ISSN: 2321-7782 (Online)
Volume 4, Issue 3, March 2016
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

NCPR using Paillier Cryptosystem to Reduced Routing Overhead and Secure Data Transmission in MANET

Dipali Sakharam Patil[1]
M.E. (C.S.E) Student
Department of Computer Science
G.H.R.I.E.M, Jalgaon, India

Prof. Prashant Rewagad[2]
Associate Professor
Department of Computer Science
G.H.R.I.E.M, Jalgaon, India

Abstract: ***Mobile Ad Hoc Network (MANETs) consists of a collection of mobile nodes which can move freely. These nodes can be dynamically self-organized into arbitrary topology networks without a fixed infrastructure. MANETs are highly dynamic network because nodes may join and leave the network at any time. Due to high mobility of nodes in network there is frequent path failure and route discovery in MANET. So the NCPR (Neighbor coverage based probabilistic rebroadcast) is used for reducing routing overhead in Mobile Ad Hoc Networks. In MANETs, when network's size exceeds a certain threshold decreases the performance, resulting in many routing algorithms performing only when network's size is small. To overcome bandwidth and battery power limitations, and reduce routing overhead, it is mandatory to make network organization smaller and manageable. So we are going to use the clustering architecture in MNAET. This significantly reduces the routing overhead in the MANET and increase the throughput, jitter and allows using energy efficiently. Once the route is selected from source to destination data is transferred between nodes. This transmission is unsecured. To make it secure we are going to use a Paillier cryptographic technique to avoid possible attacks on sensitive data. So that data will be transmitted confidentially.***

Keywords: MANET routing, communication phases, NCPR, Paillier Cryptosystem.

I. INTRODUCTION

A MANET is a network that consists of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. The mobile hosts do not have any centralized control like base stations or mobile switching centers. This offers unrestricted mobility and connectivity to the users, although the duty of network management is now entirely on the nodes that forms the network. Due to the limited transmission range of wireless network interfaces, multiple hops may be needed for one node to exchange data with another across the network.

The routing protocols for MANET are classified as table driven i.e. proactive routing protocol, on demand i.e. reactive routing protocol and hybrid routing protocol. In proactive routing, nodes attempt to maintain consistent, up-to-date routing information of the whole network. Each node has to maintain one or more tables to store routing information, and response to changes in network topology by broadcasting and propagating. Reactive routing tries to eliminate the conventional routing tables and consequently reduce the need for updating these tables to track changes in the network topology. When a source requires to a destination, it has to establish a route by route discovery procedure, maintain it by some form of route maintenance procedure until either the route is no longer desired or it becomes inaccessible, and finally tear down it by route deletion procedure. Hybrid routing protocols aggregates a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used. Consequently, in hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones [12].

Due to high mobility of nodes in network there is frequent path failure and route discovery in MANET. So the NCPR (Neighbor coverage based probabilistic rebroadcast) is used for reducing this routing overhead in Mobile Ad Hoc Networks. In this routing protocol the neighbor knowledge and rebroadcast probability is used for rebroadcasting a request. A novel rebroadcast delay is calculated to determine the rebroadcast order while routing, and it obtains the more accurate additional coverage ratio by sensing neighbor coverage knowledge. A connectivity factor is defined to provide the node density adaptation for keeping the network connectivity. By combining the additional coverage ratio and connectivity factor, the rebroadcast probability is calculated. [1].

The communication in mobile ad hoc networks comprises two phases,

1. Route discovery and
2. Data transmission.

In an adverse environment, both phases are vulnerable to a variety of attacks. The adversaries at data route discovery phase can disrupt the route discovery by impersonating the destination, by responding with stale or corrupted routing information, or by disseminating forged control traffic. This way, attackers can obstruct the propagation of legitimate route control traffic and adversely influence the topological knowledge of benign nodes. However, adversaries can also disrupt the data transmission phase and, thus, incur significant data loss by tampering with, fraudulently redirecting, or even dropping data traffic or injecting forged data packets.

To provide comprehensive security, both phases of MANET communication must be safeguarded. It is notable that secure routing protocols, which ensure the correctness of the discovered topology information, cannot by themselves ensure the secure and undisrupted delivery of transmitted data. This is so, since adversaries could abide with the route discovery and be placed on utilized routes. But then, they could tamper with the in-transit data in an arbitrary manner and degrade the network operation [17].

