Journal of Theoretical and Applied Information Technology
15th April 2024. Vol.102. No 7
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DESIGN AND EVOLUTION OF MAC ALGORITHM BASED STRATEGY TO MITIGATE BLACK HOLE ATTACKS IN WIRELESS SENSOR NETWORK

SUBHRA PROSUN PAUL[1], D. VETRITHANGAM[2], G. KRISHNA MOHAN[3], THIYAGU. T[4], SUBRAMANIAN SELVAKUMAR[5], M. MAITHILI SAISREE[6], NIMMAGADDA CHANDRA SEKHAR[7]

[1]Research Scholar, Chandigarh University, Department of CSE, Punjab, India
[2]Professor, Chandigarh University, Department of CSE, Punjab, India
[3]Professor, Koneru Lakhmaiah Education Foundation, Department of Computer Science and Engineering, Andhra Pradesh, India
[4]Assistant Professor, Madanapalle Institute of Technology & Science, Department of Computer Science and Engineering (Cyber Security), Andhra Pradesh, India
[5]Professor, Bahir Dar Institute of Technology, Department of Electrical & Computer Engineering, Ethiopia
[6]Assistant Professor, R.V.R & J.C College of Engineering, Department of Computer Science and Engineering, Andhra Pradesh, India
[7]Assistant Professor, R.V.R & J.C College of Engineering, Department of Computer Science and Engineering, Andhra Pradesh, India
E-mail: [1]subhra.phd.cu2021@gmail.com, [2]vetrigold@gmail.com, [3]gvlkm@kluniversity.in, [4]thiyagu.57@gmail.com, [5]sscseau9@gmail.com, [6]mvsaisree@gmail.com, [7]nimmagadda65@gmail.com

ABSTRACT

Despite tremendous advances in successful packet transmission in the current context of technological progress on wireless networks, network security remains an unavoidable issue in this field due to various wireless network attacks. A black hole attack is one of the most crucial threats to wireless network security. In a black hole attack, a malevolent node announces openly about the availability of the shortest route throughout the wireless network, which is totally false. Whenever a participating node forwards its packet to that malevolent node, the packets are dropped. In order to provide high-level security during packet transmission throughout the sensor network, a strong threat handling mechanism is required. In this research paper, the problem statement is to introduce the MAC algorithm-based black hole attack avoidance mechanisms, where a shareable secret key concept is used during the packet transmission process throughout the network. The proposed technique's algorithm, as well as the mathematical explanation and how the MAC algorithm is implemented, are thoroughly discussed in this paper. Using MATLAB software, the proposed algorithm is simulated, the shortest paths are identified, and the shortest path distance and time are calculated as simulation results. Furthermore, by providing a comparative analysis in this article, we have attempted to identify the clear differences between our proposed mechanisms and the existing techniques in this field.

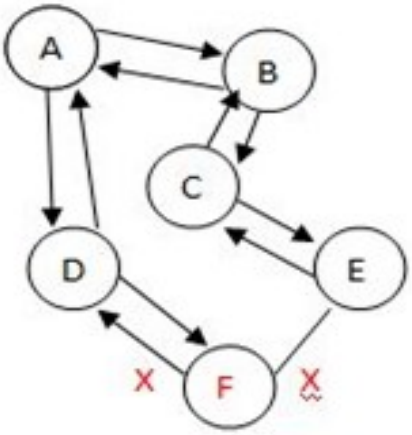
Keywords: *Black Hole Attack, MAC Algorithm, Wireless Sensor Network, Design, Detection, Security, Routing System*

1. INTRODUCTION

In the twenty-first century of the technological world, wireless sensor network (WSN) has versatile application area like telecommunication, agriculture, healthcare, road traffic control, entertainment and so on. It is a promising technique in the modern technological world. An infrastructure-free wireless network called a Wireless Sensor Network (WSN) is set up ad hoc using a large number of wireless sensors to monitor environmental, physical, and system variables. In wireless sensor networks (WSN), various types of attacks exist, such as Daniel of Service (DOS), Distributed Daniel of Service (DDOS), Wormhole, Hello Flood, Sybil, Tempering Attack, and so on [1]. A black hole (BH) attack is one of them and is the utmost commonly faced in sensor networks [2]. In this attack, a particular node removes all packets, though it is considered to forward those packets to

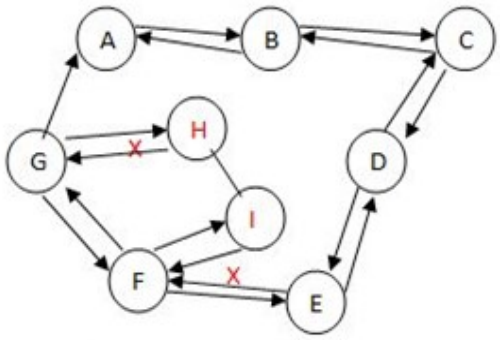
Journal of Theoretical and Applied Information Technology
15th April 2024. Vol.102. No 7
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the neighboring node [3]. It is a type of Daniel of service threat in which one or more corrupted nodes act as if they have an effective route to deliver the packet falsely by acknowledging the packet-sending nodes [4]. As a consequence, the entire received packets are absorbed by this malicious node without being transferred to the sink. In WSN, there are two categories of black hole attack (BHA): single BH and cooperative BH [5]. It can be mentioned here that there is a remarkable difference between a BH attack and a grey hole attack. In a BHA, all the received packets are discarded by the BH node, but in a grey hole attack, packets are dropped at a specific frequency [6]. But there is no doubt today that this type of attack is really a significant threat to network security [7]. There are many types of black hole attack handling mechanism have been proposed in the existing research work. In this paper we have introduced the MAC algorithm technique regarding this field. The integrity and validity of a communication may be verified using cryptographic methods called MAC algorithms. The recipient uses the same algorithm and a shared secret key to validate the tag that these methods create, which is added to a message.



