International Journal of Engineering & Technology, 7 (4.7) (2018) 389-394

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paperResearch Paper

A Novel Hybrid and Secure Clustering Black hole Attacks Mitigation Technique in Wireless LAN

Er. Harmeet Singh, Dr.Vijay Dhir

[1] *Research Scholar, Department of Computer Science & Engineering, SBBS University, Jalandhar,E-mail: hsnatt5@gmail.com*
2 Professor, Department of Computer Science & Engineering, SBBS University, Jalandhar,
**Corresponding author E-mail: drvijaydhir@gmail.com*

Abstract

Wireless LAN is a dynamic network with large number of mobile nodes. As the traffic increases over the wireless, it will lead to number of problems like congestion and packet loss. This congestion and packet loss problems occurs due to the attacks in wireless LAN.Out of the various attacks black hole attack is most dangerous attack which drops all of the packets received from the source node and which act as a black hole in the universe. In this paper we are providing solution against this attack. We propose a Novel Hybrid and Secure Clustering Black hole Attack Mitigation Technique in Wireless LAN. This technique firstly detects the black hole attack by using threshold values against different parameters, after this clustering approach is used for secure path from source to destination by reducing overhead in the network. Most of existing mechanisms are not as efficient because by isolating black hole attack overhead is increased. A HSBM approach has remarkable advantage over these existing techniques. We simulate the proposed technique by using NS2 simulator and proved that our technique effectively detects the black hole attack in terms of throughput, packet loss, end to end packet delivery ratio, delay.

Keywords: *Black hole attack; wireless LAN.*

1. Introduction

The rapid development of the internet and wireless technology the need of mobile and portable devices also increased. The wireless network provides the link between several devices to communicate to each other. The wireless LAN, that provides to user's better flexibility to communicate to each other in small geographical range [1]. 802.11 standards are recommending for wireless LAN by IEEE. The 802.11 wireless standards can vary in terms of frequency, transmission range, speed used; still in design of implementation it may be similar. The 802.11 wireless standards can use either an ad-hoc or infrastructure network, and almost all the standards can use the identical security protocols.

Wireless LAN (that does not require cables to connect with different device) uses radio waves for the communication. An intruder attacks has been exceeded due to the wireless nature of LAN. Classification of wireless neighborhood area network attacks are proposed primarily based at the vital parameters

These day's broadcasting domain, the computation of the records via wireless LAN is extra prone to attacks while it is as compared with wired networks [2]. This is mainly due to wired networks are well secured through protected cables whereas wireless signals are transmitted in open air. Wireless LAN is widely operable in any kind of situations due to its availability, flexibility and mobility. It also makes us more cost-efficient because of its easy configurability through which we are able to cowl a bigger span of transmission availability through restricting the extra wired networking infrastructure. Even though we've got many subsequent features of having a wireless LAN with its mobility and freedom that comes with it however it's far exposed to vulnerabilities and attacks. The wireless LAN security risk analysis and risk management have to be in a role to confront those forms of security risks and attacks when you consider that they are imperative in organizational marketing strategy. Wireless LAN spread hastily everywhere from domestic to large scale in these day because of ease set up and small cost. To increase the availability of wireless LAN means, increase a new threats and increased chance from attackers. Commonly vulnerabilities are equal in wireless and wired networks. Vulnerabilities occur due to the data transmitted with the help of radio waves in wireless LAN [3]. The vulnerabilities that exist inside wireless LANs get up from many source but the 802.11 protocol itself has extreme weaknesses that have been partly addressed in recent iterations of the 802.11 protocol together with 802.11i. There are some most essential and significant vulnerabilities are present in wireless LAN like access control, WEP, authentication, WPA/WPA2 vulnerabilities [23].

2. Black Hole Attack

One among the main attacks black hole attack in network layer. In this type of attack malicious node performs and serves a black hole in the universe. All the data packets which are received from source node are drop by a malicious node without and transfer to target node. In this case the attacker node comes across as a node containing the smallest path to target node with the help of minimum hope count and maximum sequence number [4]. After getting the route from source to destination, node start dropping all of the packets received from source node. In Figure 1 shows that node 3 is malicious node creating black hole attack in network.

