Maninder Kaur *et al*, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 11, November- 2017, pg. 88-94 **ISSN: 2321-8363**
Impact Factor: 5.515

Multi-Layered Security Architecture for Wireless Network for Detection and Removal of Blackhole Nodes

Maninder Kaur[1], Arshdeep Singh[2], Lakhvinder Kaur[3], Kulwinder Singh[4]
[1]Student, BMSCE MUKTSAR, manindermaan92@gmail.com
[2]Assistant Professor, BMSCE MUKTSAR, arshdeepsinghbrar@yahoo.com
[3]Assistant Professor, AIT Gharuan, lakhvinderkaur3@yahoo.com
[4]Assistant Professor, BMSCE MUKTSAR, just.brar@yahoo.com

Abstract
The wireless network security has been emerged in the recent years, as the number attacks over the wireless networks have arisen. There are several types of attacks which affects the performance of the wireless nodes in the cluster, such as denial of service (DoS), distributed DoS (DDoS), blackhole, connectivity hole etc. In this paper, the security model to protect against the blackhole attack over the wireless networks, which evaluates the incoming data in the multi-layered security architecture. The proposed model combines the node authentication (nodeAUTH), data rate control mechanism known as Flow Analytical and Overhead Recognition (FANOR), malicious node detection model, which collectively controls the ingress data over the wireless cluster. The proposed model has been designed to protect the wireless network by detecting and bypassing the blackholes in the given network, which is followed by the blackhole node removal methodology. The performance of the proposed model has been analyzed under the various circumstances over the various target wireless nodes. The proposed model results prove the efficiency of the proposed model estimated from the evaluated performance parameters.

Keywords: Multi-layered security model, node authentication, blackhole detection, blackhole removal.

1. Introduction
This module defines the algorithm, which utilizes the latter algorithms (acted as security modules) to create the secure wireless network cluster with specifically designed model to mitigate the blackhole nodes. This algorithm is known as the blackhole node recognition and mitigation algorithm (BNRMA). The main algorithm or main security algorithm has been designed to call the system modules defined earlier to perform the relevant task on the given data in order to produce the decision logic, which is used to decide the node as attacker or non-attacker. In order to interconnect the network nodes with each other, use equation (1) to estimate the average per-hop distance after obtaining hop distances and the location information of other anchor nodes.

$$c_i = \frac{\sum_{j \neq i} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)}}{\sum_{j \neq i} h_{ij}} \qquad (1)$$

(xi,yi,zi),(xj,yj,zj) denotes the coordinates of anchor node i,j,h_{ij}depicts the hop-count between anchor node i and anchor node j. The unknown nodes calculate distances to each and every anchor nodes after receiving per-

hop distance and transmit information to the adjacent nodes. The hop distance of all anchor nodes is used by unknown nodes in step 2 to determine the coordinates of unknown nodes by applying maximum likelihood estimation method or four edges measurement. (2) is used to calculate when distance from anchor node to unknown node is well-known.

$$\begin{aligned}(x_1 - x)^2 + (y_1 - y)^2 + (z_1 - z)^2 &= d_1^2 \\ (x_2 - x)^2 + (y_2 - y)^2 + (z_2 - z)^2 &= d_2^2 \\ &\vdots \\ (x_n - x)^2 + (y_n - y)^2 + (z_n - z)^2 &= d_n^2\end{aligned} \qquad (2)$$

The main security algorithm is responsible for calling all other security modules during the implementation of the security over the given wireless network structure. The main algorithm can be called as the main controller algorithm, which notifies the new entry of the nodes, and calls the appropriate module to analyze the information provided or the ingress data on the road side unit node or wireless client node.

2. **Algorithm 1:** Blackhole node recognition and mitigation algorithm

1. Begin the wireless nodes and the base stations (BTS) in the defined zone
2. Prepare the wireless network and begin the initial connectivity to inter-connect the nodes
3. Connect the nodes with the corresponding centralized and structured architecture over the Client-BTS nodes.
4. Assign the wireless BTS membership to the nearest nodes within the assigned wireless range
5. Perform the node characteristic analysis over each of the wireless node
6. Obtain the network characteristics of each wireless node after the nodes joining the networks
7. Analyze the network using the **F**low **AN**alytical and **O**verhead **R**ecognition (FANOR)
8. Detect the malicious nodes in the given wireless cluster
9. FANOR must evaluate the physical position of the wireless nodes in the cluster and returns the desired status
10. If FANOR status is positive
    a. The wireless node joins the cluster
11. Otherwise
    a. It undergoes the further analysis procedure, and marked as reported.
    b. Begin the interconnectivity between the wireless nodes in the wireless node authentication (nodeAUTH)
    c. Authenticate the reported node using the authentication procedure.
    d. Ask for the pre-shared information from the target node
    e. If the node reply with the correct data
        i. Node is assigned with the cluster membership

ii. nodeAUTH module returns true

f. Otherwise

i. The node is blocked and added to the black list

ii. nodeAUTH returns false

12. if nodeAUTH conditions are satisfied

a. Check using data volume and other related conditions

b. If the ingress traffic size is higher than channel capacity

i. Discard the overhead data

ii. Place the request for the data rate control to the target node

c. Otherwise

d. Accept the ingress data from node and add the node to the certified receiver's list