Single Black Hole Attack

In figure 1, a single BHA attack and a cooperative BHA are shown. In a single BHA, node F is the black hole node, whereas in a cooperative BHA, node H and node I are the BH nodes. BHA can be categorized into three types depending on their functionalities: active, passive, and common [8]. In this research paper, we have introduced a MAC algorithm-based BHA avoidance method for secure data transmission in WSN, as well as some suggestions to prevent this type of attack in this network [9].



Cooperative Black Hole Attack

Figure 1: Single BHA vs. Cooperative BHA

Security is a vital issue in WSN. In this security analysis, out of various types of attacks, BHA is the furthermost common and frequently occurring in this type of network. Although some algorithms exist to handle this attack, security and authenticity are not ensured by them. The main problem is the reliability of the technique. In our proposed technique, we have implemented the MAC algorithm to confirm the security of the system. To evade the black hole node, all the routes are designed and the shortest route is identified in this proposed technique. In the background study part, some theoretical concepts about black hole attacks and the MAC algorithm are discussed. Related, effective literature reviews are done in the literature genesis overview part. The MAC algorithm-based black hole attack avoidance technique is proposed in the proposal and algorithm section. In the analysis and discussion section, the introduced algorithm is discussed mathematically and evaluated properly. In the simulation and results part, the algorithm is simulated by MATLAB software, the shortest path is discovered, and their distance and time are determined as simulation results. In the comparative analysis section, a vibrant difference between our contribution and existing research work in this field is mentioned. Some limitations of our research work and how they can be handled in the future are mentioned in the challenges and further research part.

1.1 Objectives of the Research Work

The objective of this paper is to identify an effective and efficienct method of BHA avoidance

system in WSN. In order to do that MAC algorithm is introduced. The second objective is to implement the proposed mechanism mathematically and to simulate by simulation software efficiently. The third objective is to compare our proposed mechanisim with existing introduced method to justify our method.

1.2 Research Contribution

The contribution of this paper is explained in the following order: The theoretical concept and relevant technical discussion of the key term of this paper like WSN, BHA, MAC algorithm are provided in the introduction section. The background study section provides the technical backgroud of BHA in WSN field. In the section 3, existing research work on this area are ellaborated very effectively. Our introduced MAC algorithm based BHA avoidance technique is discussed in the section 4. Section 5 explains the mathematical discussion of the proposed scheme. The software simulation process is represented in section 6. Section 7 provides the significant differences between our proposed scheme and existing research work on this field. Section 8 explains some limitation and futher research scope of our proposed scheme. In the conclusion section, we have tried to justify our proposed scheme in this area.

2. BACKGROUND STUDY

A BHA field is such a region where arriving and departing traffic is silently discarded without reporting to the source node the data packet's failure to reach the correct destination [10]. In the current world, cyber security and, more specifically, ethical hacking field black hole attacks are handled very effectively [11]. Filtering is one of the most important functions related to the BHA in a WSN routing technique to ensure maximum security [12]. One type of filtering function is content filtering, in which packets are checked to see if they are malicious or genuine, and if they are, they are allowed to be forwarded [12]. Basically, black hole filtering is a comparatively cheaper technique to keep corporate data secured, and it can also remove attacks from data that is leaving the specified sensor network [13]. This filtering technique blocks information that is leaving the sensor network. Prevention, detection, and response are all prerequisites to handling BHA effectively in WSN [14].

In the security analysis field, BHA is the active attack that occurs in the routing process [15]. Basically, in WSN, the black hole area is the entrance position for other attacks [16]. Presently, black hole attacks are implemented for commercial purposes as well [17]. For example, if we want to stop unexpected traffic from entering our own network, we can install a black hole node with the help of our ISP [18]. In general, we have to wait and verify the replies from all the adjacent nodes to identify a secure path for decreasing the possibility of a BHA in WSN [19]. On the other hand, message authentication is a technique that is used to check any message's integrity with the help of a secret key [20]. Basically, the message authentication code (MAC) technique is nothing but a system that takes messages of different sizes and a secret key as input to generate authentication code and, at the same time, produce authentication code to check the message integrity [21].

3. OUTCOME OF THE LITERATURE GENESIS OVERVIEW

Using Google scholar database, we have reviewed several significant research articles to analyze the research on detection, prevention, and avoidance of BHA in WSN [22, 23]. Research shows that because of the restricted resources of WSN, a hidden Markov model-based mechanism is introduced to find false nodes in black hole attacks, which not only prevents this attack but also helps to search the shortest path in the specified network [24, 25]. Another study proposed a hierarchical security-based routing technique for identification and fighting against black hole attacks using a symmetric key cryptosystem that discovers a secure path [26, 27]. To guard the sensor network from this black hole attack, an energy-efficient hierarchical-based intrusion detection process is explained in another research paper [28, 29]. A number of base station-oriented networking concepts that are used to calculate the consequence of BH nodes on data transmission systems are explained [30]. Reliability analysis is an effective technique that can eliminate the limitations of cooperative black hole attacks with the help of the AODV routing system [31, 32]. Existing research is also implemented to overcome the restrictions of mobile ad-hoc networks in terms of BHA handling [33, 34]. We have seen that the consequences of the black hole threat are calculated carefully, and cluster-based recognition and deterrence mechanisms to handle them in wireless networks are proposed in a research paper [35]. Research also

effectively reviews the existing proposed black hole attack identification and handling mechanisms and shows the merits and demerits of several proposed methods [36, 37].

From a thorough literature review in this area, some remarkable gaps, like security and reliability, are identified in BHA exposure and avoidance techniques in WSN. In our proposed algorithm, we have used the MAC algorithm to provide security and node authenticity.

4. PROPOSED MAC ALGORITHM BASED BLACK HOLE ATTACK AVOIDANCE TECHNIQUE

The MAC algorithm is a cryptographic technique controlled by a symmetric key. In this algorithm, every function can perform on input data (messages) of different sizes to generate output data of a fixed length. A secret key is shared with both the authenticated sender and recipient. Hash function, stream cipher, and block cypher-oriented MAC is the various types of this algorithm. Data integrity is the key advantage of this algorithm. The key idea of this algorithm is that, using this shared secret key, both sender and receiver will generate MAC codes and compare them with each other. If the sender MAC value does not match with the receiver MAC value, then the message will not be transmitted accurately. Now, using this key concept of the MAC algorithm, BH detection and avoidance methods in WSN are introduced in this article.

