Secured Authentication of Node in Mobile Adhoc Network

Prabu S. [1,*], Alekhya A. [2], Kiran K. Chatragadda [3], Venkateswarlu Lingala [4]

[1]Department of Electronics and Communication Engineering, Mahendra Institute of Technology (Autonomous), Namakkal, India

[2, 3, 4] Department of Electrical and Electronics Engineering, QIS College of Engineering and Technology, Autonomous, India

Emails: drsprabu@ieee.org; alekhya.anumala@qiscet.edu.in; kiran.ch@qiscet.edu.in; venkat.l@qiscet.edu.in

Corresponding Author Mail: drsprabu@ieee.org

Abstract

Over the previous two decades, wireless communication has developed into an indispensable component of modern life. In recent years, wireless networks have acquired greater significance than wired networks as a result of improvements in technology as well as reductions in cost. The adaptability and portability of wireless devices make this feasible in a wide variety of real-time software applications. One kind of wireless network, known as an Adhoc network, can establish a connection in locations where conventional communication is not feasible. The Mobile Adhoc Network, also known as MANET, is a sort of ad hoc network that is established by the collection of mobile nodes that are each outfitted with a transceiver and interact with one another over duplex connections. Every node in a MANET functions as a router and figures out how to go from the source to the destination by going via the other nodes in the network. MANET has a number of properties, including changeable capacity and bandwidth, energy-restricted operation, speed of deployment, and dynamic topology. Because of MANET's inherent fluidity, the network is more prone to experiencing security breaches. In recent years, researchers have developed a number of solutions to security problems, including intrusion detection, routing, security protocol, and other techniques. These solutions have been made available. Even though there are a few different options to choose from, none of them are enough to safeguard the network nodes. When more nodes are added to the network while it is operating in a hostile environment, the overall performance of the network suffers. Secured Authentication with Node Isolation, often known as SAWNI, is an authentication method that aims to improve network safety by locating and isolating any hostile nodes that may be present in a network. The approach of isolation may be used to protect the ordinary node while isolating the malicious node either temporarily or permanently, depending on the situation. The network's legitimacy is improved as a result of this isolation mechanism, which takes into account the potential danger posed by the rogue node. The findings of the experiments reveal that using DHA, rather than DSA, may raise the PDR by 2% while using CBDS can increase it by 1% when there is a significant proportion of malicious nodes and the node mobility is less than 10 meters per second. When compared to DHA, the DHA-SHORT results in a 22% reduction in the delay. Finally, in comparison to DSA, SAWNI results in an increase of 8% in PDR, whereas CBDS sees an increase of 7% when there is a significant proportion of malicious nodes moving at less than 10 meters per second.

Keywords: Dual Hash Authentication; Mobile Adhoc Network; Optimized Routing Technique Routing; Secured Authentication Routing

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022

1. Introduction

This proposed work makes a proposal for a Dual Hash Authentication (DHA) [1] that can be used to ensure the safety of routing in mobile ad hoc networks. A comparison is also made between the proposed mechanism and other methods already in use, and the results obtained are plotted for a number of different parameters while malicious nodes are present. In this proposed work, a proposal and discussion are provided regarding the identification of malicious nodes through the use of a secured routing authentication. In a wireless setting, any nodes that are misbehaving will have their ability to participate in data transmission severely constrained. It is possible that this DHA will experience a significant degree of latency in the data transmission. DHA presents the delay combating Self Healing and Optimizing Routing Technique (SHORT) in order to get around the delay that it experiences. In addition, DHA and DHA-SHORT [2] are contrasted with the previously conducted research.

