IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 9, April 2013)

Cluster Based Routing Algorithm to Enhance Energy Efficiency and Security in MANET

Heena Khan
heena3520@gmail.com

Rakesh Sharma
hod.ce@rcew.ac.in

Abstract – **An Ad-Hoc network is a multi-hop wireless network where all nodes cooperatively maintain network connectivity without a centralized infrastructure. If these nodes change their positions dynamically, it is called a mobile ad-hoc network (MANET). Since the network topology changes frequently, efficient adaptive routing protocols such as AODV, DSR are used. As the network is wireless, security becomes the major issue in Mobile Ad hoc Networks. Recently many studies have focused on designing mobility based multi-hop routing protocols for wireless mobile ad hoc networks (MANET) on the assumption that the energy of host is an important parameter to be considered. As the network is wireless, security becomes the major issue in Mobile Ad hoc Networks. When we apply the security mechanism to avoid some kind of attacks, the network throughput degraded continuously. So we are using the hash signature algorithm with the proposed routing algorithm which provide the authentication, better security level and throughput is also not degraded. Our proposed routing algorithm will provide a better level of security and performance than existing works. The results parameters will show in terms of improvement of the network performance, in terms of throughput, Network lifetime, device arrangement and end to end delay for the proposed secure & efficient routing protocol.**

Keywords – **MANET, AODV, DSR, Throughput, Network lifetime.**

I. Introduction

Wireless networks are gaining popularity to its uttermost today, as the users want wireless connectivity irrespective of their geographical position.

Wireless Networks enable users to communicate and transfer data with each other without any wired medium between them. One of the reasons of the popularity of these networks is widely penetration of wireless devices. Wireless applications and devices mainly emphasize on Wireless Local Area Networks (WLANs). This has mainly two modes of operations, i.e. in the presence of Control Module (CM) also known as Base Stations and Ad-Hoc connectivity where there is no Control Module. Ad-Hoc networks do not depend on fixed infrastructure in order to carry out their operations. The operation mode of such network is stand alone, or may be attached with one or multiple points to provide internet and connectivity to networks. These networks exhibits the same conventional problems of wireless communications i.e. bandwidth limitations, battery power, enhancement of transmission quality and coverage problems.

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs contains mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are contributing in the network and are mobile.

Security in Mobile Ad-Hoc Network is the most vital concern for the basic functionality of network. The accessibility of network services, confidentiality and reliability of the data can be achieved by assuring that security issues have been met. MANETs frequently suffer from security attacks because of its features like open medium, changing its topology dynamically, absence of central monitoring and management, cooperative algorithms and no clear defence mechanism. These issues have changed the battle field situation for the MANETs against the security threats.

The MANETs work without a centralized administration where the nodes converse with each other on the basis of mutual trust. This characteristic makes MANETs more susceptible to be misused by an attacker inside the network.

Wireless links also makes the MANETs more vulnerable to attacks, which make it easier for the attacker to go inside the network and get access to the current communication [1, 2]. Mobile nodes present within the range of wireless link can overhear and even join in the network.

The objective of this paper is to make a protocol more energy efficient, and to secure routing packets of proposed protocol in MANET which is basically based on AODV protocol.

We analyse the influence of heterogeneity of mobile nodes, in terms of their energy, which is an efficiency parameter, in MANET that are classifiably clustered. In these networks nodes are selected as a cluster heads randomly, aggregate the data of their cluster members and transmit it to the sink, in our protocol this random distribution depends upon the distribution of energy criteria.

We have assumed that a percentage of mobile nodes is fortified with supplementary energy resources as compare with normal sensors— this is a reason of heterogeneity which may result from the initial situation or as the set-up of the network starts. Also the initial optimum probability is calculated through probability distribution approach. We also assume that the devices are erratically (uniformly) distributed and are mobile, the coordinates of the sink and the dimensions of the field are known. Traditional protocols assume that all the nodes are armed with the same expanse of energy and as a result, they cannot take full advantage of the presence of node heterogeneity.

The AODV protocol's routing have been improved in our approach. The proposed Protocol have a Hash Signature, The structure will be more secured when we combine this Hash Signature with the Data Packets.