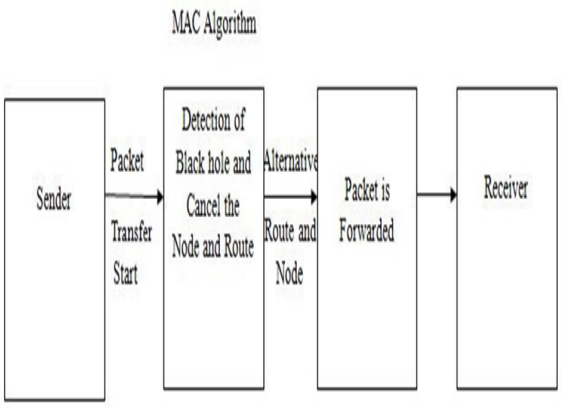


Figure 2: Block Diagram of Proposed MAC Algorithm Based Black Hole Node Detection

4.1 Algorithm

Following is the step by step algorithmic process of MAC algorithm based technique:

1. Construct the sensor network with N nodes.
2. Every node will be assigned a priority number, where a higher value indicates more priority and a lower value indicates less priority.
3. Declare node S as a introductory node and node D as a terminal node.
4. Declare K as a shared secret key.
5. Share the secret key K among all authenticated nodes across the network.
6. Declare a number of nodes (for cooperative BHA) as a black hole node or a node (for a single BHA) as a black hole node.
7. Source node S will send a route request (RREQ) into the network.
8. The closest nodes (in terms of distance) will send a route reply (RREP) to send a packet as if these were the closest nodes and have the shortest route to reach sink node D.
9. With secret key K and the MAC algorithm, source node S will broadcast packets in the network.
10. The sender generates a MAC value using the MAC algorithm and secret key K, and using only the algorithm, the sender creates the compressed message of a fixed length.
11. While the authenticated receiver is receiving the compressed message and MAC value, receiver will produce a MAC value using the shared secret key and MAC algorithm.
12. The receiver will compare the sender's MAC value with the receiver's MAC value [Because black hole nodes are not authenticated the secret shared key K will not be distributed to the black hole node. Consequently, there is no question of producing a MAC value by the black hole node]
13. If both (sender and receiver) MAC values are the same, the receiving node will be identified to receive the message (packet) and transfer packet to the subsequent node for transmission.
14. If more than one node is found to have the same MAC value, the shortest path algorithm will be implemented to forward packets to the sink node.
15. All nodes will have their adjacent node distance calculated, and the shortest distance relevant node M is selected to forward the packet for transmission.

5. ANALYSIS AND DISCUSSIONS

To ensure the authenticity of messages, we have used the MAC algorithm concept in BHA identification and avoidance mechanisms. In the following figure: 3, a logical wireless sensor network of 14 (N = 14) nodes is designed, where S is the starting node and D is the destination node. X and Y nodes are declared black hole nodes, and all other nodes remaining are safe participating nodes. Initially, source node S has begun sending the route

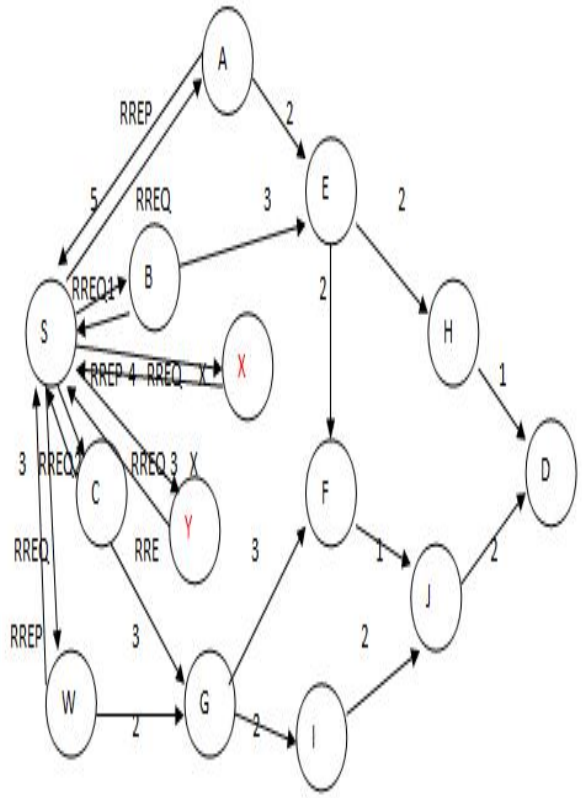


Figure 3: BHA in WSN

requests (RREQ) to all adjacent nodes A, B, C, W, X, and Y. After that, nodes A, B, C, W, X, and Y are sending route replies (RREP) as if they have the shortest path to transfer packets to the terminal node. As X and Y nodes are black hole nodes, though they send route replies (RREP), they cannot receive any messages due to the implementation of the MAC algorithm in this process. Nodes X and Y will be rendered ineffective. When the source node starts broadcasting messages, they will be automatically ignored as they (X and Y nodes) don't have any shared secret key. If only one node exists to send a route reply (RREP) and the MAC algorithm conditions are satisfied, then that node will receive the message and forward the packet to the destination node. But if more than one node exists to receive packets, then the shortest path algorithm will be implemented. Out of several nodes, which node has the shortest distance to reach the sink node, that node will receive the message and forward it to the sink node.