1.1 Dual Hash Authentication

This suggested technique includes the use of a hash chain for the purpose of authenticating the hop count of a Route Request (RREQ) and a Route Reply (RREP). [3] This is part of the methodology. It makes it possible for every node that receives the message, including an intermediate node and the node at the destination, to check that the hop count has not been reduced by an adversary in any way. A hash chain is created when a one-way hash function is applied many times in succession. Because a rogue node might relay a message without raising the hop count, the hop count authentication using a single hash chain is not foolproof. Because of this, the use of DHA is able to circumvent the limitations presented by single hash chain authentication. Instead of relying on digital signatures, the quick and efficient dual hash function is used to authenticate routing information. Assuming for the sake of argument that no two compromised nodes are working together and that they are not more than two hops apart from one another. In this dual hash authentication, one hash function is used to authenticate the routing packets that have been received, while another hash function is used to prevent the present nodes from changing the routing information themselves. [4] It is possible for a hacked node's surrounding nodes to instantly identify suspicious activity in the event that the routing information was altered. In the first stages of the process, each node will make use of the local node group in order to disseminate the common secret to the two hop node groups that it is connected to. In this, every node is tasked with disseminating a shared secret across the other nodes in its group of two hops. This secret key is guarded against its one-hop node group in order to maintain its secrecy. Private and public keys are associated with every node in the network (widely known). The source node creates a random key known as Ks and then encrypts it using the public keys of the nodes that are within two hops of it. After being given the key that has been encrypted, each node decrypts it using the private key that corresponds to it in order to get the shared secret key [5] Ks. Because of the mobility, the topology of an ad hoc network may vary, along with the organization of its local node group, and the distribution of the shared secret keys can be altered correspondingly. When some new nodes join the two-hop node group, the source node is required to distribute Ks to those new nodes. Additionally, if some nodes inside the two-hop become members of its one-hop node group (due to mobility), the source node is required to refresh and redistribute its Ks.

2. DHA Algorithm

The public one-way hash function H(.) is used to authenticate the RREQ twice, and thus, the routing packets carry not only the RREQ but also two hash values in addition to the RREQ (H1, H2). It is up to the H2 to determine whether or not the received routing packet has been altered, whereas it is up to the H1 to stop the present node from making any changes to the packet. The algorithm is described in the following way:

Step 1: Generate RREQ [6] from the source node using the following format: RREQ=S, L, H, R where S stands for "Source Identity."

L- Sequence number (RREQ) H - Count of hops

R - Information about routing

The second step is for the source to multicast S, L+1, H, R, H1, and 0 to its multicast group.

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022

When a source node multicasts an RREQ packet, two hash values, designated H1 and H2, are appended to the packet. In the beginning, the hash value H1 is produced, and the value of H2 is set to 0 (this is the case only when it is broadcast by the source node).

Step 3: Any intermediary node that is a part of this group is able to validate the legitimacy of a packet using H1 and H2 respectively.

H1=H (S\L+1\H\R\Ks)

The source identity, the sequence number, the hop count value, the routing information, and the secret key Ks are all included in H1.

Ks is an abbreviation for the secret key that is shared between the two hop nodes and the source node [7].

Step 4: Before forwarding the packet, the intermediate node will increase the hop count by 1, copy H1 to H2, and compute the new H1. In other words, H1 = H (SL+1H+1RKi); H2 = H (SL+1HRKs), where Ki is the common secret key that is shared across intermediate nodes.

Step 5: Send the routing packet with the freshly created hash values to the multicast group for which it was intended.

Step 6: Upon receiving the routing packet "SL+1H+1RH1H2," nodes inside the group may utilize "S," "L+1," "H+1," and "R" in conjunction with a public hash function to compute H(SL+1HRKs).

The seventh step is to compare this value with H2 and determine whether or not the routing packet has been changed by an intermediary node.

Step 8 requires that the H2 value be forged if the packet is modified by an intermediary node, which must be done before the packet may be sent.

The same approach may be used for RREP when going from the destination node back to the source node. Figure 3.1 presents a flow chart that depicts the DHA algorithm's processing steps. In the beginning, the Route Request [8] (RREQ) packet is generated by each node. For every packet that is created, the hash values H1 and H2 are combined together and then multicasted. After receiving a packet, every intermediary node does a check to ensure that it is legitimate. If the packet is confirmed, the hop count will be increased, and the packet will be broadcast; otherwise, the route request will be generated once again. Finally, examine the contents of the RREQ and H2 fields, and if either of them has been changed, signal that the source material has been modified. If neither of those fields has been changed, send the packet along until it reaches its destination.

