International Journal of Computer Networks and Applications
Volume 2, Issue 2, March – April (2015)

RESEARCH ARTICLE

Implementation of a Novel Protocol for Coordination of Nodes in Manet

Poonam Mittal
Department of Computer Engineering, YMCA University of Science and Technology
Faridabad, India
poonamgarg1984@gmail.com

Sanjay Batra
Department of Computer Engineering, YMCA University of Science and Technology
Faridabad, India
sanbatra1989@gmail.com

Dr. C.K.Nagpal
Department of Computer Engineering, YMCA University of Science and Technology
Faridabad, India
nagpalckumar@rediffmail.com

Abstract – A network is basically a combination of nodes and links. Nodes can be mobile or static in nature and similarly links connecting them may be wired or wireless in nature. 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 is why these nodes can act as router as well as node. Nodes can join the network with their own wish. Due to all these features of Manet it may face various challenges like no central authority, different mobility models, battery power, selfish behavior of nodes, coordination of nodes and continuously maintenance of information which is required to properly route traffic. All the above mentioned challenges affect the performance of the Manet. But cooperation among the participating nodes may overshadow these challenges. Cooperation can be achieved either by removing selfish nodes or preventing the nodes from acting as selfish because selfish nodes causes the problem of improper routing and results in drop of packets. It indicates that coordination of nodes have strong impact on the performance of the network. In this paper we implement a novel scheme for the coordination of nodes in Manet using NS2 simulator. In the proposed scheme 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 or underutilized. Proposed routing scheme uses DSR routing protocol and energy and path aware routing at network layer.

Index Terms - Manet, DSR, Routing, Cooperation, Trust, Reputation, Throughput, Packet Delivery Ratio, Energy consumption.

1. INTRODUCTION

Mobile ad hoc network (MANET) [1] is a network which has various free or autonomous nodes made of mobile devices which can arrange themselves in any topological form and can operate without any strict network administration. Each node operate 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 [2]. 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 [3, 7] can be divided into two categories based on when and how the routes are discovered:

- Table-driven routing
- On-demand routing

1.1. 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.

RESEARCH ARTICLE

1.2. 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. The protocol floods the network with route request when a request for new route arrives. This process of route finding finished when all permutations of possible routes are analyzed. As a route is finalized there is a need of some route maintenance procedure (because MANET is a Adhoc network nodes are very frequent in changing their position as well as nodes can leave and join the network at any time) unless and until that path is demanded in the network. Various on-demands routing protocols are as follows:

- AAd-hoc On-Demand Distance Vector (AODV)
- DDynamic Source Routing (DSR)
- TTemporally Ordered Routing Algorithm (TORA)
- LLocation-Aided Routing (LAR)

1.2.1. 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 Ad hoc networks [4-6]. 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.

1.3. Reputation Based System

MANET is an infrastructure-less network (because there is no central authority to manage communication). Hence cooperation of intermediate nodes is most important for successful transmission of data packets. Since battery power and bandwidth are very much important as well as scarce resources of the nodes, so the nodes deficient in any of these resources will not forwards the data packets through them (i.e. shows the selfish behavior) . As the nodes became deficient in the network they start behaving as selfish and most of the packets dropped which pass through these selfish nodes. In the available literature various researchers talked about various schemes related to cooperation of nodes in Manet. Various reputation based cooperation schemes [8-11] in MANET are:

- 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.

1.3.1. 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. Every network node has an initial stock of nuglet [8, 9].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.

1.3.2. 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 [10, 11]. It uses Dynamic source routing (DSR) 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

In the literature various routing protocol talks about reputation model of nodes and few of them are discussed as under:-

2.1.1. CONFIDANT

Bucheggar and LeBouded proposed a new protocol called as CONFIDANT [8]. This protocol was designed as an extension to an on-demand routing protocol such as DSR. Routing and forwarding behavior of nodes in a network is evaluated by seeing the reputation value of the nodes and participation of nodes is calculated by seeing the value of trust. 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 works in 4 modules on any node in network:-

RESEARCH ARTICLE

- There is a monitor module.
- Reputation module records the observation about routing and forwarding function of another node in the form of first hand and trusted second hand.
- Trust module records the trust value by seeing the control trust warnings.
- Path manager to take routing decision that avoid malicious node.

