ELRP: A Trust and IDS-Integrated Opportunistic Routing Protocol for MANETs with NS2-Based Evaluation

Jidong Zhang
School of Information Engineering, Zhengzhou College of Finance and Economics, Zhengzhou 450053, China
E-mail: JD36728001@163.com

Keywords: mobile ad-hoc networks, trust-based routing, opportunistic routing, security, reliability

Received: October 5, 2025

Mobile Ad Hoc Networks (MANETs) are widely used in diverse situations where secure communication and reliability are necessary. MANETs without a centralized infrastructure are prone to various security threats. This paper presents an Enhanced Lightweight Trusted Routing Protocol (ELRP) to ensure secure connectivity and reliability in MANETs. The primary goal of ELRP is to prevent the inclusion of malicious hosts in the route and reliably convey data. Trust metrics provide secure communication by leveraging quality of service parameters to optimize trust computation. Opportunistic routing enhances data reliability and consistency. It allows each node to choose an intermediate node dynamically based on trust levels. Depending on the trust factor, ELRP enables nodes to select the forwarder at runtime. ELRP features an Intrusion Detection System (IDS) designed to recognize and mitigate black and grey hole attacks. ELRP is scalable as it uses local information and does not consume computational resources. Simulations conducted in NS2 demonstrate that ELRP improves throughput by approximately 22%, increases packet delivery ratio by 14.4%, and reduces end-to-end delay by 37.1% compared to standard AODV under malicious attack scenarios.

Povzetek: Predlagan je varen in učinkovit usmerjevalni protokol, ki izboljša zanesljivost komunikacije in odpornost na napade v primerjavi s klasičnimi pristopi.

1 Introduction

Mobile Ad Hoc Networks (MANETs) play a significant role in delivering communication in an environment where traditional infrastructure is either impossible or impractical to coexist [1]. These networks are composed of portable nodes that are connected using wireless technology and operate without fixed infrastructure. This renders the networks extremely portable and practical in various situations, such as military operations [2], disaster response [3], and vehicle networks [4]. The basic nature of MANETs, including fluctuating network formations, limited data transmission capabilities, and the absence of a centralized command system, creates significant challenges, particularly in ensuring safe and reliable communication [5]. Comparable context-aware and adaptive decision-making structures have been studied in recent intelligent transportation research, for instance, the traffic-conscious pedestrian intention prediction model that combines spatio-temporal learning with the dynamics of traffic signal states to enhance behavioral reliability in autonomous environments [6].

MANETs are highly susceptible to various threats, highlighting the security importance. Malicious nodes can easily join the network and disrupt communication by performing black and grey hole attacks. Black and grey hole attacks involve the dropping or selective forwarding of packets, which ultimately compromise the integrity and efficiency of the network in the long run [7]. Conventional routing mechanisms, such as the Ad Hoc On-demand Distance Vector (AODV), are ineffective at identifying or mitigating these threats, resulting in network vulnerabilities [8].

To address these security issues, the current study proposes an Enhanced Lightweight Trust-based Routing Protocol (ELRP). ELRP's primary objective is to enhance the security and reliability of the MANET by eliminating the contribution of malicious nodes to the routing process and ensuring end-to-end data transmission. ELRP applies the extracted trust measures from the Quality of Service (QoS) factors to ease the selection of secure and mobile routes. ELRP enables opportunistic routing, allowing nodes to dynamically change intermediate nodes based on the level of trust, resulting in higher dependability and consistency of the transmitted data.

A unique aspect of ELRP lies in its built-in Intrusion Detection System (IDS), developed to identify and neutralize black and grey-hole attacks. It has an IDS to observe network traffic, allowing it to identify unusual activities and quarantine malicious nodes. This ensures network protection against typical security threats. ELRP is also designed to be easily customizable and resource-efficient. It determines routes based on local information, minimizes computation, and makes it applicable in environments where resources are limited.

The performance of ELRP is evaluated by comparing it with the popular AODV protocol with respect to key metrics such as throughput, delay, packet delivery ratio, and packet loss ratio. Simulation results indicate that ELRP significantly improves the safe and reliable routing

of networks, particularly in the MANET case. This work addresses the security issues inherent to networks of this type. It addresses the following two major research questions:

- Can trust metrics derived solely from local and one-hop observations improve routing reliability and security in MANETs under the presence of malicious nodes?
- Can an integrated lightweight IDS effectively detect and mitigate black-hole and grey-hole attacks without imposing significant computational or communication overhead?

2 Related work

Various routing schemes proposed are presented in Table 1 for enhancing the security and reliability of MANETs. The AODV routing protocol is widely utilized due to its efficiency and simplicity. Despite this fact, it is prone to a large number of security threats because it lacks a robust mechanism for detecting and removing malicious nodes. These vulnerabilities have been addressed through trust-based routing protocols. By evaluating trust metrics, these protocols enhance the security of communication between nodes. However, many existing trust-based protocols demand considerable computational power and are not suited to resource-constrained environments.

