Towards Secure Cloud-Enabled Wireless Ad-Hoc Networks: A Novel Cross-Layer Validation Mechanism

Zhenguo LIU
Shandong University of Political Science and Law, Jinan, Shandong, China, 250014

***Abstract*—Network security tackles a broad spectrum of damaging activities that threaten network infrastructure. Addressing these risks is essential to keep data accurate and networks running. This research aims to detect and prevent blackholes and wormholes in cloud-based wireless ad-hoc networks. A new Cross-Layer Validation Mechanism (CLVM) is introduced to detect and counter these dangerous attacks. CLVM boosts network security and ensures data travels through cross-layer interactions. CLVM is tested using NS2 software by performing several simulations and comparing the results with previous methods. The results show that CLVM effectively defends against blackhole and wormhole attacks, which makes it a crucial extra service for cloud computing. CLVM provides a strong defense against new security threats, making sure the network stays reliable and safe.**

Keywords*—Network security; wireless ad-hoc networks; cloud environments; cross-layer validation; blackhole and wormhole attacks

I. INTRODUCTION

Wireless networks play a key role in modern communication technology, enabling worldwide communication [1, 2]. Over the last two decades, progress in wireless communication has transformed our world, offering a range of wireless technologies such as Bluetooth, Wi-Fi, WiMAX, HSPA, 3G, 4G, 5G, ZigBee, Satellite, and NFC [3]. These wireless methods support different uses, from home networking to real-time multimedia and surveillance, adding to energy-saving designs on portable devices. We can split these networks into two main types: infrastructure-based wireless networks and infrastructure-less or Wireless Ad-hoc Networks (WANs) [4].

Infrastructure-based wireless networks rely on a fixed infrastructure in which nodes transmit data to a base station over predetermined routes [5]. Although these networks are reliable, they are typically expensive and unsuitable for hostile environments such as proactive disaster management or military applications where fixed infrastructure may not be available [6]. On the other hand, WANs function without predefined infrastructure. Nodes in these networks can connect to other nodes within their communication range, creating a dynamic, self-configuring, and self-organizing network [7]. They use shared radio channels and enable data forwarding between nodes.

Unlike traditional wireless networks with fixed configurations, cloud-based WANs face unique issues that make their design and operation difficult. These networks must cope with changing layouts where nodes frequently connect or disconnect, resulting in constant shifts in routing paths. Additionally, the sprawling nature of WANs, as well as limited resources such as battery life and processing power, increase the risk of security threats. In cloud environments, these problems are exacerbated as data must be moved and processed across distributed nodes without central control. This setup is vulnerable to smart attacks such as blackhole and wormhole tricks, which can compromise network reliability and access. To address these problems, we need new ideas that increase security and keep the network running. This is the main objective of the Cross-Layer Validation Mechanism (CLVM) that we propose in this study.

Key distinguishing characteristics of ad hoc networks include lack of fixed infrastructure, dynamic topology, multi-hop routing, node heterogeneity, connection variability, scarce resources (power, storage, computing power), and limited physical security [8]. Nodes in WANs can be either mobile or fixed, resulting in two main categories based on mobility: Mobile Ad-hoc Networks (MANETs) and Wireless Sensor Networks (WSNs). MANETs are mobile nodes with no fixed location, while WSNs consist of non-mobile nodes deployed at specific locations [9]. The main differences between these networks are summarized in Table I.

TABLE I. WSN VS. MANET

Feature	WSNs	MANETs
Optimization focus	Power optimization	Both QoS and performance optimization
Communication	Many-to-one	Point-to-point
Routing	Data-centric	Address-centric
Destination	The final destination is known	The final destination is unknown
Power source	Not possible to change or recharge	Can be changed or recharged
Network type	Homogeneous	Heterogeneous
Topology	Static	Dynamic

While WANs offer significant advantages, they present several design and implementation challenges due to node mobility, limited resources, and decentralized network structures. These challenges span different protocol stack layers and increase the complexity of WAN development. In addition, WANs have specific vulnerabilities compared to other traditional networks, which are described below:

- Infrastructure absence: Nodes in these networks lack prior security association and can dynamically join or exit without notice, necessitating mutual trust among participating nodes within the protocol design.
- Wireless links: The unsecured nature of wireless links allows potential adversaries to access the network, lacking the equivalent protection level of wired links, making the network vulnerable to attacks from various directions.
- Limited physical protection: Nodes in WANs are often either minimally protected or entirely unprotected, intensifying network vulnerability due to their dynamic and mobile nature, facilitating easier insertion of malicious nodes.
- Lack of central management: The absence of a central authority enables adversaries to devise new attacks, exploiting the cooperative algorithm present in WANs. Security mechanisms must be adaptive and scalable to cope with dynamic topology changes and node increases.
- Resource constraints: Nodes in these networks have limited computational and power resources, making them susceptible to Denial-of-Service (DoS) attacks that exhaust the limited power source through excessive transmissions or computations.

