International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secure Broadcasting Probability to Enhance Mobile Ad-hoc Network Using NCPR

Kajal Kunte[1], Navnath Kale[2]

[1]Department of Computer Engineering, PVPIT, Bavdhan Pune, India

[2]Professor, Department of Compuiter Engineering, PVPIT Bavdan, Pune, India

Abstract—The growing demand of wireless portable devices and the recent advances in Mobile Ad-hoc Networks (MANETs) provide a facility that users can benefit from anywhere and in situation of unplanned collaboration and more suitable for disaster relief. MANET consists of collection of mobile nodes which can freely move without any fixed infrastructure and is dynamically self-organized network. In MANET, the nodes move freely in random topology, so there is a high chance of breakage of link between the nodes. This leads to route discoveries and routing overheads and thus for reducing the routing overhead it is imperative to design such a dynamic routing protocol that will reduce the routing overhead and improves the performance scalability. In MANET, there is also have the problem of packets loss, thus showing the limitation of MANET regarding security as there is no any lines of defense in MANET. Hence, providing a secure network for MANET is another challenge. This paper proposes a protocol that will show the objectives of less overheads and good performance. According to a recent survey, authors suggested various routing protocol such as AODV, DSR, but they too have some limitations. In the proposed NCPR system, it will help to reduce routing overhead and increase in performance. In NCPR, protocol need to calculate the two factors i.e. rebroadcast delay and rebroadcast probability. Additionally, it is proposed to implement the Data Encryption Standard (DES) algorithm for security purposes i.e. use the security key. After sharing the key, the source node can encrypt the data by using DES algorithm. Encrypted data can be transferred from source to destination

Keywords: Wireless Adhoc network, NCPR, Rebroadcast Delay, Rebroadcast Probability**,** Security, DES algorithm

1. Introduction

MOBILE ad hoc networks (MANETs) consist 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. One of the fundamental challenges of MANETs is the design of dynamic routing protocols with good performance and less overhead. Many routing protocols, such as Ad hoc On-demand Distance Vector Routing (AODV)[2] and Dynamic Source Routing (DSR)[9] have been proposed for MANETs. The above two protocols are on demand routing protocols, and they could improve the scalability of MANETs by limiting the routing overhead when a new route is requested.

However, due to node mobility in MANETs, frequent link breakages may lead to frequent path failures and route discoveries, which could increase the overhead of routing protocols and reduce the packet delivery ratio and increasing the end-to-end delay. Thus, reducing the routing overhead in route discovery is an essential problem. The conventional on demand routing protocols use flooding to discover a route. They broadcast a Route REQuest (RREQ)[9] 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, especially in dense networks. Therefore, it is indispensable to optimize this broadcasting mechanism. Some methods have been proposed to optimize the broadcast problem in MANETs in the past few years. Due to node mobility in MANETs, repeated connection breakages might direct to regular path failures and route discovery [3], which could raise the overhead of routing protocols and decrease the packet deliverance ratio and increase the end delay. Thus, reducing the routing overhead in route discovery is an essential problem. The main objective of this work is to enhance the performance of the network by securing the data and to minimize the malicious nodes which disturb the stream of the network. Securing data is a critical task which can be achieved by cryptographic algorithms [10] and disturbance detection plays as a crucial ingredient in any comprehensive security solution to address the nodes. In recent years, much interest has been involved in the design of Mobile Ad-hoc Network (MANET) technologies. Mobile ad-hoc networks are characterized by their self-configuration, open peer-to-peer network architecture.

Existing security solutions for wired or wireless networks with infrastructure [11] cannot be directly applied to MANETs. Due to different factors like including absence of already established trust. It is necessary that a security association exist between network members to ensure authentication and non-repudiation for trusted nodes. Sensitive information must be exchanged confidentially. Integrity of the information exchanged within the network has to be maintained[10].