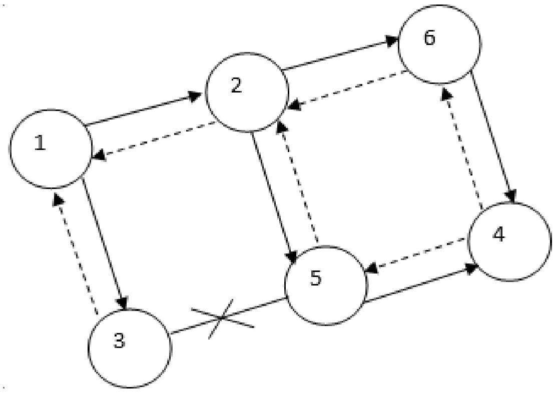


Fig.1: Black hole attack in Wireless LAN

A several methods are available to detect the black hole attack in wireless LAN. In this paper here we are discussed about a Novel Hybrid and Secure Clustering Black hole Attack Mitigation Technique in Wireless LAN. Through the simulation result also prove that proposed technique enhance the performance of wireless network in the terms of throughput, packet loss, delay and end to end packet delivery ratio.

3. Related Works

M.Rejesh et al. [5] describe a NHBADI approach for detecting and preventing the mobile ad-hoc network from black hole attack. The major objectives of this approach to reduce routing load, overhead of MANET.

Monika [6] design an algorithm to detect the black hole attack from wireless network and also prevent the same from attack on the basis of cryptography mechanism. In this paper the proposed technique use “Probability Based Routing Scheme” for the routing.

Anand et al. [7] has proposed IDS that is based on hash function to detect and prevent the MANET from grey and black hole attack. This system rejects the 1st optimal path for prevention of MANET from the intruder and additionally hash function maintains the data integrity.

Jaisankar, N[8] present a novel technique to isolate the black hole attack from mobile ad-hoc network. This technique provides high packet delivery ratio and minimum delay. This technique detects and isolates the attack in promiscuous mode.

Kurosawa, S [9] introduce a dynamic learning based approach to isolate the malicious node. This approach use dynamic updated data. The main objective of this technique to prevent the MANET from black hole attack.

Y. ping et al. [10] has describe an adaptive approach based totally on the design of cross layer to detect black hole and grey hole attack in mobile ad-hoc network. In this paper propose path-based method for network layer and “collision rate reporting system” to estimate threshold in MAC layer. He used DSR protocols for the testing of this algorithm.

G Rajni et al. [11] implement genetic algorithm with neural network for source to destination route optimization and that is used to detect and prevent the MANET from black hole attack. She also uses AODV protocols.

B Suman et al. [12] introduce the mechanism for protecting the mobile ad-hoc network through detecting the abnormal activities of each node. It also uses the particle-swarm optimization which monitor the sending packets.

N Patel et al. [13] proposed an algorithm on the basis of trust value with the use of AODV protocol which protect the network routing from the intruder. To find the trust value of nodes use the clustering pattern technique the higher trust value node is selected as a cluster head.

Kaur R [14] gives an overview on attacks like black and grey hole in wireless mesh network. To secure the network from attacks in this paper use the OLSR protocols. The drawback of this it cannot secure the WMN from intruder purely. Motamedi M [15] introduce the method to detect the black hole attack on the wireless network that cause misfortune of essential information. In this method uses the UAV and SPRT for the better result to detecting the black hole attack. It gives higher chance to detect attacks.

Mishra A et al. [16] describes the method to mitigate the cooperative and single black hole attack to find a secure route to destination node bypassing attacks. In this paper AODV security is improved for the better analysis.

O Singh et al. [17] suggested IIDPS deny black hole attack in MANET. The technique is based on trust management in which malicious node in MANET is detected by central network administrator on the basis of predefined threshold and risk factor. Malicious nodes are identifying using behavior classifier.

S Misra et al. [18] BAMNi technique is proposed for wireless sensor network to mitigate the activities of black hole attack. BAMNi use multiple BS in the wireless network opposing the collision attack in transmission.

Ghathwan K et al. [19] proposed an artificial intelligence technique to prevent the MANET from single and cooperative black hole attack. This technique use AODV routing protocol to find the shortest path.

