Implementation of A Novel Protocol for Coordination of Nodes in Manet

Poonam[1]**, Sanjay Batra**[2]**, Dr. Chander Kumar Nagpal**[3]

[1]*Assistant Professor, Computer Engineering YMCA University of Science and Technology, Faridabad, India*

[2]*Student, Computer Engineering YMCA University of Science and Technology, Faridabad, India*

[3]*Professor, Computer Engineering YMCA University of Science and Technology, Faridabad, India*

Abstract

Abstract— Network is a combination of nodes and links. Nodes can be mobile and static in nature and links can be wired and wireless. So there can be different combination of network. In MANET all the nodes are mobile and these mobile nodes are not in a fixed topology. Each node can take and receive data from another node that's why these nodes can act as router as well as node. Nodes can join the network with their own wish. Manet is facing various challenges like no central authority, different mobility models, battery power, coordination of nodes and continuously maintains the information required to properly route traffic. Coordination of nodes also plays important role in performance of Manet. Manet functions properly if the participating nodes never show selfish behavior it means nodes shows cooperation and helps in proper routing of packets. In this paper we implement a new protocol for the coordination of nodes in Manet using NS2 simulator. In this protocol nodes will not show selfish behavior because this model will distribute the load among all the nodes so that nodes will not be over utilized and underutilized. Here network layer is using DSR routing protocol and energy and path aware routing.

Key Words: *Manet; DSR; Routing; Cooperation; Trust; Reputation; Throughput; Packet Delivery Ratio; Energy consumption.*

1. INTRODUCTION

Mobile ad hoc network (MANET) [1] is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end system, but also as a router to forward packets. Nodes assist each other by passing data and control packets from one node to another. Ad hoc network topology changes as mobile hosts shift to another geographical location or dead due to less battery power. Links between nodes can be formed or break due to the movement of nodes. Capacity of wireless links also degrades over time due to multiple accesses, multipath fading and interference. So there is a need of such routing technique which can discover a route from the source node to the destination node. These routing protocols can be divided into two categories based on when and how the routes are discovered:

- Table-driven
- On-demand routing

Table-driven Routing Protocols

These protocols are extensions of wired network routing protocols. In a table driven routing protocol, routes to all destinations are available at all the time. It maintains the global topology information in the form of tables at every node. The tables are exchanged between neighbours at regular interval to keep an up to date view of network topology. They try to maintain consistent, up-to-date routing information from each node to every other node. Nodes respond to network topology changes by propagating route updates [2] throughout the network to maintain a consistent network view.

On-demand Routing Protocols

These protocols execute the path finding process and exchange routing information only when a path is required by a node to communicate with the destination. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, some form of route maintenance procedure maintains it until either the destination become inaccessible along every path from the source or until the route is no longer desired. Various source-initiated routing protocols are as follows:

- Ad-hoc On-Demand Distance Vector (AODV)
- Dynamic Source Routing (DSR)
- Temporally Ordered Routing Algorithm (TORA)
- Location-Aided Routing(LAR)

Dynamic Source Routing (DSR)

DSR is an on-demand routing protocol designed to restrict the bandwidth consumed in wireless networks. In the table driven approach periodically update of table-update message is required. But in on-demand routing protocols table –update message is required only when route demand arrives. Hence bandwidth consumed in control packets is lesser in mobile Adhoc networks. So on-demand routing protocols are beacon-less (no need of hello packets). Beacons are used by a node to inform its neighbors of its presence. First of all this protocol constructs a route by flooding RouteRequest packet, responds by sending a RouteReply packets back to the source, which carries the route traversed by the RouteRequest packet received.

Because Manet is multi hop network so packets will be transfer from source node to destination node via different nodes. So the cooperation of these intermediate nodes is very much required to successfully transmission of packets. Battery power and bandwidth are very much important part due to these low resources the owner of the nodes will not pass the packet to another node and shows the selfish behavior, but wants to use the other's resources, so a selfish behavior can be very much harmful for the complete network. There are many protocol has been designed by researchers for the cooperation of nodes in Manet. Cooperation Scheme [7,8] in Manet are-

- Reputation Based
- First hand Reputation
- First hand and second hand Reputation.

