The packet-forwarding algorithm goes secure forwarding of packet to destination posture of the node. It captures the transfer message packet from nodes that want to send the data and it retrieves the packet source and destination address. After gathering the both address it take this next hop address from that packet then it check this next hop address to its network neighbor list. If this next hop is present in the neighbor list it simply transfers the packet to next hop, otherwise it deletes the packet from its network.

We have evaluated both carousel and stretch attack and the performance of secure packet traversal algorithm. We launch the simulation on NS2. We consider constant bit rate (CBR) data traffic; packet size is 1024bytes and chooses different source-destination connections. Simulation can be conducted up to 500 nodes. Fig 4 shows the simulation for a randomly generated topology of 100 nodes. Node number 84 and node number 65 are Source and Destination respectively where those nodes are indicated by red and black color. Using packet traversal algorithm, the traversed path is 84→81→65.

6. Simulation Results

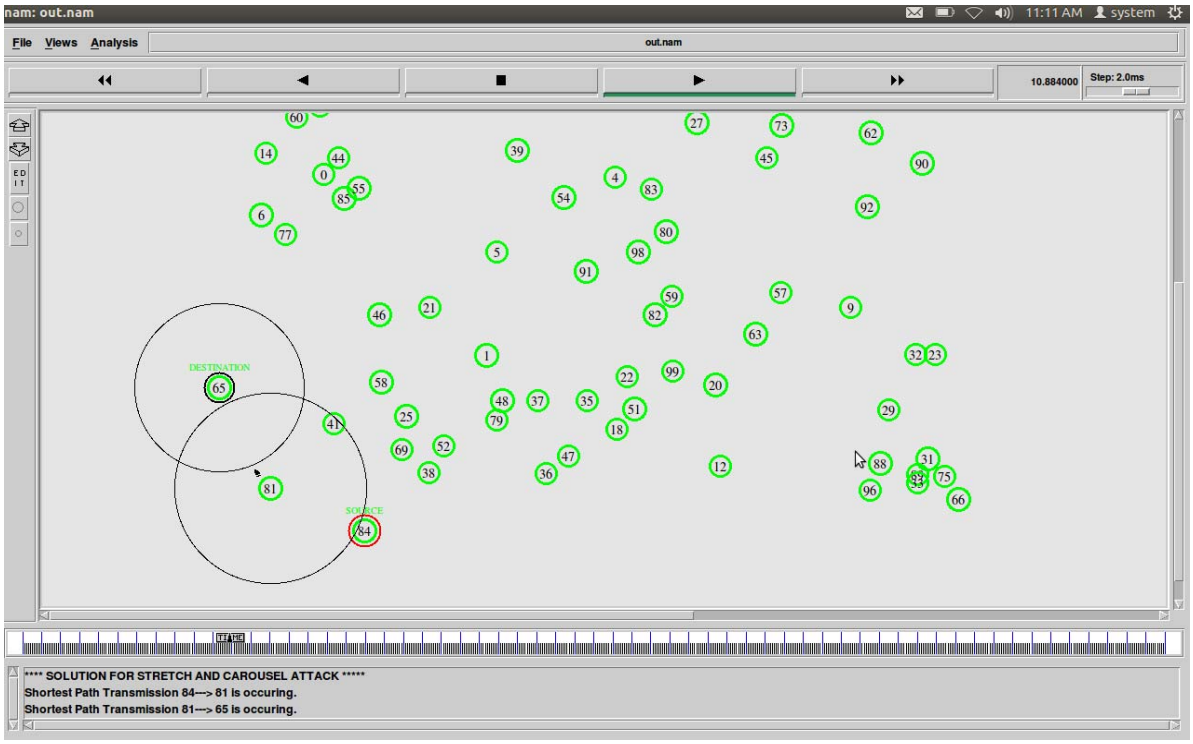

Figure 4: Shortest path transmission using secure packet traversal

6.1 Analysis

Simulation was conducted for 100 nodes for 50ms.The initial energy of all the nodes is assumed to be 30J. The data transmission begins at 0.1ms and ends at 50ms. Energy is taken along y-axis and time along x-axis. Energy gradually decreases with the transmission of data and in the presence of routing loops. The energy usage in carousel attack is shown below in Fig 5. The energy consumed is 22.41J