Characteristics of MANET network

- Infrastructure less ,
- Power limitation
- Dynamic topologies
- Self-Configuring
- No centralized controller
- weight terminals

Applications of MANET Network

- Military battlefield
- Sensor Networks

- Disaster Area Network
- Personal Area Network

Various Types of Mobile Ad hoc Network

- Vehicular Ad-Hoc Networks (VANET's)[14]
- Intelligent Vehicular Ad-Hoc Networks (In VANET's)
- Internet Based Mobile Ad-Hoc Networks (I MANET's)

Figure 1: Mobile Ad-hoc Network

2. Related Work

To design a dynamic routing protocol with good performance and less overhead in MANET is very difficult. So many routing protocols are used in MANET. Basically routing protocols are divided into three categories:

- Proactive routing protocols [15], the routes to all the destination (or parts of the network).Each node periodically broadcasts its routing table(s) to its neighbors, allowing all nodes to have a consistent network view. The protocol use DSDV, FSR, GSR etc. routing protocol.
- Reactive or On-demand routing protocols were designed to reduce the overheads in proactive protocols by maintaining information for active routes only. So that routes are determined and maintained for nodes that require sending data to an exacting destination. Route discovery usually occurs by flooding a route request packets through the network. In this type we use AODV, DSR[8][9] etc routing protocol.
- Hybrid routing protocol is combine the features of proactive and reactive protocols.

Perkins and Das [2] studied routing protocols are proposed for Ad hoc networks and their classification of these schemes according to the routing strategy (i.e., table driven and on-demand). Table-driven routing protocols, such as DSDV and OLSR, attempt to maintain consistent and up-to-date routing information from each node to every other node in the network. Each mobile node is required to periodically discover and maintain routes to every possible destination in the network. In the on-demand routing protocols, such as AODV and DSR, routes are discovered only when they are needed. Each node maintains a route for a source-destination[4] pair without the use of periodic routing table exchanges or full network topological view. The AODV establishes routes between nodes only on-demand (when they are required to send data packet). There is no need to update all routes in the network; instead it focuses only on routes that are currently used or being set up. The primary objectives of AODV are: a) to execute path discovery process when necessary. AODV uses broadcast route discovery mechanism. b) To distinguish between local connectivity management (neighborhood detection) and general topology maintenance c) To broadcast information about changes in local connectivity to those neighboring mobile nodes those are likely to need the information. The AODV algorithm enables dynamic, multi-hop, self-starting routing between participating mobile nodes wishing to establish and maintain an ad hoc network.

AlAamri et al [3] shows that new routing protocol for Ad hoc networks, called On-demand Tree-based Routing Protocol (OTRP). This protocol combines the idea of hop-by-hop routing such as AODV with an efficient route discovery algorithm called Tree-based Optimized Flooding (TOF) to improve scalability of Ad hoc networks when there is no previous knowledge about the destination. To achieve this in OTRP, route discovery overheads are minimized by selectively flooding the network through a limited set of nodes, referred to as branching-nodes. The theoretical analysis and simulation results showed that OTRP outperforms AODV, DYMO, and OLSR and it reduces overheads as number of nodes and traffic increase[13].

Abdulai et al. [4] proposed a Dynamic Probabilistic Route Discovery (DPR)[3] method based on neighbour coverage. In this method Probabilistic based scheme is used in which source node broadcast the packet by using flooding mechanism and every mobile node rebroadcast the packet based on a predetermined fixed probability determine by the neighbor coverage and local density of the node. In local density using the Hello packet [14] it collect the neighbor information by sending hello packet to its neighbor and Covered node decide whether to forward the packet or not if all node are covered by broadcast no need to broadcast the packet and if some node are not received the packet send it to that node.

Nelson [5] proposed a methodology of dynamically adjusting the Hello timer and the Timeout timer according to the conditions of the network. For example, in a high mobility network (with frequent topology changes) it is desirable to use small values for the timers to quickly detect the changes in the network. On the other hand, in a low mobility network where the topology remains stable and with few changes, a large value for the timers is more effective to reduce the overhead. In order to decide whether the mobility of the network is high or low, we use a simple way to approximate in real time of the link change rate. The reduction of the overhead is greatly achieved with the minimal cost of slightly increasing the drop rate in data traffic. While the packet loss increases around 1%, the overhead reduction reaches 40%Ould- . node, and it does not consider the neighbours receiving the duplicate RREQ packet.

