MSPA - OLSR : A Novel Multi-Tasking Secure OLSR Version for Ad Hoc Networks

Nada Mouchfiq
Smart Systems Laboratory (SSLab), ENSIAS, Mohammed V University in Rabat, Rabat, Morocco
nada_mouchfiq@um5.ac.ma (corresponding author)

Received: 2 April 2026 | Revised: 8 May 2026 | Accepted: 19 May 2026

 DOI: https://doi.org/10.48084/etasr.19070

ABSTRACT

Smart system security remains a major challenge of the wider adoption of the Internet of Things (IoT) and ad hoc networks. In this paper, we present the integration of the MSPA (Multi-task Secure Protocol for Ad-hoc networks) security concept into the OLSR (Optimized Link State Routing) protocol, resulting in the secure variant MSPA-OLSR. This approach is designed to strengthen the security of routing mechanisms in Mobile Ad Hoc Networks (MANETs) by addressing vulnerabilities and enhancing resilience against potential threats. The approach is then simulated using the NS3 network simulator to evaluate its performance in terms of key Quality of Service (QoS) metrics, such as packet delivery ratio, end-to-end delay, throughput, and routing overhead.

Keywords-security; networks; routing; MANETs; protocol; OLSR; IoT

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are used in a wide range of interactive applications, including military operations and business environments. These networks do not require a fixed infrastructure, allowing them to be deployed in any location [1, 2]. However, there are several security challenges that must be addressed [3, 4], including issues related to the physical nature of wireless connections and security problems that also exist in wired networks [5]. One solution for improving the security of MANETs is the use of the Optimized Link State Routing Protocol (OLSR). This proactive routing protocol is designed specifically for MANETs and is considered one of the top four routing protocols by the Internet Engineering Task Force (IETF). OLSR relies on the use of Multipoint Relays, which are selected nodes that forward broadcast messages during the flooding process to minimize message overhead in the network. However, OLSR is still vulnerable to certain attacks [6].

Authors in [7] present a trust-based security enhancement for MPR selection in OLSR, where trust is determined by node willingness and reputation, based on aggregated recommendations. The proposed OLSR extension selects highly trusted nodes as MPRs. Authors in [8] propose a new approach to enhance the security and energy efficiency of Wireless Sensor Networks (WSNs) by combining an energy-efficient OLSR protocol with Elliptic Curve Cryptography (ECC). This method aims to prevent Sybil attacks, which are particularly dangerous for these networks. By optimizing performance while minimizing energy consumption, the authors offer an innovative solution to improve the reliability and security of WSNs in various applications. Authors in [9] propose the Enhanced Data Accuracy-based Path Discovery (EAPD) technique to improve data transmission accuracy in mobile networks. This method selects routing paths based on maximum data accuracy and rejects low-accuracy nodes. A backup route algorithm prevents intrusion and congestion, minimizing energy consumption and packet drop rates. The method presented in [10] avoids flooding nodes by using backup routing information to recover from interference. A straddling path recovery algorithm ensures interference-free routing with resource-rich nodes, supporting reliable communication and preventing data loss during routing breakdowns.

In [11], the authors propose the TAM model to enhance MANET security through a two-tier mechanism (TTSM). The first tier selects trusted nodes based on energy capacity and message processing speed. The second anonymizes identities using duplicates generated by a recursive function, preventing attackers from identifying participating nodes. In [12], the authors propose an adaptive deep learning–based approach for detecting black hole attacks in MANETs. The proposed SA-DCBIGNet model achieves superior detection performance compared to traditional learning techniques, thereby strengthening network security and resilience. A decentralized blockchain-driven architecture aimed at enhancing privacy preservation is presented in [13]. The proposed model is structured across three layers, namely the equipment layer, the network service layer, and the application layer, while incorporating smart contracts for secure operations. Additionally, a vulnerability detection technique based on an improved tree-based convolutional neural network is introduced. In [14], a blockchain-enabled framework is proposed to ensure secure data aggregation and transmission in disaster management scenarios. The network is organized into zones and clusters, where cluster heads are optimally selected using an Adaptive Neuro-Fuzzy Inference System (ANFIS). To distinguish between regular and emergency data, the approach

integrates a two-phase STS mechanism along with a modified packet structure.