Muhammad. I et al. [20] introduce a technique for detection and prevention of black hole attack. To monitor the network performance of nodes DPS nodes are distributed in network. DPS node analyze the PREQs of neighbor nodes and send alert message in network if suspicious node is found.

4. Proposed Work

In our proposed work, focuses on the detection of black hole attack from wireless local area network with increased overhead. In this approach a first step to calculate the route reply time (RT) from several nodes that is based on the parameters of reply to the route request. Now this time need to be compare with the waiting time (WT) which is the average time of several nodes in the network that are replying with route to destination node. After receiving the route reply messages through the intermediate node. The verification as a next step to see if this intermediate node is malicious or not become necessary, in case RT of the particular node less than WT. To verify that it is malicious node or not, different parameters must be employed to check the maliciousness of the node. This technique involves the obtaining of malicious table based on the previous traffic of network. If the maliciousness of any node is traced, its information is lodged in the malicious table. The declaration of the maliciousness of a node based on different parameters. A node is said to be malicious if it false under diverse parameters and stands for the attributes of black hole attack and at the same time its ID is contained in malicious table in order to enable the isolation of this node from the network in future. The node, id comparison must be presented with all IDs, in the case of RT<=WT but if the sameness is traced between RT and WT then the route reply from the malicious node needs to be discarded. If route reply node happens to be not in the malicious_table, the calculation of distance time value should be followed. It should be taken into account that then this value should be compatible with the expected hope count value and be minimum also. If it’s so then this value should be stored in the dt_table or else that route_reply has to be discarded. If it is confirmed by next hope that the replying node has path, then there should be the storing of node_id and its seq_no. in the RREP_table, otherwise node_id and its seq_no. is deposited in the malicious_table. After the verification of all the seq_no. there should be the selection of the node having higher seq_no. from the RREP_table. This node is hailed as cluster head in the network. The algorithm and flowchart are as following.

A. Algorithm

Step A: Get the Time i.e currently recorded.

Step B: Take waiting time (WT)

Step C: whereas (RT<=WT).

Various step verification take part in the verification of route reply messages.

Srep 1: Monitoring of malicious node.

After the route replies are received through intermediate nodes, the checking of malicious_table is required for malicious node_id which is create based on the previous traffic.

If node_id matches with the malicious_table, then it is requested to discard the route reply.

If the absence of node_id in malicious_table, then going to step (b) is required.

Step 2: The distance_time value should be monitored.

If both distance_time value and expected hope match together, then the value should be stored dt_table and move to step 3.

Else discarding the route reply.

Step 3: if route request message passages a path to destination node should be ascertained by asking the next hope that node replied in this sender node.

If it is confirmed by next hope that replying node has a path, then it is necessary to store node_id and seq_no. in RREP_table.

Else node_id and seq_no. both get stored in malicious_table.

Step 4: All verification of route reply message has to be carried out if the running time is greater than waiting time.

Now make the selection of one seq_no. from RREP_table.

If this selection from RREP_table is not possible then doing two step verification is required.

The selected seq_no. and all other seq_no. which are presented on RREP_table should be compare. In case of is extremely greater than doing next step verification and move to step 4 (b).

Now, check here value of packet drop. The storing of that node_id is needed in malicious table if packet drop value is greater than 0.5. Else it is necessary to keep node_id in RREP_table and move to step 5.

Step 5: The selection of largest seq_no. from RREP_table should be done after verification of all seq_no.

If the access to RREP_table is not possible then it is necessary to find cluster head.

The find weight value of node id done through the use of energy of link (EL), speed of link (SL), and neighborhood link (NL) and distance_time value that is recorded from dt_table.

Final weight of node = (F1 * SL) + (F2 * EL) + (F3 * NL) + distance_time value.

$SL = (S_a+S_b)/2$, $EL = (E_a+E_b)/2$

Whereas a and b are two connected nodes. S_a and S_b are speed of these nodes.

E_a And E_b is the energy consumed by nodes A and B respectively.

F1, F2, F3 are weight factors.

F1 + F2 + F3 = 1.

Then calculate the battery power (BP), buffer length (BL) and serve time (ST) and move to step 6.