3. Secure NCPR System

Neighbor coverage based probabilistic rebroadcast protocol [1] which combines both neighbor coverage and probabilistic

methods. In order to effectively exploit the neighbor coverage knowledge, we need a novel rebroadcast delay to determine the rebroadcast order, and then here obtain a more accurate additional coverage ratio. In order to keep the network connectivity and to reduce the redundant retransmissions, need a metric named connectivity factor to determine how many neighbors should receive the RREQ packet [9]. After that, by combining the additional coverage ratio and the connectivity factor[13], introduce rebroadcast probability[1], which can be used to reduce the number of rebroadcasts of the RREQ packet and to improve the routing performance. By applying DES security algorithm[10] here provide security to the network which is keep the information confidential.

3.1 Rebroadcast Delay

This scheme that is calculates 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 [10]. Therefore, this rebroadcast delay enables the information about the nodes which have transmitted the packet to more neighbors, which is the key success for the proposed scheme When a node k_i receives an RREQ packet from its previous node p, node p can use the neighbor list in the RREQ packet to estimate how many its neighbors have not been covered by the RREQ packet. If node k_i has more neighbors uncovered by the RREQ packet from p, which means that if node k_i rebroadcasts the RREQ packet, the RREQ packet can reach more additional neighbor nodes. To sufficiently exploit the neighbor coverage knowledge, it should be disseminated as quickly as possible. When node s sends an RREQ packet, all its neighbors k_i, i = 1, 2 …receive and process the RREQ packet. Assume that node *kn* has the largest number of common neighbors with node s, node *kn* has the lowest delay. Once node *kn* rebroadcasts the RREQ packet, there are more nodes to receive the RREQ, because node *kn* has the largest number of common neighbors. Node *kn* rebroadcasts the RREQ packet depends on its rebroadcast probability calculated in the next subsection. The objective of this rebroadcast delay is not to rebroadcast the RREQ packet to more nodes, but to disseminate the neighbor coverage knowledge[6] more quickly. After determining the rebroadcast delay, the node can set its own timer.

3.2 Rebroadcast Probability

In this system proposed a novel scheme to calculate the rebroadcast probability. The scheme considers the information about the uncovered neighbors, connectivity metric[13] and local node density to calculate the rebroadcast probability. The rebroadcast probability is composed of two parts:

a) 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
b) Connectivity factor[5], which reflects the relationship of network connectivity and the number of neighbors of a given node.

The node which has a larger rebroadcast delay may listen to RREQ packets from the nodes which have lowered one [9]. Here do not need to adjust the rebroadcast delay because the rebroadcast delay is used to determine the order of disseminating neighbor coverage knowledge[4][6]. When the timer of the rebroadcast delay of node ki expires, the node obtains the final uncovered neighbour set. The nodes belonging to the final uncovered neighbor set are the nodes that need to receive and process the RREQ packet. Note that, if a node does not sense any duplicate RREQ packets from its neighbor, its uncovered neighbor set is not changed, which is the initial uncovered neighbor set. Here how to use the final uncovered neighbor set to set the rebroadcast probability[7]. The metric Ra indicates the ratio of the number of nodes that are additionally covered by this rebroadcast to the total number of neighbors of node ki. The nodes that are additionally covered need to receive and process the RREQ packet. As Ra becomes bigger, more nodes will be covered by this rebroadcast, and more nodes need to receive and process the RREQ packet, and, thus, the rebroadcast probability should be set to be higher.

