SERBIAN JOURNAL OF ELECTRICAL ENGINEERING
Vol. 19, No. 2, June 2022, 193-206
UDC: 004.056.53 **DOI: https://doi.org/10.2298/SJEE2202193P**

Early Detection Mechanism for Sybil Attacks on Wireless Multimedia Sensor Networks

Basavaraj Patil[1], Sangappa Ramachandra Biradar[2]

Abstract: The rapid developments in wireless multimedia sensor networks (WMSNs) have increased the demand for an efficient method of safeguarding multimedia data from attackers. As data are transmitted over a wireless medium, the authentication process needs to be provided with some efficient detection and prevention methods. The Sybil attack is one of the most common and involves replicating the identity of an original node in the network and behaving like a true node in order to retrieve/destroy information using this fake identity. An efficient enhanced random password comparison technique is proposed to detect and prevent Sybil attacks. The results of simulations indicate that the proposed method detects this type of attack more efficiently than existing methods. In addition to early detection, our application increases the throughput and reduces the average delay with an enhanced true detection rate. The identification of this malicious activity in its initial phases increases the efficiency of the system in terms of the data transmission process.

Keywords: Attacks, Sensor, Node, Sybil, Security, WMSN.

1 Introduction

A large number of applications such as monitoring and tracking rely on wireless multimedia sensor networks (WMSNs) in different domains to establish connections, fetch data, and control remote devices. In a network, it is necessary to carry out monitoring and to protect against attacks during the process of data transmission. The study in [1] noted that there are different types of malicious attacks that take place at various levels of the network with the aim of modifying data, fetching data, or preventing communication between nodes. Some of the most common attacks on networks are black hole, wormhole, sinkhole, selective forward and Sybil attacks [1]. The identification of the node in the device is the most crucial process in the process of data transmission. Nodes connecting to a network should be identified via an effective authentication process, and an ID

[1]Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire – 574240, Dakshina Kannada, Affiliated to Visvesvaraya Technological University, Belagavi, India; E-mail: bbpatilcs@gmail.com.
[2]SDM College of Engineering and Technology, Dharwad, Karnataka 580001, India;
E-mail: srbiradar@gmail.com

for each node in the network should be provided in order to allow these nodes to participate in the network for further processes.

During the process of establishing communication between nodes, malicious nodes may try to fetch the details of an existing node and imitate them in order to act like the original node. A Sybil attack misleads the network by providing a duplicate ID to allow the attacker to take part in the process of broadcasting data over the network, leading to data loss. The presence of malicious nodes hampers the performance of a WMSN. A few attacks were created in terms of nodes, while some others are created in various layers. A broad taxonomy of existing security attacks is shown in Fig. 1.