5.1 MAC Algorithm Implementation

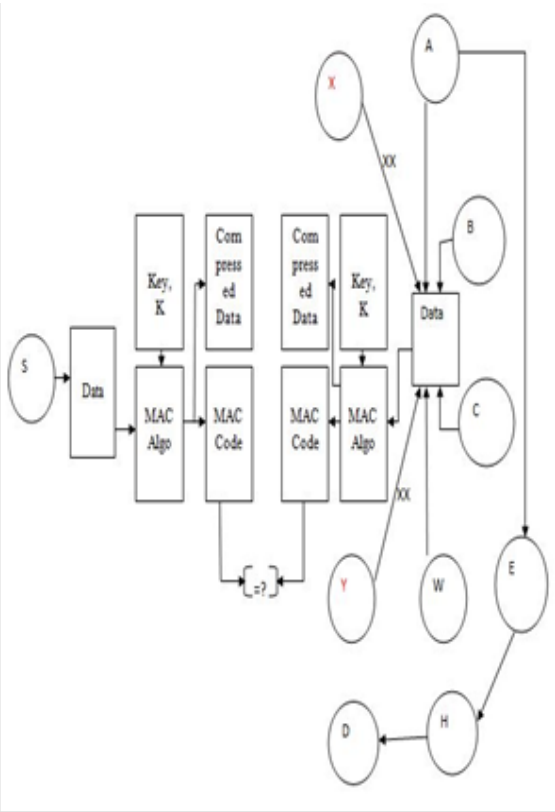


Figure 4: MAC Algorithm Based BHA Detection and Avoidance

Figure 4 is drawn from Figure 3. In figure 4, sender node S broadcasts data. The sender generates MAC code with the help of the secret shared key K and the MAC algorithm, and the MAC algorithm generates a compressed message on the sender's side. For example, in the following figure 4, as there are four adjacent nodes (A, B, C, and W) of source node S, after receiving the compressed message, all these nodes will produce their corresponding MAC code. Now all these MAC codes will be compared with the source node's S MAC code. If they are equal, the shortest path

algorithm will be implemented to find the shortest route for the node. Here, after calculation, it is observed that node A has the shortest route to transfer packets to the sink node. So, node A will forward the packet (data) to the sink node D.

5.2 Mathematical Explanation

Followings are the mathematical procedure of implementing MAC algorithm to avoid BHA in WSN:

Followings In this sensor network, no of node, N = 14, N = {S, A, B, C, W, E, F, G, H, I, J, X, Y, D}

Initialize priority number of the node as S=12, A=11, B= 10, C=9, W=8, E=7, F=6, G=5, H=4, I=3, J=2, and D=1.

Source Node = S, Destination Node = D;

Black Hole Node = {X, Y}

Safe/ Participating Node = {S, A, B, C, W, E, F, G, H, I, J, D}

Initially, S sends Route Request (RREQ) in the network.

Now adjacent node A, B, C, W, X, and Y send Route Response (RREP),

Node S, now broadcast message throughout the network,

Secret key K is shared among the authenticated all node of this network.

Using MAC algorithm and shared secret key, compressed message and MAC code will be generated on both sender and receiver side,

Compressed message and MAC code will be received by node A, B, C, and W as they are safe,

Node X and Y cannot receive the MAC code and compressed message as they are black hole node, As a result, these nodes will be avoided.

Now we compare if (sender MAC code = Receiver MAC code)?

If yes, message= Receiver node [then message will be received by corresponding receiver]

If no, message will be discarded.

If matching MAC code holder no. of node > 1

Suppose in this figure. 4, node A, B, C, and W MAC code are same as S node MAC code,

Now, according to shortest path algorithm,

Total route cost from A to D = 2 +2+1 = 5 [A to E, E to H, H to D]

Total route cost from B to D = 3 + 2 + 1 = 6 [B to E, E to H, H to D] or

Or = 3 + 2 + 1 + 2 + 1= 6 [B to E, E to F, F to J, J to D]

Total route cost from C to D = 3 + 3 + 1 + 2 = 9 [C to G, G to F, F to J, J to D]

Or = 3 + 2 + 2 + 2 = 9 [C to G, G to I, I to J, J to D]

Total route cost from W to D = 2 + 3 +1 + 2= 8 [W to G, G to F, F to J, J to D]

Or = 2 + 2 + 2 + 2 = 8 [W to G, G to I, I to J, J to D]

From the above calculation, it is clear that the total route cost from A to D is the shortest distance, which is 5.

So Node A will forward packets to Sink Node D.

If the cost of more than one node route is the same, the node with the highest priority will be chosen. A higher priority number node will be selected first, and a lower priority number node will be selected later.

6. SIMULATION AND RESULTS

We have implemented our proposed algorithm using MATLAB software. In order to transfer one-bit data, we have tried to find all possible routes. Initially, MAC addresses are distributed to all participating nodes throughout the network. Software has compared the MAC

addresses with each other. As the BH node has no MAC address, after comparison of each node with the BH node, the route participation BH node is automatically discarded. Except for the BH node route, all remaining possible routes are calculated, and then among those all routes, the shortest route is determined according to our proposed algorithm. We have considered five (05) iterations, i.e., we have checked five times to calculate the shortest path.

Parameter Consideration:
Here,
No. of nodes in the network = 50,
Source node = 1,
Destination Node = 50,
Number of black hole node = randomly declared,
Distance range of each node = 250 meter

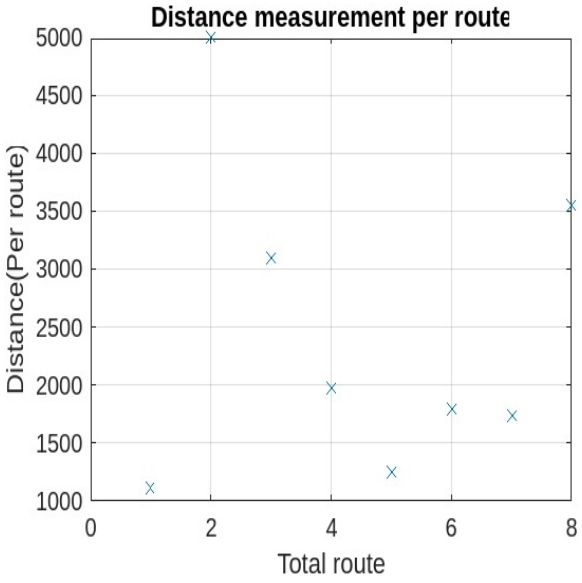


Figure 5: Iteration-1

In this figure 5, the X axis signifies the route quantity, and the Y axis signifies distance in meters. According to this figure, route 1 covers 1106.6 meter, route 2 covers 5000 meter, route 3 covers 3100 meter, route 4 covers 2000 meter, route 5 covers 1250 meter, route 6 covers 1750 meter, route 7 covers 1700 meter, and route 8 covers 3600 meter.

