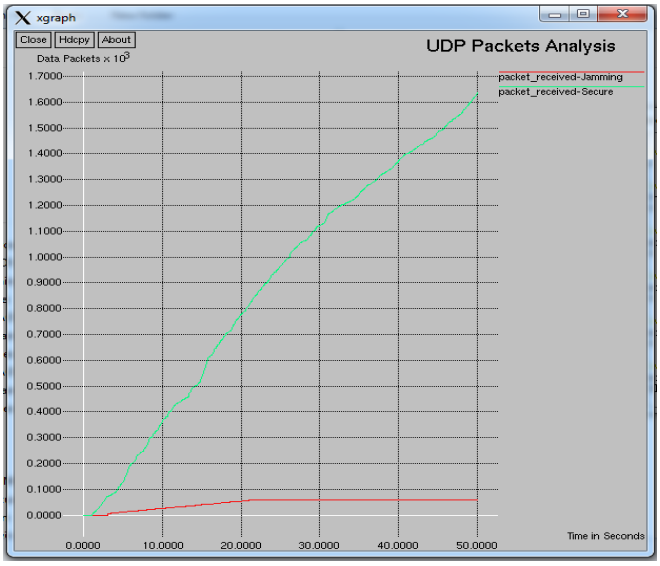

Figure 6.8: UDP Packets Received Analysis

B. PDR Analysis of Jamming Attack and Proposed Security Scheme

The attacker in MANET are easily exaggerated the routing misbehavior for the reason of independent establishment of network. The attacker aim is to drop the data packets or to hold the resources for that the communication is affected. The attacker drop of packets is humiliates the percentage ratio of data receiving. The packets percentage ratio or Packet Delivery Ratio (PDR) performance of Jamming attacker and Security scheme is specified in this graph. The PDR performance of attacker is only evaluated up to time 30 second in a simulation of 100 seconds. The attacker is obstructing the processing capability of nodes and bandwidth capacity, because of that the whole network is jam and PDR performance is not assessed. The Rest of the time only the attacker is flooding bogus connection establishment packets due to that up to end of simulation no PDR is value is count. The PDR performance of proposed security scheme is completely block the misbehavior of attacker and provides 90% receiving ratio and it is about 98 percent in some different time, undoubtedly shown in figure.

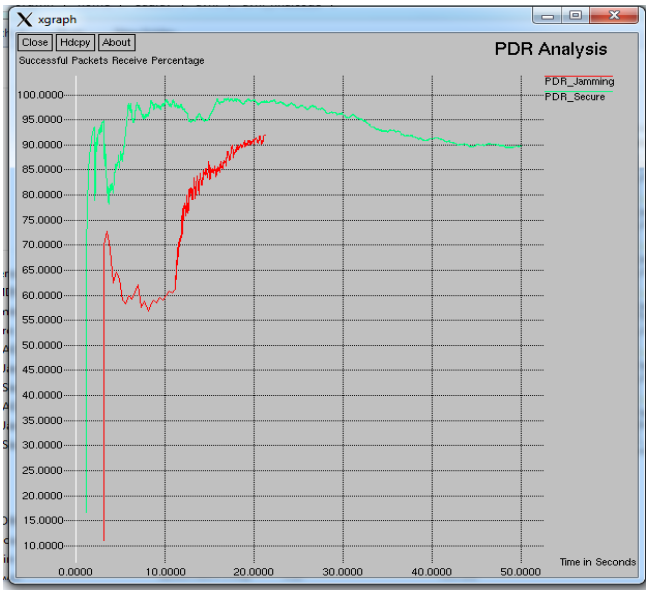

Figure 6.9: PDR Performance Analysis

C. Routing Load Analysis of Jamming Attack Security Scheme

The routing overhead performance is containing the measurement of number of data packets with respect to number of control packets in dynamic Ad hoc network. The routing flooding analysis of attacker and proposed security scheme is mentioned in given graph. In fact, in a jammaed network, where the high channel contention causes a degradation of the link reliability, the routing decision is mainly obsessed by the cost that models the quality of the link. The jammer attacker incessantly flooding the number of control packets, their calculation in given simulation time of 50 seconds is 420000 packets but the calculation is as certain change in scenario of security scheme. In security scheme the only little more than 1000 packets are flooding in network that shows the better performance and improves the link reliability by block the consumption bandwidth through attacker. In presence of security scheme the jammer attacker not produces an unwanted control packet.

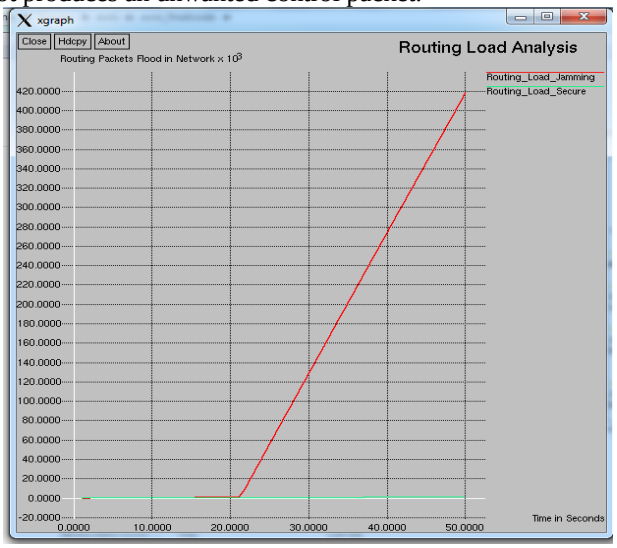

Figure 6.10: Routing Load Performance Analysis

D. Throughput Analysis of Jamming Attacker and Security Scheme

The packets forwarding capacity of jammer attacker is a strictly increase with a period of time, which causes the higher transmission of control packets forwarding in Ad hoc wireless network but the packets receiving capacity of intermediate nodes is limited for that reason the forwarding and receiving capacity is affected and after some time bandwidth is occupied by unwanted junk of jammer packets that causes the reason of degradation of network throughput. The throughput experimental performance is shown in this graph and observes the attacker is affected the throughput by block the link capacity. The throughput of attacker is evaluated only up to time 22 seconds after that the link is consumes by jammer generated packets but the proposed security scheme is steps forward the throughput up to maximum 1200 packets/seconds. The proposed security scheme is block the flooding of unwanted packets and provides normal network performance in existence of attacker.