In ad hoc networks, the absence of a central security system allows bad actors, both inside and outside the network, to put network security and privacy at risk [10]. We can split security attacks into two types based on how they work: passive and active [11]. Passive attacks try to break data privacy by listening in on conversations to gather useful info for future bad actions. This makes them hard to spot [12]. Active attacks go after data integrity and privacy by changing, blocking, repeating, or getting rid of packets being sent. They use different network functions to pull off these attacks [13]. We group these attacks into internal and external based on where they come from. Internal attacks happen when compromised nodes within the same network cause trouble and mess up how the system or network works. External attacks, on the other hand, come from unauthorized outsiders who don't belong to the network [14].

Security mechanisms for ad hoc networks include two main approaches. To prevent security attacks, cryptographic techniques are used as the first line of defense against external attacks to ensure the authenticity and integrity of the data source. However, this mechanism can fail if internal attackers have valid cryptographic keys to launch an attack. Security attack detection and response serves as a secondary line of defense, identifying abnormal activity on the network before it causes damage. The defense offers effective countermeasures against detected attacks.

The rest of this paper follows the following structure. A review of related work in the field of secure WANs is presented in Section II. CLVM is discussed in detail in Section III. The simulation results are presented in Section IV. The paper concludes with a summary of key findings and research directions in Section V.

II. Related Work

Compressive Sensing (CS) data collecting systems may efficiently decrease the transmission cost of WSNs by using the sparsity of compressible signals. While there have been explanations of CS as a symmetric cryptosystem, CS-based data-gathering systems still encounter security risks because of the intricate deployment environment of WSNs. Zhang, et al. [15] developed two viable attack methods for certain applications. They introduced a secure approach for collecting data using compressive sensing. The proposed method improves data privacy through the use of an asymmetric semi-homomorphic encryption technique and minimizes computational costs by utilizing a sparse compressive matrix. To be more precise, the asymmetric approach decreases the complexity of distributing and managing secret keys. Homomorphic encryption enables in-network aggregation in the cipher domain, thereby improving security and achieving network load balancing. The sparsity of the measurement matrix decreases both the computational and transmission costs, therefore offsetting the rising costs associated with homomorphic encryption.

Al-Shayeji and Ebrahim [16] designed a robust and energy-efficient system that minimizes energy use while ensuring privacy. The security strategy employs a customized version of the sharing-based method with a precision-enhanced and encryption-mixed privacy-preserving data aggregation procedure. The first protocol provides authentication and encryption via XOR gates, while the second protocol is a secure data aggregation method that improves security and energy efficiency. An approach to reduce energy usage is presented, which involves asynchronous scheduling duty cycling depending on location, priority, and pre-configuration. The findings indicate that the performance of the system is influenced by factors such as the sensing rate, data transmission frequency, data size, sensor placement and quantity, and smartphone battery capacity. For infrequent use and smaller amounts of data, the energy consumed by operations accounts for just 1% of the total battery capacity of the mobile device. When sensors are placed near the sink, the cost is decreased by more than 70% compared to an unsecured network, but there is an extra cost of 20%. The simulations demonstrate that the expense of encryption decreases with an increase in the quantity of sensors. In addition, as the number of sensors increases, the proximity between nodes reduces, resulting in more sensors entering sleep mode.

Wang, et al. [17] suggested a hierarchical trust system based on fog computing to address security vulnerabilities in cloud-enabled WSNs. This tiered approach has two components: confidence in the foundational framework and trust between cloud service providers (CSPs) and sensor service providers (SSPs). Monitoring behavior is built and executed inside WSNs to ensure confidence in the fundamental framework. At the same time, the intricate and detailed data analysis component is shifted to the fog layer. To establish trust between CSPs and SSPs, it is crucial to prioritize the real-time comparison of service parameters, the collection of exception information in

WSNs, and the focused quantitative assessment of entities. The experimental findings demonstrate that the fog-based topology effectively conserves network energy, swiftly detects malicious nodes, and promptly recovers misjudgment nodes within an appropriate timeframe. Moreover, the dependability of edge nodes is effectively ensured by data analyses conducted in the fog layer, and an assessment approach that relies on comparable service records is proposed.

Hsiao and Sung [18] developed an innovative method to bolster the data security of WSNs by using blockchain technology. They used blockchain technology and data transmission to provide a safe framework for WSNs based on the Internet of Things (IoT) architecture. The research employs embedded microcontrollers such as Raspberry Pi and Arduino Yun to construct a portable database node that gathers sensor data and hash values from preceding blocks. The transaction ledger is converted into a sensor data record, thereby improving the dependability of the WSN structure. The system can process data from a private cloud and display sensor data. The wireless network design is constructed utilizing embedded devices, facilitating the creation of a web server using Python or JavaScript programming languages. The research examines the efficacy of conventional methods against new data transmission methods, concluding that using innovative methods using blockchain technology renders it very difficult for operators to manipulate sensor data.

Haseeb, et al. [19] proposed a protocol for safe data collection in mobile WSNs, which utilizes cloud services. The technique aims to efficiently distribute information in dynamic networks by employing mobile sensors with little loss and power consumption. Furthermore, it guarantees the continuous presence and uniformity of the gathered data inside the cloud organizations while enhancing the routing reliability. The simulation results and their analysis demonstrate the substantial efficacy of the suggested approach.