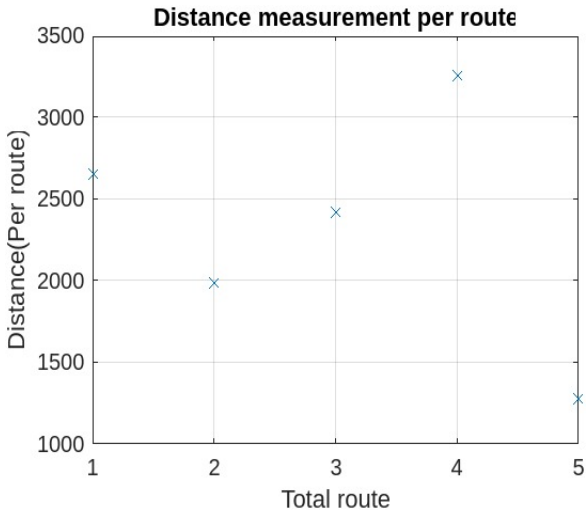


Figure 6: Iteration-2

In this figure 6, the X axis characterizes the number of routes, and the Y axis characterizes distance in meters. According to this figure, route 1 covers 2650 meter, route 2 covers 2000 meter, route 3 covers 2400 meter, route 4 covers 3250 meter, and route 5 covers 1271.6 meter.

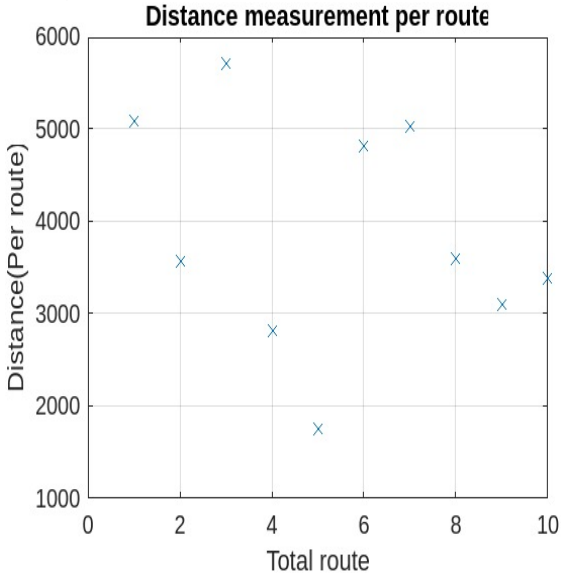


Figure 7: Iteration-3

In this figure 7, X axis symbolizes the number of route and Y axis symbolizes distance in meter. According to this figure, route 1 covers 5100 meter, route 2 covers 3300 meter, route 3 covers 5800 meter, route 4 covers 2900 meter, route 5 covers 1743.1 meter, route 6 covers 4900 meter, route 7 covers 5000 meter, route 8 covers 3600 meter, route 9 covers 3100 meter, and route 10 covers 3300 meter.

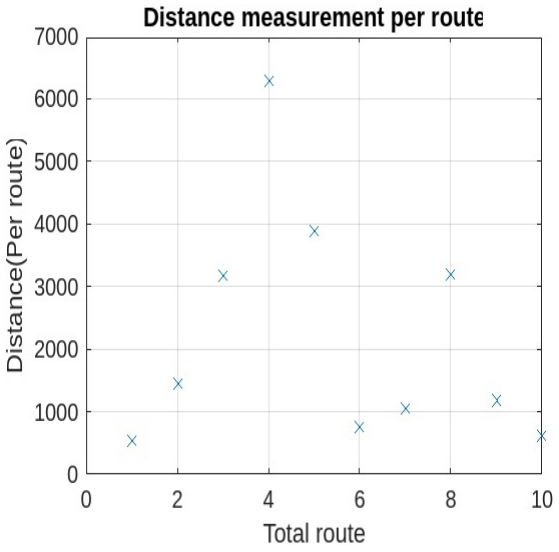


Figure 8: Iteration-4

In this figure 8, X axis exemplifies the number of route and Y axis exemplifies distance in meter. According to this figure, route 1 covers 528 meter, route 2 covers 1500 meter, route 3 covers 3200 meter, route 4 covers 6300 meter, route 5 covers 4950 meter, route 6 covers 850 meter, route 7 covers 1073 meter, route 8 covers 3211 meter, route 9 covers 1189 meter, and route 10 covers 718 meter.

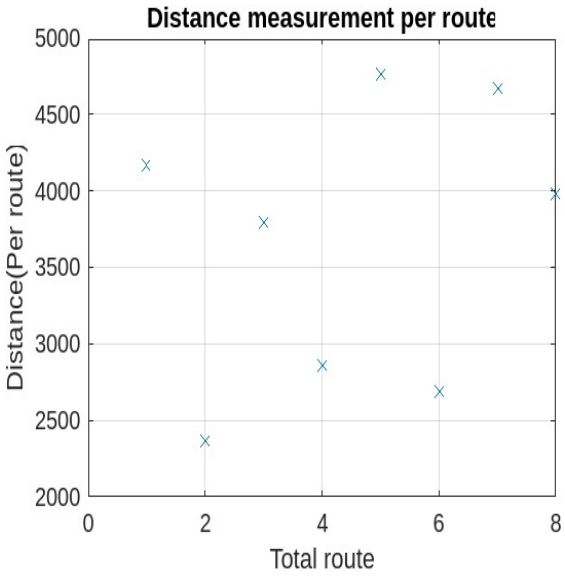


Figure 9: Iteration-5

In this figure 9, X axis exemplifies the number of route and Y axis exemplifies distance in meter. According to this figure, route 1 covers 4389 meter, route 2 covers 2360 meter, route 3 covers 3677 meter, route 4 covers 2894 meter, route 5 covers 4812 meter, route 6 covers 2696 meter, route 7 covers 4702 meter, route 8 covers 4067meter.