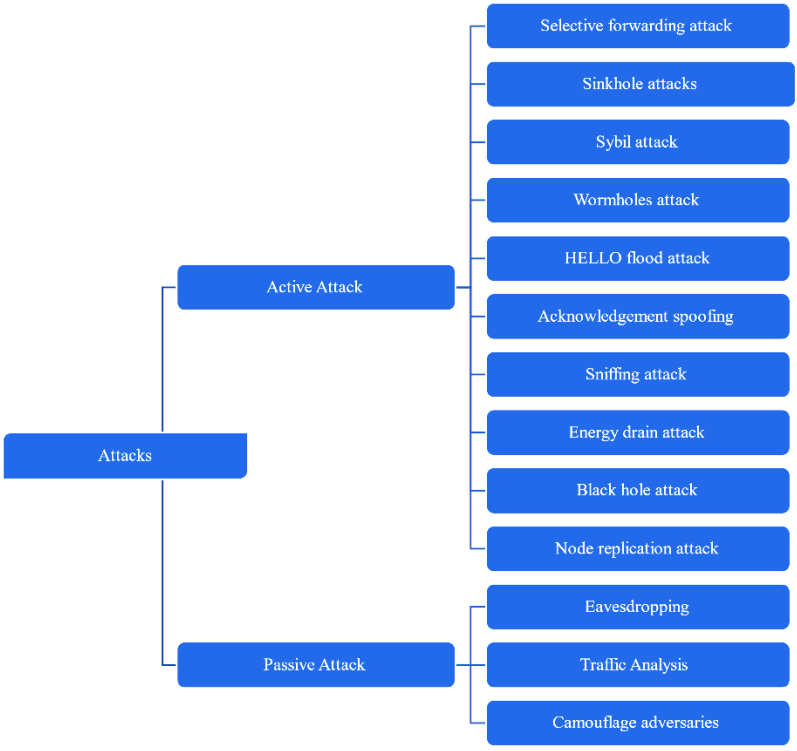

Fig. 1 – *Types of attack on WMSNs.*

Due to the mobility of the nodes in a WMSN, it is difficult to track and monitor intermediate nodes. The nodes may be configured for single-hop or multi-hop communication, or as base stations, gateways, or access points.

Attacks can be broadly categorized into active and passive types. In an active attack, a malicious user/attacker tries to modify data to deploy illegitimate data on the network, which affects the performance of the system. These include Sybil, sinkhole, and eavesdropper attacks. Passive attacks affect the properties of the

network and are monitored by unauthorised interventions, such as eavesdropping or snooping.

This paper deals with the detection and mitigation of the Sybil attack. This is one of the most hazardous types for sensor networks, and we propose an effective technique to mitigate this attack. According to Douceur [2], a peer-to-peer network is vulnerable to Sybil attacks. Karlof [2] has shown that this attack can impact the routing protocols of sensor networks. Many researchers have investigated the various kinds of critical attacks and have developed mechanisms for securing data in wireless sensor networks (WSNs). In a Sybil attack, there is a malicious node in the network with multiple identities, and this scenario is illustrated in Fig. 2. Node A is hampered by malicious activity with multiple identities and the creation of duplicate identities in the network.

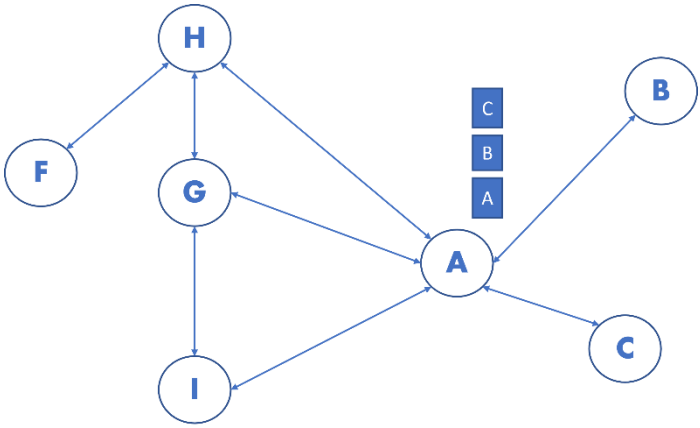

Fig. 2 – *Illustration of the Sybil attack.*

This paper is organised as follows. Section 1 gives an overview of WMSNs, introduces the types of possible attack and describes the Sybil attack and its impacts. A brief review of the existing techniques for identifying malicious activities and the countermeasures suggested by various researchers is given in Section 2. Section 3 presents the design of the system, the flow of execution and the proposed algorithms. The experimental setup and the results are discussed in Section 4. The simulation tools used, the results obtained and a comparative analysis with existing techniques are also described. Our conclusions and directions for future work are given in Section 5.

2 Related Work

WSN technology has given rise to enhanced wireless communication. The various applications of sensor networks and the factors affecting their design have been reviewed in [3]. The unique characteristics of a WSN open the way for

building exciting applications in the future, in a broad range of fields such as video surveillance, remote sensing, military applications, etc. The factors affecting the performance of sensor nodes include hardware design, power utilization, design cost, liability, and network topology changes, and these need to be considered to achieve high performance for a network. Open research issues related to each network layer of a sensor network are discussed below.

Dhamodharan et al. [4] reviewed the detection and prevention of Sybil attacks using compare and match-position verification (CAM-PV) and message authentication and passing (MAP) methods. They introduced a message authentication and passing scheme to replace CAM-PVM and MAP in order to check the trustworthiness of authentication. Their results were compared with RPC (random password comparison), and a simulation showed that MAP improved the detection accuracy by 30% compared to other methods.

In [5], the authors proposed an energy trust system (ETS) mechanism to identify Sybil attacks at multiple levels. ETS was designed based on identity and position verification. Simulation results showed that this approach achieved a detection rate of 70% at the first level and more accurate detection at the second level.