Reputation value of neighboring nodes is modified by monitoring the neighboring nodes. Selfishness of next node in the source route is determined by sensing the transmission of next node or the misbehavior shown by routing protocol.

2.1.2. CORE

This protocol 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 [9]. 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.

2.1.3. SORI

This protocol 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:-

- Neighboring monitoring
- Reputation propagation
- Punishment

A node must be capable of overhearing the transmission of its neighboring node to maintain a neighbor node list [10]. Each neighbor which is involved in 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.

2.1.4. 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). When a node receives a packet it keeps the signed receipt which is generated by source node. A node loses a credit (virtual currency) when it sends its own packet, because the other participating nodes in that route incur a cost to forward these packets [11]. In order to gain more credits and be able to send packets later, a node must forward packets through it on behalf of other. By seeing the number of receipts and number of intermediate nodes to reach to destination CCS charged the sender.

The main drawback of this scheme is CCS takes so much time in collecting the information regarding number of intermediate neighbors and number of receipts. Functionality of sprite can be extended by using the concept of digital signature to provide integrity to the packet exchange.

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 [12]. 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:-

- Neighbors verification
- Neighbors monitoring
- Intrusion reaction
- Security enhanced routing protocol

Now we are of the opinion that there is a strong need of a routing protocol which avoids selfishness [13-15] as well as congestion in the network (Selfishness of nodes in the network is directly proportional to congestion in the network because all the dropped packets are retransmitted which may result into congestion). Hence in this paper we implement a novel selfishness avoiding technique which is based on load balancing. Initially all the nodes are provided with equal resources and equally distributed services in the network which may further vary depending upon the participation of nodes.

3.1. Protocol and System Model

Nodes are using path and energy aware routing protocol. The main aim of each routing protocol is to find the most feasible path between source and destination. Feasibility (Feasibility parameter may be shortest path or stability of path etc.) of path varies depending upon the path selection criteria. The main goal is to find the shortest path between source and destination when it is feasible. In the proposed routing scheme nodes which are showing selfish behavior will not be able to send its

RESEARCH ARTICLE

own packet as well as these nodes will not be the part of ant route. 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.

Algorithm

// Initialize all nodes in the network with equal value of credit suppose the initial_assigned_credit=3

//assign some value to the variable max_credit such that max_credit<= initial_assigned_credit

```
If ((current_pos[i]!=initial_pos [i]) ||
(initial_credit [i] < max_credit))
{   N=0;
    repeat
        {passive_ack (i);
        } until (n!=3);
 }
If (n<3) then
{
    If (node[i]->packet) then
        initial_credit[i] =initial_credit[i] + 1;   //award
    else
        initial_credit[i] =initial_credit[i] - 1;   //punishment
}
If (n==3) then
{   //finds another node which in other optimal path and can overhear i, suppose that is some node j
    If (initial_credit [j] >+ max_credit) then
    {
        If (node[j] ->packet) then
        initial_credit [j] =initial_credit [j] + 1;     //award
    else
        initial_credit [j]=initial_credit[j] - 1;      //punishment
    }
}
```

Example

In the Figure-1 in which here we have a path from S to D which is optimal A and B are intermediate nodes.

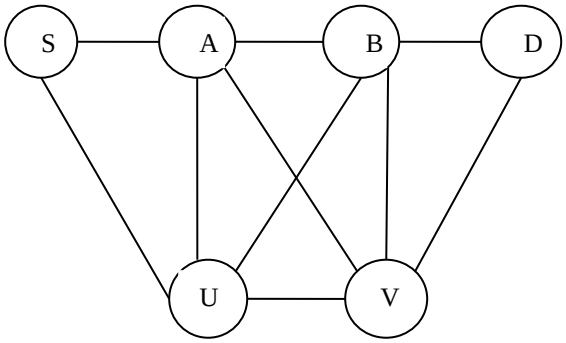

Figure-1

There are various routing schemes which uses different metrics for path selection like shortest path routing, stable path routing etc. Traditional approach of routing uses hop count as routing metric for path selection. Suppose shortest path from S-D is S-A-B-D then the node A and B will be continuously used in forwarding the packets and the other nodes in the same network will be free from the traffic load. If most of the requests for data transmit are from S-D then the resources (battery power) of intermediate nodes (A, B) will be consumed. If most of the traffic is to be traversed from S-D then battery power of intermediate nodes will be decreased and will die soon. Congestion may occur at node A that leads to delay of packet forwarding and it may further result into link failure. The solution for this situation may be based on route redirection.