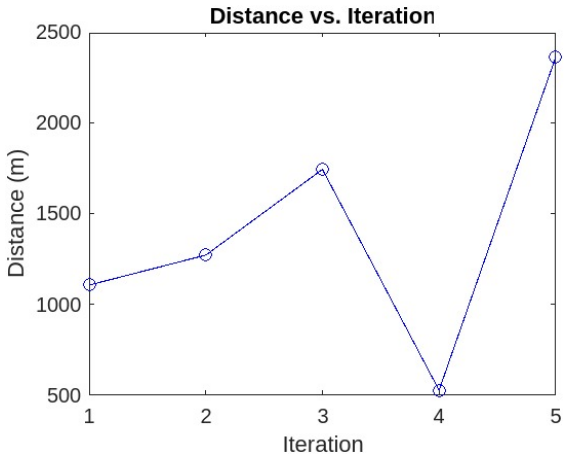


Figure 10: Minimum Distance (meter) vs. Iteration Quantity

In this figure 10, the X axis symbolizes the number of iterations, and the Y axis symbolizes the minimum distance in meters for each iteration. For example, according to this figure (10), 1106 6 meters is the minimum distance that is the shortest path for iteration 1, which is covered by route 1.

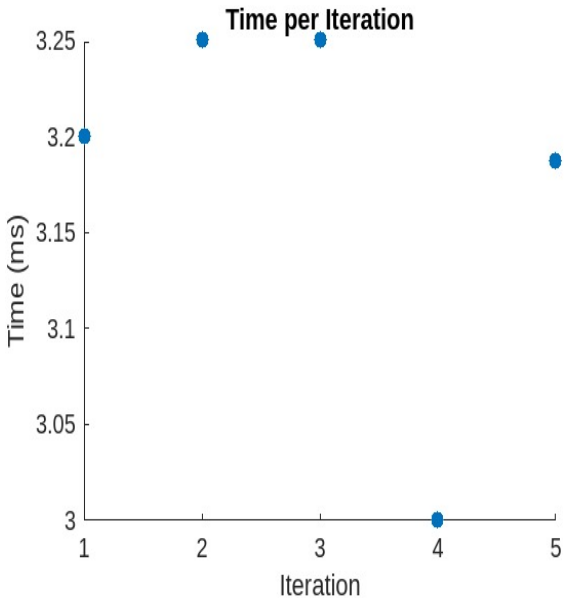


Figure 11: Minimum Time (millisecond) vs. Iteration Quantity

In this figure 11, the X axis exemplifies the number of iterations, and the Y axis exemplifies the minimum time in milliseconds for each iteration. For example, according to figure 11, 3.2 milliseconds is the minimum time for iteration 1, which is covered by route 1.

According to all iterations, that is, iteration 1 to iteration 5, the shortest routes are found by the MATLAB simulation as:

Iteration-1: shortest route
Node 1- node 21-node 47-node 31-node 40-node 43-node 37-node 50

Iteration-2: shortest route
Node 1-node 29-node 10-node 32-node 16-node 44-node 15-node 14-node 24-node 50

Iteration-3: shortest route
Node 1-node 8-node 39-node 17-node 2-node 26-node 5-node 48-node 33-node 47-node 18-node 50

Iteration-4: shortest route
Node 1-node 41-node 31-node 50
Iteration-5: shortest route
Node 1-node 12-node 14-node 21-node 23-node 25-node 18-node 7-node 22-node 20-node 13-node 17-node 30-node 44-node 32-node 49-node 10-node 39-node 50

In terms of time and distance parameter, we can summarize the simulated results of our proposed algorithm (for all iterations) in the following table-1:

Table 1: Distance vs. Time in terms of Iteration Quantity.

Iteration	Shortest Path	
	Distance (meter)	Time (millisecond)
1.	1106.6	3.2
2.	1271.6	3.25
3.	1743.1	3.25
4.	528	3
5.	2360.8	3.1875

So, the average shortest path distance in meter
= (1106.6+1271.6+1743.1+528+2360.8)/5 meter
= 1402.02 meter.

And the average shortest path time in millisecond
= (3.2+3.25+3.25+3+3.1875)/5 millisecond
= 3.1775 millisecond.

7. COMPARATIVE ANALYSIS

In the comparative analysis section, we will try to depict a clear scenario of a noteworthy dissimilarity between the existing research work and our research paper on this specified topic. In order to do this work successfully, we have considered the last seven years' (2016–2022) research papers on this topic with the help of the Google Scholar database. Let us concentrate on table-2, where the difference will be clearly visible.

Table 2: Comparative Analysis between our Introduced Work and Current Research Article

SL. No	Year	Author	Their Work	Our Work
1.	2022	Ahmad Hasan and et al.	In this article, Ad-Hoc IoT based network performance are measured using on demand basis distance vector routing technique and BHA handling mechanism in sensor network.	We have introduced MAC algorithm based black hole attack avoidance mechanism in this paper.
2.	2022	Rajesh Kumar Dhanaraj and et al.	Minimization technique of BHA in healthcare sensor network is introduced using extended gravitational search method.	Our paper is basically avoidance of BHA in general sensor network using MAC algorithm.
3.	2	Shoukat	This is a	Specific

	018	Ali and et al.	review paper where authors have analyzed different scenarios of BHA as well as identification and deterrence methods of this attack in IoT and sensor network.	MAC algorithm oriented avoidance technique of black hole attack is introduced for sensor network.
4.	2017	Veerpal Kaur and Simpel Rani	In this paper, authors have tried to integrate different detection and solution methods of BHA in mobile network.	In our paper, we exclusively focus on the avoidance technique of BHA in WSN.
5.	2016	S.S Nagamuthu Krishnan and P. Srinivasan	Quality of service constraint oriented solution technique for BHA in sensor network is proposed in this paper.	Authenticity of the participating node in sensor network is more focused in our proposed mechanism in this paper.

From the above Table 1, it is clear that there is a striking dissimilarity between our research paper and the relevant existing research articles on BHA handling techniques in wireless sensor networks.