Trust is established between two parties for a specific action. Different metrics of trust are: belief, reputation. Trust can be discrete value or continuous value. Trust is an important aspect in the design and analysis of secure distribution systems. It is also one of the most important concepts guiding decision-making. It is a before-security issue in the ad hoc networks. By knowing the trust relationship, it will be much easier to take proper security measures, and make correct decision on any security issues. There are various strategies which deal with trusted behavior. These strategies may categorize into-motivation based approach and detect and exclude method.

- **Motivation based approach:** In this approach nodes of Ad-Hoc network are motivated to participate. One of the motivation approaches is based on a virtual currency called nuglet [9]. Every network node has an initial stock of nuglets.The cost of a packet may depend upon several parameters such as required total transmission power and battery status of intermediate nodes. Packets sent by or destined to nodes that do not have a sufficient amount of nuglet are discarded. Demand for trusted hardware to secure and maintain the record of currency at central level is a major drawback of motivation-based approach.
- **Detect and exclude based protocol:** This strategy deals with the selfish nodes and tries to avoid them from the routing paths. Watchdog and Pathrater is a mechanism based on detects and exclude principle to deal with the selfish nodes. It uses Dynamic source routing (DSR) [2] as the base protocol. It has two components watchdog and Pathrater. This strategy is generic and static and do not concentrate on the levels of selfish nodes, which may change dynamically.

2. LITERATURE SURVEY

2.1 Reputation Based Model:-

CONFIDANT: - Bucheggar and LeBouded proposed a new protocol called as CONFIDANT

[3]. This protocol was designed as an extension to an on-demand routing protocol such as DSR .In this protocol reputation is used to evaluate routing and forwarding behavior according to network protocol and trust is used to evaluate participation in protocol. This protocol facilitates monitoring and reporting for route establishment that avoid the misbehaving nodes. Packets of misbehaving node will not be forwarded by the fair node.

Confidant protocol mainly employs 4 main components on any node in network:-

1. A monitor
2. Reputation record for first hand and trusted second hand observation about routing and forwarding function of another node.
3. Trust records to control the trust that is given to receive warnings.
4. Path manager to take routing decision that avoid malicious node.

Nodes monitor their neighbor and change reputation accordingly. A node can detect selfish behavior of next node in the source route either directly by sensing the transmission of next node, or indirectly by routing protocol misbehavior.

CORE:-This protocol [4] also relies on on-demand routing protocol (DSR). This protocol was designed by Michiardi and Molva. A special function is used to combine the first and second hand experience. This function is then used by Watchdog's mechanism for other node behavior. In this protocol each node of network monitors the behavior of its neighbor node with respect to requested function and collects observations about the execution of that function. A Reputation table is used to record the observation by each node.

SORI:-This protocol [6] is basically focused on packet forwarding function and it is secure and reputation based scheme for Adhoc network. There are 3 basic component of this protocol:-

1. Neighboring monitoring
2. Reputation propagation
3. Punishment

A node must be capable of overhearing the transmission of its neighboring node to maintain a neighbor node list. Each neighbor forwarding is linked with 2 parameters:-

Rfn(X):-indicate the total number of packets that node n has transmitted to X for forwarding.

Hfn(X):-total number of packets that has been forwarded by X and noticed by n. So basically combination of these 2 parameters is necessary to check the reputation of nodes in SORI [6].

OCEAN:-The Observation based cooperation enforcement in Adhoc network. This protocol introduced an intermediate layer between the network and Mac layer. The main purpose of this layer to help in intelligent routing and forwarding decisions. It uses only first hand observation. Here each node maintains a rating for each neighboring node and monitor their behavior through observation.

2.2 Credit based model:-

SPRITE: It uses a centralize credit clearance service (CCS). A When receiving a packet, a node keep the signed receipt of this packet, which was generated by source node. When a node sends its own packet, it loses a credit (virtual currency) ,because the other node incur a cost to forward these packets. In order to gain a credit and be able to send packets later, a node must forward packets on behalf of other. CCS charges the sender based on the no of receipt, the number of intermediate nodes left to reach the destination. A potential disadvantage of Sprite is the assumption that a fast connection to the CCS is needed for the reporting of the obtained receipt. An extension of the basic sprite provides integrity during packet exchange and is based on digital signature.