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022

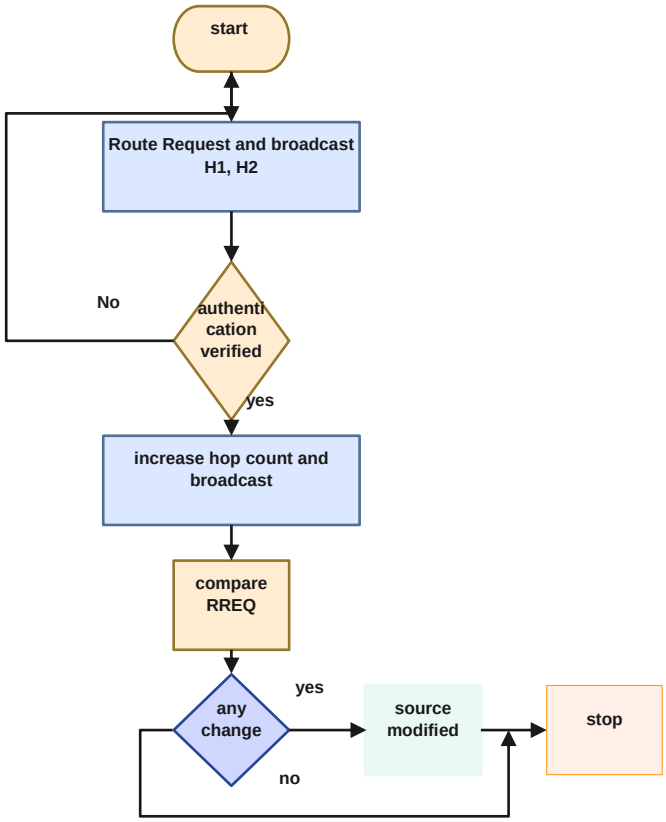

Figure 1: Flowchart of Dual Hash Authentication

On-demand routing techniques provide solutions that are both scalable and cost-effective for the process of routing packets in mobile wireless ad hoc networks. Due to a lack of information about the global topology and the mobility of nodes, the pathways that are created by these protocols may stray farther from the path that is considered to be the ideal path. The optimality of the network's routing has an impact on both its performance and its energy consumption, particularly when the load is high. This proposed work provides Self-Healing and Optimizing Routing Techniques (SHORT) for mobile Adhoc networks. [9] SHORT is for Self-Healing and Optimizing Routing Techniques. While the SHORT protocol is being used, all of the adjacent nodes keep an eye on the route and work to improve it if a more advantageous local sub-path becomes available. The SHORT improves performance in terms of bandwidth as well as latency without imposing a considerable extra financial burden on the user.

Scalability becomes a difficulty for the existing ad hoc routing protocols as the size of the network, as well as the average length of routes, continues to grow. Table-driven proactive routing methods call for periodic marketing and the widespread broadcast of connection information. These details are not appropriate for use in more extensive networks. When it comes to routing in bigger ad hoc networks, on-demand routing protocols are more effective because they automatically keep track of the routes that are immediately required and begin the process of path discovery whenever a route is required for the transmission of a message. This method has been implemented in a number of notable ad hoc routing protocols, the most notable of which are AODV [10] and DSR. When using AODV, the routing table at each node stores the information about the next hop router for a destination, and it uses this information for as long as the next hop router is still operational (originates or relays at least one packet for that destination within a specified time-out period). In order to cut down on the delay that is often experienced, DHA [11] makes use of the SHORT method.

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022

Take into consideration a situation in which there are six nodes in the network, numbered one through six and represented in Figure 6 along with some topology (an ad hoc network does not have a well-defined topology of its node mobility) [12].