Sharmila, et al. [20] introduced a hybrid key management system for WSNs linking edge devices. This system utilizes Elliptic Curve Cryptography (ECC) and a hash function to create pre-distribution keys. The key setup is accomplished by simply broadcasting the node identity. The primary purpose of implementing a hybrid technique in the key pre-distribution method is to achieve mutual authentication between the sensor nodes during the installation phase. The suggested solution decreases computing complexity while enhancing security, making it suitable for implementation in sensor nodes with limited resources.

Ensuring the reliable and secure functioning of WSNs necessitates the identification of anomalies. Maximizing resource efficiency is essential for minimizing energy use. Gayathri and Surendran [21] introduced two methods for anomaly detection in WSNs: Ensemble Federated Learning (EFL) with cloud integration and Online Anomaly Detection with Energy-Efficient approaches (OAD-EE) using cloud-based model aggregation. Cloud-integrated EFL uses ensemble approaches and federated learning to improve detection accuracy and safeguard data privacy. OAD-EE, using a cloud-based model aggregation approach, employs online learning and energy-efficient strategies to save energy on sensor nodes. A complete and efficient system for anomaly detection in WSNs is established by integrating EFL and OAD-EE. The experimental findings indicate that adopting cloud technology in EFL leads to the best accuracy in detection. On the other hand, OAD-EE, which utilizes cloud-based model aggregation, exhibits the lowest energy consumption and the shortest detection time among all algorithms. Consequently, OAD-EE is well-suited for real-time applications.

TABLE II. AN OVERVIEW OF RELATED WORKS

Reference	Methodology	Key features	Results
Zhang, et al. [15]	Compressive sensing with asymmetric semi-homomorphic encryption	Uses CS to reduce transmission cost, asymmetric semi-homomorphic encryption for data privacy, and sparse compressive matrix to minimize computational costs	Improved data privacy, network load balancing, decreased computational and transmission costs, offset rising costs associated with homomorphic encryption
Al-Shayeji and Ebrahim [16]	An energy-efficient system with a customized sharing-based method	Sharing-based method for privacy, precision-enhanced and encryption-mixed privacy-preserving data aggregation, asynchronous scheduling duty cycling	Enhanced energy efficiency and security, performance influenced by various factors, energy consumption as low as 1% of mobile device battery for infrequent use, cost reduction over an unsecured network but an additional 20% cost
Wang, et al. [17]	Hierarchical trust system based on fog computing	Trust in foundational framework and between cloud service providers and sensor service providers, real-time comparison of service parameters	Effective energy conservation, swift detection of malicious nodes, reliable data analysis in fog layer, proposed assessment approach relying on service records
Hsiao and Sung [18]	Blockchain technology for data security	Uses blockchain for WSN security, embedded microcontrollers for portable database node, transaction ledger for sensor data, web server creation with Python/JavaScript	Enhanced data dependability and security, difficulty for operators to manipulate sensor data, improved performance of WSN architecture using blockchain technology
Haseeb, et al. [19]	Protocol for safe data collection in mobile WSNs	Uses cloud services for dynamic network information distribution mobile sensors to minimize loss and power consumption, ensures continuous data presence and consistency	Significant efficiency in data collection and routing, enhanced reliability and uniformity of collected data in cloud organizations, substantial efficacy demonstrated through simulation results
Sharmila, et al. [20]	Hybrid key management system using ECC and hash function	Uses ECC and hash function for key pre-distribution, mutual authentication during installation phase, reduced computing complexity	Enhanced security and computing efficiency, suitable for resource-constrained sensor nodes, improved mutual authentication
Gayathri and Surendran [21]	Anomaly detection using EFL and OAD-EE	EFL with cloud integration for accuracy and data privacy, OAD-EE for energy-efficient anomaly detection, combined algorithm for efficient system	Best accuracy in detection with EFL, lowest energy consumption, and shortest detection time with OAD-EE, integrated algorithm improves overall efficiency, scalability, and real-time response

The reviewed related works, as outlined in Table II, address various security and efficiency challenges in wireless sensor networks (WSNs) and mobile ad-hoc networks (MANETs) using diverse methodologies, such as compressive sensing, blockchain technology, and fog computing. However, these approaches encounter specific limitations. For instance, while Zhang, et al. [15] leverage semi-homomorphic encryption to enhance data privacy, the rising costs of this encryption remain a challenge. Similarly, Al-Shayeji and Ebrahim [16] focus on energy efficiency, yet their method incurs an additional 20% cost for security enhancements. Addressing these challenges, the current study introduces a novel mechanism that synergistically integrates the strengths of various approaches to bolster network security and data integrity while minimizing computational and transmission costs. Through extensive NS2 simulations, the proposed method demonstrates superior performance in detecting and mitigating blackhole and wormhole attacks, offering a robust defensive mechanism for cloud-enabled WSNs. This study's main contributions include the development of an efficient, cost-effective security framework that ensures reliable and secure data transmission, thus advancing the state-of-the-art in network security for WSNs and MANETs.