Authors in [15] design a hierarchical group key agreement scheme leveraging sharded blockchain smart contracts for large-scale wireless ad hoc networks. However, the storage overhead associated with blockchain and the resource-intensive processes required for its creation and maintenance may negatively impact overall network performance.

This paper describes the integration of the MSPA [16] concept with the OLSR standard creating a secure version termed MSPA-OLSR. We will assess the outcomes of this solution using simulations to test how well it performs in terms of service quality metrics.

II. PROPOSED MODEL

In this section, we provide a detailed description of the original smart Multi-task Secure Protocol for Ad-hoc networks (MSPA) that aims to improve efficiency and security in ad hoc networks, since it allows for a compromise between security and performance without sacrificing either of the two. The multi-task process corresponds to the activation or deactivation of the different tasks performed by each of the delegated nodes or orchestrators according to the role of each of them. The architecture is based on the following three-step consensus:

- An initialization step to designate the delegate and the orchestrator nodes by acquiring knowledge of their environment by introducing a cooperative mechanism.
- A network filtering step that isolates malicious nodes before forwarding ensures the first level of security.
- A sending step in which the procedure applied depends on the types of nodes constituting the sending path calculated by the source.

In this paper, we will focus on the initialization and network filtering steps.

A. Initialization Step

The initial phase of MSPA consists of equipping all the nodes in the network with a new security algorithm that groups specific tasks that are activated or deactivated on demand. This model gives rise to new notions of "ND" delegated nodes and "NO" orchestrator nodes, which work together to ensure their own and their neighbors' security, depending on the purpose. It is important to note that each node must choose a unique ND, and each ND must choose a unique NO. The definitions of the mathematical symbols and notations in the scheme are described in Table I. Once the neighboring nodes are recognized, the energy values of each node are checked. The energy threshold is specified and the node energy values are compared to the threshold values. For the remainder of this section, we will be considering i, j, k ∈ [1, +∞]. NO and ND are selected as follows:

- ND are elected by the nodes in their first neighborhood as follows:
  1. The most stable (with a minimum distance).
  2. Having a residual energy that exceeds 50% of the battery.
- Orchestrator nodes NO are elected from the neighboring NDs as follows:
  1. The most stable (with a minimum distance).
  2. Having maximum residual energy. After the first transmission, a new crucial factor for the delegate and orchestrator nodes selection joins the previous criteria.

After each successful transmission, the ND and NO increment the credibility value of their participating selectors, and each node i corresponds to a credibility coefficient whose value is compared to a predefined threshold number of credibility coefficient Ci. We evaluate the credibility in the proposed scheme by a real number with a continuous value between 0 and 1. In the general case study of our approach, Ci is defined by:

$$Ci=\frac{\text{Successful\_transmissions}(i)}{\text{Total\_transmissions}(i)} \quad (1)$$

The credibility is evaluated according to the following system:

$$\begin{cases}\text{Credible if } Ci \in E=[0.8,1], E \subset R\\ \text{Not credible otherwise}\end{cases}$$

The value of the credibility coefficient is exploited in the election of ND and NO as follows:

1. An ND must have a Ci ∈ E.
2. An NO corresponds to the ND node with the largest Ci among its neighbors.

To conserve its energy and give other nodes a chance to complete the orchestrator mission, a node can only be elected as a NO twice in a row, because dynamic updating effectively resists assaults by greatly complicating the number of targets to destroy. Once elected, each delegate and orchestrator node share its tag with its selectors (Tag = ND and Tag = NO, respectively). Nodes N directly linked to an ND that was subsequently elected as their NO will be assigned to the nearest delegated nodes. This process secures this NO and isolates it from possible threats.