II. MANET

A Mobile Ad-Hoc Network (MANET) is a self-configuring infrastructure-less network of mobile devices linked by wireless. It is a group of wireless mobile computers (or nodes) in which nodes cooperate by forwarding packets for each other to allow them to communicate outside range of straight wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed [3].

Figure 1: Example of a simple Ad-Hoc Network with three

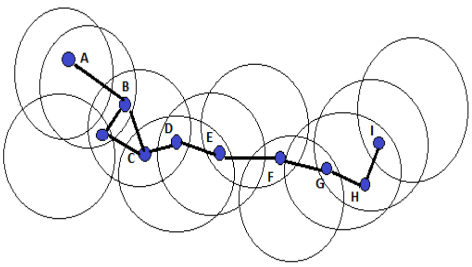

Figure 1: Example of a simple Ad-Hoc Network with three participating nodes

MANET is an independent group of mobile users that communicate over reasonably slow wireless links. The network topology may vary rapidly and unpredictably over time, because the nodes are mobile. The network is reorganised, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality will have to be incorporated into the mobile nodes.

MANET Features

Mobile ad hoc network nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), omnidirectional (broadcast), probably steerable, or some combination thereof [4]. At a given point in time, depending on positions of nodes, their transmitter and receiver coverage patterns, communication power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hop graph or "ad-hoc" network exists among the nodes. This ad hoc topology may modify with time as the nodes move or adjust their transmission and reception parameters.

A MANET has the following features:

A. Autonomous terminal

In MANET, each mobile terminal is an independent node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

B. Distributed operation

Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

C. Multi-hop Routing

Basic types of ad hoc routing algorithms can be single-hop and multi-hop, based on different link layer qualities and routing protocols. Single-hop MANET is simpler than multi-hop in terms of structure and implementation, with the cost of lesser functionality and applicability. When conveying data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded through one or more intermediate nodes.

D. Dynamic network topology

Since the nodes are mobile, the network topology may change rapidly and randomly and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network (e.g. Internet).

E. Fluctuating link capacity

The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.

F. Light-weight terminals

In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

III. MANETs Routing Protocols

Routing is the act of moving information from source to a destination in an internet work. During this process, at least one intermediate node within the internetwork is encountered. The routing concept basically involves two activities: firstly, determining optimal paths and secondly, transferring the information groups (called packets) through an internetwork. The latter concept is called as packet switching, which is straight forward, and path determination is very complex.

In mobile ad-hoc network every node is having routing capability. Nodes are within the radio range (transmission-range) are called its Neighbours. When the destination node is neighbour of source node, packets are transferred with single hop. When the destination node is neighbour of source node, packets are transferred with single hop. When the destination node is out of radio-range (not a neighbours of source node) then packet are transferred in multiple hops using intermediate nodes. These intermediate nodes (neighbours of source node) forward packets to their neighbours and so on till destination is reached. This is shown in figures below:

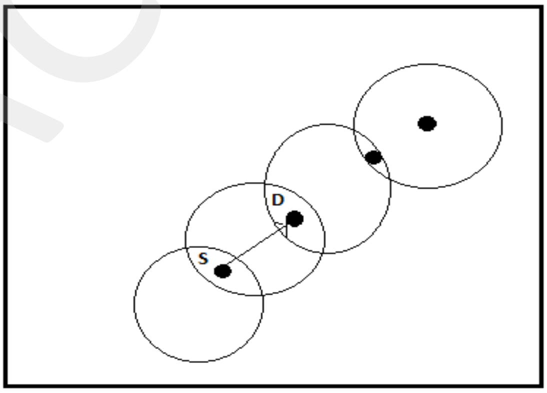

Figure 2 (a): Single hop transfer when S and D are in radio range

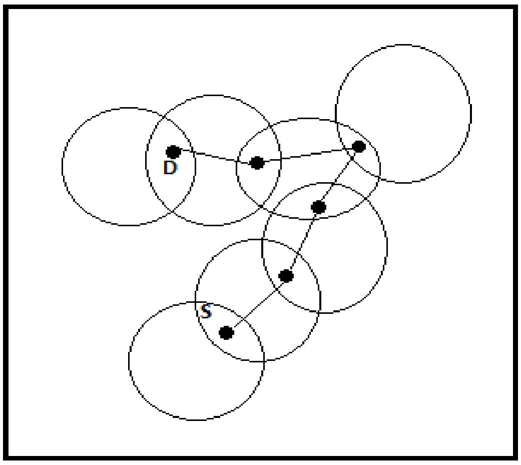

Figure 2 (b): Multiple hops when S and D are not in radio range

AODV Protocol

AODV is described in RFC 3561 [6]. It's reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network.