III. Proposed Mechanism

This paper proposes a novel CLVM framework to identify and eliminate malicious activities within network routing protocols. CLVM aims to improve network reliability and data security by setting trust values for individual network elements. This trust scoring helps to find and remove wormhole nodes, making sure data moves over trusted routes. CLVM's main goal is to keep the network secure by spotting and containing harmful activities before they cause trouble. It does this in two ways. The framework has ways to detect and stop harmful activity in the network. This includes picking trusted paths to send data, which helps avoid potential threats. CLVM gives trust scores to network parts based on a full evaluation. This lets the framework prioritize data transfer across reliable and trustworthy nodes. Fig. 1 shows how CLVM works overall. The framework spots harmful activity by looking at how individual nodes in the network behave. During route discovery, nearby nodes are picked, and each node confirms it got and sent on data packets.

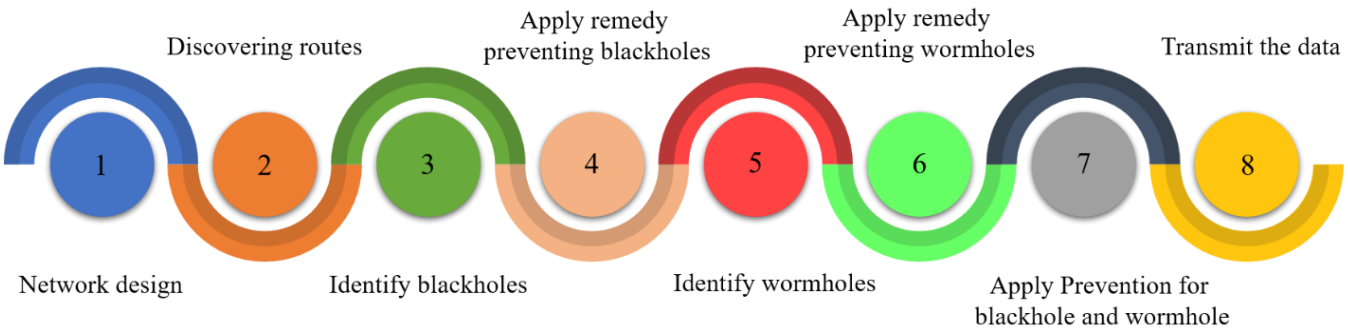

Fig. 1. Workflow of the cross-layer validation mechanism.

The Round-Trip Time (RTT) associated with data packet communication is a key anomaly detection metric. The framework leverages the Request-To-Send (RTS)/Clear-To-Send (CTS) handshake mechanism within the Media Access Control (MAC) layer to determine RTT. Significant variations in RTT can indicate the presence of a blackhole node, where a node along the designated route discards incoming packets instead of forwarding them. Fig. 2 depicts a typical blackhole attack scenario. In this example, data is transmitted from source node S to destination node D via nodes 7 and 8. However, node 2, acting maliciously, accumulates all incoming data packets without forwarding them. The extended RTT caused by this behavior can be identified through the RTS/CTS mechanism, exposing the blackhole node.

The IEEE 802.11 standard defines the Media Access Control (MAC) layer protocol for wireless local area networks (WLANs). This protocol leverages Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to minimize collisions during data transmission. CSMA/CA mandates that nodes listen for ongoing transmissions before initiating their own, significantly reducing the likelihood of packet collisions.

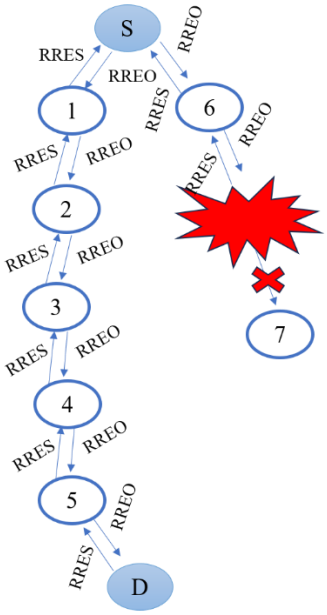

Fig. 2. Blackhole attack scenario in a WAN.

In CSMA/CA, the Request-To-Send/Clear-To-Send (RTS/CTS) handshake process offers a way to cut down on collisions even more when hidden terminals are involved. This method works like this: A node that wants to send data first transmits an RTS frame to the receiver it's aiming for. When the receiver gets this RTS frame, it sends back a CTS frame, which sets aside the channel for the upcoming data transmission. Other nodes in the area pick up on this CTS frame and hold off on sending anything during this reserved time slot, which stops collisions from happening.

While the RTS/CTS handshake solves the hidden terminal problem, it adds extra work because of the RTS and CTS frame exchange. This extra work can have a big impact on network speed when many nodes are active in a small area. Researchers have looked into other ways to reduce this extra work, but the possible benefits haven't been worth the added complexity these changes would bring.

Another consideration for WLANs is the power consumption associated with RTS/CTS frames and data packets. The Power Control Mechanism (PCM) can adjust transmission power levels based on specific needs. Typically, RTS/CTS frames are transmitted at a higher power level (Pmax) to ensure wider reception, whereas data packets might utilize a lower power level to conserve energy. However, PCM might occasionally raise the transmission power of data packets to Pmax to overcome potential signal degradation. Acknowledgment (ACK) packets are generally transmitted at a lower power level.