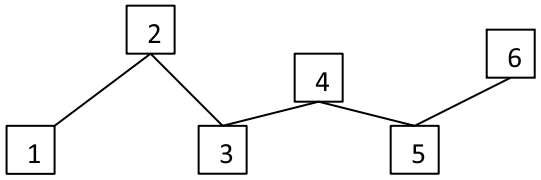

Figure 2: Routing Path

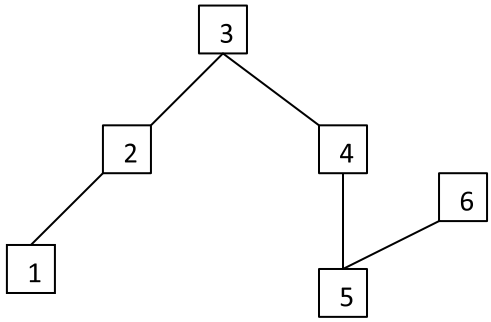

Figure 3: Path changes due to mobility

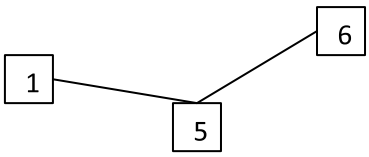

Figure 4: Shortest Path

Initial paths are discovered by the route discovery process from node 1 to node 6 in Figure 2 by passing through the intermediate nodes 2, 3, 4, and 5. The transmission of the packet from node 1 to node 6 involves a total of 5 hops. The mobility of a node will change over the course of time, which will ultimately result in a deviation from the original path, as depicted in Figure 3. When compared to Figure 4, the amount of delay experienced from node 1 all the way to node 6 is significantly higher. The shortest path algorithm is required in order to reduce the delay that is caused by the mobility of the nodes.

3. Experimental Results and Analysis

The Network Simulator (NSv2.28) [13] tool is used in order to implement the proposed DHA algorithm, and it is configured with the following parameters, which can be found in Table 1. For the simulation's network traffic, the Constant Bit Rate (CBR) [14] and User Datagram Protocol (UDP) are the protocols that are used.

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022

Table 1: Simulation setup

Parameters	Values
Application Traffic	CBR(UDP)
Transmission Range	250m
MAC	IEEE 802.11
Packet Size	512 bytes
Channel data rate	2 Mbps
Pause time	0.6s
Maximum speed	10m/s & 20m/s
Simulation time	200s
Number of nodes	1 to 70
Area	1600m x1000 m
Malicious nodes	1 to 7
Routing Protocol	AODV

Different graphs are plotted for the values that are obtained from the simulation, and these graphs are based on the input parameters. The plot of the Packet Delivery Ratio (PDR) versus the number of nodes is displayed in Figure 5. In this case, a maximum of 70 nodes are taken into consideration, and the pause time is 0.6 seconds. The result demonstrates that the PDR [15] of nodes decreases when there is an increase in the number of malicious nodes. The percentage of 10% of the total number of nodes is calculated taking into account the number of malicious nodes. Both the existing algorithm and the proposed algorithm have a nearly identical amount of packet delivery ratio with one node acting as an intruder in the beginning, when the number of nodes is at its smallest. At the same time, the PDR for DSA and CBDS falls by a significant amount whenever the number of nodes increases in proportion to the increase in the intruder. The proposed DHA performs better than both the DSA and CBDS that are currently in use. When the PDR falls below 80%, the simulation will immediately put a stop to the increase in the number of intruders