Srilakshmi, et al. [9] suggested a novel routing algorithm for MANETs that emphasizes trust, security, and energy efficiency. Their method uses the Bacteria Foraging Optimization Algorithm (BFOA) to identify optimal routes for data transmission. The first step is to use a fuzzy clustering algorithm. This algorithm groups nodes based on various trust indicators, namely direct trust, indirect trust, and current trust. Based on these trust values, cluster head nodes are selected to lead their respective clusters. In addition, value nodes that are considered trustworthy for data transfer are identified in each cluster. Cluster heads handle multi-hop routing, where data packets are forwarded across multiple nodes to reach their destination. A prediction protocol is used to select the most suitable routes. This protocol takes into account factors such as latency, throughput, and connection strength within the routing path boundaries. The proposed algorithm shows significant improvements compared to existing methods, even without causing malicious attacks. Additionally, it has an 83% detection rate in identifying malicious activities.

Mahamune and Chandane [10] introduced two novel trust-based routing schemes to enhance security and communication efficiency in MANETs. These schemes, named Trust-based Co-operative Routing (TCOR) and Trust-based Self-Detection Routing (TSDR), are implemented under the AODV routing protocol. The developed systems address multiple security issues. TSDR and TCOR are designed to successfully identify malicious hosts and maintain disruption of network operations. Both schemes define mechanisms for evaluating the trustworthiness of individual network nodes successfully. The promised schemes guarantee the secure passing of screened information between nodes, avoid tampering, and ensure the preservation of data integrity. TSDR and TCOR prefer the saving of screened communication paths and network modifications and adaptation to potential security threats. The effectiveness of the schemes is empirically proven by comparison of the performance of the current routing protocols, such as the average AODV protocol, the Generalized Trust Model (GTM), and the Evolutionary Self-Cooperative Trust (ESCT). An extensive simulation procedure was conducted for three different network scenarios, and the proposed schemes were assessed using eight key performance metrics. The results show that both TSDR and TCOR outperform the existing routing protocols in all eight metrics. In particular, TCOR has a higher degree of scalability, making it suitable for large MANETs. Conversely, TSDR's focus on small networks is better suited to smaller MANET applications.

Saravanan, et al. [11] proposed a new routing protocol for MANETs, named the Optimal Cluster Trust Asymmetric Key Management Protocol (OptCH_TAKMP). This protocol aims to strike a balance between security and energy efficiency by combining a group key management mechanism with a complex, cluster-based architecture. OptCH_TAKMP utilizes the Particle Swarm Optimization (PSO) algorithm to achieve two primary objectives. PSO is employed to identify the optimal nodes that are intended to serve as network cluster heads. Network cluster heads manage the exchange of data and serve as the controlling agents of network performance. The PSO algorithm is also used to identify malicious nodes that may compromise the network's operation. This fosters confidence among valid nodes by enabling secure and reliable communications. OptCH_TAKMP employs a distinct mechanism for key management. Two specially designed components generate secret keys for secure communication between nodes, while verifying the authenticity of these keys to prevent unauthorized access and distributing the keys safely to authorized nodes within the network. OptCH_TAKMP demonstrates considerable advancements in terms of calculating the trust error, communication cost, network lifetime, throughput, and energy efficiency when compared to current methods.

Table 1: Comparison of related works

Method	Key features	Advantages	Limitations
Trust-based Routing with BFOA [9]	Uses bacteria foraging optimization algorithm and fuzzy clustering for trust and energy efficiency	High trust and energy efficiency, 83% malicious activity detection	Computationally intensive
TSDR and TCOR [10]	Trust-based self-detection routing and trust-based co-operative routing with AODV	Effective in detecting malicious nodes	TSDR is better for small networks

OptCH_TAKMP [11]	Optimal cluster-trust asymmetric key management protocol using PSO algorithm	High security and energy efficiency, effective key management	Complex cluster management
TAM [12]	Trust and anonymous model emphasizing security and anonymity	Two-tier security, high anonymity, energy-efficient	Complexity in dual identity management
Trustworthy route discovery [13]	Trust evaluation using RSSI and packet ID analysis, multi-layered cuckoo search for cluster head selection	High security, effective cluster head selection	Potential overhead in trust evaluation
RRCC-DAODV [14]	Artificial immune systems-inspired model, V-detector algorithm for attack detection	High detection rate (94%), superior in various performance metrics	Complexity in integrating AIS and energy-based detection

Lakshmi and Vaishnavi [12] introduced a novel routing protocol called Trusted and Anonymous Mechanism (TAM) for MANETs. TAM emphasizes security and efficiency, addressing existing limitations. TAM protects data transfers through a two-stage security solution. The first stage selects reliable nodes for processing routing control messages. The speed at which a node handles these messages determines its trustworthiness. Nodes with higher energy availability are considered more trustworthy because they are less vulnerable to overload or compromise. The second stage focuses on anonymity. During data transfer, the original node identities are obscured. Trusted nodes selected in the first stage forward data packets using temporary dual identities. An advanced mathematical function produces these identities, rendering it very challenging for malicious observers to identify individual nodes that are part of the routing process. Due to the security-minded nature of TAM's design, several performance enhancements have been achieved over previous protocols, including EMBTR (an element-based secure routing protocol for embedded networks) and the power-efficient model of logical power for trusted routing, known as CEMT.