A novel identity-based scheme [6] was introduced to detect malicious nodes and broadcast the details of malicious activity to the adjoining sensor nodes. WSNs were found to be insecure against several security attacks. The experimental results reported in this paper demonstrated that the proposed scheme imposed a lower computational overhead and achieved high performance.

A lightweight detection mechanism [7] called LEACH-RSSI-ID (LRD) was introduced based on the received signal strength indicator (RSSI). Sybil attacks were rapidly identified by comparing them with RSSI-ID tables. Based on the results of a simulation, it was shown that the proposed mechanism could identify a Sybil attack with a high detection rate and high accuracy.

Nirmal Raja et al. [8] introduced an authentication scheme based on the Fujisaki Okamoto algorithm, which used an ID-based cryptographic scheme to achieve better authentication for health care applications. A simulation was carried out using Network Simulator 2 (NS2) and an analysis was conducted of key broadcasting, the time needed for various key sizes, throughput, packet delivery ratio (PDR) and energy utilisation.

M. Jamshidi et al. [9] introduced a cluster-based sensor network and proposed a distributed algorithm based on the RSSI. It was evaluated via a series of experiments in terms of the detection rate (TDR: true detection rate; FRD: false detection rate) and transmission overhead. The algorithm detected 99.8% of Sybil nodes with an average FDR of 0.008%.

A novel secure lightweight cryptographic data-aggregation algorithm (SLC-DAA) based on clustering has been presented [10], in which primitive cryptographic operations were used to provide higher security and efficient energy consumption. An experimental study of parameters such as the end-to-end delay, energy efficiency, PDR, and time taken for encryption showed that this approach achieved a better trade-off in comparison with existing methods.

3 Proposed Scheme

A network consists of N static sensor nodes (SNs), each with a unique identity, and a base station (BS), randomly deployed within a 2D region. The network is homogeneous (all network nodes have equal hardware and software facilities). A block diagram of the proposed model is shown in Fig. 3.

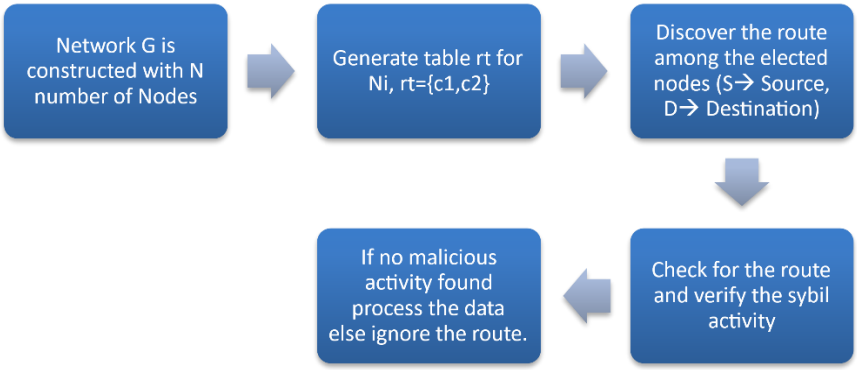

Fig. 3 – *Block diagram of the proposed model.*

The proposed method consists of the following phases:

– **Node registration**: In the initial phase, each node is registered and a valid network is formed. At this stage, each node is assigned a unique ID as it registers with the network. Then, to enable data transmission, a source and destination pair is identified. A successful route is required to provide the delivery of authentic data to the required node.

– **Routing information**: The source and destination node pair are determined, and a route is discovered using the ad-hoc on-demand distance vector (AODV) protocol.

– **Sybil detection**: The node selected during route discovery is checked for a Sybil attack using an ID (identity) comparison. A Sybil attack compromises the network's ability to operate by allowing a node to take on multiple identities in the network. This confuses the sender who is forwarding the data packets.

3.1 Proposed algorithm

To address this problem, an algorithm called Enhanced Random Password Comparison (ERPC) is proposed to detect and eliminate vulnerable activities, in order to prevent Sybil attacks. Several different traffic and security parameters are involved in data transmission in a network. The proposed network model contains a base station BS and N nodes, which are deployed randomly. Each node is required to register before being added as part of the network. A registered node is provided with a node_id, and a password is generated for each node. In the ERPC algorithm, a routing table (rtable-RPC) is generated to store each node_id and its respective password. The intermediate nodes along the path between the source and the destination are identified. If the details of each node match those in the table, the node is normal; otherwise, it is a Sybil node. A flowchart for the proposed method is shown in Fig. 4.