The importance of minimizing collisions in the MAC layer stems from the power consumption associated with retransmissions. Retransmissions not only waste bandwidth but also deplete battery life in mobile devices. While RTS/CTS-based protocols offer advantages, they do not eliminate the hidden terminal and exposed terminal problems, especially in high-density networks. Furthermore, migrating such protocols to cloud-based environments introduces additional challenges that must be addressed. This paper proposes a secure routing protocol designed to establish reliable communication paths within a network while mitigating the risks of wormhole nodes. The protocol operates under the following assumptions:

- Transmission range: All participating nodes are confined within a predefined transmission range (R).
- Node mobility: Nodes are considered stationary for routing calculations. Real-world deployments might involve mobile nodes, requiring adjustments to the protocol.
- Neighbor discovery: Nodes can discover and communicate with neighboring nodes within their transmission range.

The core objective of the protocol lies in identifying a secure path between a source node (S) and a destination node (D). The distance between these nodes (d) is calculated using Eq. (1), which factors in the transmission range (R) and the average node speed (V). The transmission range can be dynamically adjusted within a predefined threshold based on the varying distances between nodes. A weighted average distance is also employed as a stopping condition for route discovery.

$$Dist_{SD} = \frac{R - d}{V(R - D)} \quad (1)$$

To enhance security, each node maintains a counter variable initialized to zero. This counter is incremented whenever a designated operator node retrieves data from a particular node. The operator node can connect and disconnect from any node within the network. The counter reflects the number of interactions a node has had with the operator. If multiple operators collect data from the same node (node-S), the data on the destination node stored by the operator with the higher counter value takes precedence. The counter range is also configurable, with a minimum value of zero and a maximum value determined by the network's reach.

Unique identifiers are assigned to each node to facilitate secure communication. Data packets transmitted within the network encompass various fields, including a packet ID, distance traveled, counter value, and potential information regarding intermediate nodes. The validity of these parameters, including details about intermediate nodes, is verified at each network layer until the data reaches its intended destination.

Route discovery and data transmission processes leverage a routing table (R-table) that stores information about nodes and established routes. This information is constantly compared against the data packets to ensure validity. Since source nodes are assumed to be geographically close, any node can access details on neighboring nodes. Data is then forwarded to the nearest available node along the designated path.

The paper highlights a potential security concern: a wormhole attack scenario. In this scenario, a malicious node (node-S) intercepts data packets from the source node and transmits them to another colluding node (node-8) closer to the destination. Node-S then impersonates node-7, the intended recipient of the data from the source, by altering its ID to match node-7's. Consequently, the source node is deceived into believing it communicates directly with node-7, establishing a wormhole connection. The proposed protocol must have mechanisms to identify and counteract such wormhole attacks.

Unlike traditional routing protocols, where multiple nodes might operate on the same radio frequency, this approach assigns unique channels to individual nodes. This distinctiveness allows the source node to verify the legitimacy of neighboring nodes by transmitting on a randomly chosen channel.

The core principle assumes a legitimate neighboring node can detect a message transmitted on its designated channel. In contrast, a wormhole node lacking knowledge of the correct channel will miss the transmission. The probability of a source node failing to detect a wormhole node through a single random channel test can be calculated using Eq. (2). In this equation, 'n' represents the total number of neighbors, and 'S' represents the number of suspected wormhole nodes within the set of neighbors.

$$P_r = \sum_{all\ S,M,G} P_r(S,M,G)P_r(detection|S,M,G) = \sum_{all\ S,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G} S-(m-M}{\binom{n}{c} c} \quad (2)$$

The channel frequency diversity approach can be extended to enhance detection accuracy by conducting multiple rounds of random channel tests (denoted by 'r' in Eq. (3)). With each round, the source node selects a random subset of neighbors and a random channel for transmission. Eq. (3) calculates the probability of failing to detect a wormhole node after 'r' rounds of testing.

$$P_r(decontt = 1 - P_r(nondetection)_{1round}^{r} = 1 - (1 - P_r((P_r)_{1round}^{r} = 1 - \left(1 - \sum_{all,S,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G} S-m-M)}{\binom{n}{c} c}\right) r \quad (3)$$

This technique assumes a network scenario where a node's neighbors might encompass 'S' wormhole nodes, 'M' malicious nodes of other types, and 'G' legitimate nodes. Due to practical constraints, the source node can only test a limited number of neighbors at a time. Eq. (2) factors the possibility of encountering a wormhole node, a malicious node of a different type, or a legitimate node within the chosen subset of 'C' neighbors. By analyzing the probability ratio derived from Eq. (2) and Eq. (3), it can be concluded that the channel frequency diversity approach offers a viable solution for detecting wormhole nodes within various Wide Area Network (WAN) topologies.

IV. Results and Discussion

The CLVM was implemented and evaluated using the NS-2.5 network simulator. Table III summarizes the simulation parameters employed in the evaluation process. The primary objective of this evaluation was to assess the efficiency of CLVM relative to an existing approach, LBIDS [22]. The simulations were conducted in a 1000 x 1000 m network area, simulating a typical wireless ad hoc network environment. The nodes were randomly distributed across this area, with the number of nodes varying between 10 and 50 over five rounds of simulation, increasing by ten nodes per round. Node mobility was simulated using the random waypoint mobility model, with node speeds ranging from 1 to 15 m/s, reflecting the dynamic nature of real-world ad hoc networks.