TABLE I. NOMENCLATURE

Notation	Description
NO(k)	k^{th} orchestrator node
ND(i)	i^{th} ND in the NO(k) hierarchy
N(ij)	j^{th} N in the ND(i) hierarchy
$Kres\_N(ij)_{asg}$	Restoration key assigned to N(ij)
$Kres\_N(ij)_{rtd}$	Restoration key returned from N(ij)
μ	Blacklist
∈	Member of
⊂	Proper subset of
‖	Concatenation
F	Flag
Ts	Timestamp

B. Filtering and Network Preparation Step

After the delegate and orchestrator nodes elections comes the stage where the network prepares for the sending phase, which

includes isolating malicious nodes and filtering the network, thus providing the first degree of security. Each of the nodes elected as NO builds its own restoration key Kres_NO and deconstructs it into several partial restoration keys so that each part is assigned to an ND constituting its hierarchy, with ND(i) being the i^{th} ND in the NO(k) hierarchy:

Kres_NO(k) = Kres_ND(1)‖Kres_ND(2).....‖Kres_ND(i)

Each of the nodes elected as ND extracts from its Kres_ND several restoration keys via a permutation function, and activates the distribution task so that each key is assigned to a node constituting its hierarchy, N(ij) being the j^{th} N in the ND(i) hierarchy. Based on these Kres_NDs, each delegate node can clean up its batch before starting the message sending process. To do this, it will check the compatibility between the shared keys in order to isolate malicious nodes belonging to its selectors. The delegate and orchestrator nodes activate the key verification task with the nodes of their tree to isolate malicious nodes and thus clean the network as described below:

Kres_N(ij)asg = Kres_N(ij)rtd → The associated node will be kept in the network.

Kres_N(ij)asg ≠ Kres_N(ij)rtd, → The associated node will be isolated from the network.

III. CASE STUDY: APPLICATION OF THE MSPA-OLSR PROTOCOL

The Optimized Link State Routing (OLSR) protocol is a proactive routing protocol designed for MANETs. OLSR offers several advantages over and demonstrates better performance under attack scenarios. A technical comparison with DSR, AODV, and DSDV can be seen in Table II.

TABLE II. ROUTING PROTOCOLS' CHARACTERISTICS COMPARISON

Protocol Property	**DSDV**	**AODV**	**DSR**	**OLSR**
Proactive	Y	N	N	Y
Distributed	Y	Y	Y	Y
Unidirectional Link	N	N	Y	Y
Multicast	N	Y	N	Y
Periodic Broadcast	Y	Y	N	Y
Reactive	N	Y	Y	N
Routes maintained in	Route Table	Route Cache	Route Table	Route Table

We propose incorporating the MSPA security concept into the OLSR standard, resulting in a new MSPA-OLSR secure version.

A. *Initialization Step*

Figure 1 shows the network structure after isolating and blacklisting malicious nodes after the ND and NO election. Figure 1 illustrates the ad hoc network on which we will exhibit the proposed scheme and the network generated by using our MSPA-OLSR protocol. Tables III and IV and Figures 2 and 3 display ND and NO designation, respectively.

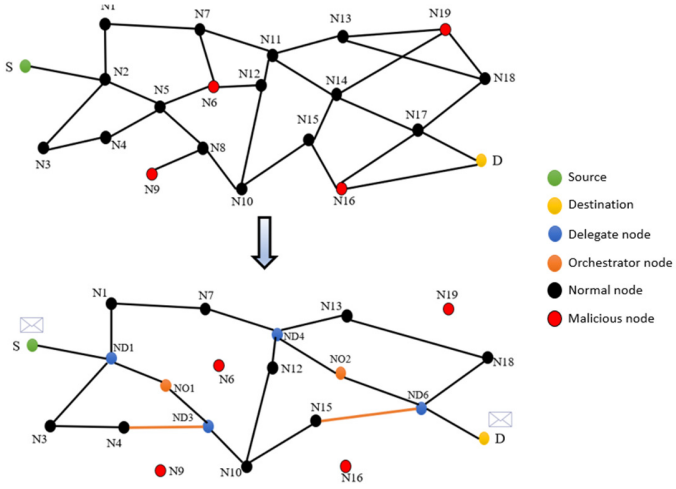

Fig. 1. Initial and final state of the network with MSPA-OLSR protocol.