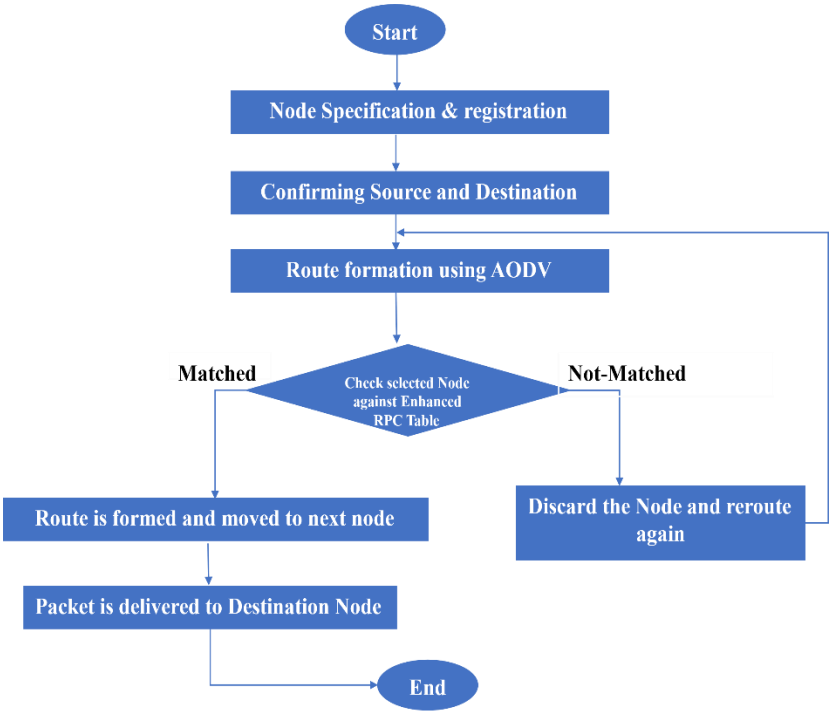

Fig. 4 – *Flowchart of the proposed model.*

The proposed algorithm has two parts: assignment of IDs and detection of Sybil attacks. The algorithm compares the node_id and password with those in the routing table (rtable) for each node. If they match, this implies that the node

has been authenticated and further processing can continue; if not, it is detected as a Sybil node. Pseudocode for this process is given in Algorithm 1.

Algorithm 1: Detection of Sybil nodes

Step 1: Network with N nodes

Step 2: Register each participating node with the base station

Step 3: Create a routing table → rt {node_id, time_delay, password} for each node Ni.

Step 4: Find a path from source S → destination D using DISROUT (S, D)

Step 5: Send a data request message from node D to node S.

Step 6: Match the node identity in BS using rtable and identify malicious Sybil activity.

The proposed algorithm initially assigns an ID to each registered node and the process of detecting a Sybil node takes place. The algorithm compares the node_id and password with those in the routing table (rt). If the entries match, this implies that the node has been authenticated and further processing can continue; otherwise, it is detected as a Sybil or malicious node. Suitable routes for data transmission are discovered using Algorithm 2.

Algorithm 2: DISROUT (S, D)

Step 1: Node n looks towards D for the next neighbour

Step 2: Get node information from neighbour node ni and compare it with the table information ti

Step 3: Check whether (ti (c1, c2) ==ni (c1, c2))

Step 4: Update route table rt={S,ni,…}

Step 5: CHKROUT(S, D): if rt matches→ accept node as a legitimate node;

else

Step 6: Reject the node ni and look for the next node ni + 1

Step 7: Repeat Step 2

Step 8: End if

In the route discovery phase, the destination node is identified based on a comparison of the information on each node, such as the node_id and password, with the details in the routing table. If the node data match, then the node is accepted as a normal or legitimate node; otherwise, it is rejected. If the node is legitimate, the route information is collected and used to update the node details in the routing table. The process is repeated for all the source and destination nodes using the CHKROUT process in Algorithm 3.