The radio propagation model used was the two-ray ground reflection model, which takes into account both direct and ground-reflected paths of signal propagation, allowing for a more realistic simulation of wireless communications. The transmission range of each node was set to 250 meters, with the MAC layer using the IEEE 802.11 standard. Traffic was generated using a constant bit rate (CBR) application with packet sizes of 50 bytes, simulating a typical data transfer scenario. Energy consumption was modeled based on the remaining energy level of nodes after each round, using mechanisms such as RTS/CTS handshakes and distance checking to save energy.

TABLE III. Simulation Parameters and Values

Parameter	Value
Simulation area	1000m x 1000m
Malicious node ID count	2
Malicious node percentage	Up to 5%
Node placement	Random
Simulation duration	100 seconds
Packet size	50 bytes
Traffic type	CBR, 100 – 500
MAC protocol	802.11
Total nodes	20 – 750
Transmission range	250 m
Propagation model	Two-ray ground reflection
Node Speed	1 – 15 m/s

A. Transmission Delay Analysis

Fig. 3 compares the average transmission delay incurred by each approach across the five rounds. The results demonstrate that CLVM consistently exhibits lower transmission delay compared to LBIDS. In the case of round five with 50 nodes, LBIDS exhibits a transmission delay of 46 milliseconds (ms), whereas CLVM achieves a delay of only 24 ms. This improvement can be attributed to the efficiency gains introduced by CLVM's mechanisms, such as trust value evaluation and route selection.

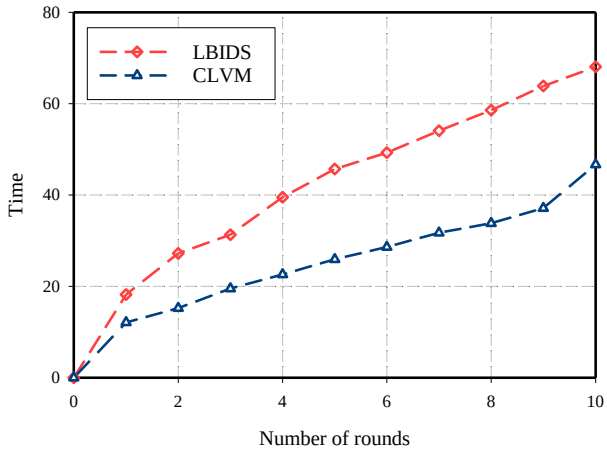

Fig. 3. Average transmission delay comparison.

B. Throughput Analysis

Throughput, measured by the successful transmission and reception of data packets, serves as another key performance metric. Fig. 4 depicts the throughput achieved by both CLVM and LBIDS across the five rounds. The results indicate that CLVM consistently delivers superior throughput compared to LBIDS. This can be primarily explained by CLVM's ability to mitigate malicious activities that disrupt data transmission within the network. For example, in round five, LBIDS achieves a throughput of 6123 packets, whereas CLVM delivers a higher throughput of 6400 packets.

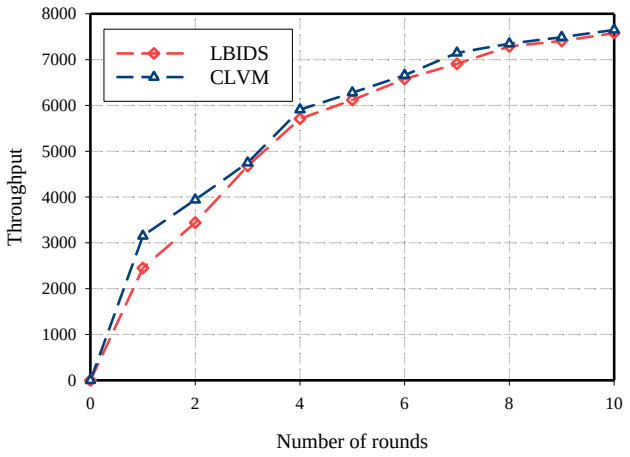

Fig. 4. Average throughput comparison.

C. Energy Consumption Analysis

The remaining energy level of network nodes after each round was evaluated to assess the energy efficiency of both approaches. Fig. 5 presents the results, indicating that CLVM nodes conserve more energy than LBIDS nodes. This is a consequence of CLVM's strategies for reducing unnecessary communication and data transmissions. Mechanisms like RTS/CTS handshakes and distance verification contribute to this energy conservation. Nodes are unable to transmit data if they fail to provide valid IDs or adhere to the RTS/CTS protocol and distance requirements. This helps to preserve node energy. The simulations reveal that in round five, the remaining energy level for LBIDS nodes is 95%, whereas CLVM nodes retain a higher energy level of 96%.