Sankaran and Hong [13] solved the problem of ensuring data transmission security in the context of MANETs by designing a reliable ad-hoc route discovery protocol. This protocol tries to establish a high level of confidence between network nodes. The reliability of neighbors is assessed by employing a two-stage mechanism. First, Received Signal Strength Indicator (RSSI) values are used to evaluate signal quality. Second, trust rates are estimated by analyzing the order of packet IDs stored in neighbor logs. Afterward, the protocol employs a multi-level Cuckoo Search optimization technique to select the best cluster heads.Cluster leaders play a key role in guiding communications within the network. To further enhance the security of data transmission, the protocol selects nodes that are most trustworthy for this leadership role. The efficiency of the protocol is evaluated using several key factors, including throughput, end-to-end delay, routing overhead, packet delivery rate, and energy dissipation.

Gowtham, et al. [14] proposed a novel security model for MANETs inspired by Artificial Immune Systems (AIS). This model uses AIS concepts to classify the behavior of a node on the basis of the Mature Context Immune Antigen Rate (MCIAR). Building on this classification, a new technique called Reliable History-dependent Resource Conscious Clustered and Defensive AODV (RRCC-DAODV) is presented. This protocol aims to locate selfish hosts and mitigate disruptive attacks. The detection in RRCC-DAODV follows a double-fold mechanism. Firstly, the current behavior and reliability of nodes are considered by using the trust value for that particular node. Secondly, the current residue level of the node's energy is taken into consideration because damaged nodes may experience erroneous energy utilization patterns. For further security defense of the system, the DAODV component also applies the V-detector algorithm. This further algorithm further enhances the detection and defense capabilities of the protocol against potential attacks. Simulation outcomes demonstrate a 94% detection rate, confirming the model's effectiveness in identifying selfish nodes. Simulation also showed the prevalence of the model over existing standard protocols. The prevalence occurs in several performance factors, including end-to-end delay, packet delivery ratio, energy consumption, and throughput.

3 Proposed approach

3.1 Trust framework

The proposed system assigns a trust score ($T_A(B)$) to each neighboring node (B) within a node's (A) communication range. This value reflects A's trust in B. To ensure scalability, the trust levels are determined entirely by local information available to A. Formally, $T_A(B)$ refers to the degree of trust A gives to B, with a value ranging from 0 to 1 (0 indicating no trust, 1 indicating complete trust). This trust value is determined by combining two variables (as depicted in Figure 1 and calculated by Eq. 1).

$$T_A(B) = \alpha T_{A(self)}(B) + \beta T_{A(neighbour)}(B) \qquad (1)$$
$$\alpha, \beta \geq 0, \alpha + \beta = 1$$

The direct component $T_{A(self)}(B)$ is computed over a sliding C_Window using local counters already maintained in the neighbor table:

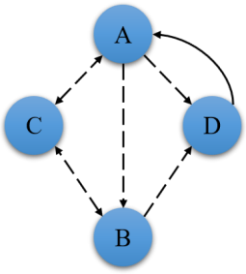

Figure 1: Trust score calculation

$$T_A(B) = \frac{Forwarded\ [A \to B]}{To\_Forwarded\ [A \to B] + \varepsilon} \quad (2)$$

Where $\varepsilon > 0$ avoids division by zero. The indirect component aggregates one-hop recommendations received via periodic TRUST packets:

$$T_{A(neighbour)}(B) = \frac{1}{|\mathcal{N}_A \cap \mathcal{N}_B|} \sum_{k \in \mathcal{N}_A \cap \mathcal{N}_B} T_{k(self)}(B) \quad (3)$$

The first component, $T_{A(self)}(B)$, represents *A*'s trust in *B* derived from *A*'s direct observations of *B*'s behavior. The second component, $T_{A(neighbour)}(B)$, signifies the average trust that *A*'s neighbors have in *B*. Since these neighbors share proximity with both *A* and *B*, their combined assessment contributes to the overall trust evaluation. By adjusting the weights (α and β) in Eq. 1, the model allows for varying the relative influence of *A*'s own observations (self-trust) and the trust evaluations of its neighbors. This mechanism effectively incorporates history into the trust assessment, considering current observations and *B*'s past behavior.

Furthermore, our model extends the trust concept beyond individual nodes to encompass routes. Each established route (*r*) is assigned a trust value to facilitate informed route selection decisions. This value enables nodes to evaluate whether a newly discovered route to a destination offers a higher level of trust (and potentially better performance) than an existing route. Intuitively, the trust value of a route reflects its overall reliability. As a route is essentially a sequence of nodes (represented by a_1, a_2, ..., a_m, in which a_i denotes i^{th} node in the list), its trustworthiness hinges on the reliability of all constituent nodes.

