are described : the Packet Purse Model and the Packet Trade Model. In the Packet Purse Model each packet is loaded with nuglets by the source and each forwarding host takes out neglects for its forwarding service. T he advantage of this approach is that it discourages users from flooding the network but the drawback is that the source needs to know exactly how many nuglets it has to include in the packet it sends. In the Packet Trade Model each packet is traded for neglects by the intermediate nodes; each intermediate node buys the packet from the previous node on the path. Thus, the destination has to pay for the packet. The direct advantage of this approach is that the source does not need to know how many nuglets need to be loaded into the packet. On the other hand, since the packet generation is not charged, malicious flooding of the network cannot be prevented. T here are some further issues that have to be solved; concerning the Packet Purse Model, the intermediate nodes are able to take out more nuglets than they are supposed to; concerning the Packet Trade Model, the intermediate nodes are able to deny the forwarding service after taking out nuglets from a packet.

Packet forwarding is a service provided by intermediate nodes to the source and the destination of the packet. Therefore, either the source or the destination should pay for it. They presented two conceptual models for charging for the packet forwarding service. In the first one, called packet purse Model, the source of the packet is charged, where as in the second one, called packet Trade Model, the destination is charged. The two models can also be combined to provide a hybrid solution.

V. CONCLUSION

In this paper, we attempted to present the most basic proposals for modeling routing in ad hoc networks. These networks have energy constrained nodes and the topology of this network is dynamic. We believe that combining these techniques with other mathematical methods could result in a totally new perspective of ad-hoc routing despite the results accomplished so far, there is space for more detailed investigation of the effects of selfishness in wireless ad-hoc networks.Furthermore, topology changes seem to play a critical role in selfish packet forwarding that has not been investigated in detail yet.

ACKNOWLEDGEMENT

I wish to acknowledge my co-author for the valuable suggestions and my institute for providing the facility and support in writing this research paper.

REFERENCES

[1] Siva Ram Murthy C. and Manoj B.S., Ad Hoc wireless Networks, Architectures and protocols, second edition, person Education (2007)

[2] C.Perkins, Ad hoc Networking, New York; Addison Wesley, 2000.

[3] Amith Khandakar,"Step by Step procedural comparison of DSR,AODV and DSDV Routing protocols "ICCET 2012, IPCSIT vol.40(2012), Singapore

[4] Pratik Gitel,Manish sharma2 "performance evaluation of ad-Hoc Network Routing Protocols using ns2 simulator", proceedings of international conference on Advances in computer science 2011

[5] S.Marti, T.Giuli, K.Lai, and M.Baker "Mitigating routing misbehavior in mobile ad-hoc networks." in proceedings of MOBICOM. 2002.

[6] P.Michiardi and R.Molva, "Core : A collaborative reputation mechanism to enforce node co-operation in mobile ad-hoc networks." In proc, 6th IFIP/CMS 2002, Vol.228 (Portoroz, Slovenia), Sept.26-27, 2002 PP.107-121

[7] L.Buttyan and J.P.Hubaux, "Nuglets : a virtual currency to stimulate co-operation in self-organized ad hoc networks." Technical Report DSC/2001/001, Swiss Federal Institute of Technology – Lausanne. 2001.