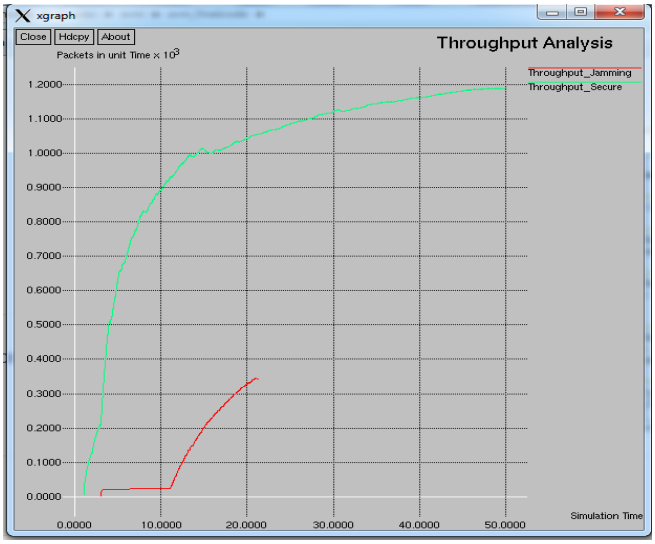

Figure 11: Throughput Performance Analysis

6. Conclusion and Future Work

The absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic network. The MANET suffers from attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node or nodes in the network, which causes routing misbehavior in network. The AOMDV protocol are improves the routing capability and also ignores the path where the attacker is exists in network. The IDS security scheme id identified the loss of percentage because of attacker and block the attacker misbehavior by the attacker is totally disabled in network and produces zero loss percentage because of attacker in MANET. The simulation results are illustrating the performance of security scheme in presence of jamming attacker in MANET. The proposed security scheme is secure the network from attacker evaluated the routing performance metrics like routing load, throughput and delay in network. The routing performance of normal AOMDV protocol is equivalent to the proposed IDS security scheme, which represents the normal network performance in presence of attacker. The flooding of packets enhanced the routing load in network and prevention security scheme provides the normal performance in presence of jammer attacker.

In MANET the attacker is also consumes the communication resource like battery power due to that nodes are early going to sleep mode. In future we also work on resource consumption attack or vampire attack in MANET.

References

[1] S.Madhavi, “An Intrusion Detection System in Mobile Ad Hoc Networks”, International Journal Of Security And Its Applications Vol. 2, No.3, Pp. 1-16, July, 2008

[2] Sunilkumar S. Manvi, Lokesh B. Bhajantri, And Vittalkumar K. Vagga, “Routing Misbehavior Detection In Manets Using 2ACK”, Journal of Telecommunication and Information Technology (JTIT), pp. 105-111, 2010.

[3] Adnan Nadeem and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks" IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, pp. 2027-2043, Fourth Quarter 2013.

[4] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma "Review of Various Routing Protocols for MANET" International Journal of Information and Electronics Engineering, Vol. 1, No. 3, pp. 251-259, November 2011.

[5] Marina, M.K., Das, S.R., "On-demand Multipath Distance Vector Routing in Ad Hoc Networks" IEEE Proceedings of the International Conference for Network Protocols (ICNP), 2001.

[6] Jae-Joon Lee And Jaesung Lim, "Effective and Efficient Jamming Based nn Routing in Wireless Ad Hoc Networks", IEEE Communications Letters, Vol. 16, Pp. 1903-1906, No. 11, November 2012.

[7] Dr. N. Sreenath, A. Amuthan, & P. Selvigirija “Countermeasures Against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs”, 2012 International Conference On Computer Communication And Informatics (ICCCI - 2012), Jan. 10 – 12, 2012, Coimbatore, INDIA.

[8] Fenye Bao, Ing-Ray Chen, Moonjeong Chang, and Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-Based Routing and Intrusion Detection", IEEE Transactions on Network And Service Management, pp. 169-182, Vol. 9, No. 2, June 2012

[9] Preeti Sachan, Pabitra Mohan Khilar, “Security Attacks and Solutions in MANET”, Proceedings of International Conference on Advances in Computer Engineering (ACEEE), Pp 172-176, 2011.

[10] Pravina Dhurandher, “FACES: Friend Based Ad Hoc Routing using Challenges To Establish Security in MANET Systems” IEEE SYSTEMS Journal ,Volume 5, No 2, June 2011,pp:176- 188.

[11] Yi Zhang, Qiangliu “A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis”, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), Pp. 163 – 167, 2010.

[12] Husain. Shahnawaz, Gupta S.C., Chand Mukesh “Denial Of Service Attack in AODV & Friend Features Extraction to Design Detection”, IEEE International Conference On Computer & Communication Technology (ICCCT), pp. 292-297, 2011.

[13] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, “Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks”, Publication in the IEEE Globecom 2011.

[14] Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala, “A Review of Current Routing Attacks in Mobile Ad Hoc Networks”, International Journal Of Computer Science And Security, Volume 2, 2008.

[15] Marc Greis's tutorial (now maintained by VINT group), available on http://www.isi.edu/nsnam/ns/tutorial/index.html.