To support decentralized trust propagation, ELRP introduces a lightweight control packet named TRUST. Each node periodically broadcasts a TRUST packet to its one-hop neighbors containing the trust values it maintains for them. The packet uses a compact TLV-based format to minimize bandwidth use. The structure is summarized in Table 2.

Table 2. Structure of the TRUST packet

Field	Description	Data type	Size (bytes)
PacketType	Identifies control packet as TRUST (value = 0x07)	uint8	1
Version	Protocol version identifier	uint8	1
SenderID	Unique address of the sending node	uint16	2
SeqNo	Sequence number for duplicate suppression	uint16	2
Timestamp	Local time of packet generation	uint32	4
NumEntries	Number of neighbor entries included	uint8	1
NeighborID [i]	Address of neighbor *i*	uint16 × *n*	2×n
TrustValue[i]	Encoded trust score (0–1, scaled to 8 bits)	uint8 × *n*	1×n
Variance[i] (opt.)	Optional confidence or variance field	uint8 × *n*	1×n
TTL	Time-to-live (restricted to one hop)	uint8	1

Each node rebroadcasts its TRUST packet every 5 seconds using a TTL of 1, limiting dissemination to local neighborhoods. With an average of 10 neighbors per node, this adds roughly 150 bytes every 5 seconds, corresponding to ~0.24 kbps, or less than 5 % additional control traffic relative to AODV. Because ELRP reuses counters already maintained for trust computation, the additional computational and storage cost is negligible. This lightweight design ensures that trust information remains current while maintaining high scalability and minimal overhead.

3.2 Integration with AODV

While our trust estimation strategy is adaptable to various routing protocols, we have integrated it with the AODV protocol for this implementation. Traditionally, AODV prioritizes the selection of the shortest route during path discovery. Our modification alters this behavior to favor routes with higher trust values, enhancing security against malicious attacks. In cases where multiple paths exhibit equivalent trust values, the selection process reverts to prioritizing the route with the fewest nodes.

As illustrated in Figure 2, the source node determines the most trustworthy path through the following steps. Eq. 2 defines the trust value (*Tr(r)*) for a given route (*r*). The origin ultimately picks the path boasting the most trustworthiness. This emphasis on well-trusted routes fosters secure communication and safeguards from threats like black and gray hole attacks.

$$R_r = T_{a1}(a2)T_{a2}(a3)\dots T_{ai-2}(a_{m-1}) = \prod_{i=m}^{m-2} T_{ai}(ai+1) \quad (4)$$

To accommodate the trust estimation scheme within AODV, specific modifications to the data structures are required. The existing neighbor table entries are augmented with five new fields:

- To forward: Indicates the number of packets forwarded by the neighbor.
- Forwarded: Indicates the number of packets received from the neighbor and successfully forwarded.
- Current window (C_Window): Employs a sliding window mechanism for trust value calculations.
- Source list (Sc_List): Maintains a list of source nodes for received packets.
- Neighbor trust (Nb_Trust): Represents the trust value assigned to the specific neighbor.

The route table entries are similarly expanded with a single additional entry: Route trust (Rt_Trust), which stores the calculated trust value for the corresponding route. Trust value fields are also incorporated into Route Request (RREQ) and Route Reply (RREP) packets to propagate trust information across the network.

3.3 Trust value dissemination

One approach to disseminate trust values maintained by individual nodes involves periodic broadcasts. Each node transmits a TRUST packet to its single-hop neighbors,

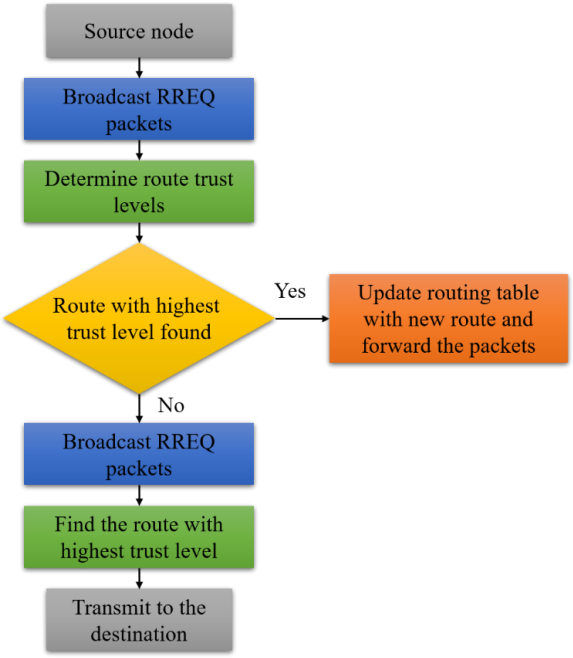

Figure 2: Trust-based path selection process in the modified AODV protocol

carrying its trust values. This necessitates introducing a new control packet type: the TRUST packet. The initial two fields within the TRUST packet specify the packet type and the number of neighbors for which trust values are conveyed. Additionally, a node periodically calculates the average trust value contributed by its neighbors alongside broadcasting the TRUST packet.

