Algorithm1 : SHA for MAC model

Start
Source: compute MAC $_K$ (M)= H_K(M)
Source: transmit M and MAC $_k$ (M)
Neighbour node : gets M and MAC $_k$ (M)
Neighbour nc 'e: compute MAC $_K$'(M)=H_K'(M)
Neighbour node : compare MAC $_K$' and MAC $_K$
If compare MAC $_K$' = MAC $_K$ then
Neighbour node : trusted

Else

Neighbour node : Un trusted

End if

End

3.2 Step2: Rating

The trusted nodes are rated on the basis of the amount of data transmission they accomplish and their friendship with other nodes in the network. The rating is done by the data rating and friend rating. Data rating based on the data packets transfer through the node. That is based on the packet size. Data rating portrays its capacity to transfer the data packets. Friend rating is done through the account of friendship of a node with other nodes in the network. If a node wants to calculate its rating, its behaviour with the neighbour node is noted and it is rated. Now every node has the Data rating and friend based rating. Net rating is calculated from that. This rating helps to identify how good the trusted node. Now the trusted node along with its rated value is available. The list is shared with source sensor node and to its destination (sink node).

3.3 Step3: Routing

The source has the list of trusted node. if the source node receives the signal it starts to route the data packets through the nodes which are identified and rated by the above steps. Now the routing is done through the trusted node that makes the routing more secure. Therefore we avoid the attacks and information loss. The trusted node list are shared to the destination so that it assures the information is from the trusted node and also the sensed data is from the node with the high rating is considered as accurate sensed data.

3.4 Step4: Cross Check

The un trusted node which are in the separate list are identified by MAC model are not completely removed from the entire network and it is given a chance to check whether it is really malicious or not. In step1 if the MAC matches it sends the ACK back to the source within the specified period. But there is possibility that the MAC matches, and the ACK does not receive the source node within the time or it may lost because of its wireless nature. This condition may lead to trusted node is identified as malicious node. Therefore, the cross check is needed. This process is separate. Consider the Node N1, N 2, N 3 which are identified as an un trusted node by MAC model. In this N1 sends packet and forwards it to N2, and N2 forwards it to N3, once N3 received the packet it send back the ACK to N1. If the node receives ACK, then the nodes are again checked by using the step1. Otherwise the nodes are considered as malicious and it is removed from the network. If the nodes satisfy the conditions in step 1, these nodes are undergo the rating process and added to the source list. These newly added nodes are considered for the next data transfer.

4. Simulation and Evaluation

We have used NS2 (Network Simulator 2) for simulation. NS is an Object-oriented Tcl(Otcl) script interpreter that has a simulation event scheduler and network component object libraries, and network set_up module libraries. The simulated results show the malicious node identification in the nertwork. In this the simulated model designed as such the source node receives the signal it performs the process and identifies the trusted and malicious nodes and routing is done that is the data packet is transferred. And the performance metrics are analysed by using graph. In this the simulated graph results are analysed. The existing system, ASER[20], is compared with our proposed work. The main factors include energy consumption, memory overhead and packet delivery ratio.

4.1 Energy Consumption

Energy consumption is the usage of battery source. Energy overhead of monitoring involves− (i) the energy spent by the CPU for running algorithm (ii) the energy spent in sending/receiving packets related to monitoring such as neighbor discovery and malicious node detection announcements. The power is used to transmit and receive the packets. It is an flooding based technique, it does not retransmit any packets. It is done on the basis of on demand which improves the energy efficiency. This all reduces the energy consumption. FIG1 represents the energy consumption with respect to time. When compared to ASERT [20], the malicious node is found by using two phases. In our work it is done by using single phase MAC model.

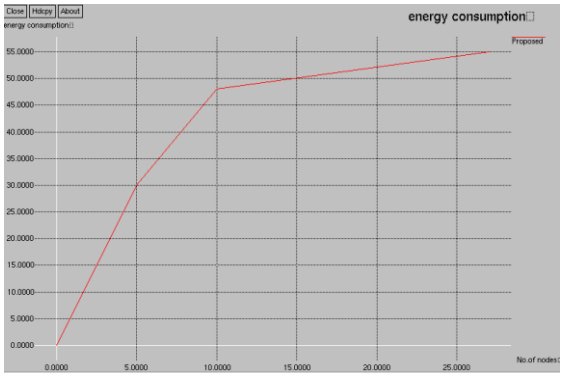

Figure 1: Energy Consumption

4.2 Memory Overhead

Memory overhead is the amount of memory it requires to store the values that is need for the process of finding malicious node. ASERT[20] it needs more memory space to store each nodes parameters. In our work the source node only has the list of trusted node. It establishes the routes when the node wants to transmit it. FIG2 deals with the memory overhead of our work with time.