TABLE III. ND DESIGNATION

ND Tuple	ND Selector set
ND1	S, N1, N2, N3
ND2	N4, N5, N6
ND3	N8, N9, N10
ND4	N7, N11, N12, N13, N14
ND5	N14, N15, N19
ND6	N16, N17, N18, D

TABLE IV. NO DESIGNATION

NO Tuple	NO Selector set
NO1	ND1, ND2, ND3
NO2	ND4, ND5, ND6

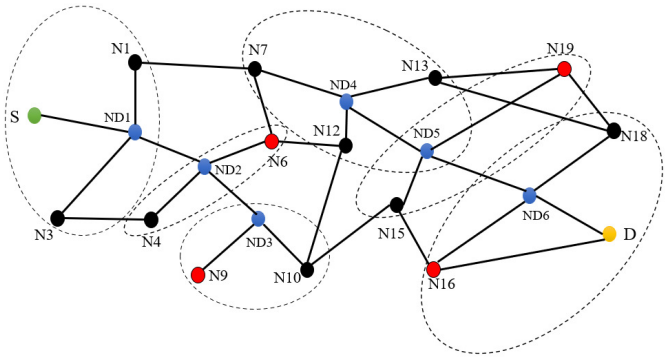

Fig. 2. Demonstration of ND designation.

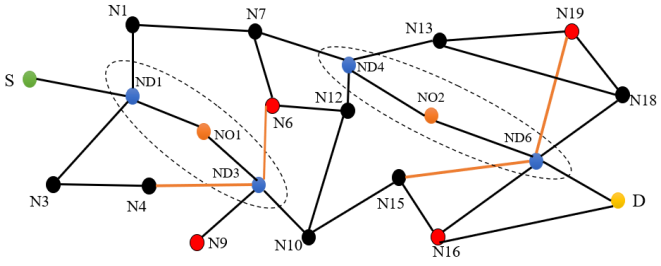

Fig. 3. Demonstration of NO designation.

B. Filtering and Network Preparation Step

After the election of NDs and NOs and the necessary link redirections, comes the stage of preparing the network for sending. This phase involves isolating malicious nodes and filtering the network, thus guaranteeing the first level of security.

Each of the nodes elected as NO builds its own restoration key Kres_NO from which it generates several restoration keys Kres_ND so that each part is sent to an ND constituting its hierarchy. Each of the nodes elected as ND deconstructs it into several partial restoration keys and activates the distribution task so that each part is sent to a node constituting its hierarchy.

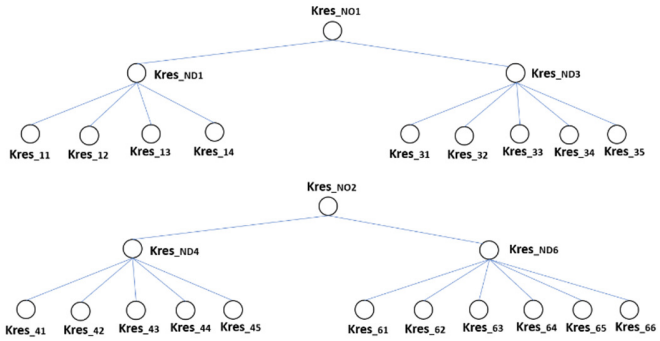

Fig. 4. Demonstration of restoration keys repartition.

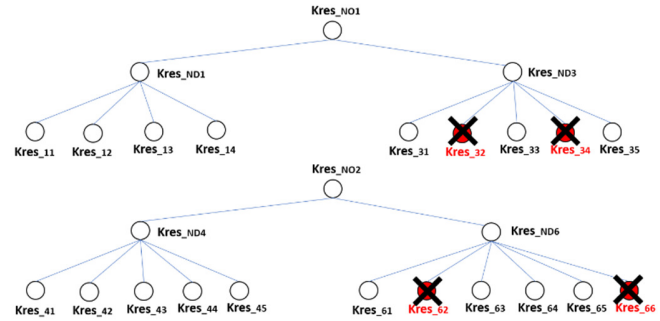

Fig. 5. Demonstration of restoration keys check.