ELRP incorporates a lightweight IDS to identify black-hole and grey-hole behaviors. Each node continually observes its neighbors within the current C_Window and computes a forwarding ratio as follows:

$$F(B) = \frac{N_{fwd}(B)}{N_{exp}(B) + \varepsilon} \quad (5)$$

Where $N_{fwd}(B)$ is the number of packets successfully forwarded by node B and $N_{exp}(B)$ is the number expected during the observation window. A node is considered suspicious when:

$$F(B) < \tau_{IDS} \quad (6)$$

Where τ_{IDS} is an adaptive threshold defined by Eq. 7:

$$\tau_{IDS} = \mu_F - \kappa\sigma_F \quad (7)$$

With μ_F and σ_F representing the network-wide mean and standard deviation of forwarding ratios estimated locally, and κ controlling sensitivity. If a neighbor remains below this threshold for n consecutive windows, its trust value $T_A(B)$ is exponentially decreased:

$$T_A(B) \leftarrow (1 - \lambda)T_A(B) \quad (8)$$

Where $\lambda \in (0,1)$ is the decay factor. Nodes marked as malicious are excluded from subsequent route discovery and are not considered for opportunistic forwarding. This adaptive IDS design ensures that ELRP can distinguish genuine link errors from intentional packet drops while maintaining minimal overhead, since all metrics are derived from local counters already maintained for trust computation.

4 Performance evaluation

4.1 Simulation setup

The simulation experiments were conducted in NS-2 using 15 mobile nodes randomly distributed in an $800 \times 800\ m^2$ area for 900 seconds. Node mobility followed the Random Waypoint model with speeds uniformly distributed between 0 and 15 m/s and zero pause time. Communication used CBR traffic over UDP, with ten randomly selected source–destination pairs transmitting 512-byte packets at 4 packets/s. The wireless configuration employed IEEE 802.11 DCF at 2 Mb/s, a Two-Ray Ground propagation model, an omni-directional antenna with a 250 m range, and a DropTail/PriQueue of length 50.

Both AODV and the proposed ELRP (AODV + trust) were evaluated under two attack scenarios in which 3 (20%) and 5 (33%) nodes behaved maliciously by dropping 100% (black-hole) or 50% (grey-hole) of data packets. Trust values were updated every 2 s within a sliding observation window (C_Window) of 50 packets, and TRUST packets were broadcast every 5 s. All results were averaged over five independent runs using different random seeds (20241–20245). This configuration mirrors prior lightweight trust-based MANET studies and includes all parameters necessary for reproducibility.

4.2 Performance metrics

The simulations assessed the proposed method (ELRP) using four key indicators: throughput, end-to-end delay, Packet Delivery Rate (PDR), and Packet Loss Rate (PLR).

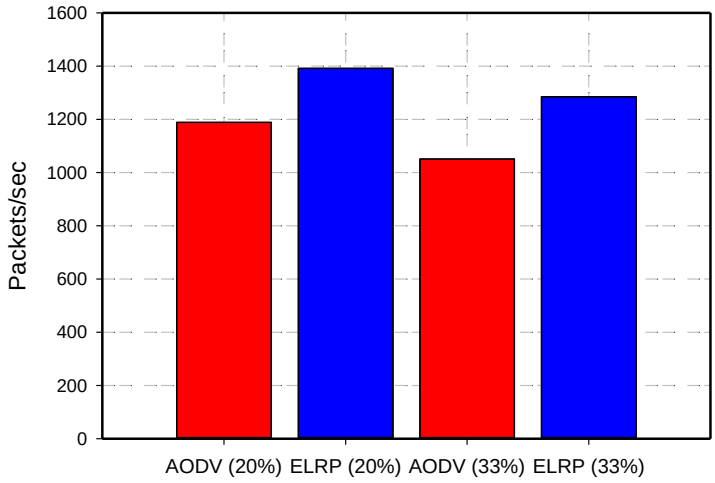

Figure 3: Throughput comparison

Throughput is measured as the total number of packets successfully delivered to the destination divided by the total simulation time, formally defined as:

$$Throughput = \frac{Total\ packets\ delivered}{Total\ simulation\ time} \quad (9)$$

As depicted in Figure 3, ELRP exhibits superior throughput compared to the traditional AODV protocol. This improvement is primarily due to ELRP's ability to dynamically select routes based on trust levels, which minimizes packet loss caused by malicious nodes and ensures more reliable data transmission. By prioritizing trustworthy routes, ELRP enhances the overall network stability and efficiency, leading to a higher throughput compared to AODV.