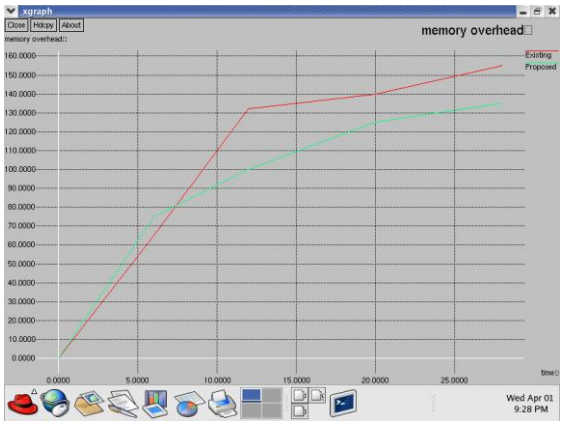

Figure 2: Memory Overhead

4.3 Packet Delivery Ratio (PDR)

PDR is defined as the number of data packets transmitted to the data packet received at the destination. The malicious nodes are identified accurately, the possibility of packets drop is minimum. Thereby the PDR is increased in our work. FIG 3 represents the PDR of our work with respect to number of nodes.

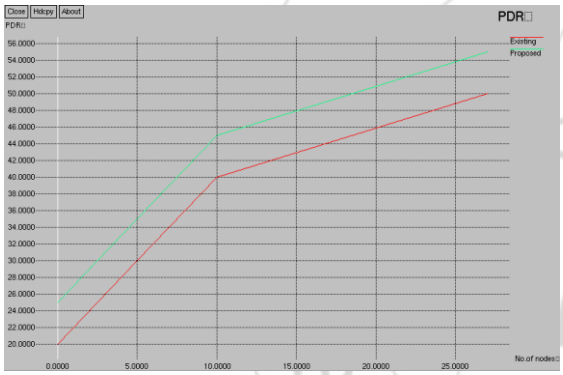

Figure 3: Packet Delivery Ratio

4.4 Delay

The delay of a network specifies how long it takes for the data to travel across the network from source node to destination. The time required to compute the MAC model, finding the malicious nodes also determines the delay of the network. In our work the malicious nodes are identified effectively, so that the data packets travel through the trusted node minimize the delay in network. FIG 4 depicts the delay with respect to our work.

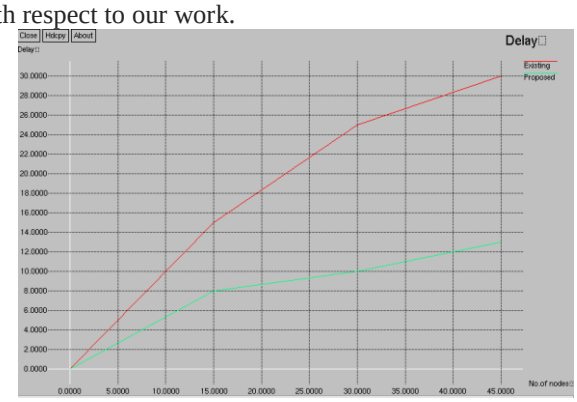

Figure 4: Delay

4.5 Security Analysis

The security features include confidentiality, integrity authentication. We achieve this features and free from network attacks by routing through identified trusted nodes. In our work, we use SHA-1 Algorithm. In this the Hash values are unique and it is difficult to determine the MAC values. Un authorized person should not compute the MAC without knowing the shared key. Thereby computing the MAC, the nodes behaviour is determined, this ensures the node trustworthy nature.

5. Conclusion

WSN are deployed in hostile environment and because of its wireless nature it is subjected to various kinds of attacks, information loss and modification. It is important in WSN the sensed data packets should reach the destination within the particular time and also the data packets should not undergo any modification. Secure routing is the way to avoid this kind of problems. In WSN secure routing is done to route the data packets securely without modification. Therefore trusted nodes are identified and routing is done through it.