Algorithm 3: CHKROUT (Node m, Node n)

Step 1: Receive route information from rt.

Step 2: Get the node information from the neighbour node ni and compare it with the table information ti

Step 3: Check whether (ti(c1,c2)==ni(c1,c2))

Step 4: Update route table rt={S,ni,…}

else

Step 5: Reject the node ni and look for ni + 1

Step 6: Repeat Step 2 until D

Step 7: End if

Step 8: Return rt

4 Simulation Results and Discussion

NS2 [13] is the most extensively used simulator for performing real-time analysis in academia and industry. It was created in 2000 to study TCP's congestion control network performance and is a robust tool for simulating and analysing network performance using a variety of parameters such as packet loss, throughput, and delay. It is an object-oriented, event-driven simulator that supports C++ and TCL/oTCL.

The proposed approach was implemented in NS2 to detect Sybil nodes. The AODV protocol was used for malicious node discovery and data delivery. Our experiments were conducted using NS2, and the simulation environment was as shown in Fig. 5. The simulation network was configured with the parameters in **Table 1** to identify the type of node. Node 1 is the source, node 5 is the destination, and node 2 is a malicious node. Node 2 creates a duplicate identity to mimic the destination node 5, and acts as a legitimate node in the network.

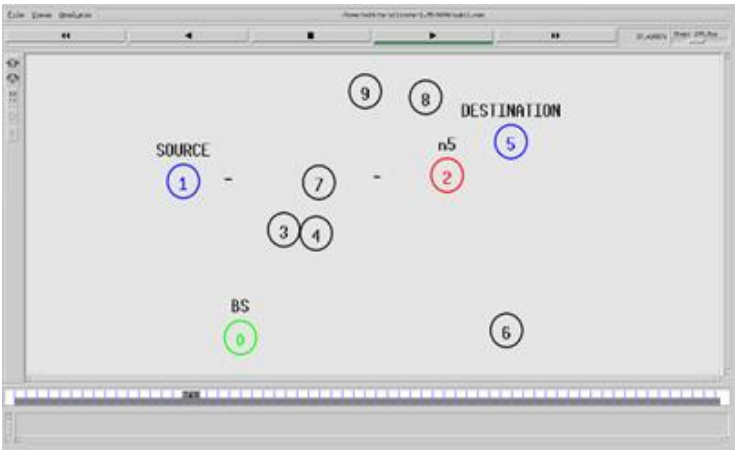

Fig. 5 – *Network simulation environment.*

Table 1
Parameter values used for simulation.

Parameter	Values
Number of nodes	20 – 100
MAC	802.11
Packet size	50 B
Malicious population	5–20%
Pause time	2 ms
Initial energy	100 J
Traffic	CBR
Simulation time	100 s
Location	Random

4.1 Performance analysis

The performance of the proposed method in the simulations was evaluated based on various network parameters such as the throughput, average delay, and Sybil node detection rate. The experimental results obtained from ERPC were compared with those of two existing techniques, RPC [4] and MAP [4], based on the same parameters. The results presented below prove that the proposed ERPC algorithm is more efficient in terms of the early detection of malicious Sybil nodes in the specified network.

4.1.1 Throughout

In the simulated environment, the number of nodes was varied from 20 to 100, with the inclusion of some malicious nodes. The PDR was high compared to existing techniques. In the proposed ERPC method, malicious activity is

detected and authenticated in the initial stages to provide better throughput. The enhancement in the throughput is shown in Fig. 6.