Step 6: Calculating the node value by adding the final weight of node and all the components of step 5 (b).

Node value = Final weight of node + BP + BL + ST.

And store the node value in node_value_table.

Step 7: Make the selection of one largest node value from node_value table and after that send the packets to the cluster head through the node cluster head. If this done the selection from neighbors nodes of sender will be automatically performed.

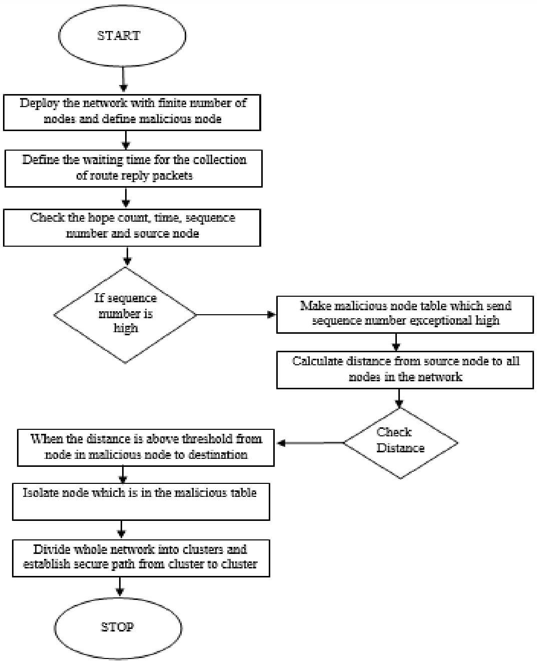
Step 8: Deletion of all other seq_no. from RREP_table should be performed.

5. Simulation Result

In order to test the proposed technique, the NS2 simulator [21] is used to evaluate the performance with parameter shown in table 1. In this section the proposed Hybrid and Secure Clustering Black hole Attack Mitigation (HSBM) Technique has been compared with the fuzzy based DDoS attack mitigation (FDAM) Technique [22]. We estimate the black hole attack and their detection accuracy for wireless LAN with Hybrid and Secure Clustering Black hole Attack Mitigation (HSBM) Technique, the result demonstrated that the misbehavior nodes are detected in higher throughput, False Positive Rate with the HSBM. Evaluate performance in terms of Delay, Throughput, packet loss, end to end packet delivery ratio and false positive rate.

Table.1:-Parameters used for simulation

Parameter	Value
Simulator used	NS 2
Area (meter)	800X800
No. of nodes	19
Routing Protocol	AODV
Channel Type	Wireless
Packet Size	512 bytes
Mobility Model	Two ray ground propagation model


START
Deploy the network with finite number of nodes and define malicious node
Define the waiting time for the collection of route reply packets
Check the hope count, time, sequence number and source node
If sequence number is high
Make malicious node table which send sequence number exceptional high
Calculate distance from source node to all nodes in the network
Check Distance
When the distance is above threshold from node in malicious node to destination
Isolate node which is in the malicious table
Divide whole network into clusters and establish secure path from cluster to cluster
STOP

B. Flowchart

Effect of Varying Transmission Range

In this section the result of HSBM technique are evaluated by varying the transmission range such as 100,200,300,350 and 400m. From Figure 2, it is clearly shown throughput when the transmission range is increased. From the figure it is cleared that the performance of HSBM approach is enhanced in the terms of throughput when compared to Fuzzy Based DDoS Attack Mitigation technique.