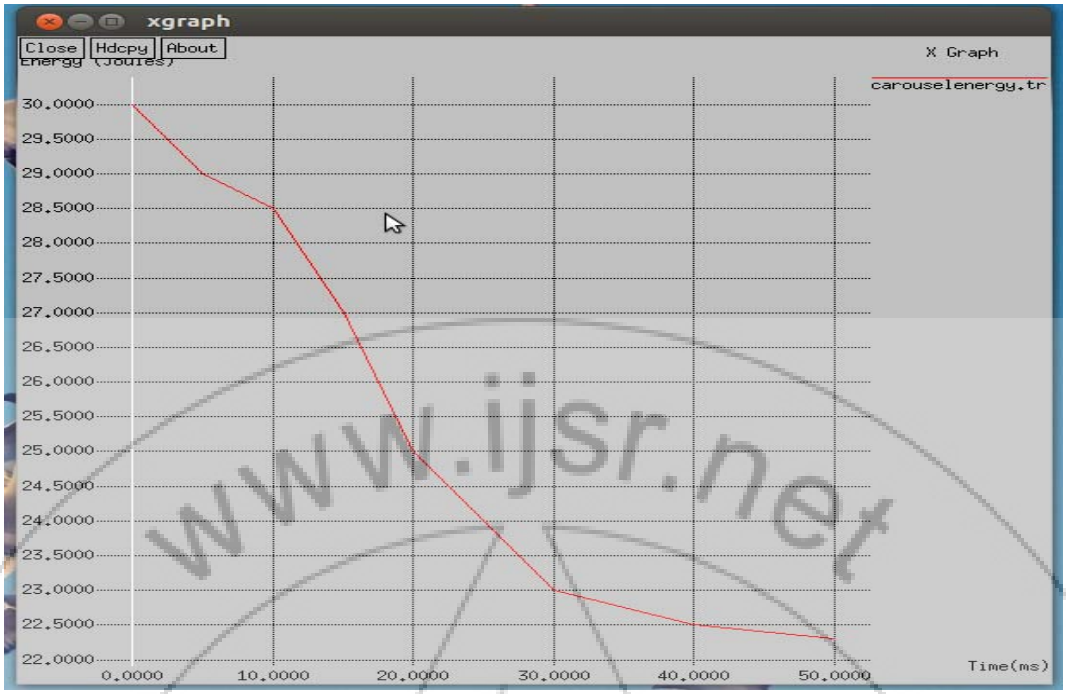

Figure 5: Energy Consumption in Carousel attack

Fig. 6 shows the energy consumption during a Stretch attack. Energy gradually decreases with the transmission of data and in the presence of increased number of nodes. All network nodes are involved in the transmission.The energy consumed is 24.81J

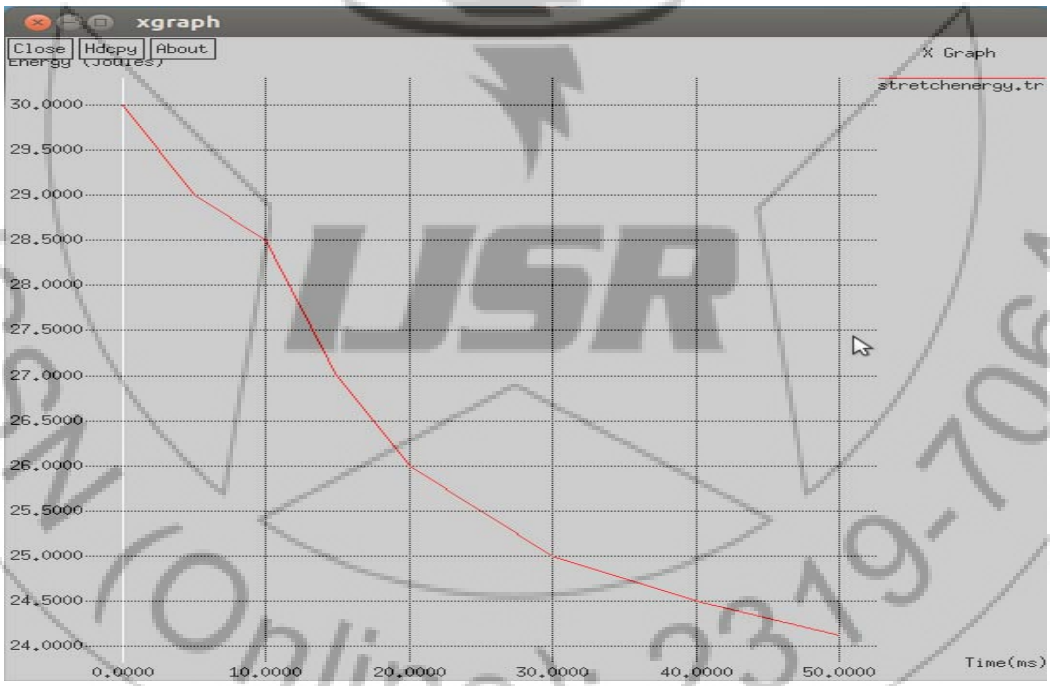

Figure 6: Energy Consumption in Stretch attack

Fig 7 shows the mitigation of carousel and stretch attack energy using Secure packet traversal where the x-axis is taken as Time(ms) and the y-axis is taken as the Energy(J). From the analysis of the graph mentioned below the energy consumption is less and stable. The energy consumed is 27J. Using secure packet traversal we can can increase the lifetime of the nodes. This concept increases the overall lifespan of the network by choosing the shortest path.