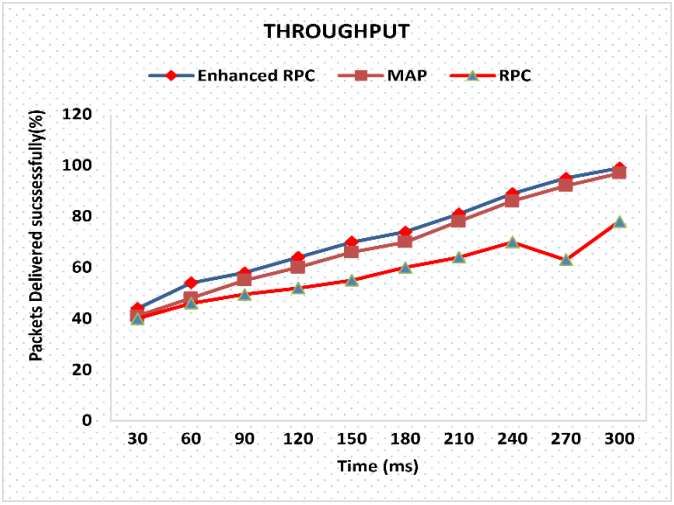

Fig. 6 – *Throughput comparison.*

4.1.2 Average delay

As the throughput increases, the packet loss is reduced and delivery of the packets becomes faster. Our results prove that the average delay in terms of packet transmission is low compared to existing techniques. The results for the average delay are shown in Fig. 7.

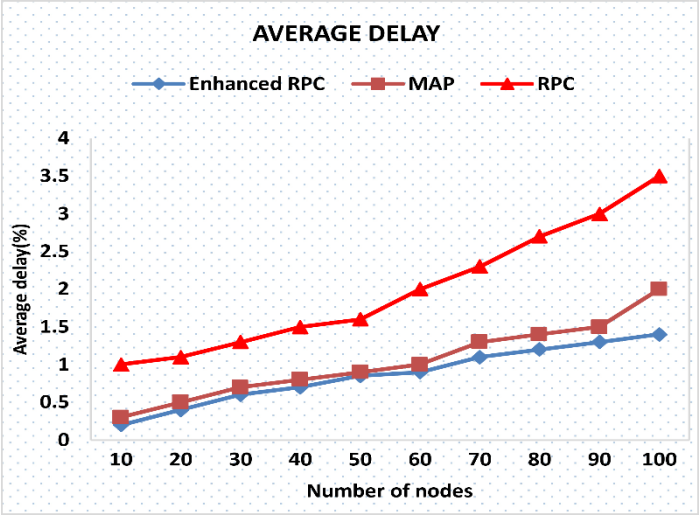

Fig. 7 – *Average delay for data packets.*

4.1.3 Detection rate

In comparison with existing techniques, ERPC gives a better detection rate for Sybil nodes, as shown in **Table 2** and Fig. 7. Our method was also assessed for the detection rates of malicious Sybil nodes using the performance metrics of TPR and FPR.

TPR is based on the numbers of malicious nodes that have been correctly detected, while FPR reflects the number of good or legitimate nodes that have been incorrectly detected as malicious. These metrics help to indicate the accuracy in terms of the correct detection of legitimate nodes or false detection. TPR and FPR are calculated using (1) and (2).

$$\text{True positive rate}\,(\text{TPR}) = \frac{\text{Correctly detected Sybil nodes}}{\text{Total number of nodes}}, \quad (1)$$

$$\text{False positive rate}\,(\text{FPR}) = \frac{\text{Wrongly detected Sybil nodes}}{\text{Total number of nodes}}. \quad (2)$$

For example, if the number of correctly detected nodes is 13, then:

– $\text{TPR} = 13/100 = 13\%$;

– $\text{FPR} = 3/13 = 0.23\%$.

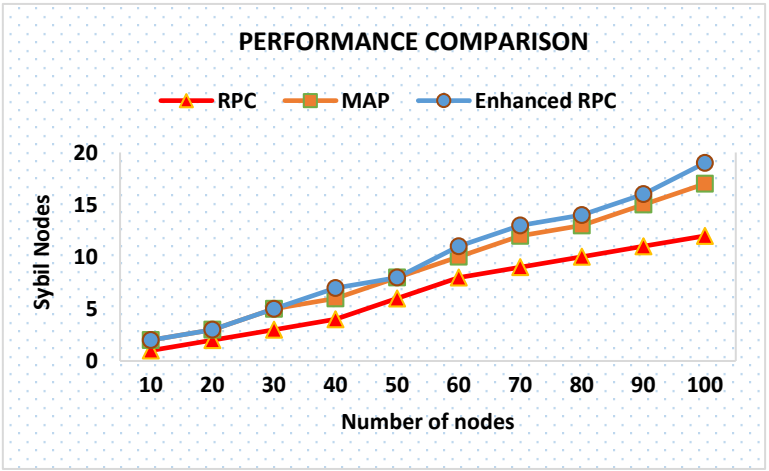

Fig. 8 – *Performance comparison.*

In each round of the simulation, the TPR and FPR were calculated for varying numbers of nodes in the network.