4. Mathematical Model

4.1 Uncovered Neighbors Set and Rebroadcast Delay

When node k_i receives an RREQ packet from its previous node p, it can use the neighbor list in the RREQ packet to estimate how many its neighbors have not been covered by the RREQ packet from p. If node k_i has more neighbors uncovered by the RREQ packet from p, which means that if node k_i rebroadcasts the RREQ packet, the RREQ packet can reach more additional neighbor nodes. The UnCovered Neighbors set $U(k_i)$ of node k_i as follows

$$U(k_i) = N(k_i) - [N(k_i) \cap N(p)] - [p] \quad (1)$$

Where $N(p)$and $N(k_i)$ are the neighbors sets of node p and k_i, respectively. p is the node which sends an RREQ packet to node k_i.Due to broadcast characteristics of an RREQ packet, node k_i can receive the duplicate RREQ packets from its neighbors. Node k_i could further adjust the U(k_i)with the neighbor knowledge. In order to sufficiently exploit the neighbor knowledge and avoid channel collisions, each node should set a rebroadcast delay. The choice of a proper delay is the key to success for the proposed scheme because the scheme used to determine the delay time affects the dissemination of neighbor coverage knowledge. When a neighbor receives an RREQ packet, it could calculate the rebroadcast delay according to the neighbor list in the RREQ packet and its own neighbor list. The rebroadcast delay Td(k_i) of node k_i is defined as follows according to the neighbor list in the RREQ packet and its own neighbor list. The rebroadcast delay Td (k_i) of node k_i is

$$T_p(k_i) = 1 - \frac{|N(p) \cap N(k_i)|}{|N(p)|}$$

$$T_d(k_i) = MaxDelay \times T_p(k_i) \quad (4)$$

Where $T_p\ (k_i)$ is the delay ratio of node k_i , and MaxDelay is a small constant delay. Its value is 0.01. Consider that node k_n has the largest number of common neighbors with node *p*, according to (3). Then the node n_k has the lowest delay [1]. The node can set its own timer after determining the rebroadcast delay

4.2 Neighbor Knowledge and Rebroadcast Probability

The node which has a larger rebroadcast delay may listen to RREQ packets from the nodes which have lowered one. For example, if node ki receives a duplicate RREQ packet from its neighbor kj, it knows that how many its neighbors have been covered by the RREQ packet from ki . Thus, node ki could further adjust its UCN set according to the neighbor list in the RREQ packet from kj.
The rebroadcast probability is collection of two factors:

a) Additional coverage ratio[1]: It is the ratio of the number of nodes that should be covered by a single broadcast to the total number of neighbors.
b) Connectivity factor[6]: It is the relationship of network connectivity[13] and the number of neighbors of a given node that are additionally covered by the node which has a more rebroadcast delay might listen to RREQ packets from the nodes. node ki could further adjust its UCN set according to the neighbor list in the RREQ packet from kj. Then the U(ki) can be adjusted as follows:

$$U(ki) = U(ki) - [U(ki) \cap N(kj)] \quad (3)$$

After adjusting the U(ki), the RREQ packet received from kj is discarded.

Do not need to adjust the rebroadcast delay because the rebroadcast delay is used to determine the order of disseminating neighbor coverage knowledge to the nodes which receive the same RREQ packet from the upstream node. Thus, it is determined by the neighbors of upstream nodes and its own. When the timer of the rebroadcast delay of node ki expires, the node obtains the final UCN set. The nodes belonging to the final UCN set are the nodes that need to receive and process the RREQ packet. If a node does not sense any duplicate RREQ packets from its neighborhood, its UCN set is not changed, which is the initial UCN set. So use the final UCN set to calculate rebroadcast probability.
Define the additional coverage ratio (Ra(ki)) of node ki as

$$R_a(k_i) = \frac{|U(k_i)|}{|N(k_i)|} \quad (5)$$

This metric indicates the ratio of the number of nodes that are additionally covered by this rebroadcast to the total number of neighbors of node ki. The nodes that are additionally covered need to receive and process the RREQ packet. As Ra becomes bigger, more nodes will be covered by this rebroadcast, and more nodes need to receive and process the RREQ packet, and, thus, the rebroadcast probability should be set to be higher.

