and issues the a new public key pk. This public key needs for a digital certificate which is sign by its CA.

d. Off-Signcrypt

This is a probabilistic offline signcryption algorithm run by a dispatcher that obtains as participation in the system stricture param, a publisher's private key sks and a recipient's public key pkr , and outputs an offline signcryption δ.

e. On-Signcrypt

On-Signcrypt is a probabilistic signcryption algorithm which is also an online algorithm. This algorithm is run by a correspondent which takes as an input system constraints, a message named as m and an offline signcryption referred to as δ, and gives an output as a full signcryption ciphertext σ [26].

f. Unsigncrypt

Unsigncrypt is a probabilistic signcryption algorithm which is run by the receiver which takes as an input cipher text, sender public key, and receiver private key and gives output in the form of plaintext.

6. Proposed Methodology

To provide the security and improvement in the infrastructure of MANET, a fresh scheme has been applied called HOOSC Scheme along with an efficient routing protocol AODV. The concept works on the principal of multihop routing technique in which the data or information can be sent to the destination node from the source node by the use of some of the intermediate nodes.

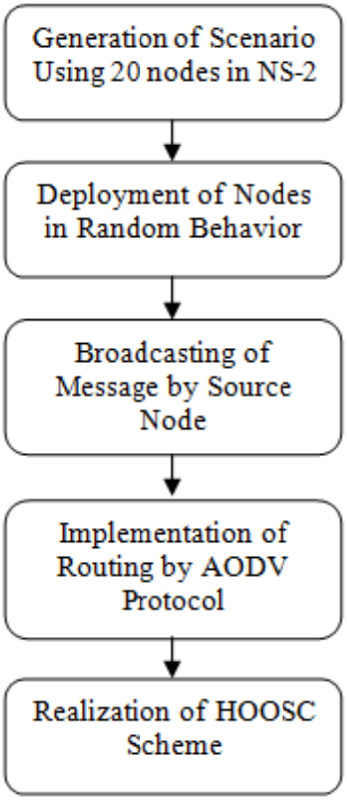

Figure 3: Flow of Work

The information to be sent to the destination node has to be encrypting first and then the source node sends the information. By applying this encryption to the data or information to be sent, the malicious node become unable to retrieve the information stored in the packets.

The phase 1 is the generation of scenario phase which is generated by the use of simulator NS-2 where 20 nodes are used. In the phase 2 the deployment of nodes is done by the use of random behavior i.e. in an ad hoc style which is arbitrary in shape. The nodes in this phase can also be showed haphazard behavior. The source node broadcasts the message or information in the phase 3 and the AODV protocol is applied to the message or information in order to provide the security to the routing scheme in the phase 4. Then, to provide security to the transmitted messages, HOOSC Scheme is applied which encrypts the message and adds the digital signature to it in order to avoid the attacks and to minimize them in the final phase.

7. Simulation Results and Discussion

In this section, the results have been carried out by the implementation of AODV protocol with HOOSC Scheme. A comparative analysis also been taken out by using AODV protocol without security, MD5 algorithm and HOOSC Scheme along with AODV algorithm. All the simulations been done on NS-2 simulator.

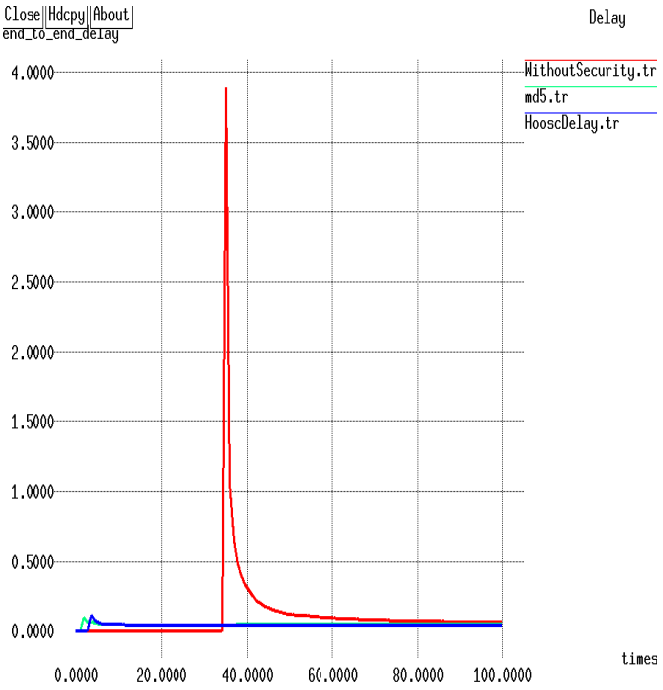

Figure 4: End to end delay

Figure 4 shows the end to end delay between the source node and destination node whiles the transference of information or messages. It is clearly shows that the HOOSC Scheme is better as compared to traditional ones.