The requirements of Secure Communication in MANET are

(a) It is necessary that a security association exist between network members to ensure authentication and non-repudiation for trusted nodes.

(b) Sensitive information must be exchanged confidentially.

(c) Integrity of the information exchanged within the network has to be maintained [4].

There are numerous security routing protocols and key management schemes that have been designed based on cryptographic techniques. These techniques include public key infrastructures and identity-based cryptography. In fact, some of them are fully adapted to fit the network requirements on limited resources such as storage, CPU, and power limitations [9]. The Paillier Cryptosystem is a modular, public key encryption scheme, created by Pascal Paillier, with several interesting properties [11].

MANETs require no fixed infrastructure or central administration. Mobile nodes in an ad hoc network work not only as hosts but also as routers, and communicate with each other via packet radios.

Since most wireless nodes in ad hoc networks are not connected to a power supply and battery replacement may be difficult, optimizing the energy consumption in these networks has a high priority and power management is one of the most challenging problems in ad hoc networking.

Routing in a network is the process of selecting paths to send network traffic. Routing can take place either in a flat structure or in a hierarchical structure [14]. In a flat structure [14, 16], all nodes in the network are in the same hierarchy level and thus have the same role. Although this approach is efficient for small networks, it does not allow the scalability when the

number of nodes in the network increases. In large networks, the flat routing structure produces excessive information flow which can saturate the network.

Hierarchical routing protocols [16] have been proposed to solve this problem among others. This approach consists of dividing the network into groups called clusters. This results in a network with hierarchical structure. Different routing schemes are used between clusters (inter-cluster) and within clusters (intra- cluster). Each node maintains complete knowledge of locale information (within its cluster) but only partial knowledge about the other clusters. Hierarchical routing is a solution for handling scalability in a network where only selected nodes take the responsibility of data routing [15].

This paper covers the literature review of routing protocol and different techniques used for secure communication in MANET in section II. Section III contains the overview of proposed work and section IV contains the implementation methodology used. The results of simulation are presented in section V. In section VI we conclude the paper and present the future work.

II. LITERATURE REVIEW

In [2] C. Perkins has proposed the Adhoc on Demand Distance Vector Routing AODV is a novel algorithm for the routing operation of such mobile adhoc networks. AODV is an on demand routing protocol i.e. the routes are obtained as needed. The route request packet (RREQ) is sent from source to destination and the route is returned in route reply packet (RREPL) from destination to source. In [1] Xin MingZhang proposed the neighbor coverage based probabilistic rebroadcast protocol (NCPR) has proposed that utilizes the AODV mechanism. NCPR reduces routing overhead as part of rebroadcast.

In [4] Wenjia Li and Anupam Joshi have discussed several main requirements that need to be achieved to ensure the security of the mobile ad hoc network to find out how to judge if a mobile ad hoc network is secure or not. The security criteria include availability, Integrity, Confidentiality, authenticity, nonrepudiation, authorization, anonymity. There are some types of attacks in mobile ad hoc network. The attacks in MANET can be briefly classified into two categories: external attacks and internal attacks the main attack types in the mobile ad hoc network, which are denial-of-service (DoS) attacks, impersonation attacks, eavesdropping attacks and attacks against routing. Two kinds of popular security techniques in the mobile ad hoc network, which are intrusion detection techniques and secure routing techniques.

To provide comprehensive security, both phases of MANET communication must be safeguarded. To secure the data transmission phase, [3] Panagiotis Papadimitratos propose and evaluate the Secure Message Transmission (SMT) protocol, an end-to-end secure data forwarding protocol tailored to the MANET communication requirements. The SMT protocol safeguards pairwise communication across an unknown frequently changing network, possibly in the presence of adversaries that may exhibit arbitrary behavior.

In [9] Hongmei Deng has discussed the scenario for using symmetric and asymmetric cryptosystem in a MANET network. If all routing messages are encrypted with a symmetric cryptosystem, it means that everybody those want to be able to participate in the network has to know the key. If there is a team of persons, let every member of the team to know the “team-key”. They assume that a member of the team will not do anything nasty to the other members because the members of team trust each other. They trust and authorize the other members to change their routing tables. Suppose that a MANET network need to be created where everybody can participate. May be in a convention, in a meeting room, in a campus, or in our neighborhood. At that time there is problem, they do not trust others. With this scenario in mind, the best option could be to use an asymmetric cryptosystem (with public and private key pairs) so that the originator of the route messages signs the message. It would not be needed to encrypt the routing messages because they are not secret. The only requirement is that the nodes will be able to detect forged routing messages.