Connectivity factor: It is the relationship of network connectivity and the number of neighbors of a given node that are additionally covered by the node which has a more rebroadcast delay might listen to RREQ packets from the nodes

$$(k_i) = |N(k_i)|$$

By Combining the additional coverage ratio and connectivity factor, obtain the rebroadcast probability Pre(k_i) of node k_i:

$$(k_i) = F_c(k_i).R_a(k_i) \quad (6)$$

5. DES Security Algorithm

In recent years, much interest has been involved in the design of Mobile Ad-hoc Network (MANET) technologies. Mobile ad-hoc networks are characterized by their self-configuration, open peer-to-peer network architecture. Existing security solutions for wired or wireless networks with infrastructure cannot be directly applied to MANETs. Due to different factors like including absence of already established trust An ad-hoc network is a collection of various wireless mobile hosts Mobile Ad-hoc networks are self-configuring as well as self-organizing multi-hop wireless networks. Nodes communicating to physical media; they transmit and get signals [7]. If the destination node is not inside range of the source node, the source node helps to intermediate nodes in order to communicate with the other node. Fig1 represent the Mobile ad-hoc network. The node transmit a message to another node that is out of range, the cooperation of other nodes in the network is required; it is represented by multi-hop communication [5]. Therefore, each node at the same time must act both as a host as well as router. Mobile Ad-Hoc Networks (MANETs) are used to communication infrastructure in the Department of Defense's [14] vision Network Centric Warfare [1]. Global Information Grid (GIG), and MANETs can serve in War fighter Information Tactical Network- (Win T) to give command, communications, intelligence and reconnaissance (C4ISR) support [2].

5.1 Data Encryption Standard

DES is a block cipher. It encrypts the data in a block of 64 bits. It produces 64 bit cipher text. The key length is 56 bits. Initially the key is consisting of 64 bits. The bit position 8, 16, 24, 32,40,48,56, 64 Discarded from the key length [15].

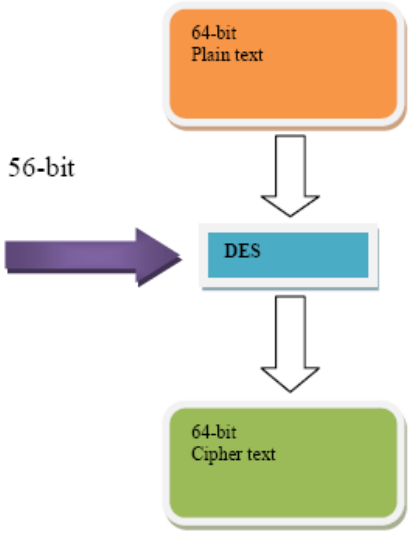

Figure 2: The conceptual working with DES

DES is based on two fundamental attributes of cryptography: Substitution (confusion) and transposition (Diffusion). DES consists of 16 steps, each of which called as a Round.

Algorithm:-
[1] In the first step, the initial 64-bit plain text block is handed over to in Initial Permutation (IP) function.
[2] The Initial permutation is performed on plain text.
[3] The initial permutation produce two halves of permuted block: Left Plain text (LPT) and Right Plain Text (RPT).
[4] Now, each of LPT and RPT goes through 16 rounds of encryption process, each with its own key: a. From the 56-bit key, a different 48-bit Sub-key is generated using Key Transformation. b. Using the Expansion Permutation, the RPT is expended from 32 bits to 48 bits. c. Now, the 48-bit key is XORed with 48-bit RPT and resulting output is given to the next step. d. Using the S-box substitution produced the 32-bit from 48-bit. e. These 32 bits are permuted using P-Box Permutation. f. The P-Box output 32 bits are XORed with the LPT 32 bits. g. The result of the XORed 32 bits are become the RPT and old RPT become the LPT. This process is called as Swapping. h. Now the RPT again given to the next round and performed the 15 more rounds.
[5] After the completion of 16 rounds the Final Permutation is performed [10][16].DES but repeated same process 2 times using two keys K1 and K2.First it takes plain text, produced the cipher text using K1 and then take up the cipher text as input, produced another cipher text using K2 shown in fig. 2 The Decryption Process is shown in fig.3[10].
.