In our work, The trusted nodes are identified by the MAC model and it is rated. MAC model effectively identifies the un trusted node by using SHA algorithm. The data packets are routed through the trusted node. Trusted node gives security features such as confidentiality, integrity and authentication because it is identified by MAC model. The nodes are rated which is based on data transfer and friendship with other nodes, this provides complete information of the node. And also the un trusted nodes are given a chance to prove it is really malicious or not. The trusted nodes are identified effectively. The nodes are free from attacks.

Therefore the data packets reach the destination without loss and modification because it routes through the trusted node. Thus makes the routing secure. The security goals are achieved with less memory overhead, energy consumption and improve the Packet delivery ratio.

References

[1] Pandey, A. and Tripathi, R. (2010). A Survey on Wireless Sensor Networks Security. International Journal of Computer Applications, 3(2), pp.43-49.

[2] V. Kumar, A. Jain, and B. P N, “Wireless Sensor Networks Security Issues, Challenges and Solutions,” *Int. Res. Publ. House*, vol. 4, no. 8, pp. 859–868, 2014.

[3] Latha, D, and Palanivel, K. 'Secure Routing Through Trusted Nodes In Wireless Sensor Networks – A Survey'. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 3.4 (2014): 8.

[4] Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: A survey. Journal of Information Assurance and Security, 5, 31–44.

[5] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, *1*, 293–315.
[6] Momani, M. and Challa, S. (2010). Survey of Trust Models in Different Network Domains. IJASUC, 1(3), pp.1-19.
[7] Bin, T.,Xian,Y.Y., Dong, L.,Qi, L.,&Xin,Y. (2010).A security framework for wireless sensor networks. *The Journal of China Universities of Posts and Telecommunications*, *17*, 118–122.
[8] Zhang,Y.,Yang, J.,Li,W.,Wang, L.,&Jin, L. (2010).An authentication scheme for locating compromised sensor nodes in WSNs. *Journal of Network and Computer Applications*, *33*, 50–62.
[9] Bellare M, Micciancio D. A new paradigm for collision-free hashing: incrementality at reduced cost. In: Eurocrypt'97, Lecture notes in computer science, vol. 1233, 1997.
[10] Zhan, G., Shi, W., & Deng, J. ((2010). TARF: A Trust-aware routing framework for wireless sensor networks. In European Conference on Wireless Sensor Networks (EWSN) (pp. 65–80).
[11] Sheela, D., Nirmala S., Nath, S., & Mahadevan, G. (2011, July). A Recent technique to detect sink hole attacks in WSN. White paper, Anna University.
[12] Marmol, F. G., & Perez, G. M. (2011). Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication System*, *46*, 163–180.
[13] Khalil, I., Bagchi, S., Rotaru, C. N., & Shroff, N. B. (2010). UNMASK: utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks. *Ad Hoc Networks*, *8*(2), 148–164.
[14] Babu, S. S., Raha, A., & Naskar, M. K. (2011). A Direct trust dependent link state routing protocol using route trusts for WSNs (DTLSRP). *Scientific Research, Wireless Sensor Network*, *3*, 125–134.
[15] Dhulipala, V., Karthik, N. and Chandrasekaran, R. (2012). A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Networks. Wireless Pers Commun, 70(1), pp.189-205.
[16] Yim, S. J., & Choi, Y. H. (2012). Neighbor-based malicious node detection in wireless sensor networks. Wireless Sensor Networks, 4, 219–225.
[17] Gheorghe, L., Rughin, R. and tapus, N. (2012). Trust and Energy-aware Routing Protocol for Wireless Sensor Networks. In: The Eighth International Conference on Wireless and Mobile Communications. IARIA,.
[18] Gheorghe, L., Rughiniş, R., Deaconescu, R. and Ţăpuş, N. (2010). Adaptive Trust Management Protocol Based on Fault Detection for Wireless Sensor Networks. In: The 2nd Intel. Conferences on Advanced Service Computing. IARIA.
[19] Abduvaliev, Abror, Sungyoung Lee, and Young-Koo Lee. 'Simple Hash Based Message Authentication Scheme For Wireless Sensor Networks'. 5.
[20] Devanagavi, Geetha D., N. Nalini, and Rajashekhar C. Biradar. 'Trusted Neighbors Based Secured Routing Scheme In Wireless Sensor Networks Using Agents'. Wireless Pers Commun (2014): 1-28.