TABLE V. UPDATED ORCHESTRATION TABLE

ND	ND Selector set	Redirected nodes	Isolated nodes	Updated ND selectors set
ND1	S, N1, N2, N3	∅	∅	S, N1,N2, N3
ND3	N8, N9, N10	N4, N6	N6, N9	N4, N8, N10
ND4	N7, N11, N12, N13, N14	∅	∅	N7, N11, 12, N13, N14
ND6	N16, N17, N18, D	N15, N19	N16, N19	N15, N17, N18, D

IV. MSPA-OLSR MESSAGE FORMATS

A. Initialization Step

OLSR is a proactive routing protocol that operates without a central entity in a distributed mobile ad hoc environment. We have implemented a secure version named MSPA-OLSR by incorporating the MSPA security concept into the OLSR protocol. This achievement was made possible through modifications to the structure of the standard protocol's Hello message, which now includes the essential parameters for selecting ND and NO. According to MSPA-OLSR, a node calculates its relative speed, relative acceleration, and relative direction with its neighbors, which reflects its stability, while the credibility coefficient C reflects the behavior of the node in terms of receiving and forwarding packets whose value is updated periodically each time HELLO messages are exchanged, and Resid-Energy reflects the energy remaining of the node. Figure 6 displays the standard HELLO message and Figure 7 illustrates the new HELLO message format which includes all the information mentioned above.

Byte 0 0 1 2 3 4 5 6 7	Byte 1 0 1 2 3 4 5 6 7	Byte 2 0 1 2 3 4 5 6 7	Byte 3 0 1 2 3 4 5 6 7
Reserved		Htime	Willingness
Link Code	Reserved	Link Message Size	
Neighbor Interface Address			
Neighbor Interface Address			
. . .			

Fig. 6. Standard HELLO message format.

Byte 0 0 1 2 3 4 5 6 7	Byte 1 0 1 2 3 4 5 6 7	Byte 2 0 1 2 3 4 5 6 7	Byte 3 0 1 2 3 4 5 6 7
Reserved		Htime	Willingness
Rel_Velocity	Rel_Acceleration	Resid_energy	C
Link Code	Reserved	Link Message Size	
Neighbor Interface Address			
Neighbor Interface Address			
. . .			

Fig. 7. MSPA-OLSR HELLO message format.

B. Initialization Step

In the implementation of the proposed MSPA-OLSR, we introduce specific messages, as can be seen in Figures 8 and 9.

Byte 0 0 1 2 3 4 5 6 7	Byte 1 0 1 2 3 4 5 6 7	Byte 2 0 1 2 3 4 5 6 7	Byte 3 0 1 2 3 4 5 6 7
Reserved		Timestamp	
Issuer Identifier			
Assigned Kres			

Fig. 8. KresREQ message format.

Byte 0 0 1 2 3 4 5 6 7	Byte 1 0 1 2 3 4 5 6 7	Byte 2 0 1 2 3 4 5 6 7	Byte 3 0 1 2 3 4 5 6 7
Reserved		Timestamp	
Issuer Identifier			
Returned Kres			

Fig. 9. KresREP message format.

The KresREQ (Restoration Key Request) message and KresREP (Restoration Key Reply) message are attached to all outgoing OLSR packets. The KresREQ message includes the issuer identifier and restoration key assigned to the node, while the KresREP message includes the returned restoration key and issuer identifier.

Algorithm 1 presents the creation of the restoration key by each NO and the splitting that it performs in order to assign each part of this key to one of its selectors. For the restoration keys allocated to NDs and will be affected to their selectors, we utilize the permutation Algorithm 2.

```
Algorithm 1: Restoration key split
function
1: Initialize
2: s=number of NoSelectors
3: 4 is the length of the substrings
(subKres to be affected to
NoSelectors)
 4: Generate a random string of length
4*s, KresNO
5: For i ranging from 0 to (4*s – 1) with
a step of 4
6: Display the substring of KresNO from i
to i + 4
7: End for
8: End

Algorithm 2: Permutation function
1: Initialize
2: String KresND
3.Number of permutations = w
4: list ← convert string to a list of
characters
5: Build a max heap from the list
6: result ← an empty list to store the
permutations
7: i ← 0
8: While i <= w
9: permutation ← convert the list to a
string
10: result[i] ← permutation
11: i ← i+1
12: Permute the elements of the max heap
to get the next     permutation
13: end while
14: return result
15: End
```

V. SIMULATION AND DISCUSSION

A. Network Simulator and Simulation Environment

We simulated the first and second phases of the proposed MSPA-OLSR protocol and the results were compared with those of the standard OLSR protocol. The third phase of our solution will be the subject of a future study. To test the functionality and performance of our protocol, we used the NS-3.29 simulator [17] by running the mobile nodes in the network with random positions. The simulation environment parameters are outlined in Table VI.

