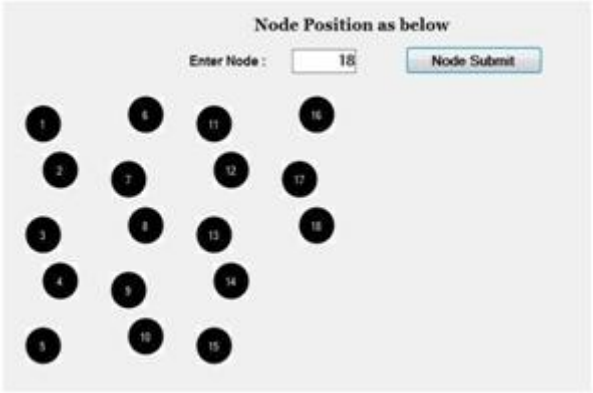

Figure 4: Dynamic network of nodes.

The message is encrypted as the user applies digital sign. Packet is transmitted as users asks for transmit.

Figure 5: Digital Signature application.

The message is encrypted as the user applies digital sign.

6. Result and Discussion

Proposed algorithm is simulated using a custom .net based simulator. In the custom simulator, Different scenarios are created for cluster formation, routing and topology control. Topology control considering random deployment of nodes in the network is achieved. The graph of nodes versus key size of our simulated network environment.

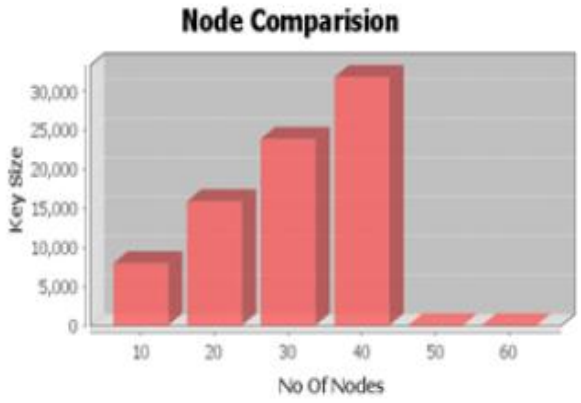

Figure 6: Graph of number of nodes Vs key size

As shown in the graph, when the number of nodes increases it results into the increase in the size of key size.

Proposed system uses a time between sender and receiver nodes to achieve asymmetry property. It associates chain of keys which are associated with a time interval. At sender's end MAC is attached to each packet which is computed on the message. sender gives a disclosure key from the key chain after a constant pre-defined time. Receiver receives the packets and stores the received packets in the buffer. Receiver knows the schedule of the key disclosure. As it gets the disclosure key receivers verifies the packets in the buffer. Each receiver checks the key in the hash of key chain and then checks the correctness of MAC. If the MAC value is correct then only the receiver accepts the packet otherwise it rejects the packet.

7. Conclusion

In recent years, mobile ad hoc networks (MANETs) have become popular, because of their easy of deployment. As single packet reaches many users it creates potential danger of malicious user, who is able to inject packet, can reach to many receivers with a malicious packet. AS nodes in network join and leave the group randomly, it becomes challenging to track them for security mechanisms. In this research work, we presented the proposed system, a scalable and light-weight mechanism to address the problems of authentication in multicast mobile ad hoc networks. It uses symmetric cryptography, and time-delayed key disclosure to achieve authenticated broadcast. Feasibility of the proposed approach can be seen by prototype implementation. Future scope of the project is to develop hop to hop connectivity and integrity.

8. Acknowledgment

I am profoundly grateful to prof. Ram Joshi for his expert guidance and continuous encouragement throughout to see that this review work rights its target since its commencement to its completion. His invaluable guidance supported me in completing this survey. At last I must express our sincere heartfelt gratitude to all staff members of Computer Engineering Department who helped us directly or indirectly during this course of work.

References

[1] Quansheng Guan, Richard Yu,"Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 6, JULY 2012.
[2] Dimitris Glynos, Panayiotis Kotzanikolaou, Christos Douligeris, "Preventing Im- personation Attacks in MANET with Multi-factor Authentication", IEEE transactions published at Department of Informatics, University of Piraeus, Greece, 2008
[3] Qiwei Lu; Yan Xiong; Wenchao Huang; Xudong Gong; Fuyou ,"Distributed ECC-DSS Authentication Scheme Based on CRT-VSS and Trusted Computing in

MANET", Miao2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 656 665, 2012
[4] Kavitha Ammayappan, V.N.Sastry and Atul Negi, "Authentication And Dynamic Key Management Protocol Based On Certified Tokens For Manets", Institute for Development and Research in Banking Technology, Hyderabad, India, 2009
[5] Striki, M.Inst. for Syst. Res., Maryland Univ., College Park, MD, USA ; Baras, J.S."Towards integrating key distribution with entity authentication for efficient, scalable and secure group communication in MANETs", Communications, 2004 IEEE International Conference on (Volume:7)
[6] Rajaram Ayyasamy1 and Palaniswami Subramani, "An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Adhoc Networks", The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012
[7] Na Ruan, Yoshiaki Hori, âA˘ IJDoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Thingsâ˘A´I, 2012 International Conference on Selected Topics in Mobile and Wireless Networking, pp 60 65, Apr. 2012
[8] Soumyadev Maity and R. C. Hansdah, "Membership Models and the Design of Authentication Protocols for MANETs", 26th International Conference on Advanced Information Networking and Applications Workshops, pp 544-551, July 2012.
[9] Aasia Samreen and Seema Ansari," Certificateless ID-based Authentication using Threshold signature for P2P MANETs", Department of Computer Science, University of Aasia, Ireland, pp 25 30, July 2009
[10] M. Suguna, P. Subathra, "Establishment of Stable Certificate Chains for Authentication in Mobile Ad Hoc Networks"IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011
[11] Wei Liu, Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments" Nov. 2014 Vehicular Technology, IEEE Transactions on (Volume:63 , Issue: 9)
[12] Jason L. Wright, Milos Manic, "Time Synchronization in Hierarchical TESLA Wireless Sensor Networks", Int. J. Comput. Sci. Netw. Security, pp 36 39, 2009.

Author Profile

Tejashree Kokate receieved the B.E degree in computer Engineering from Cummins college of Engineering (Savitribai Phule Pune University) in 2011. During 2013 -14 she worked as lecturer in Shivaji college, Barshi. She started her post graduation program at Marathwada mitra mandal college of engineering in 2013. Currently she is studying for Masters in engineering at MMCOE, Pune.