End-to-end delay is the average time a data packet takes to travel from the source node to the destination across the network, calculated by Eq. The results in Figure 4 demonstrate that our method achieves lower end-to-end delay than AODV. This improvement is primarily due to the trust-based route selection in our method, which ensures that data packets are routed through more reliable and stable paths, reducing the likelihood of packet retransmissions and detours caused by malicious or unreliable nodes. Consequently, the overall time required for packets to reach their destination is minimized, enhancing the efficiency and performance of the network.

$$End-to-end\ delay = \frac{\sum(Packet\ received\ time - Packet\ sent\ time)}{Total\ packets\ received} \quad (10)$$

PDR, a crucial metric for evaluating system quality, signifies the proportion of data packets successfully delivered to the destination, given by Eq. 11.

$$PDR = \frac{Total\ packets\ received}{Total\ packets\ sent} \times 100\% \quad (11)$$

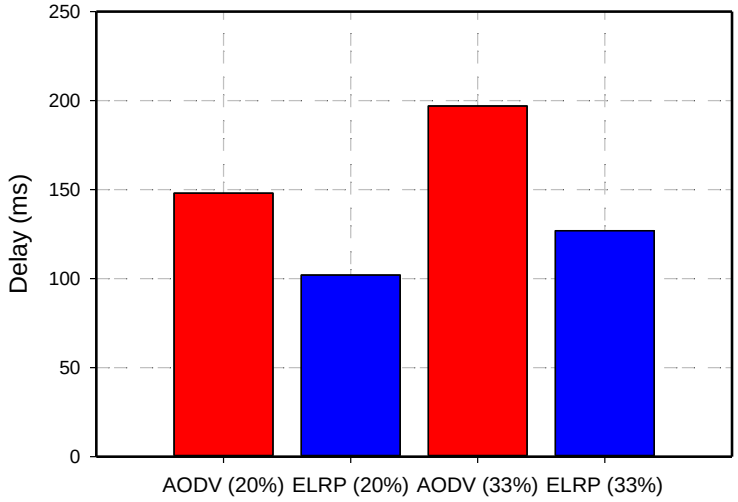

Figure 4: End-to-end delay comparison

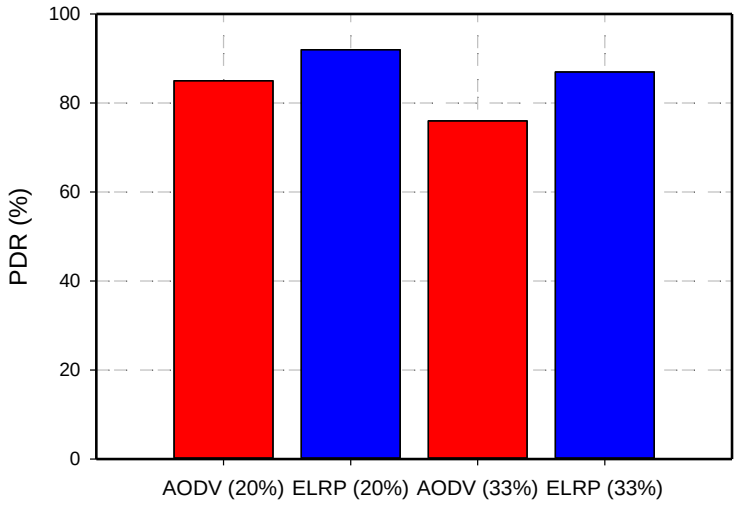

Figure 5: PDR comparison

Conversely, PLR represents the percentage of packets dropped during transmission, calculated as follows:

$$PDR = \frac{Total\ packets\ sent - Total\ packets\ received}{Total\ packets\ sent} \times 100\% \quad (12)$$

As shown in Figures 5 and 6, ELRP achieves a significant improvement in PDR and PLR. This enhancement is primarily due to the trust-based routing mechanism, which prioritizes secure and reliable routes, effectively mitigating the impact of malicious nodes and reducing packet loss. By ensuring that data is transmitted through trusted paths, our scheme increases the likelihood of successful packet delivery and minimizes the number of packets dropped during transmission. This dual improvement highlights the scheme's effectiveness in fostering secure and reliable communication within MANETs.

4.3 Discussion

ELRP enhances the performance of MANET in evaluation metrics like throughput, end-to-end delay, PDR, and PLR. ELRP significantly improves these entities, particularly in terms of prime efficiency and reliability indicators of a network. ELRP distinguishes between malicious and trustworthy nodes by dynamically assessing the entities of trust and integrating opportunistic routing techniques. Opportunistic routing strategies are helpful when the network environment and node characteristics are highly dynamic. ELRP responds to such variations by refining the values of trusts and routing channels accordingly, thereby optimizing the security and resilience of the network.