3. TOKEN BASED COOPERATION ENFORCEMENT

It is self organized without assuming any a-priori trust between the nodes or the existences of any centralize trust entity. The scheme is fully localized and its credit based strategy produced overhead that is significantly decreased when a network is not harmed [5]. The system's secret key is shared among the network node and each node maintains limited portion of it. Each node carries a token, signed with a system's secret key as derived from the threshold cryptography process. This scheme includes 4 components:-

1. Neighbors verification
2. Neighbors monitoring
3. Intrusion reaction
4. Security enhanced routing protocol

I decide to implement a protocol which avoids selfishness [10] as well as congestion in the network. We implement a new selfishness avoiding technique which is based on load balancing. Each node in the network use the resources equally and equally distributed the services among all the nodes in the network.

Protocol and System Model

Nodes are using path and energy aware routing protocol. The main goal is to find the shortest path between source and destination when it is feasible. The nodes which are showing selfish behavior will not be able to send its own packet. A small amount is memory is maintained by each node to maintain a signed integer called credit. This credit is used to show that whether the node is selfish or not. If a node is selfish then it cannot send its own packet. A node is called as selfish if its credit is less than some predefined limit. The punishment of selfish node is that he cannot send its own packet so this type of punishment will motivate them not to be selfish.

The transmission power of every node is equal initially. when a node send its packet to some intermediate node then that intermediate node send an ACK to conform that packet has been forwarded.

Algorithm

1. If intermediate node change its position or shows selfish behavior. Then the previous node to intermediate node waits for passive ack for 3 times.
2. The value of credit of each node is 3.
3. Credit is increase for each message that a host forward and decrease if it doesn't forward.
4. Initially we have defined a max credit; max credit is upper bound to the credit.
5. If the intermediate node comes during the previous node waits for passive ack. Then this node forwards the message if its credit is less than max credit. Otherwise, some other node which is in the sub optimal path that overhears the packet 3 times can participate in forwarding packet and increase its credit by 1,credit=credit+1.
6. For each packet forwarded and is credit is less than the max-credit. If node forwards a packet its credit increases by 1 if it receives a packet and do not send the packet credit decreased by 1.
7. *punishment*/ A node with credit less than 3 cannot send its own packet If any participating node which attains the max-credit then some other node which is in the optimal path and also in the radio range of the node replaces the participating node. When a node will not send packet then its credit will be decrease by 1.

4. SIMULATION

For the purpose of implementation we have used NS2 (Network Simulator). NS2 is event driven simulator. Front end language for ns2 is tcl (tool command language) and back end language is C++ and in the simulator we have done the complete implementation of the new protocol and show the results via graphs i.e. throughput, packet delivery ratio, and energy efficiency.

TABLE I. Parameters used for simulation

Properties	Values
Antenna	Omni directional
Channel	Wireless
Routing Protocol	DSR
Radio Propagation Mode	Two Ray Ground
Initial Energy(joules)	100
Area	710X710
Initial credit of nodes	3

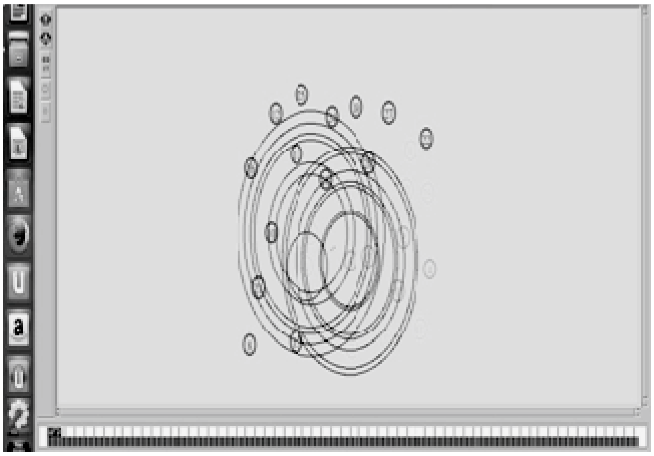

Fig.1 sending route request in MANET
Figure 1 shows sending request to find route between source and destination node. Circles indicate broadcasting of route request packets.