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022

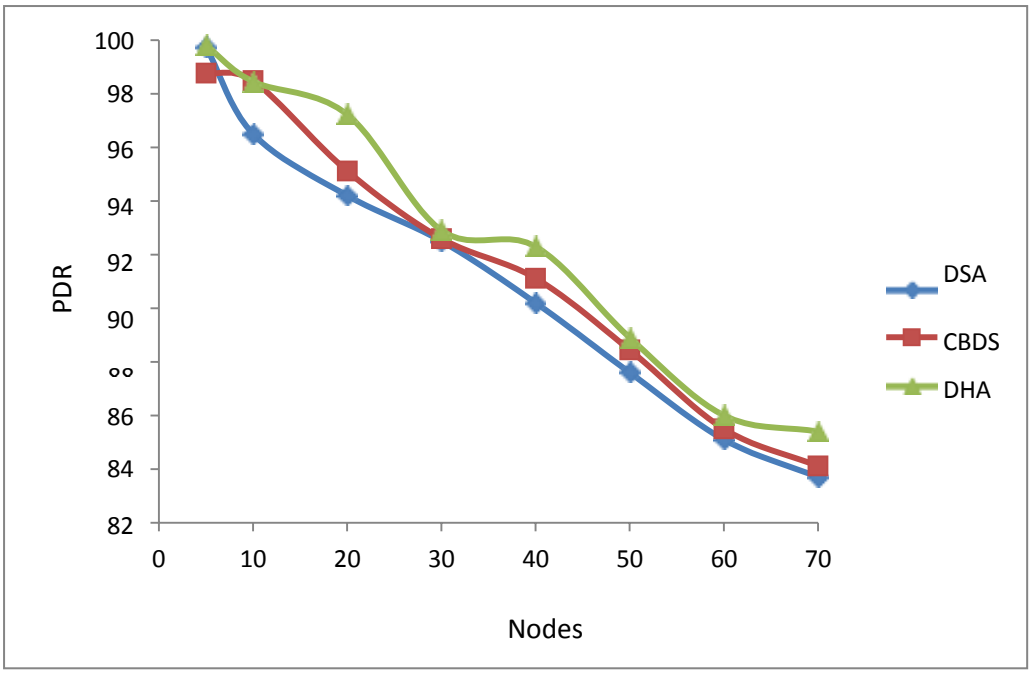

Figure 5: PDR Vs Nodes

Table 2 shows the PDR comparison of the proposed DHA with the existing DSA and CBDS methods.

Table 2: Comparison of PDR and nodes for DSA, CBDS, and DHA

Nodes	PDR		
	DSA	CBDS	DHA
5	99.75	98.77	99.8
10	96.5	98.49	98.45
20	94.2	95.12	97.23
30	92.5	92.6	94.9
40	90.2	91.12	92.3
50	87.6	88.45	88.9
60	85.1	85.5	86
70	87	84.12	85.4

The comparison of throughput and the number of nodes for the existing DSA, CBDS, and proposed DHA methods is shown in Figure 6.