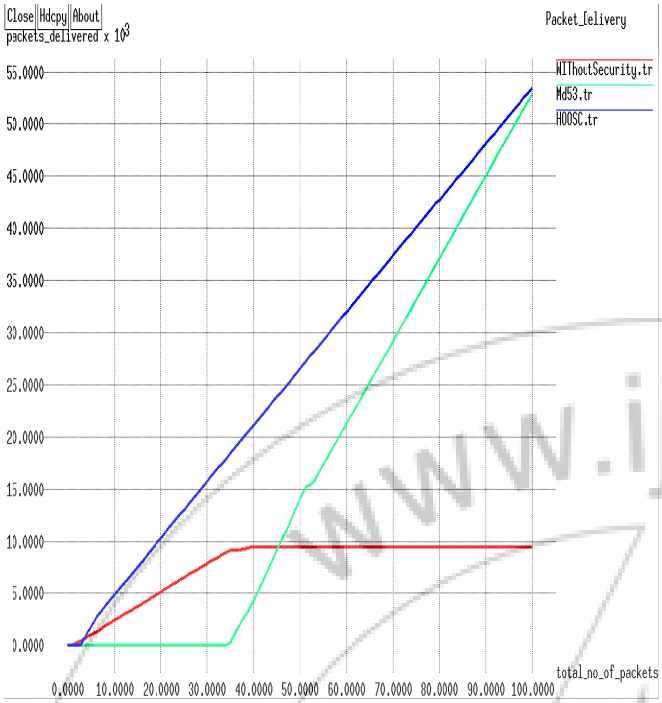

Figure 5: Packet Delivery Ratio

Figure 5 discusses the packet delivery ratio of nodes. It can be shown that the delivery of packets is excellent in HOOSC Scheme despite the other two algorithms.

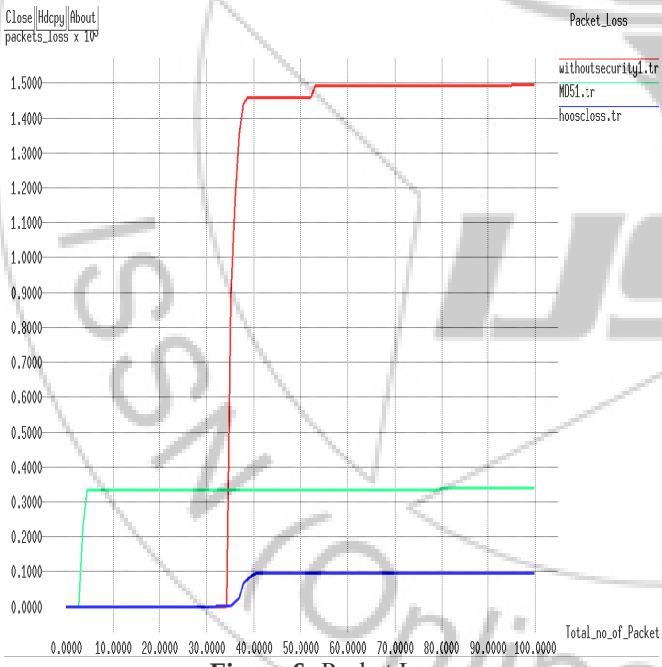

Figure 6: Packet Loss

Figure 6 describes that the loss of packets in HOOSC Scheme occur less than that of MD5 algorithm and when AODV protocol get used without security. Hence, HOOSC Scheme is more efficient and effective in the delivery of packets by minimizing the loss of packets.