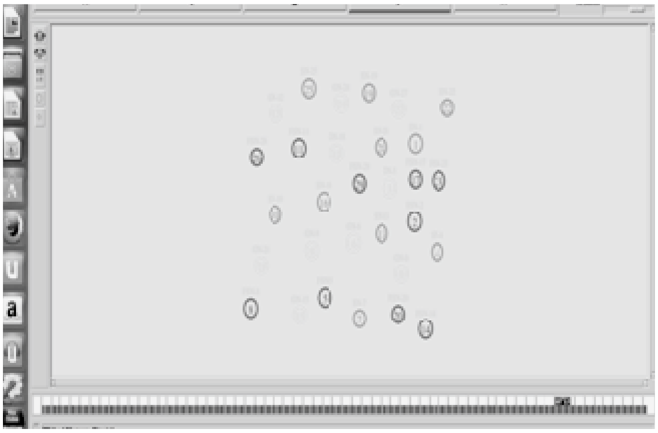

Fig.2 Selfish and good nodes in MANET
System finds all the selfishness and good nodes (non selfish node) as shown in figure 2.

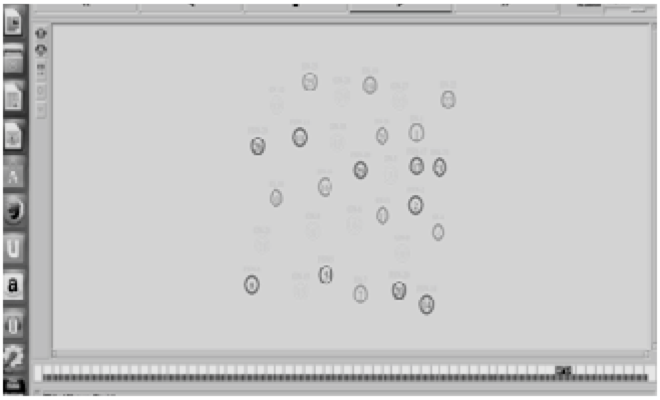

Fig.3 Data transmission in MANET
Figure 3 indicates actual data transmission between source and destination via good nodes. We can analyze the effect of cooperation on the mobile ad hoc network working with DSR as the routing protocol by the help of packet received and the performance graphs shown below-

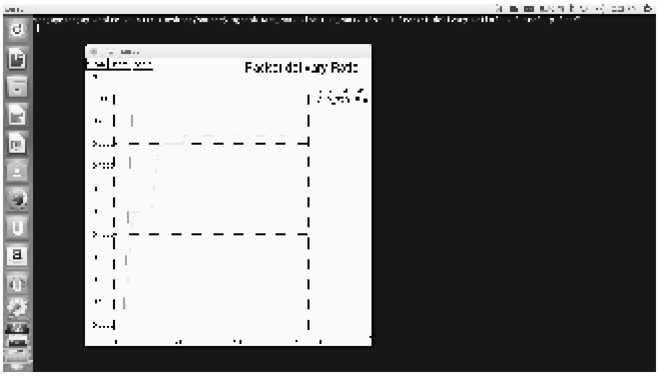

Fig.4 Packet delivery ratio in MANET

In figure 4, time on x-axis and no. of packets delivered on y-axis while plotting the graph. As we saw in simulation data, the no. of packet delivered are more in proposed protocol (as shown by red line) comparative to the existing protocol (as shown by green line).