There are two cases happens. Case1: If one node found in the optimal path here node U is in the radio range of both S and A. Node U can overhear packet which is intended for A. Since all the packets are routed to D with the route S-A-B-D and suppose node. A change its position or it gets dead due to lack of battery power then there is a need of a new optimal path. As shown in the figure 2, suppose node U is in the radio range of S and S-U-B-D is also an optimal path. Then if node U overhears the same packet for 3 times or different packet for more than 3, then in such a scenario node U would voluntarily take part in the routing process and informs the source node to update its routing table (cache). This scenario may also happen if node a is congested and packets are dropped due to this congestion and if this happens 3 times then second optimal path is searched and in the given example node A will be replaced by node U.

Thereafter the source node would follow the path S-U-B-D for further communication i.e. the path S-A-B-D would be replaced as S-U-B-D.

RESEARCH ARTICLE

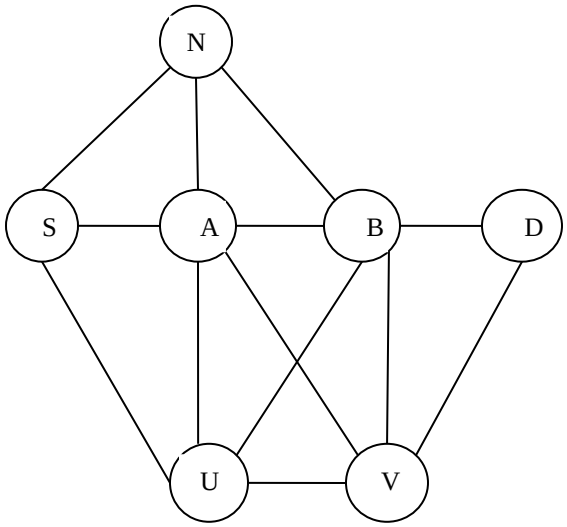

Figure-2

Case2: More than one common neighbor node found in optimal path.

Here in this figure both nodes U and N are nearby nodes which are common neighbors of both S and A. So both the nodes U and N can overhear packets which are intended for node A. If link failure occurs at node A, now we have two optimal paths one is S-U-B-D and another one is S-N-B-D. Now the question is which node between U and N will take part in the routing process. Here source node will decide based on which node has approached first Open mobile Adhoc networks should implement a protocol to get an expected service that give punishment to the users that exhibits selfish behavior intentionally or unknowingly. If a node shows selfish behavior then the node cannot send its own packet in the network. In other words if a node does not cooperate in forwarding packets of other nodes, then its own packets would not be forwarded by other nodes in the networks.

4. SIMULATION

For the purpose of implementation we have used NS2 (Network Simulator). This based on two languages an object-oriented simulator (C++), and OTcl (object-oriented Tcl) interpreter. NS2 simulator has rich library of network and protocol object. It has Compiled C++ hierarchy which gives efficiency in simulation and faster execution times. The proposed cooperation scheme is implemented using NS2 simulator and we obtain 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

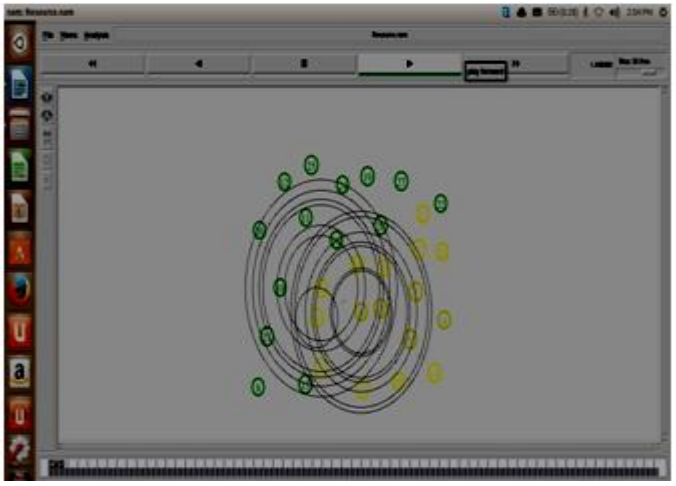

Figure 3 Sending route request in MANET

Figure 3 shows sending request to find route between source and destination node. Circles indicate broadcasting of route request packets.