Table 2
Comparison of detection rates for Sybil nodes.

Number of nodes	Sybil nodes	RPC [4]	MAP [4]	ERPC [Proposed]
10	2	1	2	2
20	4	2	3	3
30	6	3	5	5
40	8	4	6	7
50	10	6	8	8
60	12	8	10	11
70	14	9	12	13
80	16	10	13	14
90	18	11	15	16
100	20	12	17	19

6 Conclusion

It is important to study the problem of Sybil attacks, as these can be harmful and pose a threat to the security of a WMSN. The proposed algorithm discovers a legitimate route by authenticating each node as a trusted node or detecting a malicious Sybil node, and then transmits data safely. Our ERPC algorithm is dynamic and generates passwords more effectively to avoid duplication of IDs. The efficiency of the ERPC algorithm is demonstrated by the results of a set of experiments. Since Sybil nodes are identified in the early stages of route discovery, this helps the network to continue with data communication without intervention due to attack. An experimental analysis proves that the proposed method is efficient, robust, and gives faster detection than alternative methods. In future work, a route-repair technique could be considered in the occurrence of route failure.

7 References

[1] H. K. Deva Sarma, A. Kar: Security Threats in Wireless Sensor Networks, Proceedings of the 40th Annual International Carnahan Conference on Security Technology, Lexington, USA, October 2006, pp. 243 – 251.

[2] J. R. Douceur: The Sybil Attack, Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS), Cambridge, USA, March 2002, pp. 251 – 260.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci: Wireless Sensor Networks: A Survey, Computer Networks, Vol. 38, No. 4, March 2002, pp. 393 – 422.

[4] U. S. R. Kumar Dhamodharan, R. Vayanaperumal: Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method, The Scientific World Journal, Vol. 2015, July 2015, p. 841267

[5] N. Alsaedi, F. Hashim, A. Sali, F. Z. Rokhani: Detecting Sybil Attacks in Clustered Wireless Sensor Networks based on Energy Trust System (ETS), Computer Communications, Vol. 110, September 2017, pp. 75 – 82.

[6] V. Sujatha, E. A. Mary Anita: Identity-Based Scheme Against Sybil Attacks in Wireless Sensor Networks, International Journal of Engineering and Advanced Technology, Vol. 9, No. 1, October 2019, pp. 5350 – 5355.

[7] W. Shi, S.- Y. Liu, Z. Zhang: A Lightweight Detection Mechanism Against Sybil Attack in Wireless Sensor Network, KSII Transactions on Internet and Information Systems, Vol. 9, No. 9, September 2015, pp. 3738 – 3750.

[8] K. Nirmal Raja, M. Maraline Beno: Secure Data Aggregation in Wireless Sensor Network-Fujisaki Okamoto (FO) Authentication Scheme Against Sybil Attack, Journal of Medical Systems, Vol. 41, No. 7, July 2017, pp. 107.

[9] M. Jamshidi, E. Zangeneh, M. Esnaashari, A. M. Darwesh, M. R. Meybodi: A Novel Model of Sybil Attack in Cluster-Based Wireless Sensor Networks and Propose a Distributed Algorithm to Defend It, Wireless Personal Communications, Vol. 105, No. 1, March 2019, pp. 145 – 173.

[10] R. Kowsalya, B. Roseline Jeetha: Cluster Based Data-Aggregation Using Lightweight Cryptographic Algorithm for Wireless Sensor Networks, Materials Today: Proceedings, February 2021, pp. 1 – 8.

[11] S. Alam, D. De: Analysis of Security Threats in Wireless Sensor Network, International Journal of Wireless & Mobile Networks, Vol. 6, No. 2, April 2014, pp. 35 – 46.

[12] A. Kardi, R. Zagrouba: Attacks Classification and Security Mechanisms in Wireless Sensor Networks, Advances in Science, Technology and Engineering Systems Journal, Vol. 4, No. 6, November 2019, pp. 229 – 243.

[13] T. Issariyakul, E. Hossain: Introduction to Network Simulator 2 (NS2), Ch. 2, Introduction to Network Simulator NS2, 2nd Edition, Springer, New York, London, 2009.