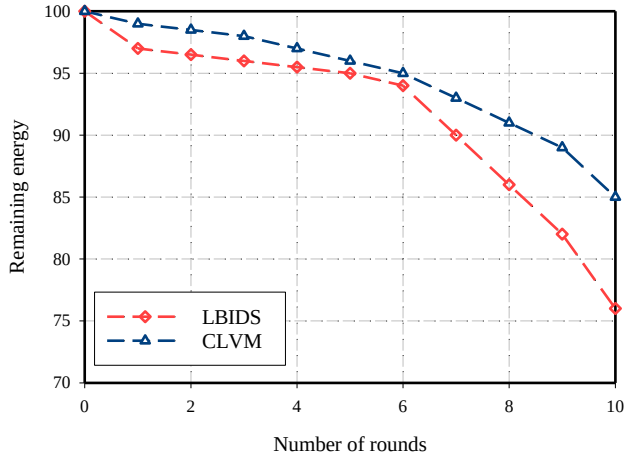

Fig. 5. Remaining energy comparison.

D. Malicious Activity Detection Analysis

The simulations also evaluated the effectiveness of both approaches in detecting malicious activities within the network. CLVM's algorithm leverages a long-established foundation and incorporates node behavior analysis for comprehensive malicious node identification. Fig. 6 compares the number of malicious activities detected using LBIDS and CLVM. The results demonstrate that CLVM significantly reduces the number of malicious activities within the network. This improvement stems from CLVM's verification of critical parameters like node ID, RTS/CTS compliance, and transmission distance during data exchange. Additionally, CLVM maintains a database for comparison purposes, enabling it to identify nodes that deviate from expected behavior and potentially block them. While LBIDS focuses on detection, CLVM prioritizes prevention by proactively identifying and mitigating potential threats.

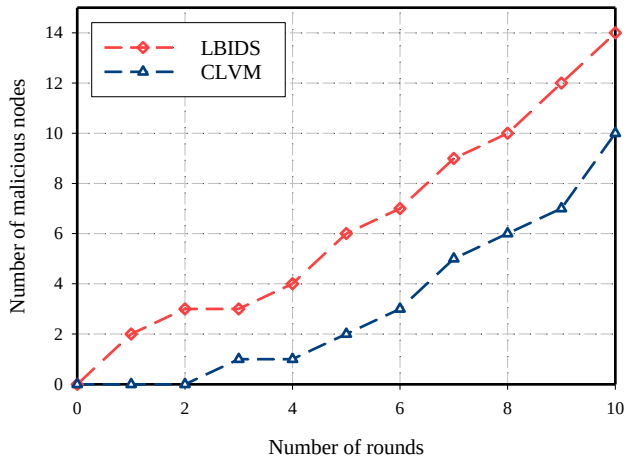

Fig. 6. The number of malicious activities comparison.

The obtained results clearly show that CLVM not only outperforms the existing LBIDS approach in practical metrics such as transmission delay, throughput, and energy consumption but also embodies significant theoretical advances. CLVM's integration into existing network protocols is achieved through its trust-based validation process, which improves route selection and mitigates malicious activity more effectively than traditional methods. By prioritizing trust assessment at multiple levels, CLVM eliminates the limitations of LBIDS, which focuses primarily on detection rather than prevention. This cross-layer approach allows CLVM to reduce transmission delays and energy consumption while maintaining high throughput, providing a more holistic and efficient network security solution. CLVM's theoretical robustness, combined with its practical effectiveness, makes it a superior alternative to existing security mechanisms in cloud-enabled wireless ad hoc networks.

The simulation setup was designed to closely mimic real-world scenarios by incorporating widely used models such as random waypoint mobility and two-ray ground reflection. These models simulate the unpredictable movement of nodes or realistic signal propagation in an open environment. The range of node speeds and the random distribution of nodes reflect the dynamic and decentralized nature of cloud-enabled wireless ad hoc networks. However, it is important to note that certain simplifications were made in the simulation. For example, environmental factors such as obstacles and interference, which can significantly impact signal propagation and network performance in real-world scenarios, have not been fully modeled. In addition, the simulations assumed idealized conditions for node operations and communications, which may differ from the more complex and variable conditions encountered in actual operations.

V. CONCLUSION

This study introduced CLVM as an innovative solution to enhance the security and efficiency of cloud-enabled wireless ad-hoc networks. Extensive evaluations demonstrated that CLVM significantly outperforms the existing LBIDS approach in key performance metrics, including transmission delay, throughput, energy consumption, and malicious activity detection. CLVM achieves a remarkable reduction in transmission delay, evidenced by a delay of only 24 milliseconds in a 50-node network compared to LBIDS's 46 milliseconds. Additionally, CLVM consistently delivers higher throughput, with a notable increase to 6400 packets in the same network configuration. Energy efficiency is another critical advantage, as CLVM nodes retain 96.59% of their energy compared to LBIDS's 95.1%, thanks to effective strategies like RTS/CTS handshakes and distance verification protocols. Moreover, CLVM excels in detecting and mitigating malicious activities, leveraging comprehensive node behavior analysis and a proactive approach to threat prevention. These improvements underscore the robustness and reliability of CLVM in securing data transmission and maintaining network integrity.