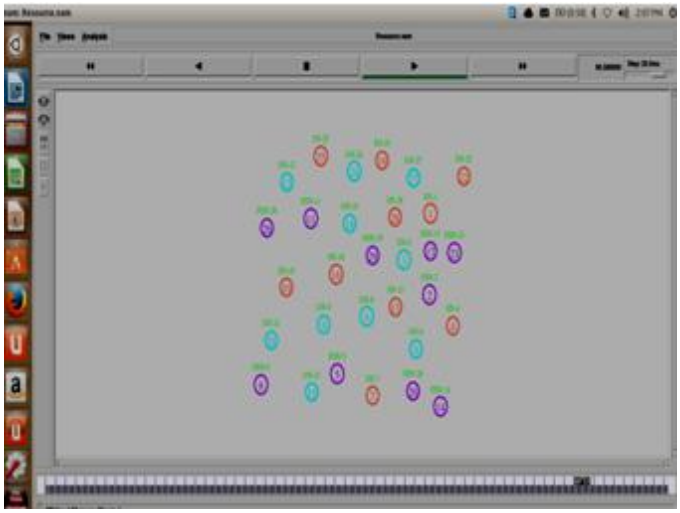

Figure 4 Selfish and good nodes in MANET

System finds all the selfishness and good nodes (non selfish node) as shown in figure 4.

RESEARCH ARTICLE

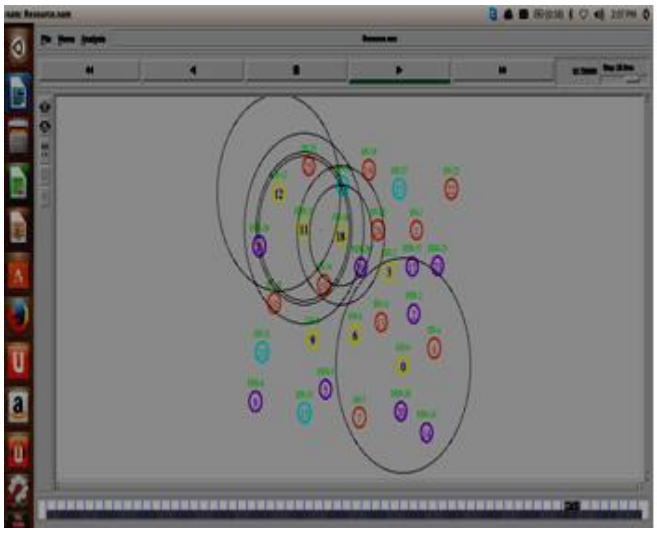

Figure 5 Data transmission in MANET

Figure 5 indicates actual data transmission between source and destination via good nodes.

5. RESULT ANALYSIS

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-

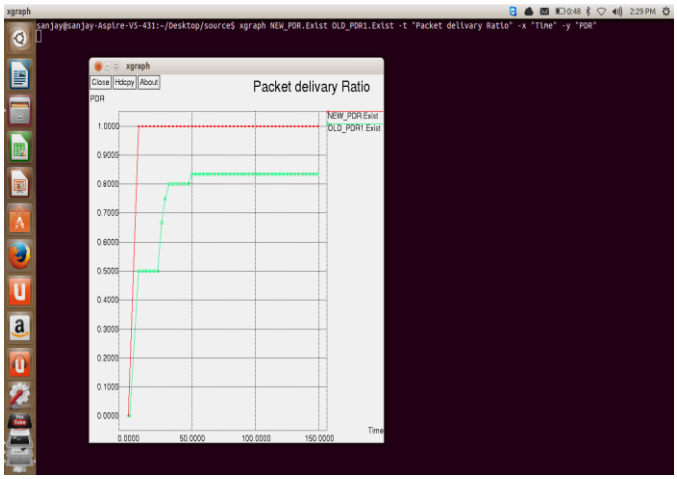

Figure 6 Packet delivery ratio in MANET

In Figure 6, time is on x-axis and number of packets delivered on y-axis while plotting the graph. As we saw in simulation data, initially the delivered packets are same in the existing protocol as well as in the proposed routing scheme. The main reason behind this is initially all the nodes are full of resources like battery etc. (initially there is no point of selfishness). But with time as the nodes participate in forwarding the packets resources are consumed and they start behaving like selfish which can easily conclude by the Figure 6 that the number of packet delivered are more in proposed protocol (as shown by red line) comparative to the existing protocol (as shown by green line).