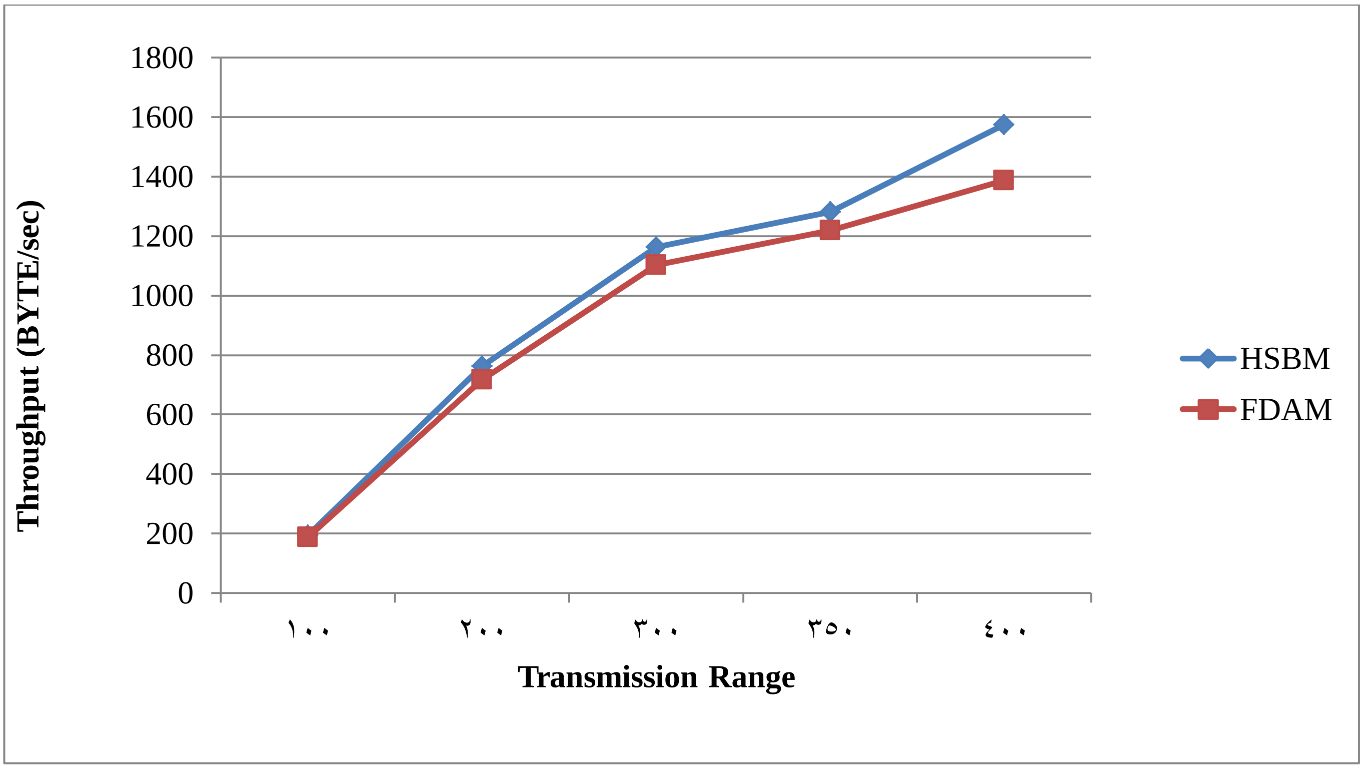


Fig.2: Throughput vs Transmission Range

Figure 3 shows the Hybrid and Secure Clustering Black hole Attack Mitigation (HSBM) and FDAM techniques end to end delay when the transmission range is increased in the case of wireless LAN. The figure shows that the proposed technique end to end delay is less when compare to FDAM technique.

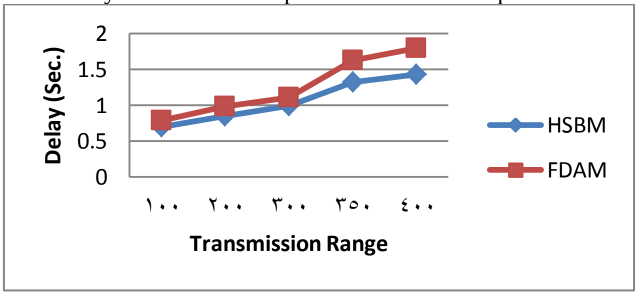


Fig.3: Delay vs Transmission Range

From Figure 4, it is clearly shown packet delivery ratio when the transmission rangeis increased. The figure is clearly shows that the packet delivery ratio of Hybrid and Secure Clustering Black hole Attack Mitigation approach is more as compared to FDAM techniques.