Characteristics of AODV

- Unicast, Broadcast, and Multicast communication.
- On-demand route establishment with small delay..
- All routes are loop-free through use of sequence numbers.
- Use of Sequence numbers to track accuracy of information.
- Only keeps track of next hop for a route instead of the entire route.
- Use of periodic HELLO messages to track neighbours [13].

Advantages and Disadvantages of AODV

The main advantage of AODV protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is less. The HELLO messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network. One of the disadvantages of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also multiple Route-Reply packets in response to a single Route-Request packet can lead to heavy control overhead [13]. Another disadvantage of AODV is that the periodic beaconing leads to unnecessary bandwidth consumption.

IV. Proposed Methodology

AODV

- In AODV, the network is silent until a connection is needed.
- Setting up Devices & field in the Network
- Calculate Distance vector between nodes, and update look up matrix with respect to distance matrix.
- Calculate path and cost with respect to source device, destination device and lookup values between them.
- Start Sending Packets according to Distance vector.
- When a link fails, a routing error is passed back to a transmitting node, and the process repeats.
- The advantage of AODV is that it creates no extra traffic for communication along existing links.
- Also, distance vector routing is simple, and doesn't require much memory or calculation.
- However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.
- Finally Update Efficiency Parameters defined in Network for results.

Figure below shows the basic flow diagram of proposed SECRP protocol.

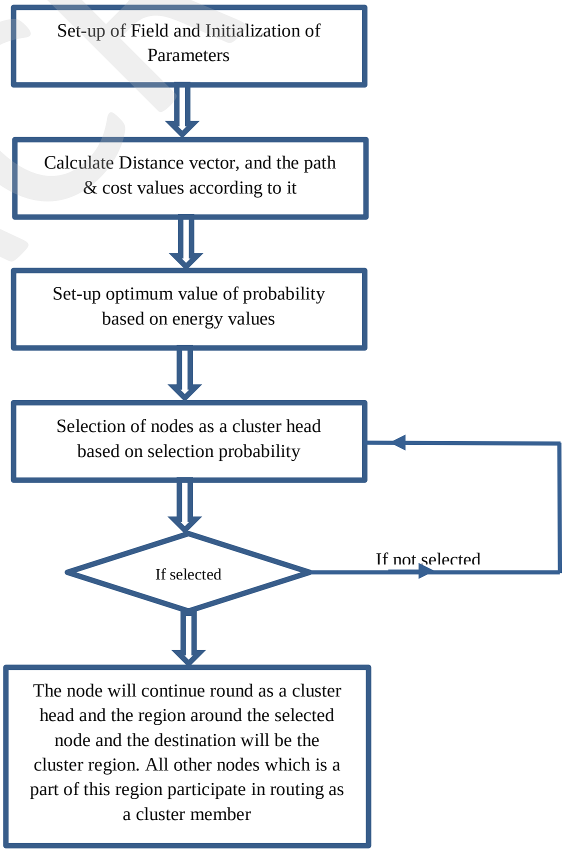
Set-up of Field and Initialization of Parameters
Calculate Distance vector, and the path & cost values according to it
Set-up optimum value of probability based on energy values
Selection of nodes as a cluster head based on selection probability
If selected
If not selected
The node will continue round as a cluster head and the region around the selected node and the destination will be the cluster region. All other nodes which is a part of this region participate in routing as a cluster member

Figure 3: Basic Flow diagram of Proposed SECRP Algorithm

SECRP (Proposed Algorithm)

In recent years there have been some different approaches on cluster-based routing. In Cluster based Routing Protocol, the devices of a wireless network are divided into several disjoint or overlapping clusters. Each cluster elects one node as the so-called cluster-head. These special nodes are responsible for the routing process. Neighbours of cluster-heads cannot be cluster-heads as well. But cluster-heads are able to communicate with each other by using gateway nodes. A gateway is a node that has two or more cluster-heads as its neighbours or— when the clusters are disjoint—at least one cluster-head and another gateway node. The routing process itself is performed as source routing by flooding the network with a route request message. Due to the clustered structure there will be less traffic, because route requests will only be passed between cluster-heads.