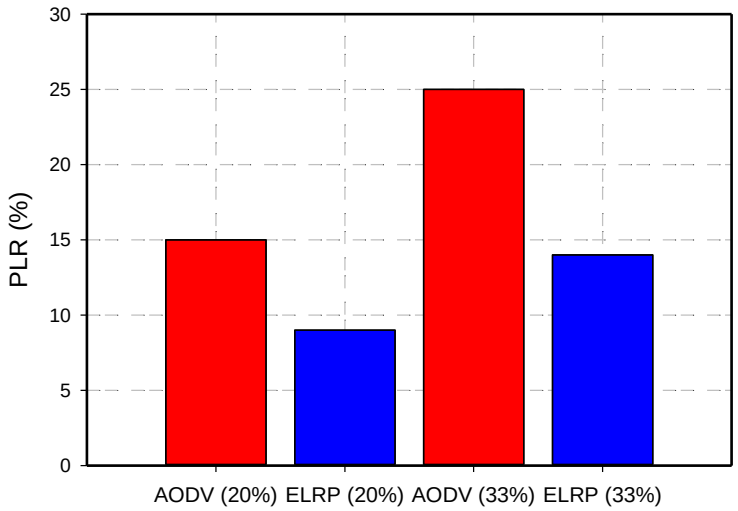

Figure 6: PLR comparison

The superior performance of ELRP compared with the standard AODV routing protocol, particularly in malicious node-based applications, underscores the strong need to incorporate trust concepts and IDS into routing protocols. Although AODV has garnered considerable interest within the research community owing to its simplicity and improved performance, it still lacks security mechanisms, making it susceptible to various attack types. The proposed ELRP method can address these challenges by using trust values to evaluate node performance and opportunistic routing to identify the most trusted and optimal routes dynamically. The addition of an IDS system further enhances reliability.

Such developments render ELRP a stronger and more dependable communication model for MANETs, ensuring secure and reliable data transmission even in highly unpredictable and possibly hostile environments. The fact that the protocol is efficient in tackling primary security flaws while maintaining high performance in key network parameters makes it a promising candidate for MANET applications in the military, emergency services, and vehicular communications systems. ELRP's flexibility and opportunism are most suitable in environments where the network's topological configuration and node behavior are nondeterministic. This ensures that data transmission remains secure and efficient, regardless of the challenges posed by the network operational context.

The adaptational property of ELRP enables it to maintain stable routing even in highly dynamic network environments where node mobility and topological variations are frequent. Like adaptive control schemes for nonlinear control systems, such as adaptive fuzzy control and robust neural adaptive control, ELRP opportunely recalculates the trust measures and optimally updates the next-hop choices as it adapts to network variations. This property enables the protocol to perform optimally, regardless of the unpredictability of link quality or node movement. ELRP's adaptational property, hence, mirrors the self-tuning property of control systems treated in the adaptive backstepping and the robust synchronization schemes [15-17], for the purpose of guaranteeing stable and efficient communications in time-varying, decentralized, and mobile environments.

To further contextualize ELRP’s performance, it is notable that protocols such as TCOR, TSDR, and OptCH_TAKMP also employ trust-based routing mechanisms. However, while these depend on extensive inter-node communications and optimization algorithms that add to processing complexity, ELRP achieves comparable or better reliability with significantly lower computational overhead. This benefit derives from its localized computation of trust and a light-weighted intrusion detection module. Furthermore, future developments of ELRP may leverage adaptive control mechanisms, such as optimal and backstepping control styles. Such mechanisms would permit a dynamically adjustable set of trust thresholds for each node, depending on network feedback observed and the intensity of the attack, thereby enhancing resilience and response latency in highly variable or malicious environments. Because ELRP relies on the periodic refresh of trust using local information, it remains scalable for larger networks, where the computational expense scales linearly with the number of neighbor nodes, but not with the overall network size.

Besides resolving black-hole and grey-hole behaviors, ELRP also demonstrates resilience to additional typical trust-oriented attacks, such as collusion, Sybil, and bad-mouthing attacks. Since the ELRP's trust estimation procedure is based mainly on locally perceived forwarding activity and one-hop indirect recommendations, malicious nodes have limited control over the global distribution of trust. Under conditions of Sybil or bad-mouthing activity, the requirement for direct observation ensures that only nodes with a verifiable history of packet forwarding can obtain or retain high values for trust. Furthermore, the legitimacy of the TRUST broadcasts is ensured through the use of one-hop exchanges embedded in the current AODV control messaging, which can be supported by the addition of link-layer authentication or lightweight cryptographic tags without compromising scalability. Hence, ELRP remains safe for independent and collaborative attempts to manipulate the trust while retaining its lightweight style.

5 Conclusion

MANETs are highly adaptive, plug-and-play wireless networks that are suitable for military purposes, disaster scenarios, rural regions lacking radio infrastructure, and outdoor environments. With highly changeable and variable network structures, security becomes the most problematic aspect, as it is susceptible to attack through eavesdropping, routing mechanisms, and modifications to applications. We introduced ELRP to enhance the reliability and security of the MANET. With the use of a dynamic trust metric and the incorporation of an IDS, ELRP effectively locates malicious nodes and isolates them, ensuring secure and reliable communication. Our NS2 network simulator simulation demonstrated ELRP's superiority over the conventional AODV protocol in key performance measures, including throughput, end-to-end delay, packet delivery ratio, and packet loss rate. This enhancement is particularly significant in the presence of a large number of malicious nodes, underscoring the effectiveness of ELRP in countering security threats.