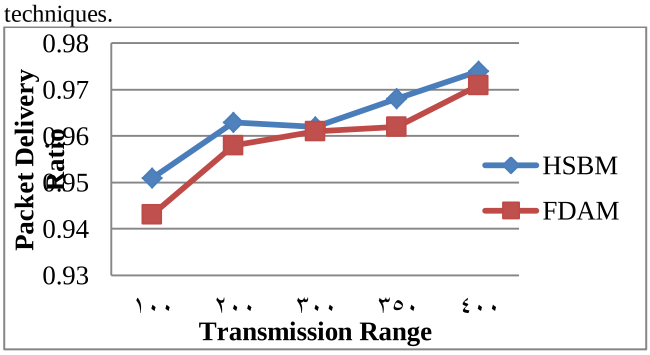


Fig.4: Packet Delivery Ratio vs Transmission Range

The false positive rate of the Hybrid and Secure Clustering Black hole Attack Mitigation (HSBM) Technique and FDAM technique is shown in Figure 5. The false positive rate is significantly less in our Hybrid and Secure Clustering Black hole Attack Mitigation (HSBM) Technique when compared with FDAM scheme when the transmission range is increased.

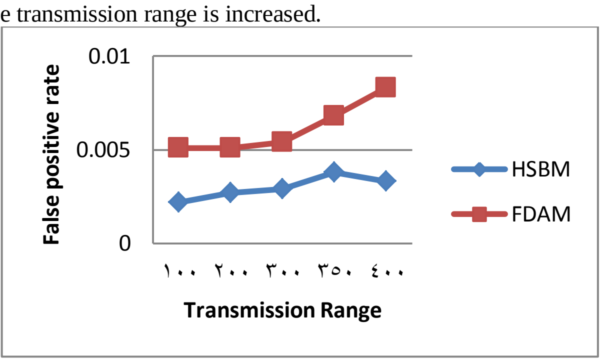


Fig.:5: False positive rate vs Transmission Range

From Figure 6, it is clearly shown that the number of attack packets loss when the transmission range is increased. From the results it has been found that the Hybrid and Secure Clustering Black hole Attack Mitigation approach has less packet loss when compared to FDAM approach.

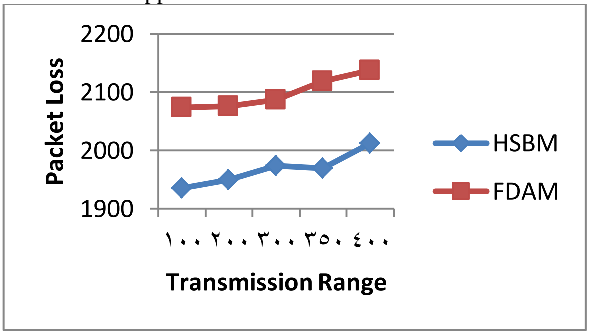


Fig.6: Packet Loss vs Transmission Range

Effect of Varying Attack Rates

In this section the result of Hybrid and Secure Clustering Black hole Attack Mitigation (HSBM) Technique are evaluated by varying the traffic rate such as 100,150,200,250 and 300kb.

The Delay of the Hybrid and Secure Clustering Black hole Attack Mitigation (HSBM) Technique and FDAM technique is shown in

Figure 7. In the figure, it is revealed that the Delay is significantly less in our Hybrid and Secure Clustering Black hole Attack Mitigation (HSBM) Technique when compared with FDAM scheme when the rate is increased.

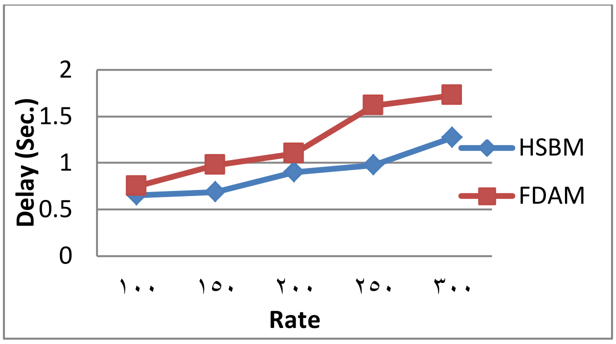


Fig.7: Delay vs Rate

From Figure 8, it is clearly shown packet delivery ratio when the rate is increased. The figure is revealed that the packet delivery ratio of Hybrid and Secure Clustering Black hole Attack Mitigation approach is more than as compared to FDAM techniques.