- In SECRP, the network is silent until a connection is needed.
- Setting up Devices & field in the Network.
- Setup initial Energies of devices depend upon user defined scenario.
- Create a Cluster network of these devices, and divide a bunch of devices into number of clusters. The cluster mechanism in it is, in each cluster there is a cluster head, all devices transmit there data to cluster head and then cluster head route the data to the destination.
- The problem in it is a proper selection of these cluster heads.
- Model an secured energy based cluster Head selection scheme, in which selection criteria depends upon a bunch of energies (average, dissipated, residual, and current)
- The benefit of applying such a behaviour in network, is to increase network lifespan and hence the efficiency parameters like throughput, end to end delay.
- Calculate Distance vector between nodes, and update look up matrix with respect to distance matrix.
- Calculate path and cost with respect to source device, destination device and lookup values between them.
- Devices Start Sending Packets to cluster heads according to Distance vector.
- The Cluster head route the data gathered from devices to Destination depends upon the Distance vector between nodes in network (One can simply say it as Cluster based Distance vector routing scheme).
- Finally Update Efficiency Parameters defined in Network for results.

Clustering Hierarchy

Consider a Mobile Ad-Hoc network that is hierarchically clustered. The protocol contains clustering hierarchy. In basic routing, the clusters are re-established in each “round.” New cluster heads are elected in each round and as a result the load is well distributed and balanced among the nodes of the network. Moreover each node transmits to the closest cluster head so as to split the communication cost to the sink (which is tens of times greater than the processing and operation cost.) Only the cluster head has to report to the sink and may expend a large amount of energy, but this happens periodically for each node. In traditional clustering there is an optimal percentage p_{opt} (determined a priori) of nodes that has to become cluster heads in each round assuming uniform distribution of nodes in space.

If the nodes are homogeneous, which means that all the nodes in the field have the same initial energy, the traditional protocol guarantees that every one of them will become a cluster head exactly once every 1/ p_{opt} rounds. Throughout this work, this number of rounds refer to, 1/p_{opt}, as epoch of the clustered Mobile Ad-Hoc network. Initially each node can become a cluster head with a probability p_{opt}. On average, n × p_{opt} nodes must become cluster heads per round per epoch. Nodes that are elected to be cluster heads in the current round can no longer become cluster heads in the same epoch. The non-elected nodes belong to the set G and in order to maintain a steady number of cluster heads per round, the probability of nodes €G to become a cluster head increases after each round in the same epoch. The decision is made at the beginning of each round by each node s € G independently choosing a random number in [0, 1]. If the random number is less than a threshold T(s) then the node becomes a cluster head in the current round. The threshold is set as:

$$T(s) = \begin{cases} \dfrac{P_{OPT}}{1 - P_{OPT}(rmod\ 1/P_{OPT})} & if\ s \in G \\ 0 & Otherwise \end{cases}$$

Where, r is the current round number (starting from round 0.) The election probability of nodes € G to become cluster heads increases in each round in the same epoch and becomes equal to 1 in the last round of the epoch. Note that by round a time interval is defined that where all cluster members have to transmit to their cluster head once. It is shown in this work how the election process of cluster heads should be adapted appropriately to deal with heterogeneous nodes, which means that not all the nodes in the field have the same initial energy.

Optimal Clustering

This clustering is optimal in the sense that energy consumption is well distributed over all devices and the total energy consumption is minimum. Such optimal clustering highly depends on the energy

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 9, April 2013)

model uses. For the purpose of this study this work use similar energy model and analysis.

It consider all energy parameters like residual energy, average energy, initial energy and the total energy, and make an optimal mobile device selection structure which depend upon these energies to extend the lifetime of the network.