Looking forward, future research will focus on several key areas to build on the findings of this study. One possible path is to extend the CLVM to other types of wireless networks, such as Vehicular Ad-hoc Networks (VANETs) or industrial IoT environments, where security challenges are even more pronounced. Additionally, optimizing CLVM for larger deployments with hundreds or thousands of nodes is critical to ensure its scalability and efficiency in various network scenarios. Further research could also include integrating CLVM with advanced machine learning algorithms to improve its ability to detect and adapt to new types of security threats in real-time. These future efforts aim to refine and expand CLVM's capabilities, ensuring its relevance and effectiveness in the ever-evolving network security landscape.

REFERENCES

[1] M. A. Tofighi, B. Ousat, J. Zandi, E. Schafir, and A. Kharraz, "Constructs of Deceit: Exploring Nuances in Modern Social Engineering Attacks," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2024: Springer, pp. 107-127, doi: https://doi.org/10.1007/978-3-031-64171-8_6

[2] S. R. Abdul Samad et al., "Analysis of the performance impact of fine-tuned machine learning model for phishing URL detection," Electronics, vol. 12, no. 7, p. 1642, 2023.

[3] B. Pourghebleh, N. Hekmati, Z. Davoudnia, and M. Sadeghi, "A roadmap towards energy‐efficient data fusion methods in the Internet of Things," Concurrency and Computation: Practice and Experience, vol. 34, no. 15, p. e6959, 2022.

[4] B. Pourghebleh and V. Hayyolalam, "A comprehensive and systematic review of the load balancing mechanisms in the Internet of Things," Cluster Computing, pp. 1-21, 2019.

[5] A. Lolai et al., "Reinforcement learning based on routing with infrastructure nodes for data dissemination in vehicular networks (RRIN)," Wireless Networks, vol. 28, no. 5, pp. 2169-2184, 2022.

[6] D. K. Sharma, S. K. Dhurandher, and S. Kumar, "Hierarchical search-based routing protocol for infrastructure-based opportunistic networks," International Journal of Innovative Computing and Applications, vol. 12, no. 2-3, pp. 134-145, 2021.

[7] A. Förster et al., "A beginner's guide to infrastructure‐less networking concepts," IET Networks, vol. 13, no. 1, pp. 66-110, 2024.

[8] S. Al Ajrawi and B. Tran, "Mobile wireless ad-hoc network routing protocols comparison for real-time military application," Spatial Information Research, vol. 32, no. 1, pp. 119-129, 2024.

[9] M. Sohail et al., "Routing protocols in vehicular adhoc networks (vanets): A comprehensive survey," Internet of things, vol. 23, p. 100837, 2023.

[10] V. Chandrasekar et al., "Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm," Scientific Reports, vol. 14, no. 1, p. 7818, 2024.

[11] S. Dong, H. Su, Y. Xia, F. Zhu, X. Hu, and B. Wang, "A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular ad-hoc networks," IEEE Transactions on Intelligent Transportation Systems, 2023.

[12] K. Vamshi Krishna and K. Ganesh Reddy, "Classification of distributed denial of service attacks in VANET: a survey," Wireless Personal Communications, vol. 132, no. 2, pp. 933-964, 2023.

[13] V. Hayyolalam, B. Pourghebleh, and A. A. Pourhaji Kazem, "Trust management of services (TMoS): Investigating the current mechanisms," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 10, p. e4063, 2020.

[14] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9326-9337, 2019.

[15] P. Zhang, S. Wang, K. Guo, and J. Wang, "A secure data collection scheme based on compressive sensing in wireless sensor networks," Ad Hoc Networks, vol. 70, pp. 73-84, 2018.

[16] M. Al-Shayeji and F. Ebrahim, "A secure and energy-efficient platform for the integration of Wireless Sensor Networks and Mobile Cloud Computing," Computer Networks, vol. 165, p. 106956, 2019.

[17] T. Wang, G. Zhang, M. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, "A novel trust mechanism based on fog computing in sensor–cloud system," Future Generation Computer Systems, vol. 109, pp. 573-582, 2020.

[18] S.-J. Hsiao and W.-T. Sung, "Employing blockchain technology to strengthen security of wireless sensor networks," IEEE Access, vol. 9, pp. 72326-72341, 2021.

[19] K. Haseeb, Z. Jan, F. A. Alzahrani, and G. Jeon, "A secure mobile wireless sensor networks based protocol for smart data gathering with cloud," Computers & Electrical Engineering, vol. 97, p. 107584, 2022.

[20] Sharmila, P. Kumar, S. Bhushan, M. Kumar, and M. Alazab, "Secure key management and mutual authentication protocol for wireless sensor network by linking edge devices using hybrid approach," Wireless Personal Communications, vol. 130, no. 4, pp. 2935-2957, 2023.

[21] S. Gayathri and D. Surendran, "Unified ensemble federated learning with cloud computing for online anomaly detection in energy-efficient wireless sensor networks," Journal of Cloud Computing, vol. 13, no. 1, p. 49, 2024.

[22] S. A. Razak, S. Furnell, N. Clarke, and P. Brooke, "A two-tier intrusion detection system for mobile ad hoc networks–a friend approach," in Intelligence and Security Informatics: IEEE International Conference on Intelligence and Security Informatics, ISI 2006, San Diego, CA, USA, May 23-24, 2006. Proceedings 4, 2006: Springer, pp. 590-595.