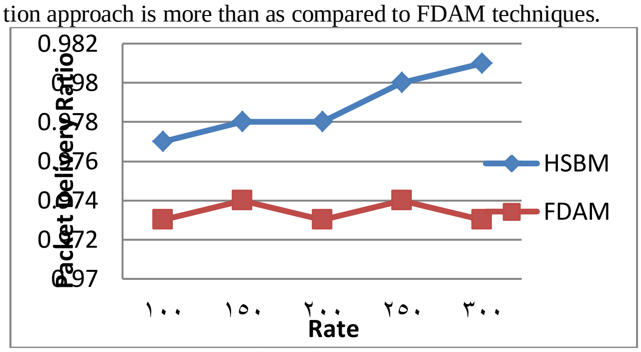


Fig.8: Packet Delivery ratio vs Rate

The false positive rate of the Hybrid and Secure Clustering Black hole Attack Mitigation (HSBM) Technique and FDAM technique in terms of attack rate is shown in Figure 9. The false positive rate is significantly less in our Hybrid and Secure Clustering Black hole Attack Mitigation (HSBM) Technique when compared with FDAM scheme when the rate is increased.

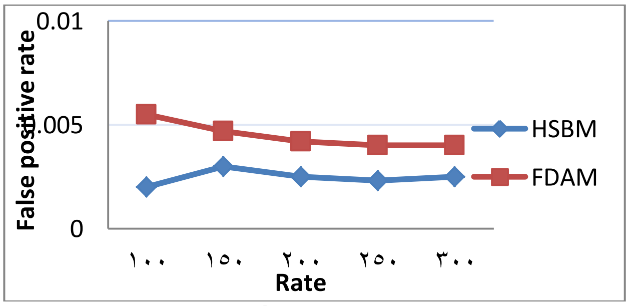


Fig.9: False positive rate vs Rate

From Figure 10, it is clearly shown that the number of attack packets loss when the rate is increased. From the results it has been found that the Hybrid and Secure Clustering Black hole Attack Mitigation approach has less packet loss when compared to FDAM approach.

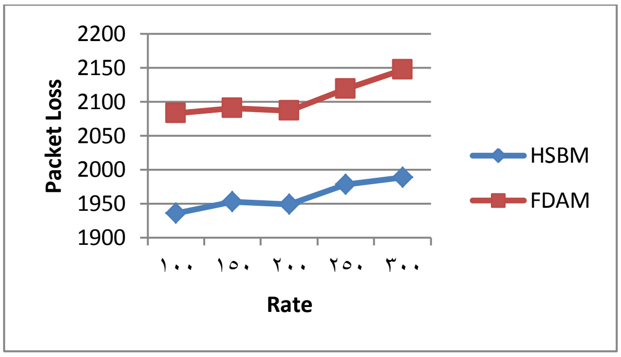


Fig. 10: Packet Loss vs Rate

6. Conclusion

Black hole attack is very hard to detect in wireless LAN. Due to wireless nature of network launching the black hole attack is very easy. In this paper proposed a Novel Hybrid and Secure Clustering Black hole Attack Mitigation Technique in Wireless LAN. This technique is used to detect and prevent the wireless local area network from black hole attack. This technique detects the attack node by minimum route reply, minimum hope count and maximum sequence number. Clustering used to reduce the overhead after detecting and isolating the attack. Evaluate the performance of proposed technique with parameters end to end packet delivery ratio, packet loss, throughput, delay and false positive rate by using NS2 simulator. The proposed HSBM technique compare with the FDAM technique. The simulation results show that our proposed HSBM technique has better performance than FDAM technique.

References

[1] Haitao Wu, Yong Peng, Keping Long, Shiduan Cheng, Jian Ma (2002), “Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN:Analysis and Enhancement” IEEE INFOCOM 2002.

[2] Bellaaj H., Ketata R. and Hsini A (2007), "Fuzzy approach for 802.11wireless intrusion detection", 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, March 25-29, Tunisia.