3. Result and Discussion

The proposed model has been implemented in the NS-2 simulator using a scenario of 15 wireless nodes. All of the nodes are having a transmission radius of 250 meters. The nodes are divided into two types of wireless network clusters. The nodes in the mobile network cluster are represented in the black color. The mobile network cluster is representing the communications between the mobile network users and BTSes. The mobile network cluster is made of total 9 nodes. Node IDs ranging between 0 and 8 are the 9 number of nodes members of the mobile network part of the proposed model simulation. The other cluster is Wi-Fi cluster or campus cluster. The campus cluster is made of 6 nodes ranging between 9 and 14. The mobile cluster is using the traffic speeds ranging between 10 Kbps and 100 Kbps whereas the Wi-Fi cluster (Campus Cluster) is using the traffic speeds ranging between 1 Mbps and 10 Mbps. The mobile nodes are using AODV based mobile communications. The mobile communications offer the long range connectivity to facilitate the inter-nodal calling and internet connectivity between the mobile network users during the existence of the blackhole nodes within the give wireless network.

The proposed model has been well tested under various situations in the sensor network simulation. The proposed energy based routing protocol on sensor network has been well tested for the performance parameters of delay, throughput, and network load. The nodes in the proposed model simulation have performed well in terms of all of the above parameters. The network load and throughput have been recorded lesser than the ordinary sensor networks with mobility or stationary positioning under the similar situations.

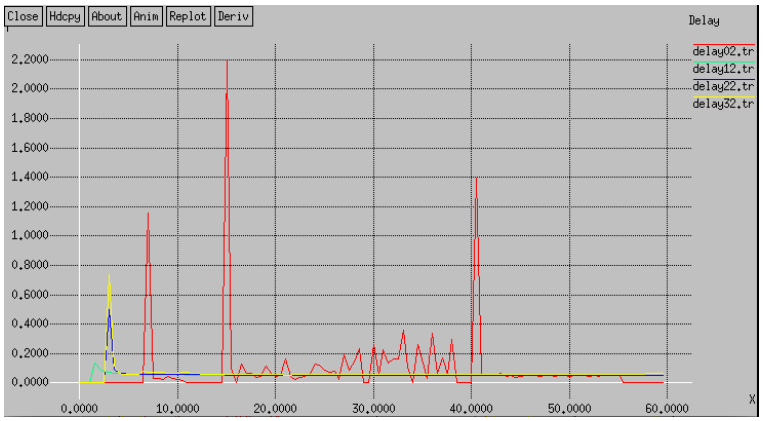

Figure 1: The delay obtained from the various groups of nodes in the topology

The maximum delay recorded in the simulation is ranging between 0.2 and 2 millisecond. (Figure and table 1) The delay is the parameter represents latency of a packet when it was being sent between two nodes. The time taken for a packet to reach the destination from the source is called the total delay.