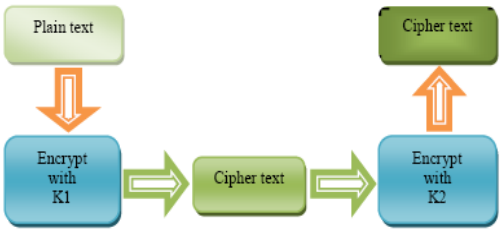

Figure 3: Encryption process using two keys K1 and K2

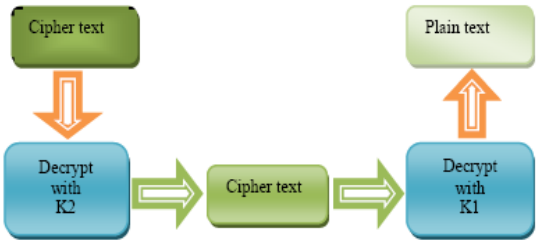

Figure 4: Decryption process using two keys K1 and K2

6. Result and Discussion

The figure 1 shows the performance of packet's deliver ratio, retransmission rate, underflow rate, overflow rate of NCPR. The figure 2 shows the performance graph of nodes according to rebroadcast probability of nodes in the network, NCPR find out the shortest path between then source and destination node. The Figure 3 shows the graph result of rebroadcast delay of NCPR protocol compared with previous system. Secure NCPR system provides security to the network to keep information confidential by applying DES algorithm.

Figure 1: Packet Delavary Ratio

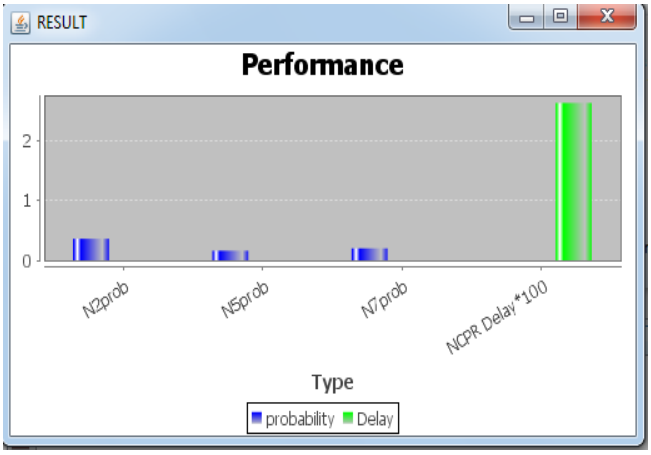

Figure 2: Probaility of connected node in shortest path

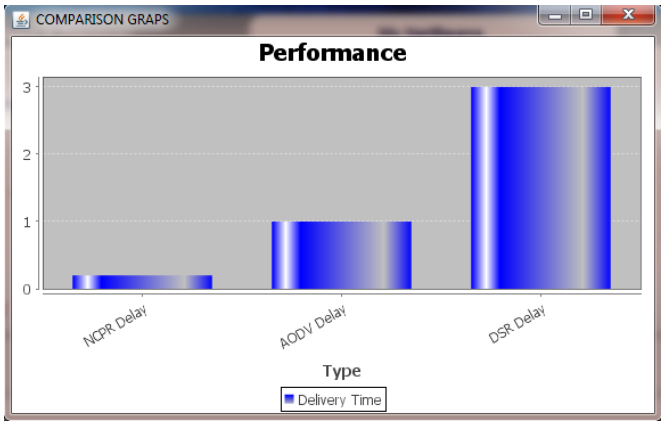

Figure 3: Compare Rebroadcast delay with Previous system

7. Conclusion

Mobile Ad-hoc Networks (MANETs) provides a facility that users can benefit from anywhere and in situation of unplanned collaboration and more suitable for disaster relief.