TABLE VI. SIMULATION PARAMETERS

Parameter	Value
Simulator	NS-3.29
Routing protocol	OLSR, MSPA-OLSR
Number of nodes	20, 30, 40, 50, 60, 70, 80, 90 and 100
Simulation time	200 s
Transmission range	100 m
Wi-Fi mode	Ad hoc
Mobility model	Random Waypoint
Pause time	0
Node speed	10 m/s
Environment area	1000 m × 1000 m
Attacker node (Blackhole)	10% of the network nodes

B. Evaluation Metrics

The performance evaluation was based on several network metrics associated with packet transmission efficiency and delay characteristics. These parameters were considered under different network density conditions by progressively changing the number of participating nodes. The utilized metrics are:

- End-to-End (E2E) delay: describes the transfer time of the packet from the source to destination. If it is not respected the contained data in the transmitted packet become useless for the application.
- Packet Delivery Ratio (PDR): A percentage of whether a protocol sent all outgoing data. Its value is the ratio between received packets by the destination node D_p and those sent by the source node S_p.
- Throughput (bits/sec): refers to the network connection quality, calculated as the amount of data successfully transferred across nodes in a given time.

C. Experimental Results and Discussion

Mobile ad hoc networks are vulnerable to several security threats, among which the black hole attack is particularly significant. In this attack, malicious nodes falsely advertise optimal routes to attract traffic, then intentionally drop routing and data packets, thereby disrupting end-to-end communication while appearing as legitimate forwarding nodes. This section evaluates the effect of Black Hole (BH) attacks.

Figure 10 depicts the evolution of the PDR for OLSR and MSPA-OLSR as a function of network density, with and without BH attacks. Under normal operating conditions, where no attack is present, both protocols exhibit a similar pattern in terms of PDR since the added filtering algorithm is not yet activated. However, when an attack is detected, OLSR's PDR decreases by an average of 63%, whereas MSPA-OLSR only experiences an average decrease of 15%. This represents a 48% gain highlighting its effectiveness against BH attacks by eliminating a set of malicious nodes from the network. As a result, MSPA-OLSR manages to maintain a higher PDR compared to OLSR, demonstrating its ability to detect and eliminate malicious nodes, thereby enhancing packet delivery reliability in the network.

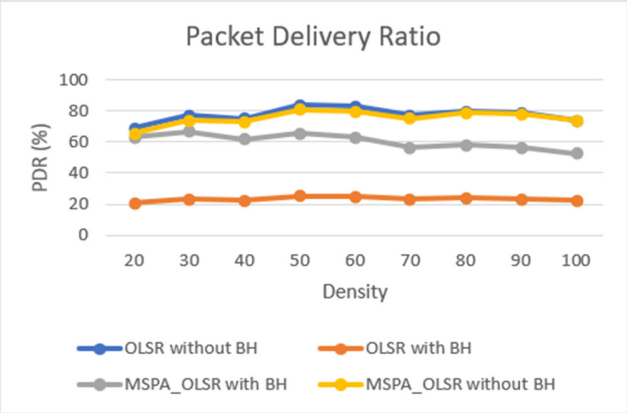

Fig. 10. PDR as a function of network density.