8. LIMITATIONS AND FURTHER RESEARCH DIRECTION

In our research, we have tried to implement the MAC algorithm for the avoidance of BHA in WSN. Despite the use of the MAC algorithm in this attack, there are still some challenges, such as the requirement of establishing a confidential shared key, which is a very complex process. Non-repudiation of service cannot be achieved by using this algorithm in this attack. So, in future, research can be done on this field considering non-repudiation service implementation. As message sender and receiver's authenticity are ensured in the MAC algorithm, we have focused on the authentic participating node in the sensor network to handle this attack. Our main concern is to avoid any unauthentic node, like a black hole node, which cannot participate in the data transmission process, as well as those nodes. We have only proposed the algorithm and shown the mathematical simulation process to avoid BH node attacks in WSN.

9. CONCLUSION

In the current century throughout the world, research on the latest technology is concerned with the network security field as it is an emerging and growing research field [38, 39]. The BHA is one of the most common attacks in the network security area. A shared secret key-oriented MAC algorithm is proposed and implemented by both mathematical and simulation software to avoid BHA in WSN, which is our main contribution. In this paper, we have introduced a unique avoidance algorithm as well as a mathematical implementation process to avoid this attack. In our proposed algorithm, we have tried to highlight node authenticity throughout the network. Existing proposed mechanisms in this field have some limitations that are considered in our proposed algorithm, like quality of service and authenticity. Our contribution to this field of research is unique, which undoubtedly identifies the differences between our research and existing research in this area in the comparative analysis field. We believe that our proposed mechanism and corresponding explanation will open a new research direction in this BHA handling technique in WSN.

REFERENCES:

[1] H. Kalkha, H. Satori, and K. Satori, "Preventing Black Hole Attack in Wireless Sensor Network Using HMM," Procedia Comput. Sci., vol. 148, pp. 552–561, 2019, doi: 10.1016/j.procs.2019.01.028.

[2] D. Virmani, A. Soni, and N. Batra, "Reliability Analysis to overcome Black Hole Attack in Wireless Sensor Network," [Online]. Available: http://arxiv.org/abs/1401.2540.

[3] S. Misra, K. Bhattarai, and G. Xue, "BAMBi: Blackhole attacks mitigation with multiple base stations in wireless sensor networks," IEEE Int. Conf. Commun., no. June, 2011, doi: 10.1109/icc.2011.5962856.

[4] R. Alattas, "Detecting black-hole attacks in WSNs using multiple base stations and check agents," FTC 2016 - Proc. Futur. Technol. Conf., no. December, pp. 1020–1024, 2017, doi: 10.1109/FTC.2016.7821728.

[5] V. Kumar and R. Kumar, "An adaptive approach for detection of blackhole attack in mobile Ad hoc Network," Procedia Comput. Sci., vol. 48, no. C, pp. 472–479, 2015, doi: 10.1016/j.procs.2015.04.122.

[6] J. Kaur, "BHDP Using Fuzzy Logic Algorithm for Wireless Sensor Network under Black Hole Attack International Journal of Advance Research in," pp. 142–151, 2014.

[7] P. Yadav, R. K. Gill, and N. Kumar, "A Fuzzy Based Approach to Detect Black hole Attack," Int. J. Soft Comput. Eng., no. 2, p. 388, 2012.

[8] S. S. Ramaswami and S. Upadhyaya, "Smart handling of colluding black hole attacks in MANETs and wireless sensor networks using multipath routing," Proc. 2006 IEEE Work. Inf. Assur., vol. 2006, pp. 253–260, 2006, doi: 10.1109/iaw.2006.1652103.

[9] M. Wazid, A. Katal, R. Singh Sachan, R. H. Goudar, and D. P. Singh, "Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network," Int. Conf. Commun. Signal Process. ICCSP 2013 - Proc., pp. 576–581, 2013, doi: 10.1109/iccsp.2013.6577120.

[10] M. U. Farooq, X. Wang, R. Yasrab, and S. Qaisar, "Energy Preserving Detection Model for Collaborative Black Hole Attacks in Wireless Sensor Networks," Proc. - 12th Int. Conf. Mob. Ad-Hoc Sens. Networks, MSN 2016, pp. 395–399, 2017, doi: 10.1109/MSN.2016.072.

[11] V. Kaur and S. Rani, "Prevention / Detection Methods of Black Hole Attack : A Review," Adv. Wirel. Mob. Commun., vol. 10, no. 4, pp. 747–756, 2017.

[12] S. Ali, M. A. Khan, J. Ahmad, A. W. Malik, and A. Ur Rehman, "Detection and prevention of Black Hole Attacks in IOT & WSN," 2018 3rd Int. Conf. Fog Mob. Edge Comput. FMEC 2018, no. April, pp. 217–226, 2018, doi: 10.1109/FMEC.2018.8364068.

[13] S. S. Nagamuthu Krishnan and P. Srinivasan, "A QOS parameter based solution for black hole denial of service attack in wireless sensor networks," Indian J. Sci. Technol., vol. 9, no. 38, 2016, doi: 10.17485/ijst/2016/v9i38/88145.

[14] Paul, S. P., & Aggarwal, S. (2022, March). A Systematic Analysis of Research Trends on Network Control System in Wireless Sensor Network. In 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 1758-1763). IEEE.

[15] R. K. Dhanaraj, R. H. Jhaveri, L. Krishnasamy, G. Srivastava, and P. K. R. Maddikunta, "Black-Hole Attack Mitigation in Medical Sensor Networks Using the Enhanced Gravitational Search Algorithm," Int. J. Uncertainty, Fuzziness Knowlege-Based Syst., vol. 29, no. December, pp. 297–315, 2021, doi: 10.1142/S021848852140016X.

[16] U. Ghugar, J. Pradhan, and M. Biswal, "A Novel Intrusion Detection System for Detecting Black Hole Attacks in Wireless Sensor Network using AODV Protocol," IJCSN Int. J. Comput. Sci. Netw. ISSN, vol. 5, no. 4, pp. 2277–5420, 2016, [Online]. Available: www.IJCSN.org.