According to the radio energy dissipation model, in order to achieve an acceptable Signal-to-Noise Ratio (SNR) in transmitting an L-bit message over a distance d, the energy expended by the radio is given by:

$$E_{T2}(l,d) = \begin{Bmatrix} L.E_{elec} + L.\epsilon_{fs}.d^2 \ \ if\ d \le d_0 \\ L.E_{elec} + L.\epsilon_{mp}.d^4 \ \ if\ d > d_0 \end{Bmatrix}$$

Where E_{elec} is the energy dissipated per bit to run the transmitter or the receiver circuit, ϵ_{fs} and ϵ_{mp} depend on the transmitter amplifier model uses, and d is the distance between the sender and the receiver, By equating the two expressions at $d = d0$, It has $d_0 = \sqrt{\epsilon_{fs}/\epsilon_{mp}}$. To receive an L-bit message the radio expends $E_{Rx} = L.E_{elec}$.

V. SIMULATION AND RESULTS

Simulation is carried out using MATLAB R2009a

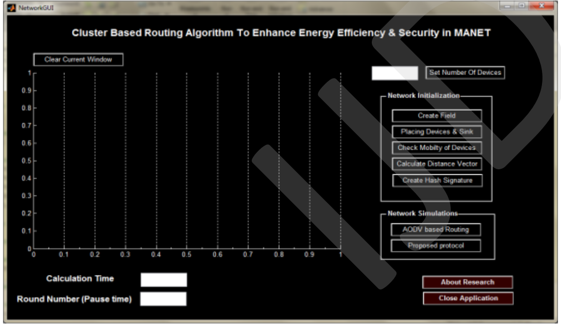

Figure 4: Main Graphical User Interface of proposed protocol developed in MATLAB

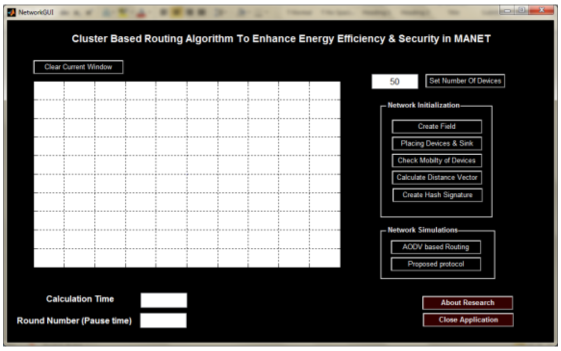

Figure 5: 10000 square meter field created

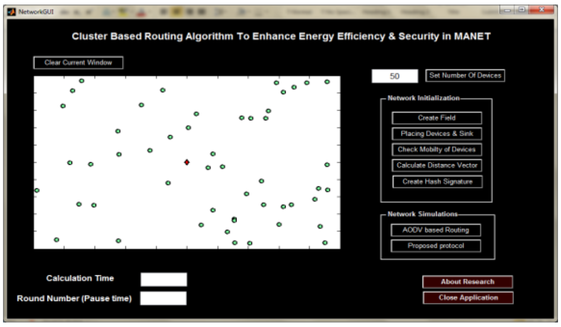

Figure 6: Device placement in the field

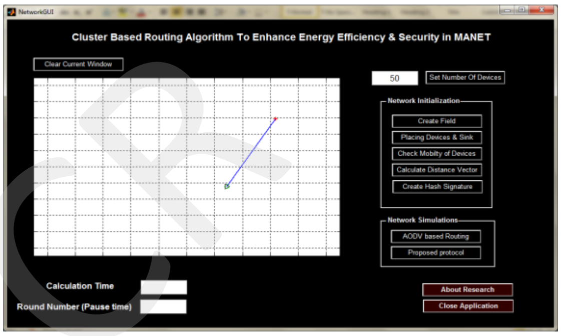

Figure 7: The distance-vector calculated between two nodes

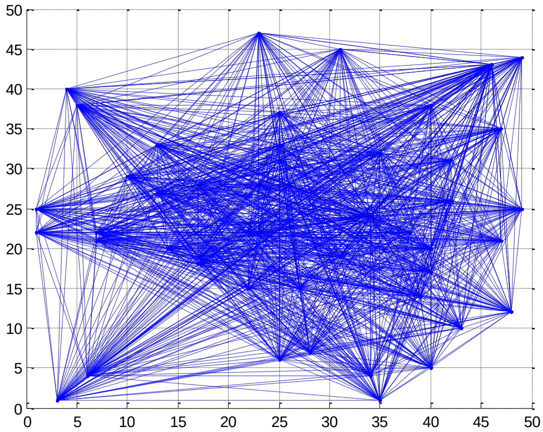

Figure 8: Communication between 50 different nodes, cluster heads and destination