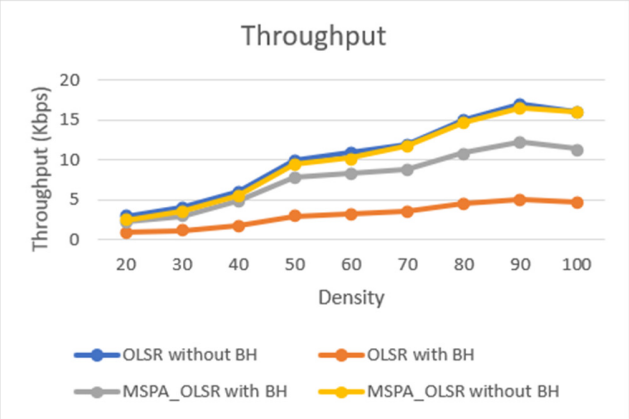

Fig. 11. Throughput as a function of network density.

According to Figure 11, when the network density is low (i.e., with 20 and 30 nodes), the throughput values obtained for OLSR and MSPA-OLSR are similar. This is because the BHs are not numerous or strategically positioned enough to have a significant impact on the network's throughput, and consequently, the performance of both protocols is comparable. However, as the network density increases, the presence of a BH attack has a more significant impact on throughput. In this case, OLSR experiences a 70% decrease in throughput, while MSPA-OLSR only incurs a decrease of approximately 11%. This outcome demonstrates that the proposed protocol ensures better quality of service and greater resilience against BH attacks.

MSPA-OLSR has successfully surpassed OLSR in terms of PDR, indicating an improvement in packet delivery reliability. However, as a trade-off, it has experienced a 23% increase in E2E delay, as shown in Figure 12, meaning that the average packet transmission was slightly prolonged. This increase in E2E delay can be attributed to the addition of new messages that facilitate the functioning of MSPA and the filtering algorithm aimed at eliminating malicious nodes in the network. The filtering algorithm requires additional processing time to analyze and verify nodes, leading to a slight overall delay increase.

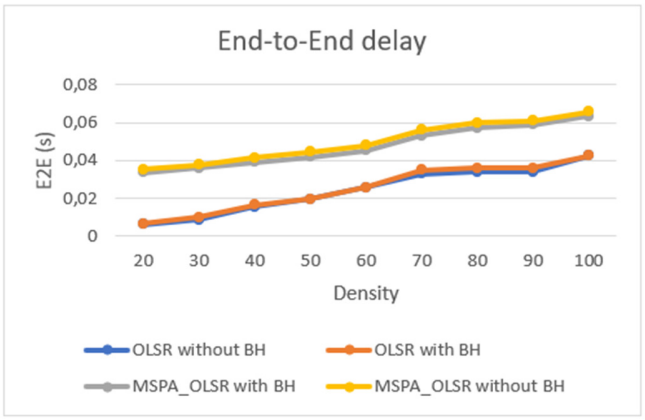

Fig. 12. E2E delay as a function of network density.

VI. CONCLUSION

In this paper, we presented the incorporation of the MSPA security concept into the OLSR standard, resulting in a new secure version called MSPA-OLSR. The simulation results of the proposed protocol under NS3 simulator show that MSPA-OLSR leads to an average improvement of 48% in the packet delivery ratio and 59% in throughput in a black hole attack scenario, depending on network density. This new version provides better security and quality of service metrics compared to the original version in an attack network. However, the filtering algorithm may slightly increase the end-to-end delay. Nevertheless, in security-critical domains such as healthcare, military, emergency, and Industry 4.0 networks, this trade-off remains acceptable given the enhanced security and reliability of data transmission.

DECLARATION OF COMPETING INTERESTS

The authors declare no conflicts of interest.

ACKNOWLEDGMENT

Not applicable to this work.

DATA AVAILABILITY

Simulation parameters are given within the paper.

REFERENCES

[1] R. Jain, "Ant Colony Inspired Energy Efficient OLSR (AC-OLSR) Routing Protocol in MANETS," *Wireless Personal Communications*, vol. 124, no. 4, pp. 3307–3320, June 2022, https://doi.org/10.1007/s11277-022-09514-3.

[2] I. Baird, I. Wadhaj, B. Ghaleb, and C. Thomson, "Impact Analysis of Security Attacks on Mobile Ad Hoc Networks (MANETs)," *Electronics*, vol. 13, no. 16, Aug. 2024, https://doi.org/10.3390/electronics13163314.