The success of ELRP in improving MANET security and performance demonstrates its potential and applicability across domains such as military scenarios, disaster recovery networks, and vehicular communications. Nevertheless, several research avenues may be explored in the future to improve and extend related research. For example, applying machine learning concepts and methodologies to forecast and proactively mitigate potential future threats and malicious activities. The degree of flexibility of the developed protocol and its appropriateness across various network sizes and mobility models may also yield critical new perspectives. In any case, ELRP provides an attractive foundation and a potentially fertile area that may facilitate new research and progress in this important and timely field.

References

[1] B. H. Khudayer *et al.*, "A comparative performance evaluation of routing protocols for mobile ad-hoc networks," *International Journal of Advanced Computer Science and Applications,* vol. 14, no. 4, 2023.

[2] 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.

[3] S. Mangasuli and M. Kaluti, "Efficient multimedia content transmission model for disaster management using delay tolerant mobile adhoc networks," *International Journal of Advanced Computer Science and Applications,* vol. 14, no. 1, 2023.

[4] B. Pourghebleh and N. Jafari Navimipour, "Towards efficient data collection mechanisms in the vehicular ad hoc networks," *International Journal of Communication Systems,* vol. 32, no. 5, p. e3893, 2019.

[5] S. Kaisar, J. Kamruzzaman, G. Karmakar, and M. M. Rashid, "Decentralized content sharing in mobile ad-hoc networks: A survey," *Digital Communications and Networks,* vol. 9, no. 6, pp. 1363–1398, 2023.

[6] F. O. Nia and H. Lin, "Traffic-Aware Pedestrian Intention Prediction," in *2025 American Control Conference (ACC)*, 2025: IEEE, pp. 3455–3460, doi: https://doi.org/10.23919/ACC63710.2025.11107953.

[7] S. Li and B. Gong, "Developing a reliable route protocol for mobile self-organization networks," *High-confidence computing,* vol. 4, no. 3, p. 100194, 2024.

[8] C. Bharanidharan, S. Malathi, and H. Manoharan, "Detection of black hole attacks in vehicle-to-vehicle communications using ad hoc networks and on demand protocols," *International Journal of Intelligent Unmanned Systems,* 2024.

[9] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks," *IEEE Access,* vol. 10, pp. 14260–14269, 2022.

[10] A. A. Mahamune and M. Chandane, "Trust-based co-operative routing for secure communication in mobile ad hoc networks," *Digital Communications and Networks,* 2023.

[11] S. Saravanan, D. Prabakar, and S. Sathya, "Trust aware ad hoc routing protocol with key management based mechanism and optimal energy-efficient cluster head selection in mobile ad hoc networks," *Concurrency and Computation: Practice and Experience,* vol. 35, no. 7, p. e7599, 2023.

[12] G. V. Lakshmi and P. Vaishnavi, "A trusted security approach to detect and isolate routing attacks in mobile ad hoc networks," *Journal of Engineering Research,* 2023.

[13] K. S. Sankaran and S.-P. Hong, "Trust Aware Secured Data Transmission Based Routing Strategy Using Optimal Ch Selection in Mobile Ad-Hoc Network," *Mobile Networks and Applications,* pp. 1–13, 2023.

[14] M. Gowtham, M. Vigenesh, and M. Ramkumar, "An artificial immune system-based algorithm for selfish node detection in Mobile Ad Hoc Networks (MANETs)," *Transactions on Emerging Telecommunications Technologies,* vol. 35, no. 2, p. e4938, 2024.

[15] A. Boulkroune, F. Zouari, and A. Boubellouta, "Adaptive fuzzy control for practical fixed-time synchronization of fractional-order chaotic systems," *Journal of Vibration and Control,* p. 10775463251320258, 2025, doi: https://doi.org/10.1177/10775463251320258.

[16] A. Boulkroune, S. Hamel, F. Zouari, A. Boukabou, and A. Ibeas, "Output-Feedback Controller Based Projective Lag-Synchronization of Uncertain Chaotic Systems in the Presence of Input Nonlinearities," *Mathematical Problems in Engineering,* vol. 2017, no. 1, p. 8045803, 2017, doi: https://doi.org/10.1155/2017/8045803.

[17] G. Rigatos, M. Abbaszadeh, B. Sari, P. Siano, G. Cuccurullo, and F. Zouari, "Nonlinear optimal control for a gas compressor driven by an induction motor," *Results in Control and Optimization,* vol. 11, p. 100226, 2023, doi: https://doi.org/10.1016/j.rico.2023.100226.