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 9, April 2013)

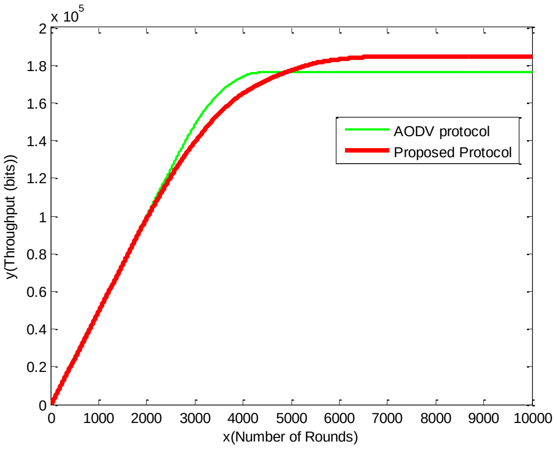

Figure 9: Network throughput in bits/sec with respect to number of rounds or pause time of packet delivery for 50 devices

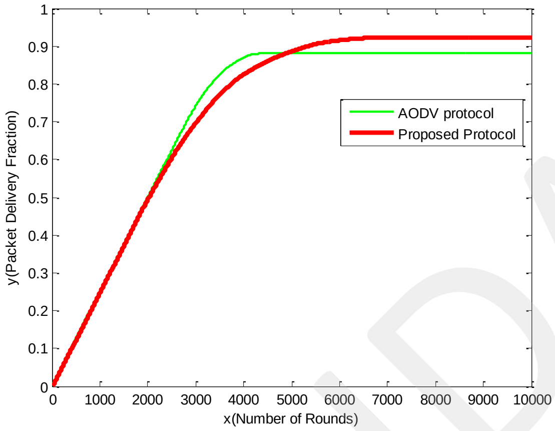

Figure 10: Packet delivery fraction with respect to number of rounds or pause time of packet delivery for 50 devices

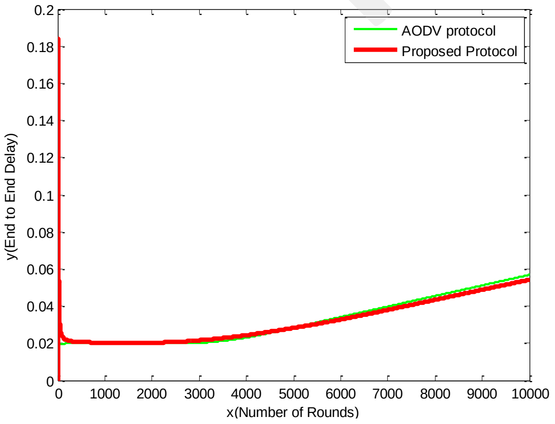

Figure 11: End to End delay for both the AODV protocol and the proposed protocol with respect to number of rounds or pause time of packet delivery for 50 devices

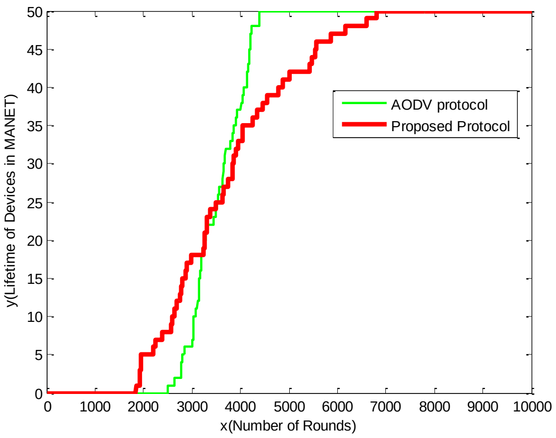

Figure 12: Network life-time for both the AODV protocol and the proposed protocol with respect to number of rounds or pause time of packet delivery for 50 devices

IV. CONCLUSIONS

This paper presents a novel routing protocol and a comprehensive study of the proposed protocol with AODV protocol in different scenario. Our routing protocols are analysed in a mobile Ad-Hoc network in the presence of some higher energy devices.

