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].
.

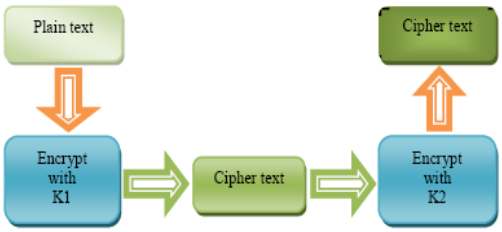

Figure 3: Encryption process using two keys K1 and K2

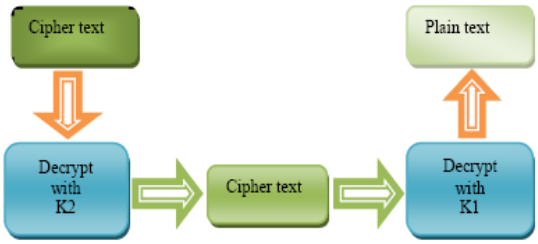

Figure 4: Decryption process using two keys K1 and K2

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

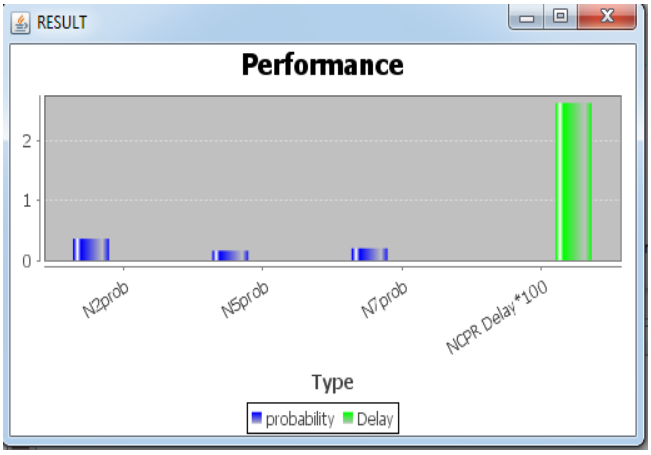

Figure 2: Probaility of connected node in shortest path

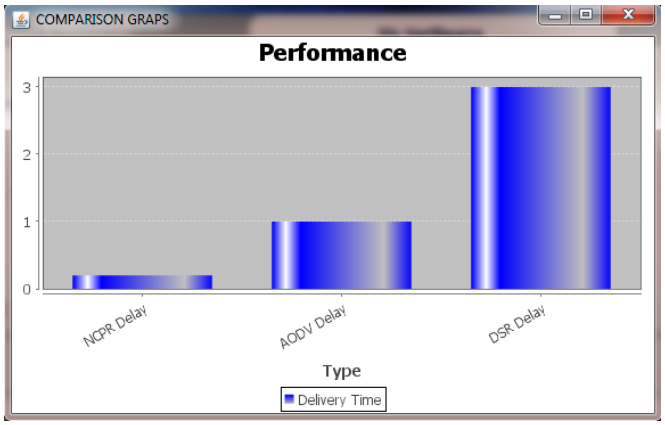

Figure 3: Compare Rebroadcast delay with Previous system

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