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022

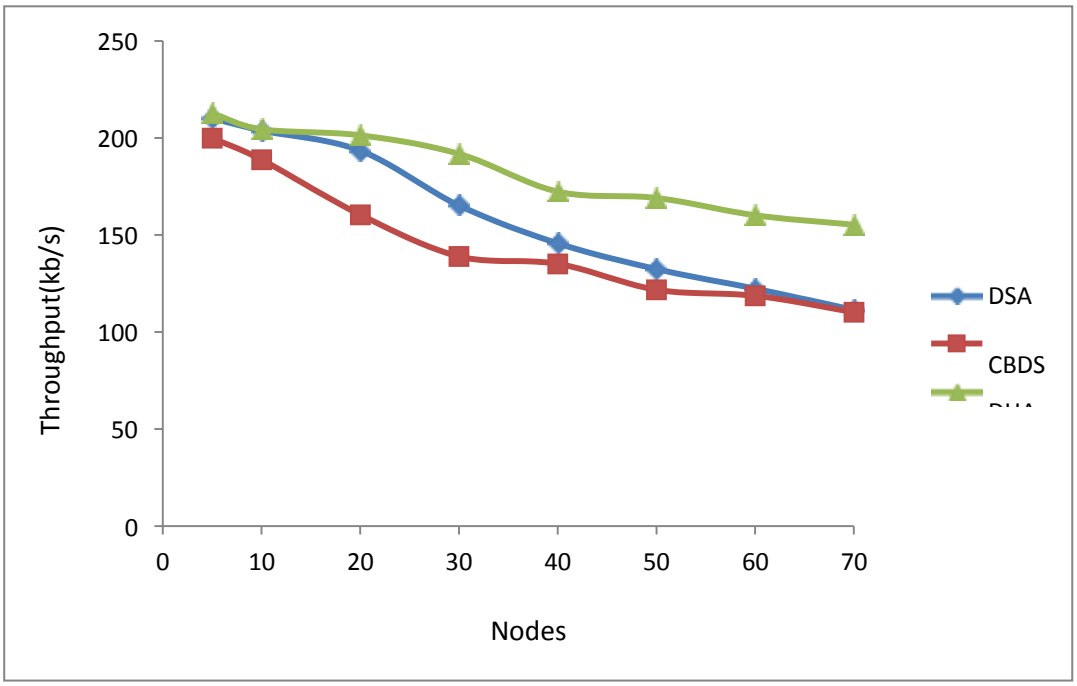

Figure 6: Throughput Vs Nodes

The throughput increases for DHA as the number of malicious nodes increases when compared with DSA and CBDS. DSA and DHA [16] provide better security and throughput when compared to CBDS with an almost minimal number of nodes. The variation in the throughput occurs when the regular nodes and malicious nodes increase due to mobility. Table 3 shows the throughput comparison of existing DSA, CBDS, and proposed DHA method.

Table 3: Comparison of throughput and nodes for DSA, CBDS, and DHA

Nodes	Throughput		
	CBDS	DSA	DHA
5	199.94	210.12	212.81
10	188.78	203.81	204.51
20	160.42	193.45	201.42
30	138.95	165.2	191.85
40	135.13	145.71	172.39
50	121.75	132.41	169.15
60	118.67	122.32	160.21
70	110.23	111.43	155.34

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022

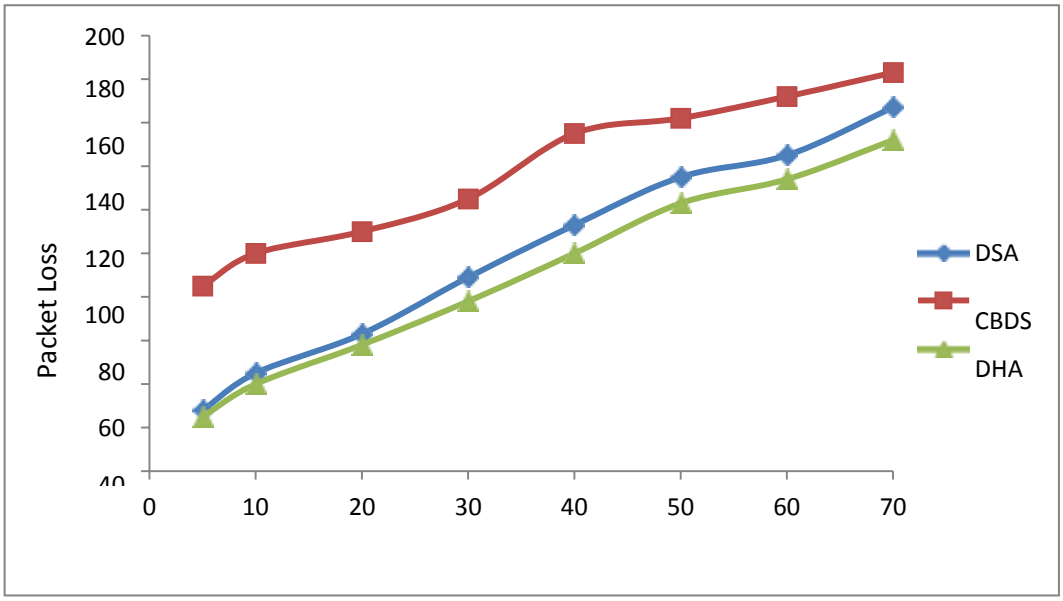

Figure 7: Packet Loss Vs Nodes

The packet loss decreases for DHA as the number of nodes increases when compared with the DSA and CDBS as shown in Figure 7. Conventional packet loss increases when the number of regular and malicious nodes increases [17]. The authentication mechanism of DHA decreases the packet loss when compared with DSA and CBDS and the comparison for DSA, CBDS, and DHA is shown in Table 4.