[3] N. Mouchfiq, A. Habbani, and C. Benjbara, "Security Issues in MANETs: A Survey," in *Proceedings of Fifth International Congress on Information and Communication Technology*, 2021, pp. 288–295, https://doi.org/10.1007/978-981-15-5859-7_28.

[4] S. Sangheethaa, "A comparative study for block chain applications in the MANET." arXiv, June 15, 2023, https://doi.org/10.48550/arXiv.2306.08899.

[5] J. M. Kizza, "Introduction to Computer Network Vulnerabilities," in *Guide to Computer Network Security*, J. M. Kizza, Ed. Cham: Springer International Publishing, 2017, pp. 87–103.

[6] C. Selvan, M. A. Gunavathie, S. A. Alex, and S. J. Hussain, "An Energy-Efficient Multipath Routing Protocol for Secure Video-Packet Transmission Across MANETs Using a Blockchain Framework," *International Journal of Communication Systems*, vol. 39, no. 2, 2026, Art. no. e70363, https://doi.org/10.1002/dac.70363.

[7] F. Lakrami, M. E. Kamili, N. Elkamoun, H. Sounni, and O. Labouidya, "A secure based trust model for Optimized Link State Routing protocol (OLSR)," in *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, July 2023, pp. 1–5, https://doi.org/10.1109/WINCOM59760.2023.10323026.

[8] P. Mohanraj and S. Anbu Karuppusamy, "Efficient security framework against sybil attack in mobile adhoc network using EE-OLSR protocol scheme," *Wireless Networks*, vol. 30, no. 2, pp. 661–669, Feb. 2024, https://doi.org/10.1007/s11276-023-03502-6.

[9] R. P. Premanand and A. Rajaram, "Enhanced data accuracy based PATH discovery using backing route selection algorithm in MANET," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 2089–2098, Nov. 2020, https://doi.org/10.1007/s12083-019-00824-1.

[10] S. Rahamat Basha *et al.*, "Implementation of Reliability Antecedent Forwarding Technique Using Straddling Path Recovery in Manet," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, 2022, Art. no. 6489185, https://doi.org/10.1155/2022/6489185.

[11] G. Vidhya Lakshmi and P. Vaishnavi, "A trusted security approach to detect and isolate routing attacks in mobile ad hoc networks," *Journal of Engineering Research*, vol. 12, no. 3, pp. 379–386, Sept. 2024, https://doi.org/10.1016/j.jer.2023.100149.

[12] M. M. Muhammad and H. A. A. AL-Asadi, "A Deep Learning-Based Enhancement to OLSR for Robust Attack Detection and Secure Multimedia Transmission in MANETs," *Journal of Basrah Research Sciences*, vol. 51, no. 1, pp. 15–15, June 2025, https://doi.org/10.56714/bjrs.51.1.17.

[13] X. Huo, "Blockchain-Based Distributed Network Security Architecture with Smart Contract Vulnerability Detection Using Improved Tree CNN," *Informatica*, vol. 49, no. 17, Mar. 2025, https://doi.org/10.31449/inf.v49i17.8050.

[14] V. R. Sugumaran, E. Dinesh, R. Ramya, and E. Muniyandy, "Distributed blockchain assisted secure data aggregation scheme for risk-aware zone-based MANET," *Scientific Reports*, vol. 15, no. 1, Mar. 2025, Art. no. 8022, https://doi.org/10.1038/s41598-025-92656-8.

[15] V. S. Naresh, V. V. L. D. Allavarpu, S. Reddi, P. S. R. Murty, N. V. S. L. Raju, and R. N. V. J. Mohan, "A provably secure sharding based blockchain smart contract centric hierarchical group key agreement for large wireless ad-hoc networks," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 3, 2022, Art. no. e6553, https://doi.org/10.1002/cpe.6553.

[16] Nada Mouchfiq, "Novel Collaborative Approaches for Mobile Environment's Security," Ph.D. dissertation, Mohammed V University in Rabat, Rabat, Morocco, 2023.

[17] "ns-3 Network Simulator," *ns-3*. https://www.nsnam.org/.