[17] S. P. Dongare and R. S. Mangrulkar, "Implementing energy efficient technique for defense against Gray-Hole and Black-Hole attacks in wireless sensor networks," Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015, pp. 167–173, 2015, doi: 10.1109/ICACEA.2015.7164689.

[18] D. Airehrour, J. Gutierrez, and S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism," 26th Int. Telecommun. Networks Appl. Conf. ITNAC 2016, pp. 115–120, 2017, doi: 10.1109/ATNAC.2016.7878793.

[19] J. Yin and S. K. Madria, "A hierarchical secure routing protocol against black hole attacks in sensor networks," Proc. - IEEE Int. Conf. Sens. Networks, Ubiquitous, Trust. Comput., vol.

2006 II, pp. 376–383, 2006, doi: 10.1109/SUTC.2006.1636203.

[20] S. Athmani, D. E. Boubiche, and A. Bilami, "Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs," 2013 World Congr. Comput. Inf. Technol. WCCIT 2013, pp. 0–4, 2013, doi: 10.1109/WCCIT.2013.6618693.

[21] B. Baviskar and V. Patil, "Black Hole Attacks Mitigation and Prevention in Wireless Sensor Network," Int. J. Innov. Res. Adv. Eng., vol. 1, no. 4, pp. 2349–2163, 2014.

[22] A. Zahedi and F. Parma, "An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks," Peer-to-Peer Netw. Appl., vol. 12, no. 1, pp. 167–176, 2019, doi: 10.1007/s12083-018-0654-0.

[23] K. Sha, J. Gehlot, and R. Greve, "Multipath routing techniques in wireless sensor networks: A survey," Wirel. Pers. Commun., vol. 70, no. 2, pp. 807–829, 2013, doi: 10.1007/s11277-012-0723-2.

[24] M. H. Anisi, G. Abdul-Salaam, M. Y. I. Idris, A. W. A. Wahab, and I. Ahmedy, "Energy harvesting and battery power based routing in wireless sensor networks," Wirel. Networks, vol. 23, no. 1, pp. 249–266, 2017, doi: 10.1007/s11276-015-1150-6.

[25] K. Thangaramya, K. Kulothungan, R. Logambigai, M. Selvi, S. Ganapathy, and A. Kannan, "Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT," Comput. Networks, vol. 151, pp. 211–223, 2019, doi: 10.1016/j.comnet.2019.01.024.

[26] Paul, S. P., & Vetrithangam, D. (2023, March). A Scientometric Study of Research Development on Cloud Computing-Based Data Management Technique. In *Doctoral Symposium on Computational Intelligence* (pp. 617-625). Singapore: Springer Nature Singapore.

[27] S. Dehghani, B. Barekatain, and M. Pourzaferani, "An Enhanced Energy-Aware Cluster-Based Routing Algorithm in Wireless Sensor Networks," Wirel. Pers. Commun., vol. 98, no. 1, pp. 1605–1635, 2018, doi: 10.1007/s11277-017-4937-1.

[28] A. Mohajerani and D. Gharavian, "An ant colony optimization based routing algorithm for extending network lifetime in wireless sensor networks," Wirel. Networks, vol. 22, no. 8, pp. 2637–2647, 2016, doi: 10.1007/s11276-015-1061-6.

[29] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks," Wirel. Pers. Commun., vol. 110, no. 4, pp. 1637–1658, 2020, doi: 10.1007/s11277-019-06788-y.

[30] Paul, S. P., & Vetrithangam, D. (2023, June). A Thorough Assessment on Orthogonal Frequency Division Multiplexing (OFDM) based Wireless Communication: Challenges and Interpretation. In 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS) (pp. 1145-1151). IEEE.

[31] R. Logambigai, S. Ganapathy, and A. Kannan, "Energy–efficient grid–based routing algorithm using intelligent fuzzy rules for wireless sensor networks," Comput. Electr. Eng., vol. 68, no. June 2017, pp. 62–75, 2018, doi: 10.1016/j.compeleceng.2018.03.036.

[32] R. Zagrouba and A. Kardi, "Comparative study of energy efficient routing techniques in wireless sensor networks," Inf., vol. 12, no. 1, pp. 1–28, 2021, doi: 10.3390/info12010042.

[33] Paul, S. P., & Vetrithangam, D. (2022, November). A Comprehensive Analysis on Issues and Challenges of Wireless Sensor Network Communication in Commercial Applications. In 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 377-382). IEEE.

[34] Praveenchandar, J., Vetrithangam, D., Kaliappan, S., Karthick, M., Pegada, N. K., Patil, P. P., & Umar, S. (2022). IoT-Based Harmful Toxic Gases Monitoring and Fault Detection on the Sensor Dataset Using Deep Learning Techniques. Scientific Programming, 2022.

[35] Paul, S. P., & Vetrithangam, D. (2023), Design and Analysis of an Efficient and Load-Balanced Multipath Routing Algorithm for Energy-Effective Wireless Sensor Networks. International Journal of Intelligent Systems and Applications in Engineering, 11(10s), 601-617,

[36] Paul, S. P, & Vetrithangam D, (2023), A Full Scale Analysis on Challenges and Issues of Next Generation (5G) Communication in Heterogeneous Wireless Network Based Enterprise Applications. Journal of Theoretical and Applied Information Technology (JATIT), 101(11s).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[37] J. Wang, Z. Zhang, F. Xia, W. Yuan, and S. Lee, "An energy efficient stable election-based routing Algorithm for wireless sensor Networks," Sensors (Switzerland), vol. 13, no. 11, pp. 14301–14320, 2013, doi: 10.3390/s131114301

[38] M. Hajiee, M. Fartash, and N. Osati Eraghi, "An Energy-Aware Trust and Opportunity Based Routing Algorithm in Wireless Sensor Networks Using Multipath Routes Technique," Neural Process. Lett. vol. 53, no. 4, pp. 2829–2852, 2021, doi: 10.1007/s11063-021-10525-7.

[39] A. Hasan et al., "Forensic Analysis of Blackhole Attack in Wireless Sensor Networks/Internet of Things," Appl. Sci., vol. 12, no. 22, 2022, doi: 10.3390/app122211442.