In [5] Seung Yi, Prasad Naldurg proposed a new routing technique called security aware ad hoc routing that incorporates security attributes as parameters in to ad hoc route discovery. SAR enables the use of security as a negotiable metric to improve

the relevance of route discovered by ad hoc routing protocols. A two tier classification of routing protocol security metrics, and propose a framework to measure and enforce security attributes on ad hoc routing paths. In addition to determining a secure route, the information in routing messages must also be protected against alteration that can change routing behavior. The security of ad hoc routing algorithm is improved with respect to transmission of routing messages. Zapata and Asokan in [6] proposed SAODV i.e. a secure version of AODV which uses digital signature and hash chains to secure the routing messages.

In [7] Lidong Zhou and Zygmunt J. Haas have discussed the security of routing protocols for ad hoc network. In an ad hoc network, from the point of view of a routing protocol, there are two kinds of messages: the routing messages and the data messages. Both have a different nature and different security needs. Data messages are point-to point and can be protected with any point-to-point security system (like IP Sec). On the other hand, routing messages are sent to immediate neighbors, processed, possibly modified, and resent. Moreover, as a result of the processing of the routing message, a node might modify its routing table. This creates the need for the intermediate nodes to be able to authenticate the information contained in the routing messages (a need that does not exist in point-to-point communications) to be able to apply their import authorization policy.

B. A. Correa et al [8], discussed the concepts related to network topology, routing schemes, graphs partitioning and mobility algorithms. The authors described lowest-ID heuristic, highest degree heuristic, DMAC (distributed mobility-adaptive clustering), WCA (weighted clustering algorithm).

R. Agarwal and M. Motwani [9] examined the important issues related to cluster-based MANETs, such as the cluster structure stability, the control overhead of cluster construction and maintenance, the energy consumption of mobile nodes with different cluster-related status, the traffic load distribution in clusters, and the fairness of serving as cluster head for a mobile node.

M. Anupama and B. Sathyanarayana [10], analyzed, compared and classified some clustering algorithms into: location based, neighbor based, power based, artificial intelligence based, mobility based and weight based. They also presented the advantages and disadvantages of these techniques and suggest a best clustering approach based on the observation and the comparison.

III. PROPOSED WORK

In this section we focus on problem that occurs when the no of nodes in the network increases, there is increased routing overhead in MANET. So for that we need to organize the network in some way to reduce routing overhead and improve efficiency of network. Also once route is found we should ensure the confidentiality of data transmission. So we propose the architecture that removes the problem and improve the performance.

To secure the data transmission phase, we propose and evaluate the system, an end-to-end secure data forwarding tailored to the MANET communication requirements. We underline that the goal of system is not to securely discover routes in the network. The goal of system is to ensure secure data forwarding, after the discovery of routes between the source and the destination has been already performed.

In MANETs, when network's size exceeds a certain threshold decreases the performance, resulting in many routing algorithms performing only when network's size is small. To overcome bandwidth and battery power limitations, and reduce routing overhead, it is mandatory to make network organization smaller and manageable.

Though reactive routing protocol performs well with mobile nodes, it piles up high overheads with increased network size, nodal degree or number of communicating source-destination pairs. A clustering architecture provides solution for the Problem in MANET environments: network scalability and reduction of communication overheads.

This will save energy since the transmissions will only be done by such cluster heads rather than all mobile sensor nodes. Clusters are maintained when data is to be forwarded. Such integrated routing and clustering scheme can improve throughput and reduce routing overhead. The proposed work includes:

1) Use of Cluster Architecture
2) Use of Paillier Cryptography

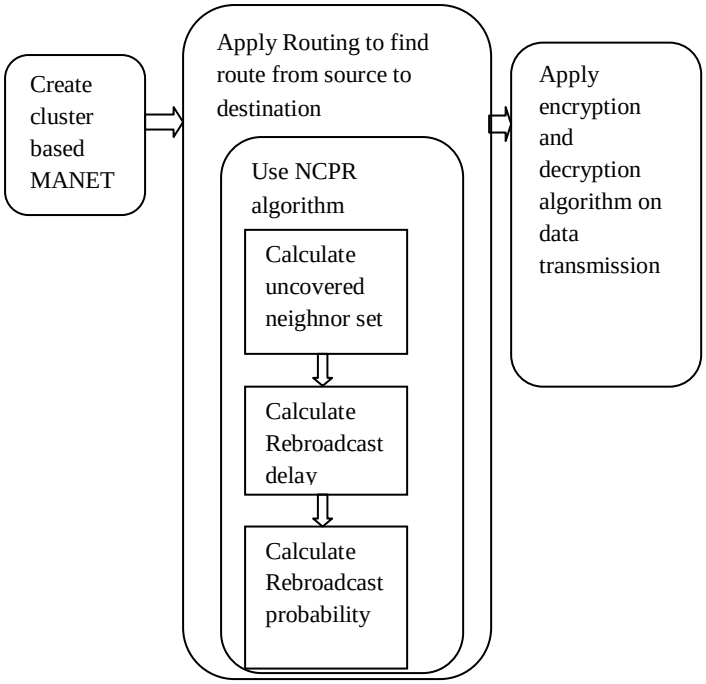

Figure 1 Proposed Work

The Figure 1 shows the proposed work architecture. The first stage is to create a cluster based mobile adhoc network. This creates several clusters inside MANET. Each cluster has a cluster head. This cluster head is elected as the node inside cluster that has maximum energy. The second maximum energy node is elected.

In the second stage there is finding route form source node to destination node. For finding route we apply the routing protocol and use the neighbor coverage based probabilistic rebroadcast technique to reduce routing overhead in finding route. So there are three important stages that we need to implement in neighbor coverage based probabilistic rebroadcast (NCPR). In that before rebroadcasting, first stage is to calculate uncovered neighbor set between the node and the all its neighbors. Then at second stage calculate the delay and set timer of node for rebroadcasting the RREQ packet to neighbor nodes. And at the last stage calculate the probability for rebroadcasting RREQ packet. In this way NCPR protocol is applied to find rout from source to destination.

Now there are two types of communication that take place using cluster first is inter cluster communication and second is intra cluster communication. If both the source and destination nodes are within the same cluster then intra cluster communication takes place. In that the source node first send RREQ to the cluster head then cluster head finds the route to the destination and return to the source node.

In another case if the source node is in another cluster and destination node is in another cluster then the inter cluster communication takes place. In that the source node sends RREQ to its cluster head and then the cluster head sends the RREQ to all the other clusters through gateway nodes. All the cluster heads find whether there is destination node in cluster if there is destination then RREP packet is returned to the source node. In this way a path is returned to the source node.

Once the route is find out the data transmission takes place. The data is transmitted from source to the destination node using the route. Before transmission of each data packet it is first encrypted using Paillier cryptographic algorithm. And when it

reaches to the destination it is first decrypted into original data. In this way data security is provided. To exchange data confidentially between nodes this Paillier cryptographic algorithm is applied.

IV. IMPLEMENTATION

In this section we focus on the methodology to implement the proposed architecture. We provide the methodology for the implementation of parts of the proposed work. These include the creation of clusters in network, the Neighbor coverage Based Probabilistic Rebroadcast technique and the Paillier cryptographic algorithm in details

The conventional on demand routing protocols use flooding to discover a route. They broadcast a Route REQuest (RREQ) packet to the networks, and the broadcasting induces excessive redundant retransmissions of RREQ packet and causes the broadcast storm problem, which leads to a considerable number of packet collisions. Therefore, it is essential to optimize this broadcasting mechanism. Some methods have been proposed to optimize the broadcast problem in MANETs in the past few years. These broadcasting protocols were categorized into four classes: "simple flooding, probability-based methods, area based methods, and neighbor knowledge methods." Since limiting the number of rebroadcasts can effectively optimize the broadcasting, a neighbor coverage-based probabilistic rebroadcast (NCPR) protocol is used [2].

This protocol consists of a novel scheme to calculate the rebroadcast delay. The rebroadcast delay is to determine the forwarding order. The node which has more common neighbors with the previous node has the lower delay. If this node rebroadcasts a packet, then more common neighbors will know this fact. Therefore, this rebroadcast delay enables the information that the nodes have transmitted the packet spread to more neighbors.