[3] Waliullah, M. D. G. (2014). “Wireless LAN Security Threats & Vulnerabilities” (IJACSA) International Journal of Advanced Computer Science and Applications, 5(1), 176–183. https://doi.org/10.1017/CBO9781107415324.004

[4] Banerjee, S.; Majumder, K. A Survey of Blackhole Attacks and Countermeasures in Wireless Mobile Ad-hoc Networks. Springer.Volume 335, of the series Communications in Computer and Information Science.pp 396-407.

[5] Rajesh, M.; Usha, G. (2016) “A Novel Honeypot Based Detection and Isolation Approach (NHBADI) to Detect and Isolate Black Hole Attacks in MANET”, Wireless PersonalCommunication. Springer, New York.

[6] Monika (2016) “Black Hole Attack Detection and Prevention in Wireless Networks”, International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 06 page 1376-1380.

[7] Anand, A.; Bhandari, A. (2014) “Prevention of Black Hole Attack on AODV in MANET using hash function”, Proceeding of 3rd international conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions).

[8] Jaisankar, N.; Saravanan, R.; Swamy, K. “A Novel Security Approach for Detecting Black Hole Attack in MANET”, Communications in Computer and Information Science. Vol. 70, pp 217-223.

[9] Kurosawa, S.; Nakayama, H.; Kato, N.; jamalipour, A.; Nemoto, Y. (2007) “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security. Vol. 5(3): 338-346, November 2007.

[10] Ping YI, Ting ZHU, Ning LIU, Yue WU, Jianhua L, (2012) "Cross-layer Detection for Black Hole Attack in Wireless Network", Journal of Computational Information Systems.

[11] Rajni Garg, Vikas Mongia (2018), "Mitigation of Black Hole Attack in Mobile Ad-Hoc Network Using Artificial Intelligence Technique", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3, Issue 1, ISSN: 2456-3307, pages 1168-1174.

[12] Suman Brar, Mohit Angurala (2017) "Cooperative Black Hole Attack Prevention by Particle Swarm Optimization with Multiple Swarms", International Journal of Advance Research, Ideas and Innovations in Technology, Volume3, Issue 1, pages 858-863.

[13] Neelam Janak Kumar Patel, Dr. Khushboo Tripathi (2017) "Trust Value based Algorithm to Identify and Defense GrayHole and Black-Hole attack present in MANET using Clustering Method", IJSRSET, Volume 4, Issue 4 pages 281-287.

[14] Rupinder Kaur, Parminder Singh (2014) "Black Hole and Greyhole Attack in Wireless Mesh Network", American Journal of Engineering Research (AJER), Volume-3, Issue-10, pp-41-47.

[15] Maryam Motamedi, Nasser Yazdani (2015) "Detection of Black Hole Attack in Wireless Sensor Network Using UAV", IEEE IKT2015 7th International Conference on Information and Knowledge Technology.

[16] Ankur mishra, Ranjeet Jaiswal, Sanjay Sharma (2013) "A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network",2013 3rd IEEE International Advance Computing Conference (IACC). Pages 499-504.

[17] Opinder Singh, J Singh et. al. (2016)," An Intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks against Malicious Nodes", International Journal of Science & Technology, Vol.10,pp.1-12.

[18] Satyajayant Misra, Kabi Bhattarai, and Guoliang Xue (2011) "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks", IEEE ICC 2011 proceedings.

[19] Ghathwan K.; Yaakub, A. (2014) An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET. SCDM 2014, Advances in Intelligent Systems and Computing. Springer International Publishing Switzerland.

[20] Galeeva G., Aktasheva A. Forecasting the Dynamics of Foreign Direct Investment in the Russian Economy, Astra Salvensis, Supplement No. 2, p. 137, 2017.

[21] Dashkin R. Determinations of Investment Activity of Russian Companies, Astra Salvensis, Supplement No. 2, p. 397, 2017.

[22] Gabdrakhmanov N., Ergunova O. Industrial Production Zones as a Tool of Development of the Regional Economy (on the Example of the Republic of Tatarstan and the Sverdlovsk Region), Astra Salvensis, Supplement No. 2, p. 447, 2017..

[23] Jatinder Singh, Lakhwinder Kaur and Savita Gupta (2010), "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN", International Journal of Computer Science and Information Security, Vol. 7, No. 1, pp. 284-291.