MANET consists of collection of mobile nodes that move freely without any fixed infrastructure i.e. dynamically self organized network. In MANET, because the nodes are freely moving in random topology, so there is a high chance of breakage of link between the nodes and thus it leads to route discoveries and routing overheads. So for reducing routing

overhead, it is necessary to design such a dynamic routing protocol that will improve the performance scalability and reduce the routing overhead. NCPR is the routing protocol used for routing overheads by which it increases the delivery ratio and decreases the end to end delay. DES algorithm performs the security function by using the cryptography method to prevent issues from outsiders and attackers. Sensitive information must be exchanged confidentially. Integrity of the information exchanged within the network has to be maintained [4]. Network must be secure and sensitive information must be exchanged confidentially.

References

[1] XinMing Zhang, 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,.2013
[2] C. Perkins, E. Belding-Royer, and S. Das, Ad Hoc On-Demand Distance Vector (AODV) Routing, IETF RFC 3561, 2003.
[3] *H. AlAamri, M. Abolhasan, and T. Wysocki*, "On Optimising Route Discovery in Absence of Previous Route Information in MANETs," Proc. IEEE Vehicular Technology Conf. (VTC), pp. 1-5, 2009
[4] J.D.4 Abdulai, M. Ould-Khaoua, L.M. Mackenzie, and A. Mohammed,"Neighbour Coverage: A Dynamic Probabilistic Route Discovery for Mobile Ad Hoc Networks," Pr oc. Int'l Symp. Performance Evaluation of Computer and Telecomm. Systems (SPECTS '08), pp. 165-172, 2008.
[5] X.M. Zhang, E.B. Wang, J.J. Xia, and D.K. Sung, "An Estimated Distance Based Routing Protocol for Mobile Ad Hoc Networks,IEEE Trans. Vehicular Technology, vol. 60, no. 7, pp. 3473-3484, Sept. 2011
[6] J.D. Abdulai, M. Ould-Khaoua, L.M. Mackenzie, and A. Mohammed,"Neighbour Coverage: Proc. Int'l Symp. PerformanceEvaluation of Computer and Telecomm. Systems (SPECTS '08), pp. 165-172, 2008.
[7] J. Kim, Q. Zhang, and D.P. Agrawal, "Probabilistic Broadcasting Based on Coverage Area and Neighbor Confirmation in Mobile Ad Hoc Networks," Proc. IEEE GlobeCom, 2004.
[8] B. Williams and T. Camp, "Comparison of Broadcasting Techniques for Mobile AdHoc Networks," Proc. ACM MobiHoc, pp. 194-205,2002.
[9] D. Johnson, Y. Hu, and D. Maltz, The Dynamic Source Routing Protocol for Mobile Ad Hoc Network (DSR) for IPv4, IETF RFC 4728, vol. 15, pp. 153-181, 2007.
[10] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, November 16, 2005
[11] Hongmei Deng, Wei Li, and Dharma P. Agrawal," Routing Security in Wireless Ad Hoc Networks" IEEE Communications Magazine October 2002
[12] HD.Verma,D.Chandrawanshi,"Comparative Performance Evaluation of AODV over CBR and TCP Traffic, International Journal of Computer Science and Technology," Vol. 2, Issue 2, June 2011.
[13] F. Xue and P.R. Kumar, "The Number of Neighbors Needed for Connectivity of Wireless Networks," Wireless Networks, vol. 10, no. 2, pp. 169-181, 2004 **13**
[14] E.B. Wang, J.J. Xia, X.M. Zhang, and D. K. Sung, "Estimated distance based routing protocol for mobile ad hoc networks," IEEE vol.60, pp.3473-3484,2011
[15] B. Paul , Md. Ibrahim , Md. Bikas , "Experimental Analysis of AODV & DSR over TCP & CBR Connections with Varying Speed and Node Density in VANET," International Journal of Computer Applications (0975 – 8887) Vol. 24, No.4, June 2011.
[16] Wuling Ren, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication",Second International Conference on Modeling", Simulation and Visualization Methods (WMSVM), 2010