This protocol also has a novel scheme to calculate the rebroadcast probability. The scheme considers the information about the uncovered neighbors (UCN), connectivity metric and local node density to calculate the rebroadcast probability. The rebroadcast probability is composed of two parts: additional coverage ratio, which is the ratio of the number of nodes that should be covered by a single broadcast to the total number of neighbors; and connectivity factor, which reflects the relationship of network connectivity and the number of neighbors of a given node. The neighbor coverage based rebroadcast protocol is used to reduce routing overhead [2].

We intend to integrate clustering with routing functionalities. The main design goals of our clustering scheme are:

1. The algorithm should use a routing protocol's control messages for cluster formation with minimal overhead.
2. The algorithm must operate in localized and distributed manners and interoperate with nodes.
3. The algorithm must incur minimal cluster formation and maintenance overhead and support on-demand cluster formation.
4. The algorithm should minimize network-wide flooding and be scalable.

In most clustering techniques nodes are selected to play different roles according to a certain criteria. In general, three types of nodes are defined:

1. Ordinary nodes

Ordinary nodes are members of a cluster which do not have neighbours belonging to a different cluster [12].

2. Gateway nodes Gateway nodes are nodes in a non-cluster head state located at the periphery of a cluster. These types of nodes are called gateways because they are able to listen to transmissions from another node which is in a different cluster [12]. To accomplish this, a gateway node must have at least one neighbour that is a member of another cluster
3. Cluster heads

Most clustering approaches for mobile ad hoc networks select a subset of nodes in order to form a network backbone that supports control functions. A set of the selected nodes are called cluster heads and each node in the network is associated with

one. Cluster heads are connected with one another directly or through gateway nodes. The union of gateway nodes and cluster heads form a connected backbone. This connected backbone helps simplify functions such as channel access, bandwidth allocation, routing power control and virtual circuit support [15]. Since cluster heads must perform extra work with respect to ordinary nodes they can easily become a single point of failure within a cluster.

For this reason, the cluster head election process should consider for the cluster head role, those nodes with a higher degree of relative stability. The main task of a cluster head is to calculate the routes for long-distance messages and to forward inter-cluster packets. A packet from any source node is first directed to its cluster head. If the destination is located in the same cluster, the cluster head just forwards the packet to the destination node.

If the destination node is located in a different cluster, the cluster head of the sending node routes the packet within the substructure of the network, to the cluster head of the destination node. Then, this cluster head forwards the packet to its final destiny.

This section shows how to encrypt and decrypt messages using paillier cryptosystem, with the underlying mathematical principles that make the system work clearly outlined. It is assumed that the reader is familiar, to some degree, with modular arithmetic, as well as the concept of converting an alphanumeric message into a purely numeric message, which can be broken into blocks, m_i, such that, for each i, $0 < m_i < n$, for a predetermined value, n. Also, the term plaintext will be used to refer to a message that is numeric, but is not encrypted, while the term cipher text will be used to refer to plaintexts which have been encrypted, but not yet decrypted [11].

Using Paillier Cryptosystem

Select two large prime numbers p and q randomly and independently of each other such that $gcd(pq, (p-1)(q-1)) = 1$ This property is assured if both primes are of equal length

1. Compute $n = pq$ and $\lambda = lcm(p-1, q-1)$
2. Select random integer g where $g \epsilon \mathbb{Z}^*_{n^2}$
3. Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse $\mu = \left(L\left(g^\lambda \bmod n^2\right)\right)^{-1} \bmod n$,where function $L$is defined as $L(u) = \frac{u-1}{n}$

Note that the notation $\frac{a}{b}$does not denote the modular multiplication of a times the modular multiplicative of b but rather the quotient of a divided by b i.e., the largest integer value $v \geq 0$ to satisfy the relation $a \geq vb$

- The public encryption key is (n, g)
- The private (decryption) key is(λ, μ)

If using p, q of equivalent length a simpler variant of the above key generation steps would be set $g = n + 1, \lambda = \varphi(n)$and $\mu = \varphi(n)^{-1} mod\ n$,where $\varphi(n) = (p-1)(q-1)$

- **Encryption**

  1. let m be a message to be encrypted where $m \epsilon \mathbb{Z}_n$

  2. select random r where $r \epsilon \mathbb{Z}^*_n$

  3. Compute cipher text as: $c = g^m . r^n mod\ n^2$

- **Decryption**

  1. Let c be the cipher text to decrypt, where $c \in \mathbb{Z}^*_{n^2}$

2. Compute the plaintext message as: $m = L(c^{\lambda} mod\ n^2).\mu\ mod\ n$

V. RESULTS

1. Simulation Environment:

In order to evaluate the performance of the proposed work, we simulate it using the NS-2 simulator. Simulation parameters are as follows: We consider constant bit rate (CBR) data traffic and randomly choose different source-destination connections. Every source sends four CBR packets whose size is 512 bytes per second. The mobility model is based on the random waypoint model in a field of 300 m × 300 m.