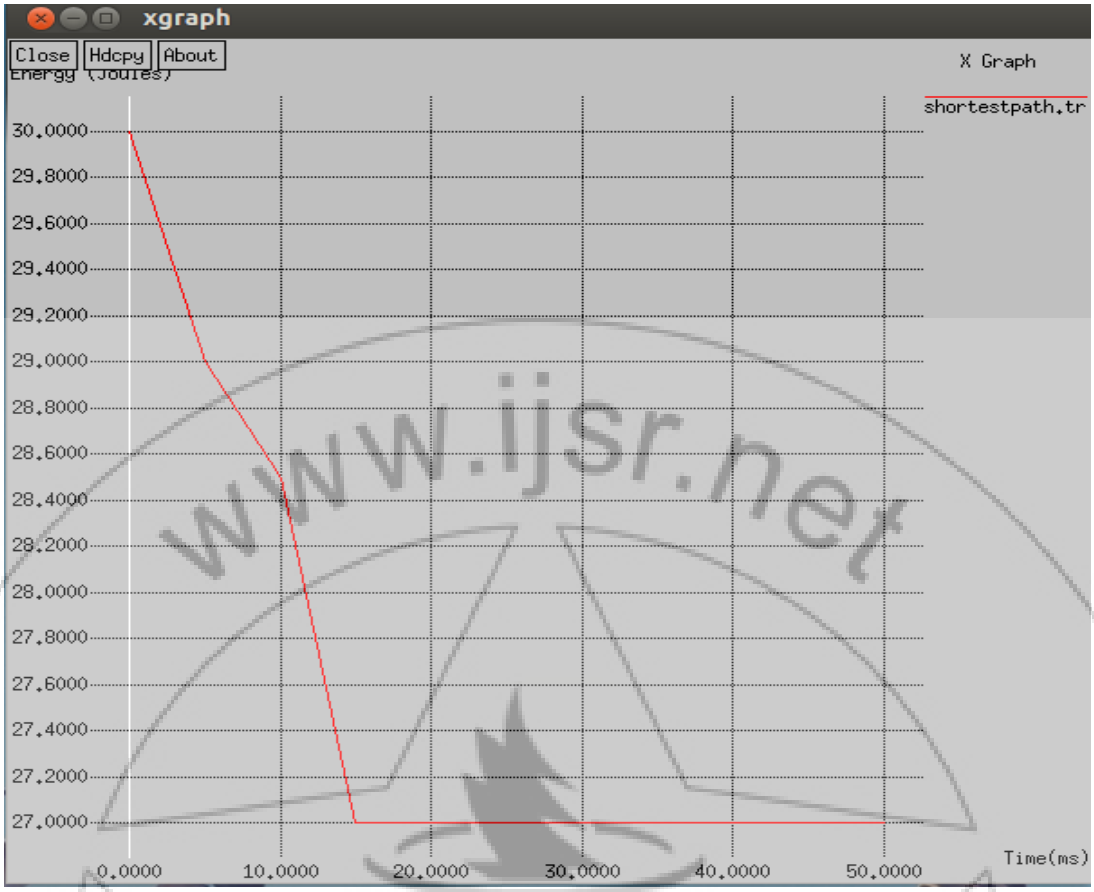

Figure 7: Mitigation of Vampire attacks and Energy Consumption in Secure packet traversal

7. Conclusion

Vampire attacks, a new class of resource consumption attacks that drain the battery power by using more energy of the nodes during data transmission. These attacks do not depend on any specific type of protocol or condition. According to the simulation results, the energy usage in carousel attack is 22.41J and energy consumption in stretch attack is 24.81J. Using the secure packet Traversal method, secured transmission is established in the packet forwarding process from source to destination which consumes relatively less energy i.e. 27J. The simulations results show that the impact of attacks on the system was reduced to a great extend after implying the algorithm. A full solution is not given yet but some amount of damage was avoided.

8. Acknowledgment

I would like to thank my guide Dr. Poornima K M for her continuous support and helpful comments on the project. Finally, I thank almighty, my Parents, Friends and Family members for the constant support and encouragement without them it was impossible for me to complete my work.

References

[1] Eugene Y. Vasserman and Nicholas Hopper, “Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks”, IEEE Transactions on Mobile Computing, Vol. 12, No. 2, February 2013
[2] C.Balasubramanian, R. Sangeetha, R.Deepa,, “Provably Secure Routing and Defending Against Vampire Attacks in Wireless Ad Hoc Sensor Networks”,ICIET,2014
[3] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, “Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols,” IEEE Trans. Vehicular Technology, vol. 58, no. 1,pp. 367-380, Jan. 2009
[4] A.D. Wood and J.A. Stankovic, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002
[5] Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syncookies.html.
[6] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford, “Path-quality monitoring in the presence of adversaries”, SIGMETRICS,2008.
[7] Jing Deng, Richard Han, and Shivakant Mishra, “Defending against path-based DoS attacks in wireless sensor networks”, ACM workshop on security of ad hoc and sensor networks, 2005.
[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, “Packet leashes: A defense against wormhole attacks in wireless ad hoc networks”, INFOCOM, 2003.