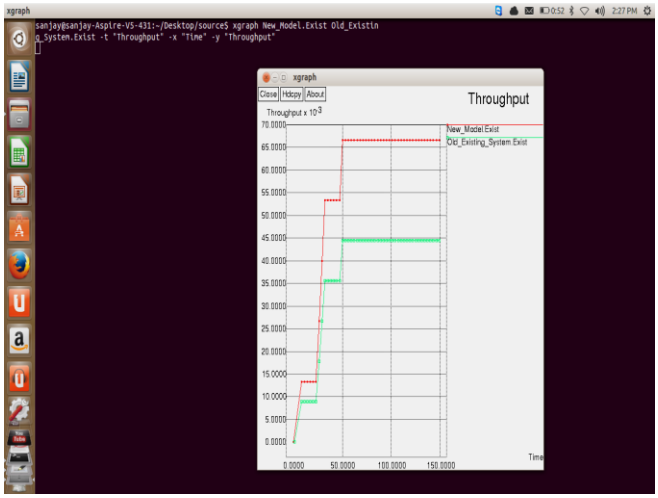

Figure 7 Throughput in MANET

In Figure 7, time on x-axis and number of bytes delivered is on y-axis and plotted the graph using xGraph for a run of simulation. As we saw in simulation data, initially the delivered bytes are same in the existing protocol as well as in the proposed routing scheme. The main reason behind this is initially all the nodes are full of resources like battery etc. (initially there is no point of selfishness). But with time as the nodes participate in forwarding the packets resources are consumed and they start behaving like selfish which can easily conclude by the graph 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).

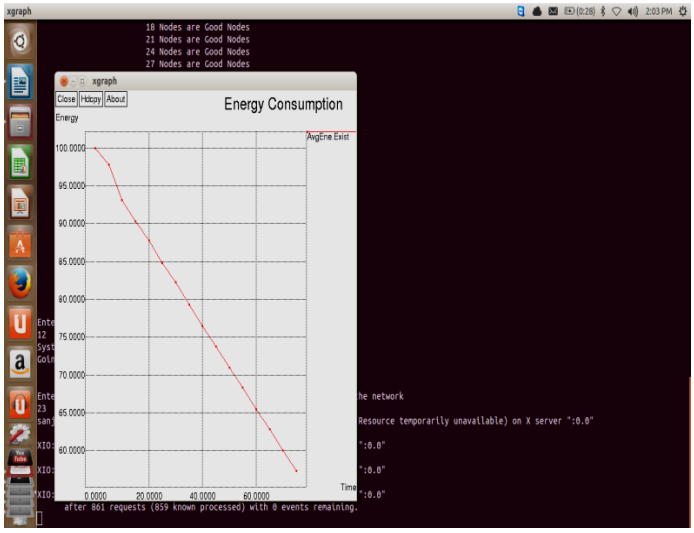

Figure 8 Energy consumption in MANET

Figure 8 indicates the energy consumed by the system which is unpredictable in the existing protocol but it decreases with

RESEARCH ARTICLE

time as the proposed protocol starts its working to route the packets.

Brief comparison of existing and proposed routing scheme is shown in the table given below:-

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

6. 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 used 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] Harminder, Qian Feng, Jhongmin Cai, Jin Yang, Xunchau Hu," A Performance Comparison of Adhoc Routing Protocol" published in second International workshop on Computer Science and Engineering, IEEE-2009.

[4] B.Ramakrishnan, Dr. R.S. Rajesh, R.S. Shaji,"Analysis of routing protocols for Highway model without using Roadside unit and cluster" published in International Journal of Science and Research in vol.-2, issue-1,ISSN 2229-5518, IJSER-2010.

[5] B.Ramakrishnan, "Performance analysis of AODV routing protocol in Vehicular Adhoc Network Service Discovery Architecture" published in ARPN Journal of Systems and Software, vol.-2, issue-2, ISSN 2222-9833, AJSS-2012.

[6] Dr. B.Ramakrishnan, Dr. Milton Joe, R. Bhagwadh Nishant," Modelling and Simulation of Efficient Cluster based Manhattan Mobility model for Vehicular Communication" published in Jounal of Emerging Technologies in Web Intelligence", vol.-6, issue-2,JETWI-2014.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

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

[14] 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.

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