In this mobility model, each node moves to a random selected destination with a random speed from a uniform distribution [1, max-speed]. After the node reaches its destination, it stops for a pause time interval and chooses a new destination and speed. In order to reflect the network mobility, we set the max-speed to 5 m/s and set the pause time to 0.

The Max Delay used to determine the rebroadcast delay is set to 0.01 s, which is equal to the upper limit of the random jitter time of sending broadcast packets in the default implementation of AODV in NS-2. Thus, it could not induce extra delay in the route discovery. The simulation time for each simulation scenario is set to 1000 seconds. In the results, each data point represents the average of 30 trials of experiments. The detailed simulation parameters are shown in Table 1.

We evaluate the performance of routing protocols using the following performance metrics:

Average end-to-end delay: the average delay of successfully delivered CBR packets from source to destination node. It includes all possible delays from the CBR sources to destinations.

Average Throughput: It is defined as the total number of packets delivered over the total simulation time. **Average Jitter**: Jitter is the amount of variation in latency/response time, in milliseconds. Reliable connections consistently report back the same latency over and over again. Lots of variation (or 'jitter') is an indication of problems.

Average Energy: The amount of energy consumed by all nodes in network is the energy consumed by all nodes in network.

Table 1 Performance Parameters

Simulation Parameter	**Value**
Simulator	NS2 (2.35)
Topology size	300×300
Number of nodes	30
Interface Queue length	50
Packet size	512 bytes
Simulation Time(sec)	1000

2. Performance with Varied Time:

The figure 2 shows the change in throughput in our proposed work. This indicates that there is rise in throughput when compare with the original protocol. In figure the throughput shows throughput change with time for original protocol, while opt_throughput shows the optimized throughput values because of our proposed work.

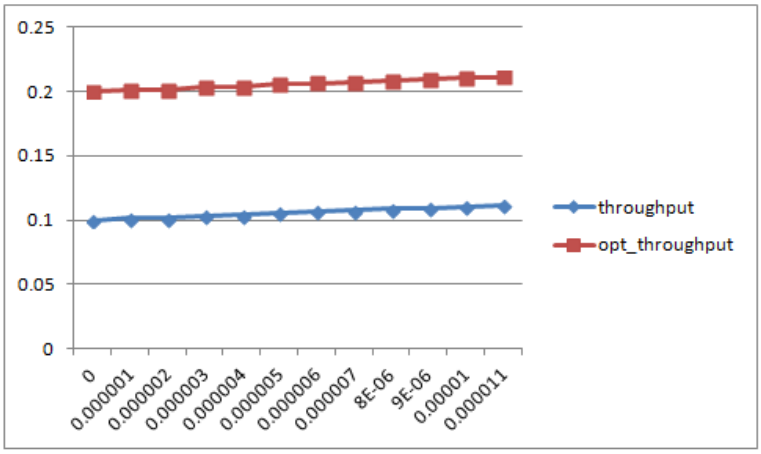

Figure 2 Throughput vs. Time graph

The Figure 3 shows the line graph that represents the change in delay value with optimized protocol. This indicates that there is reduction in delay when compare with the original protocol. In figure the delay shows delay change with time for original protocol, while opt_delay shows the optimized throughput values because of our proposed work.