Table 1: Delay

10 nodes	20 nodes	30 nodes	40nodes
0.017	0.051	0.051	0.054

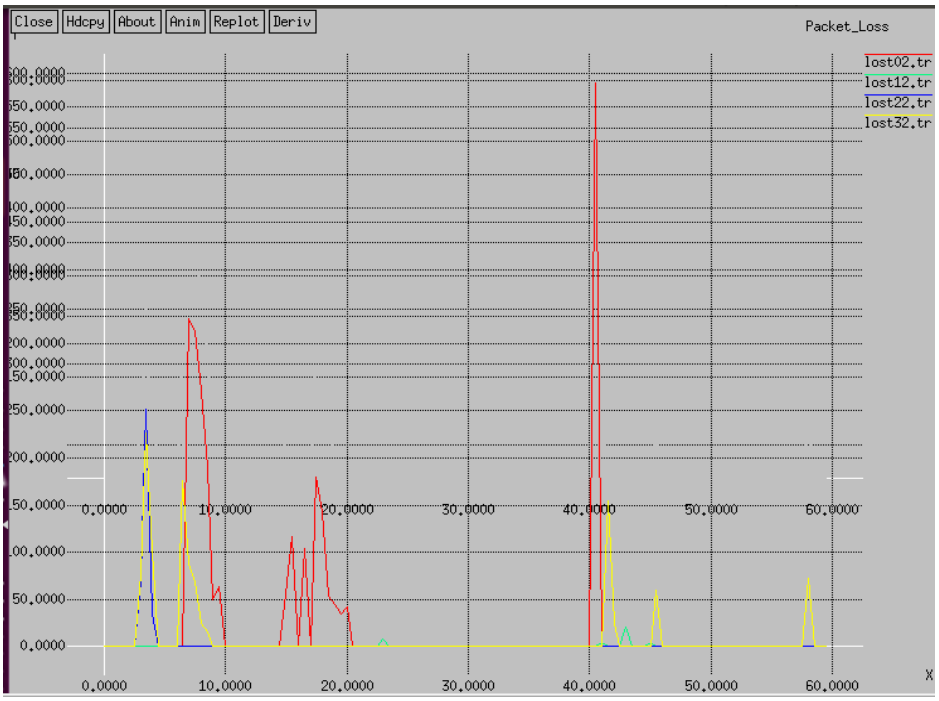

Figure 2: The graph of loss across the groups of nodes in the given cluster

The network load is the parameter which shows the loss of packet during the runtime. The proposed mode has been well tested for the loss on the different times in the simulation. The proposed model has been found showing the minimum loss at 20 packets and maximum load at 226 percent resource usage, where the sensor network is over-flown with the data, because a number of nodes are transmitting the heavier amount of data towards the sink nodes.

Table 2:Loss

10 nodes	20 nodes	30 nodes	40nodes
598	20	252	226

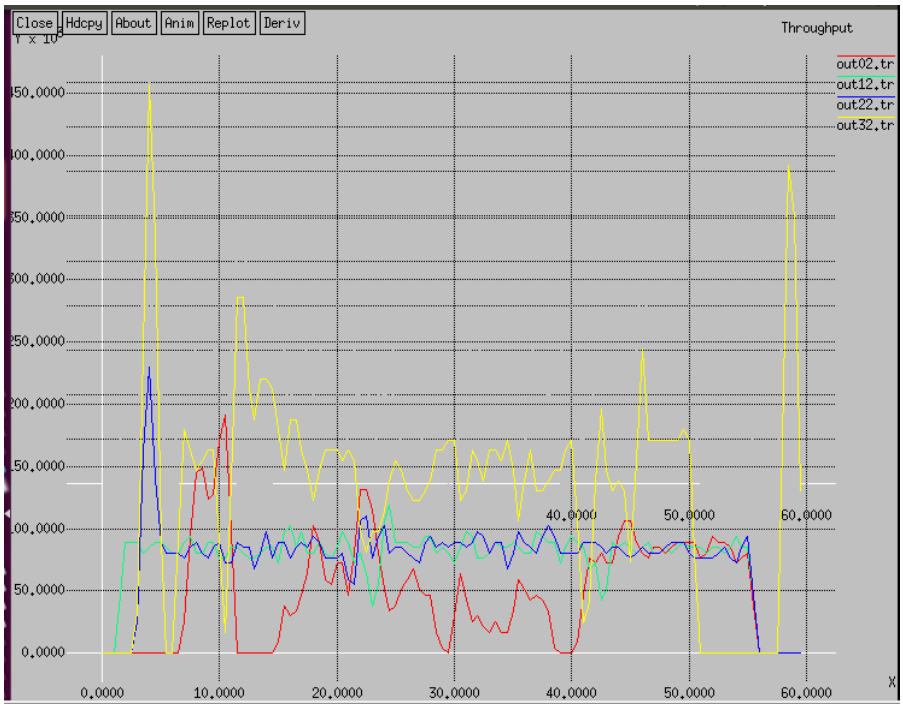

Figure 3: The graph of throughput obtained from different groups in the given topology

The throughput (Figure 3) is the parameter represents the capacity of a node or a network to send the data per second. The throughput of the sensor network using our proposed energy aware tree based routing protocol has been recorded between 80 and 456 Kbps. The 0 kpbs is the value recorded when no data is being sent between the nodes in the initial stages. Once the data transfers start, the throughput starts going up. The maximum limit of the throughput is 456 Kbps. In previous work the maximum throughput is 156.79kbps. This shows the better that the purposed work has better performance than previous work.