Table 4: Comparison of Packet Loss and nodes for DSA, CBDS, and DHA

Nodes	Packet Loss		
	DSA	CBDS	DHA
5	28	85	25
10	45	100	40
20	63	110	58
30	89	125	78
40	113	155	100
50	135	162	123
60	145	172	134
70	167	183	152

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022

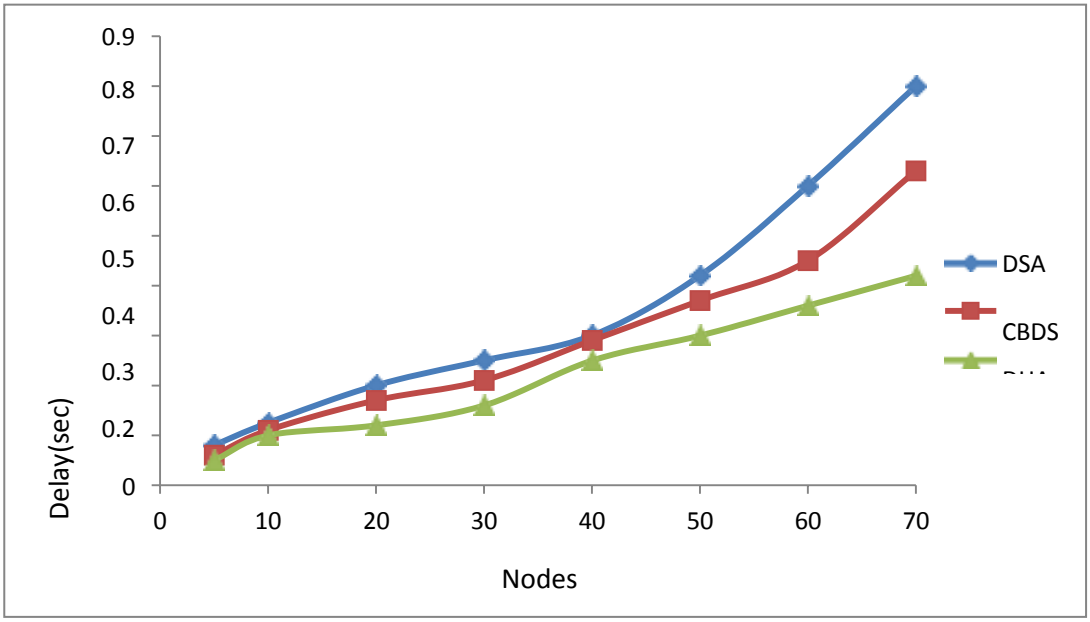

Figure 8: Delay Vs Nodes

The increase in delay for DHA is considerably less when compared to DSA and CBDS as shown in Figure 8. The increase in the delay is due to the increase in the number of nodes and it has to be brought down. So a delay-efficient algorithm has to be incorporated to encounter the significant delay. Even though DHA has a small delay variation with DSA and CBDS, it has to be reduced with a delay-efficient algorithm. The comparison of delay for DSA, CBDS, and DHA is shown in Table 5

Table 5: Comparison of Delay and nodes for DSA, CBDS, and DHA

Nodes	Delay		
	DSA	CBDS	DHA
5	0.08	0.06	0.05
10	0.125	0.11	0.1
20	0.2	0.17	0.12
30	0.25	0.21	0.16
40	0.3	0.29	0.25
50	0.42	0.37	0.3
60	0.6	0.45	0.36
70	0.8	0.63	0.42

4. Conclusion

DHA, which stands for the Secured Routing Authentication Algorithm, was designed, and NS2.28 was used to run a simulation of the performance study. Based on the findings, it is clear that the proposed DHA offers superior protection against harmful behavior shown by normal nodes. The

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022

latency that is experienced as the number of nodes rises is significant, despite the fact that it offers superior security than the systems that are now in use. The DHA-SHORT protocol was added both to cut down on the wait time and to give a considerable equivalent degree of protection. The performance result compares both approaches by analyzing their PDR, throughput, packet loss, and latency. The comparative findings demonstrated that our study is effective in moving MANET in the direction of secured authentication.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Wald, L. (1999). Some terms of reference in the Internet of Things. *IEEE Transactions on geoscience and remote sensing*, *37*(3), 1190-1193.