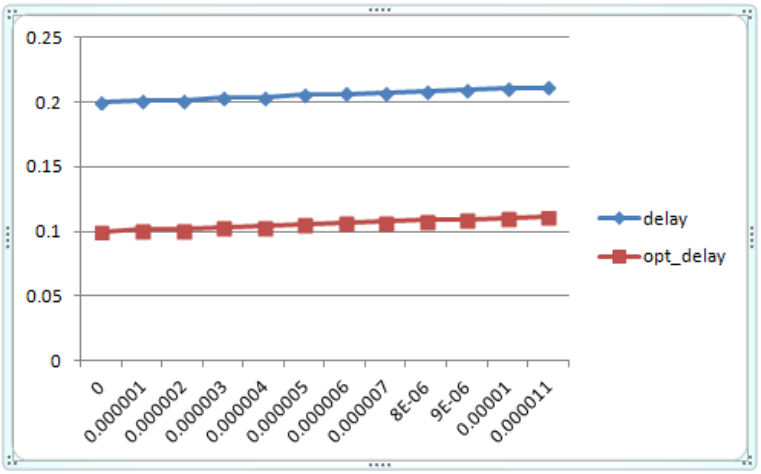

Figure 3 Delay vs. Time graph

The Figure 4 shows the line graph that represents the change in jitter value with optimized protocol. This indicates that there is rise in jitter when compare with the original protocol. In figure the jitter shows delay change with time for original protocol, while opt_jitter shows the optimized jitter values because of our proposed work.

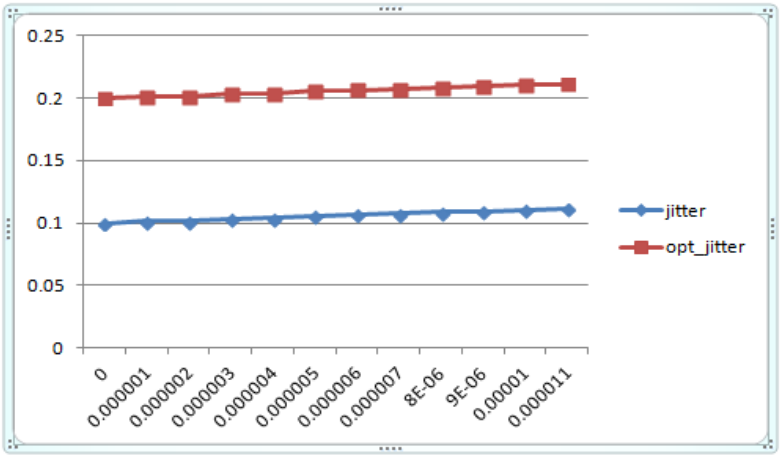

Figure 4 Jitter vs. Time graph

The Figure 5 shows the line graph that represents the change in energy value with optimized protocol. This indicates that there is reduction in energy conservation when compare with the original protocol. In figure the energy shows energy change with time for original protocol, while opt_energy shows the optimized energy values because of our proposed work.

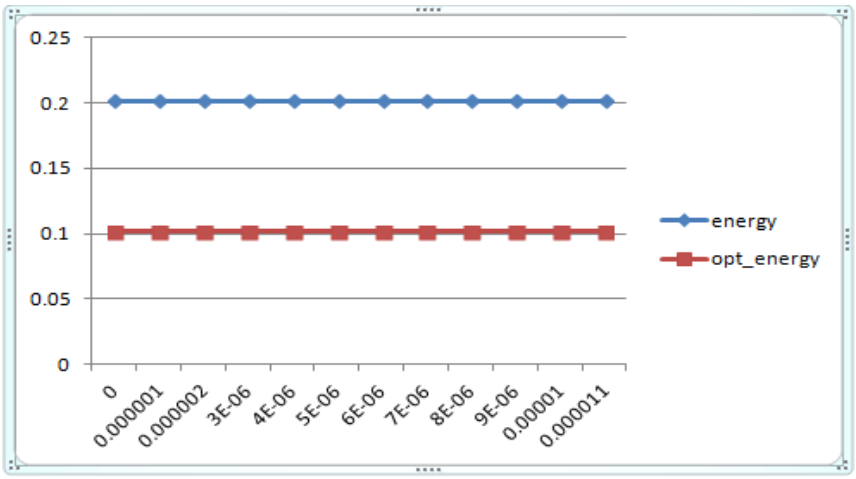

Figure 5 Energy vs. Time graph

The Figure 6 shows bar graph that represents the average values for all performance parameters. The normal represents the original protocol values whereas the optimized represents the optimized protocol values