After creation of scenario of mobile network between devices, above proposed protocol is simulate on MATLAB 2009a. In simulation rounds of nodes varies and speed of node is constant and vice versa. After the several simulation runs and their analysis, it was observed that our protocol can perform better in almost all situations and the Hash Signature Mechanism provide more security to data packets, which is further proven by comparing results with the traditional AODV protocol. Our protocol can give better results in high density network where nodes move with different pause time. AODV also performed better in some conditions, but the results were not promising in all cases.

As a piece of future work it can simulate routing protocols by using other protocols with the help of other different parameters in wide network size with different mobility models and check its performance.

REFERENCES

[1] P.V. Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17, 2002.

[2] K. Biswas. Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.

[3] Geetha Jayakumar, Gopinath Ganapathy, "Performance Comparison of Mobile Ad-hoc Network Routing Protocol", IJCSNS, VOL.7 No.11, November 2007.

[4] Mobile Ad-hoc Networks (MANET), Online Available at- http://www.ietf.org/html.charters/manetcharter.html.

[5] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[6] http://www.faqs.org/rfcs/rfc3561.html

[7] Mohamed S. El-azhari, Othman A. Al-amoudi, Mike Woodward, Irfan Awan, “Performance Analysis in AODV Based Protocols for MANETs”, International Conference on Advanced Information Networking and Applications Workshops, 2009.

[8] Idris Skloul Ibrahim, Peter J.B King, Robert Pooley, “Performance Evaluation of Routing Protocols for MANET”, Fourth International Conference on Systems and Networks Communications, 2009.

[9] Mohammad M. Qabajeh, Aisha-Hassan A. Hashim, Othman Khalifa, Liana K. Qabajeh, “Quality of Service Multicast Routing Protocol for Large Scale MANETs”, International Conference on Computer Technology and Development, 2009.

[10] Liana Khamis Qabajeh, Dr. Miss Laiha Mat Kiah, Mohammad Moustafa Qabajeh, “A Scalable Secure Routing Protocol for MANETs”, International Conference on Computer Technology and Development, 2009.

[11] Ashish Shrestha, Firat Tekiner, “On MANET Routing Protocols for Mobility and Scalability”, International Conference on Parallel and Distributed Computing, Applications and Technologies, 2009.

[12] David Oliver Jorg, “Performance Comparison of MANET Routing Protocols in Different Network Sizes” International Conference on Computer Technology and Development, 2003.

[13] Luke Klein-Bernd, “A Quick Guide to AODV Routing”, National Institute of Standards and Technology, US.

[14] Elis Kulla, Makoto Ikeda, Leonard Barolli, Rozeta Miho, Vladi Kolici, “Effects of Source and Destination Movement on MANET Performance Considering OLSR and AODV Protocols”, 13th International Conference on Network-Based Information Systems, 2010.

[15] Idris Skloul Ibrahim, Peter J.B King, Robert Pooley, “Performance Evaluation of Routing Protocols for MANET”, IEEE, Fourth International Conference on Systems and Networks Communications, 978-0-7695-3775-7, 2009.

[16] Chansu Yu, Ben Lee, Hee Yong Youn, “Energy Efficient Routing Protocols forMobile Ad Hoc Networks”, Cleveland State University, EFFRD ISSN No. 0210-0630, 2010.

[17] Suchismita Rout, Ashok Kumar Turuk, Bibhudatta Sahoo, “Energy Aware Routing Protocol in MANET using Power Efficient Topology Control Method”, International Journal of Computer Applications (0975 – 8887) Volume 43– No.5, April 2012.

[18] Neha Gupta, Manish Shrivastava, Angad Singh, “Greedy Cluster Head Selection Based Routing Protocol for Mobile Ad Hoc Networks”, International Conference on Electrical Engineering and Computer Science Engineering (ICEECS) Sept, 2012.

[19] Aswathy M C, Tripti C, “Cluster based enhancement to AODV for inter-vehicular communication in VANET”, International Journal of Grid Computing & Applications (IJGCA) Vol.3, No.3, September 2012.

[20] Tripti Nema, Akhilesh waoo, P. S. Patheja, Sanjay Sharma, “Energy based AODV Routing Algorithm with Sleep Mode in MANETs”, International Journal of Computer Applications (0975 – 8887), Volume 58– No.19, November 2012.