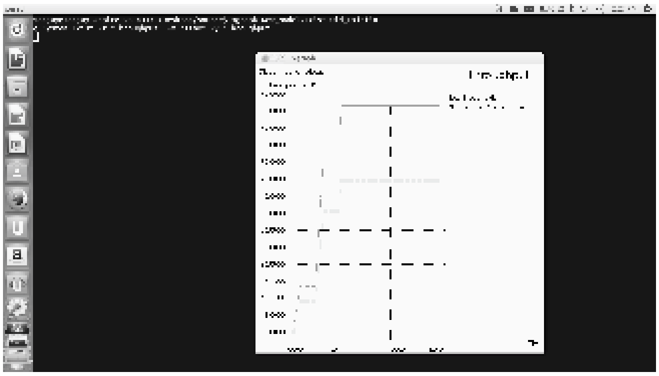

Fig.5 Throughput in MANET

In figure 5, time on x-axis and no. of bytes on y-axis and plotted the graph using xGraph for a run of simulation. Throughput is much higher in the proposed protocol as shown by red line in the graph compared to the existing protocol (as shown by green line).

Figure 6 indicates the energy consumed by the system which is undefined in the existing protocol but it decreases with time as the proposed protocol starts its working to route the packets.

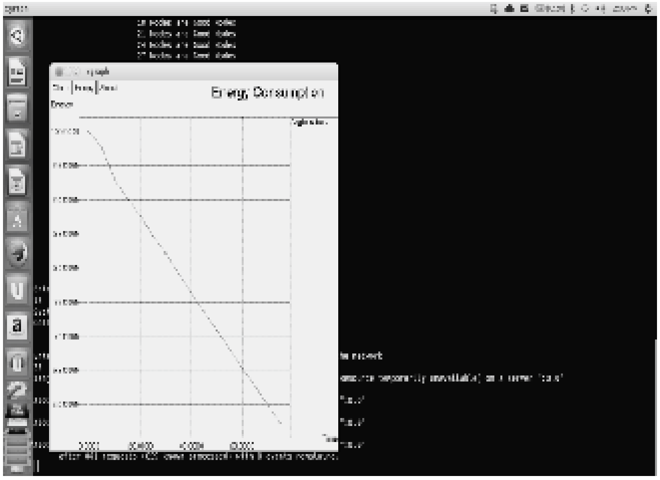

Fig.6 Energy consumption in MANET

TABLE II: Comparison table

Parameter	**Old system**	**New system**
Throughput	Not much better	Better than old system
Packet delivery ratio	Not good	Good
Energy consumption	Not defined	Decrease with time

5. CONCLUSION

Battery power and bandwidth are very much important, so the nodes will not pass the packet to another node and shows the selfish behavior. But wants to use others resources, so a selfish behavior can be very much harmful for the complete network. We can conclude that our new implemented protocol is better and can be use easily. Congestion and selfishness can be reduced in the proposed protocol. In the future researchers can apply different scheme in different scenario and they can also apply different another scheme like punishment scheme and memory detail so to get some better results, and also can do changes in algorithm to get some better results.

REFERENCES

[1] C. Siva Ram Murthy and B.S. Manoj, "Ad-Hoc wireless networks", Architecture and protocols, Pearson Education, Fourth Impression,2009.

[2] Piet demeester, Jeroenhoebeke," An overview of Mobile Ad hoc Networks : Applications and Challenges "

[3] Changling Liu,Jorg Kaiser."a Survey of Mobile Ad hoc network routing protocols". The survey was published as: University of ULM Tech. Report Seried Nr. 2003-2008. Buchegger S, Le Boudec JY. Performance analysis of the CONFIDANT protocol. In Proceedings of 3rd ACM International Symposium, on Mobile Ad Hoc Networking and Computing, June 2002.

[4] 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.

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

[6] 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.

[7] Zhong S, Chen J, Yang R. Sprite: a simple, cheat-proof, credit base system for mobile ad-hoc networks. In Proceedings of IEEE INFOCOM2003, April 2003.

[8] Yang H, Meng X, Lu S. Self-organized network-layer security in mobile ad hoc networks. In Proceedings of ACM WiSe02, September2002.

[9] Anderegg L, Eidenbenz S. Ad-hoc-VCG: a truthful and cost efficient routing protocol for mobile ad-hoc networks with selfish agents. In Proceedings of 9th Annual International Conference on Mobile Computing and Networking, September 2003.

[10] Dipti Dash, New protocol for node co-operation in Manet.In the proceeding of IJERT,Vol.2 Issue 4,April-2014, ISSN:2278-0181.rison table