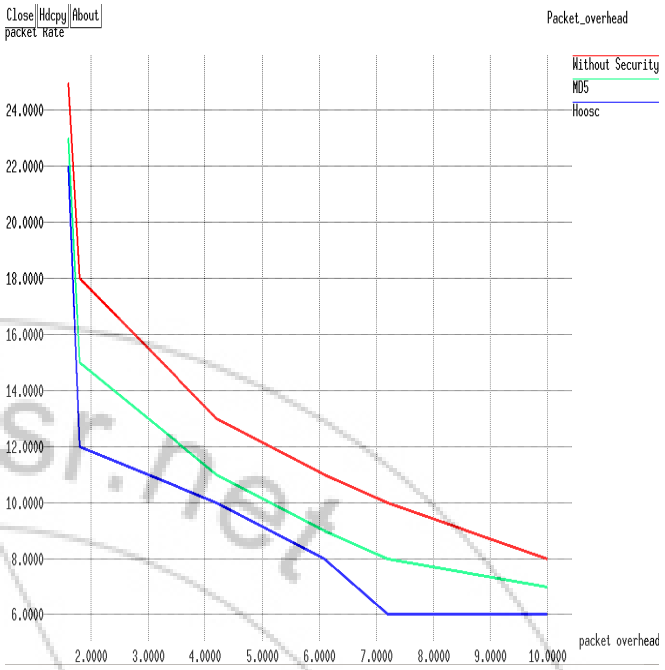

Figure 7: Packet Overhead

The overhead of packets while transferring the information from source node to destination node is shown in Figure 7. The graphical representation describes the behavior of HOOSC Scheme in which less overhead occurs.

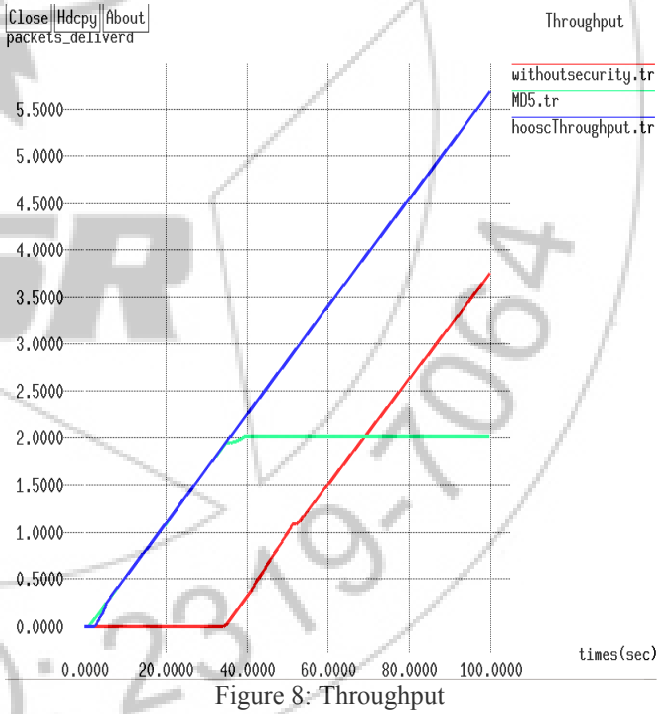

Figure 8: Throughput

Figure 8 represents the throughput of proposed HOOSC algorithm as compared to conventional ones. As shown in figure, the throughput provided by proposed HOOSC Scheme is much more efficient than that of AODV Protocol without security and by using MD5 algorithm.

8. Conclusion and Future Scope

In this paper, HOOSC scheme is used that provide more security and the comparative analysis of three different

algorithms has been carried out to find the most efficient and effective protocol used for the transference of information from source to destination node. The analysis has been taken out among MD5 algorithm, HOOSC Scheme and AODV protocol without security. In AODV protocol, the discovery of route is vulnerable to various threats like Black Hole and Gray Hole attacks. Hence, to diminution of these attacks, the HOOSC Scheme is implemented mainly to provide the security to the packets transmitted. The results in this paper revealed that the HOOSC Scheme outperforms the conventional schemes and algorithms in various aspects and parameters. With HOOSC scheme, it provides more security solutions and parameters like end to end delay decreases, packet delivery ratio increases.

In future work we can improve the performance by using PGP (Pretty Good Privacy) security protocol instead of AODV protocol along with HOOSC scheme with minimum delay & overhead and maximum Packet Delivery Ratio.