[14] M. Keerthika, D. Shanmugapriya: Wireless Sensor Networks: Active and Passive Attacks-Vulnerabilities and Countermeasures, Global Transitions Proceedings, Vol. 2, No. 2, November 2021, pp. 362 – 367.

[15] J. Wadii, H. Rim, B. Ridha: Detecting and Preventing Sybil Attacks in Wireless Sensor Networks, Proceedings of the IEEE 19th Mediterranean Microwave Symposium (MMS), Hammamet, Tunisia, October 2019, pp. 1 – 5.

[16] M. Elhoseny, A. E. Hassanien: Secure Data Transmission in WSN: An Overview, Ch. 6, Dynamic Wireless Sensor Networks: Studies in Systems, Decision and Control, Vol. 165, pp. 115 – 43, 1st Edition, Springer, Cham, 2019.

[17] H. Gao, R. Wu, M. Cao, C. Zhang: Detection and Defense Technology of Blackhole Attacks in Wireless Sensor Network, Proceedings of the 14th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP), Dalian, China, August 2014, pp. 601 – 610.

[18] S. Jayashree, T. Mohanraj: Vampire Attack Detection in Wireless Sensor Networks, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, No. 2, February 2015, pp. 751 – 756.

[19] L. Vinet, A. Zhedanov: A 'Missing' Family of Classical Orthogonal Polynomials, Journal of Physics A: Mathematical and Theoretical, Vol. 44, No. 8, February 2011, pp. 1 – 16.

[20] S. Akourmis, Y. Fakhri, M. D. Rahmani: Reducing Blackhole Effect in WSN, Proceedings of the International Conference on Innovations in Bio-Inspired Computing and Applications, Kochi, India, December 2018, pp. 13 – 24.

[21] S. Abbas, M. Merabti, D. Llewellyn-Jones, K. Kifayat: Lightweight Sybil Attack Detection in MANETs, IEEE Systems Journal, Vol. 7, No. 2, June 2013, pp. 236 – 248.

[22] A.- U. Rehman, S. U. Rehman, H. Raheem: Sinkhole Attacks in Wireless Sensor Networks: A Survey, Wireless Personal Communications, Vol. 106, No. 4, June 2018, pp. 2291 – 2313.

[23] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, M. Hosseinzadeh: Secure Data Aggregation Methods and Countermeasures against Various Attacks in Wireless Sensor Networks: A Comprehensive Review, Journal of Network and Computer Applications, Vol. 190, September 2021, pp. 103118.

[24] D. Kumari, K. Singh, M. Manjul: Performance Evaluation of Sybil Attack in Cyber Physical System, Procedia Computer Science, Vol. 167, 2020, pp. 1013 – 1027.

[25] C. Karlof, D. Wagner: Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, USA, May 2003, pp. 113 – 127.

[26] W. Mi, L. Hui, Z. Yan-fei, Ch. Ke-fei: TDOA-Based Sybil Attack Detection Scheme for Wireless Sensor Networks, Journal of Shanghai University, Vol. 12, No. 1, February 2008, pp. 66 – 70.

[27] M. Saud Khan, N. M. Khan: Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks, Journal of Sensors, Vol. 2016, August 2016, pp. 9783072.

[28] G. Santhi, R. Sowmiya: A Survey on Various Attacks and Countermeasures in Wireless Sensor Networks, International Journal of Computer Applications, Vol. 159, No. 7, February 2017, pp. 7 – 11.

[29] T. Hemanth Kumar, K. V. K. Kowshik, M. Revathi: Detection of Blackhole Attacks in Wireless Sensor Networks, International Journal of Innovative Technology and Exploring Engineering, Vol. 8, No. 11s, September 2019, pp. 1203 – 1205.

[30] C. Portillo, J. Martínez-Bauset, V. Pla: Modelling of S-MAC for Heterogeneous WSN, Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, February 2018, pp. 1 – 6.

[31] M. A. Jan, P. Nanda, X. He, R. P. Liu: A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application, Future Generation Computer Systems, Vol. 80, March 2018, pp. 613 – 626.

[32] J. Newsome, E. Shi, D. Song, A. Perrig: The Sybil Attack in Sensor Networks: Analysis & Defenses, Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks (IPSN), Berkeley, USA, April 2004, pp. 259 – 268.