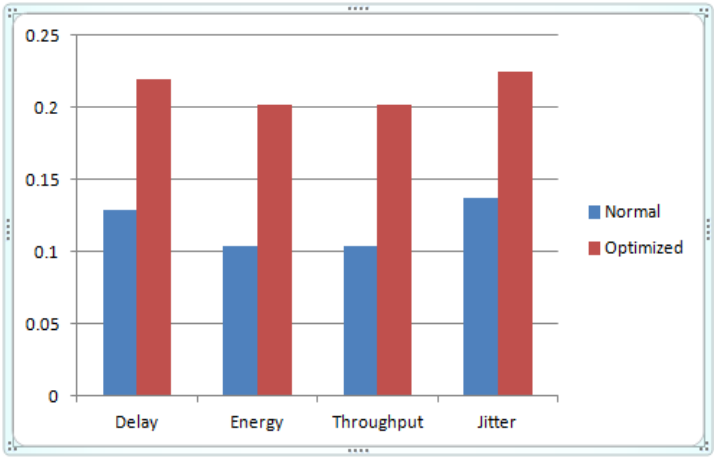

Figure 6 Bar graph of all performance parameters with average values

VI. CONCLUSION

We proposed the work that includes the NCPR with Paillier cryptography and the clustering architecture. Clustering in MANET overcomes bandwidth and battery power limitations, and reduces routing overhead. A clustering architecture allows in MANET environments: network scalability and reduction of communication overheads.

This will allow to effective utilization of energy since the transmissions will only be done by such cluster heads rather than all mobile sensor nodes. Clusters are maintained when data is to be forwarded. Such integrated routing and clustering scheme can improve throughput and reduce routing overhead.

To provide comprehensive security, at data transmission phase of MANET communication we are using a Paillier cryptography. It allows data transmission confidentially. For future work we can work to improve packet delivery ratio.

References

1. Xin MingZhang, En Bo Wang, Jing Jing Xia, Dan Keun Sung (2013) "A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad Hoc Networks" IEEE transactions on Mobile Computing, Vol. 12,.
2. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing", IETF RFC 3561, 2003.
3. Panagiotis Papadimitratos and Zygmunt J. Haas," Secure Data Transmission in Mobile Ad Hoc Networks" ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003.
4. Wenjia Li and Anupam Joshi," Security Issues in Mobile Ad Hoc Networks" Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County.
5. Seung Yi, Prasad Naldurg, Robin Kravets," SecurityAware Ad hoc Routing for Wireless Networks".

6. M. G. Zapata and N. Asokan, "Securing Ad hoc routing protocols" In wise'02 proceedings of ACM workshop on wireless security ACM press 2002.
7. Lidong Zhou and Zygmunt J. Haas," Securing Ad Hoc Networks" Cornell University IEEE Network –November/ December 1999.
8. B. A. Correa, R.C. Hincapie and Laura Ospina, "Survey on Clustering Techniques for Mobile Ad Hoc Networks," Revista Facultad de Ingenierí, No. 41, 2007.
9. R. Agarwal and M. Motwani, "Survey of Clustering Al-gorithms for MANET," International Journal on Com-puter Science and Engineering ,Vol. 1, No. 2, 2009.
10. M. Anupama and B. Sathyanarayana. "Survey of Cluster Based Routing Protocols in Mobile Ad hoc Networks," International Journal of Computer Theory and Engi-neering, Vol. 3, No. 6, 2011.
11. Michael O'Keeffe," The Paillier Cryptosystem" Mathematics Department April 18, 2008.
12. B. Maqbool, M.A.Peer, "Classification of Current Routing Protocols for Ad Hoc Networks," IJCA, 2010.
13. Y.Y. Su, S.F. Hwang, and C.R. Dow, "An Efficient Cluster Based Routing Algorithm in Ad Hoc Networks with Unidirectional Links," Journal of Information Science and Engineering 24, 2008, pp.1409-1428.
14. R. Agarwal and M. Motwani, "Survey of Clustering Algorithms for MANET," International Journal on Com-puter Science and Engineering ,Vol. 1, No. 2, 2009.
15. C.C. Chiang, H.K. Wu, W. Liu and M. Gerla, Routing in Clustered Multihop, Mobile Wireless Networks With Fading Channel, Proceedings of IEEE Singapore International Conference on Networks SICON'97, pages 197-211, Singapore, Apr. 14-17, 1997.
16. B. Lee, C. Yu, S. Moh, "Issues in Scalable Clustered Network Architecture for Mobile Ad Hoc Networks," Handbook of Mobile Computing, 2004.
17. Hongmei Deng, Wei Li, and Dharma P. Agrawal," Routing Security in Wireless Ad Hoc Networks" IEEE Communications Magazine • October 2002.