[2] S. Jafar Ali Ibrahim and Thangamani, M "Proliferators and Inhibitors Of Hepatocellular Ca," Sonoma," International Journal of Pure and Applied Mathematics (IJPAM) Special Issue of Mathematical Modelling of Engineering Problems Vol 119 Issue. 15. July 2018 ISSN 1311-8080, https://acadpubl.eu/hub/2018-119-16/1/94.pdf

[3] S. Idowu, "Customer Segmentation Based on RFM Model Using K-Means, Hierarchical and Fuzzy C- Means Clustering Algorithms," no. August 2019, 2020, doi: 10.13140/RG.2.2.15379.71201.
Probl. Eng., vol. 2020, no. November 2017, 2020, doi:

[4] Meng, T., Jing, X., Yan, Z., & Pedrycz, W. (2020). A survey on machine learning for the Internet of Things. *Information Fusion*, *57*, 115-129.

[5] Khaleghi, B., Khamis, A., Karray, F. O., & Razavi, S. N. (2013). Multisensor Internet of Things: A review of the state-of-the-art. *Information fusion*, *14*(1), 28-44.

[6] J. Wu *et al.*, "An Empirical Study on Customer Segmentation by Purchase Behaviors Using an RFM Model and K -Means Algorithm," *Math.*

[7] Ibrahim, S. Jafar Ali, and M. Thangamani. "Prediction of Novel Drugs and Diseases for Hepatocellular Carcinoma Based on Multi-Source Simulated Annealing Based Random Walk." Journal of medical systems 42, no. 10 (2018): 188. https://doi.org/10.1007/s10916-018-1038-y

[8] Hall, D. L., & Llinas, J. (1997). An introduction to multisensor Internet of Things. *Proceedings of the IEEE*, *85*(1), 6-23.

[9] Elhadi M Shakshuki, Nan Kang & Tarek R Sheltami 2013, _EAACK— A Secure Intrusion-Detection System for MANETs', IEEE Transactions on Industrial Electronics, vol. 60, no. 3, pp. 1089-1098.

[10] Dube, Rais, CD, Wang, KY & Tripathi, SK 1997, _Signal stability based adaptive routing (SSA) for Ad-hoc mobile networks', IEEE personal communications, pp. 36-45.

[11] Castanedo, F. (2013). A review of Internet of Things techniques. *The scientific world journal*, *2013*.

[12] C. Pascal, S. Ozuomba, and C. kalu, "Application of K-Means Algorithm for Efficient Customer Segmentation: A Strategy for Targeted Customer Services," *Int. J. Adv. Res. Artif. Intell.*, vol. 4, no. 10, pp. 40–44, 2015, doi: 10.14569/ijarai.2015.041007.

[13] Bleiholder, J., & Naumann, F. (2009). Internet of Things. *ACM computing surveys (CSUR)*, *41*(1), 1-41.

[14] Bhaumik A Patel & Hitesh Ishwardas, 2013, _Improvement in Routing for MANET using Double Signature Security Scheme', Indian Journal of Research- Paripex, vol. 3, no. 4, pp. 150-152. 11. Chakravarti, S & Mishra, A 2001, _QoS issues in Adhoc wireless networks', IEEE Communication Magazine, vol. 39, pp. 142−148.

[15] Bar-Shalom, Y., Willett, P. K., & Tian, X. (2011). *Tracking and Internet of Things* (Vol. 11). Storrs, CT, USA:: YBS publishing.

[16] A. M. A. Zamil and T. G. Vasista, "Customer Segmentation Using RFM Analysis: Realizing Through Python Implementation," *Pacific Bus. Rev. Int.*, vol. 13, no. 11, pp. 24-36 WE-Emerging Sources Citation Index (ESCI), 2021. doi: 10.1155/2020/8884227.

Doi: https://doi.org/10.54216/IJWAC.050202
Received: March 19, 2022 Accepted: October 25, 2022