Table 3: Throughput

10 nodes	20 nodes	30 nodes	40nodes
191520	119168	229824	456960

4. Conclusion

The blackhole protection based wireless routing approach is considered the most balanced and secured routing approach in the case of wireless networks, because it uses the low size neighbor information table, which saves a lot of space on the memory hence energy. The proposed model is based upon the secure authentication based routing mechanism. The proposed model has been designed to work efficiently during the existence of the blackhole nodes in the target cluster. The proposed routing protocol for the mobile wireless sensor network has been designed for energy based metric calculation with quick updates and fast convergence. All of the latter mentioned properties are the reason behind the rise in the energy efficiency levels of the proposed model. The proposed model has been evaluated on the basis of load, routing overhead and other communication parameters. The proposed model has been proved better than the exiting scheme and highly adaptable to the mobile wireless networks. In the future, the proposed model will be extended for the very fast convergence for the mobile WSNs along with small route updated in the controlled cluster scenarios. The controlled neighbor update can be also used to improve the performance of the proposed algorithm, which will increase the time of neighbor communication for alive/activity check and lowers the levels of data produced by the topology change packets.

References

[1] Tariq A. Alahdal, Saida M, 2013, "Performance of Standardized Routing Protocols in Ad-hoc Networks", *ICCEEE*, **ISBN:** 978-1-4673-6232-0 vol. 1, pp. 23-28.

[2] Kuppusamy P., Dr. Thirunavukkarasu K., 2011, "A Study and Comparison of OLSR, AODV and TORA Routing Protocols in Ad Hoc Networks", *IEEE*, pp. 143-147.

[3] Lamyaa M. T. Harb, Dr. M. Tantawy, Prof. Dr. Elsoudani M., 2013, "PERFORMANCE OF MOBILE AD HOC NETWORKS UNDER ATTACK", *IEEE*, pp. 1201-1206.

[4] Asma T., 2010, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2", *ICACE, IEEE*, pp. 330-33.

[5] Samir R. D., 1998, "Comparative Performance Evaluation of Routing Protocols for Mobile, Ad hoc Networks", *ICCCN, IEEE*, pp. 153-161.

[6] Jaya J., 2012, "Performance Analysis and Enhancement of Routing Protocol in Manet", *IJMR*, vol. 2, issue 2, pp. 323-328.

[7] Anuj K. G., Dr. Harsh S., 2010, "Performance analysis of AODV, DSR & TORA Routing Protocols", *IACSIT*, vol. 2, no. 2, vol. 226-231.

[8] Anu B., Munish B., Jagpreet S., 2009 "Performance Analysis of MANET under Blackhole Attack", *ICNC*, vol. 1, pp. 141-145.

[9] Gaurav K. G., Jitendra S., 2010, "Truth of D-DoS Attacks in MANET", *GJCST*, vol. 10, issue 15.

[10] Debarati R C., Leena R., Nilesh M., 2015, "Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack", *International Conference on Advanced Computing Technologies and Applications (ICACTA), ELSEVIER*, pp. 564-570.

[11] Samara G., Al-Salihy W. A.H., Sures R., 2010, "Security Issues and Challenges of Vehicular Ad Hoc Networks", *New Trends in Information Science and Service Science 2010 4th International Conference on IEEE*, ISBN: 978–89-88678-17-6, pp. 393-398.

[12] Singh M., Mehta G., Vaid C, 2012, "Detection of Malicious Node in Wireless Sensor Network based on Data Mining", *International Conference on Computing Sciences IEEE* no. 978-#6-7695-4817-3/12, pp. 291-294.

[13] YAN G., OLARIU S., WEIGLE M., 2008, "Providing VANET security through active position detection", *Comput.Commun.*, vol. 31, no. 12, pp. 2883-2897.

[14] Kaur R., Kaur A., 2014, "Blackhole Detection In Manets Using Artificial Neural Networks", *International Journal For Technological Research In Engineering*, vol. 1, no. 9, pp. 959-962.

[15] Lakshmi Praba V., Ranichitra A., 2013, "Detecting Malicious Vehicles and Regulating Traffic in VANET using RAODV Protocol", *International Journal of Computer Applications*, vol. 84, no. 1, pp. 0975-8887.

[16] Mahmoud O., 2014, "A feature selection method for classification within functional genomics experiments based on the proportional overlapping score", *BMC Bioinformatics*, vol. 15.1:274, pp. 1-20.

[17] Ramkumar J., Murugeswari R., 2014, "Fuzzy Logic Approach for Detecting Black Hole Attack in Hybrid Wireless Mesh Network", *2014 IEEE International Conf. on Innovations in Engineering and Technology (ICIET'14)*, vol. 2347 - 6710, pp. 877-882.

[18] Vaza B. N. R., Parmar A , Trupti M., 2014, "Implementing Current Traffic Signal Control Scenario in VANET Using Sumo", *International J. of Advance Engineering and Research Development (IJAERD)*, no. 2348–#6, pp. 1-4.