References

[1] IETF MANET work group. http://www.ietf.org/dyn/wg/charter/manet- charter.html
[2] F.Lilieblad, O.Mattsson, P.Nylund, D.Ouchterlony, "A. Roxenhag. Mad-hoc AODV Implementation and Documentation" http://mad-hoc.fiyinglinux.net
[3] C. E Perkins and E. M. Royer (1999), "Ad-hoc On-Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp-90-100.
[4] C. Lohi and S.K. Sharma "A Survey of Mitigation Techniques to Black Hole Attack and Gray Hole Attack in MANET", International Journal Computer Technology and Applications, 5(2), 560-567
[5] S. Marti, T. Guili, K. Lai, and M. Baker (2000), "Mitigating routing misbehavior in mobile ad hoc networks" ,In Proceedings of MOBICOM 2000, pp. 255-265.
[6] David B. Johson, David A. Maltz and Josh Broch (2001), "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad-Hoc networks", in Ad-hoc Networking, Edited by Charles E. Perkins, Chapter-5, pp-139-172, Addison-Wesley
[7] H. Deng, H. Li, and D.P. Agrawal (2002), "Routing security in wireless ad hoc networks," IEEE Communications Magazine, Vol. 40, No. 10.
[8] H. Deng; W. Li; D. Agrawal (2002) "Routing Security in Wireless Ad-Hoc Networks" Communications Magazine, IEEE, 70 - 75.
[9] H. Deng, H. Li, and D.P. Agrawal, (2002),"Routing security in wireless ad hoc networks," IEEE Communications Magazine, Vol. 40, No. 10.
[10] I. D. Chakeres and E. M. Belding-Royer(2002), The Utility of Hello Messages for Determining Link Connectivity in Proceedings of the 5th International Symposium on Wireless Personal Multimedia Communications (WPMC), pages 504. 508, Honolulu, Hawaii.
[11] S. Lee, B. Han, and M. Shin, (2003), "Robust Routing in Wireless Ad Hoc Networks," 2002 Int'l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.
[12] M. Jackobsson, J. Hubaux, and L. Buttyan, "A micro-payment scheme encouraging collaboration in multi-hop cellular networks," In Proceedings of Financial Crypto.
[13] Y.C. Hu; A. Perrig, (2004), "A Survey of Secure Wireless Ad Hoc Routing [J]", IEEE Security and Privacy, 2(3), 28-39.
[14] Humaira Ehsan and Zartash Afzal Uzmi, "Performance Comparison of Ad Hoc Wireless Network Routing Protocols," Proceedings of INMIC 8th International, 24-26 Dec. 2004, pp-457- 465
[15] Jaydip sen et. al (2007),"A Mechanism for Detection of Gray Hole Attack in Mobile AD Hoc Networks" ICICS, IEEE.
[16] Bala A., Bansal M. and Singh J.(2009), "Performance Analysis of MANET under Blackhole Attack", In Proc. of First International Conference on Networks &Communications, pp. 141–145.
[17] Akanksha Saini and Harish Kumar(2010), "Comparison between Various Black Hole Detection Techniques in MANET", In Proc. of National Conference on Computational Instrumentation, pp. 157-161.
[18] Rajiv Ranjan, Naresh Trivedi and Anoop Srivastava (2011), "Mitigating of Black Hole Attack in Manets", VSRD International Journal of Computer Science and Information Technology, 1(2), 53-57.
[19] S. J. Patel et.al. (2012),"A Novel Approach to Gray-hole and Black-hole Attacks in Mobile Ad-hoc Networks" Second International Conference on Advanced Computing & Communication Technologies,IEEE, Pp 556-560.
[20] M. Wahengbam and N. Marchang, (2012),"Intrusion Detection in MANET using Fuzzy Logic", IEEE, pp. 456-460.
[21] Rajesh Yerneni and A.K. Sarje (2012), "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks" ICCCNT', IEEE, pp. 248-252.
[22] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, (2012),"DoS Attacks in Mobile Ad- hoc Networks: A Survey", In Proc. Of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS), pp.535-5 41.
[23] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala (2012),"A Novel Approach for Grayhole and Blackhole Attacks in Mobile Ad-hoc Networks", In Proc. of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS),, pp.556-560
[24] R. H. Jhaveri, (2013), "MR-AODV: A Solution to Mitigate Black-hole and Gray-hole Attacks in AODV Based MANETs" Third International Conference on Advanced Computing & Communication Technologies, IEEE, Pp. 254-260.
[25] K.Mahalakshmi et.al. (2013), "Intrusion Detection System Based MANET Security against Selective Black Hole Attacks" International Journal of Research in Computer Engineering and Electronics.
[26] Li., F., and Xiong., P.,(2013), "Practical Secure Communication for Integrating Wireless Sensor Networks into the Internet of Things", IEE Sensors Journal, vol.13, No. 10.

Author Profile

Amanpreet Kaur completed her bachelor of technology degree in 2012 from lovely professional university and master of technoloy in Computer sciene & engineering in 2014 from Chandigarh Groups of College, Gharuan. She has attended various research seminar. Her research interest area are in network security and networks.