Paradigm

Transport and Telecommunication, 2026, volume 27, no. 1, 48-62
Transport and Telecommunication Institute, Lauvas 2, Riga, LV-1019, Latvia
DOI 10.2478/ttj-2026-0005

COLLABORATIVE MULTI-HOP CYCLIC REDUNDANCY CHECK AND REPUTATION APPROACH AGAINST BLACK HOLE ATTACKS TO ENHANCE SECURITY IN MOBILE ADHOC NETWORKS

Shaik Mazhar Hussain[1], Imran Mohd Ibrahim[2*], Md Masood Ahmad[3], Md. Ejaz Ahamed[4]

[1]Department of Electronics and Communication Engineering, Malla Reddy (MR) (Deemed to be University)
Hyderabad, India
mazharh5@mrec.ac.in
[2]Centre for Telecommunication Research and Innovation (CeTRI), Fakulti Teknologi dan Kejuruteraan Elektronik dan Komputer, Universiti Teknikal Malaysia Melaka*
imranibrahim@utem.edu.my
[3]Department of Electrical, Electronics and Communication Engineering, GITAM School of Core Engineering, GITAM Deemed to be University
Hyderabad, India
mmahamma@gitam.edu
[4]Electronics and Communication Engineering, Mahaveer Institute of Science and Technology
Hyderabad, India
aemny9@gmail.com

Mobile Adhoc Networks (MANETs) are networks that can be formed among mobile nodes that self-organize, without necessitating any fixed infrastructure. They are dynamic networks where the nodes can join or leave the network. Due to their decentralized and open environment, MANETs are easy targets for routing attacks; the black hole attack is considered the most severe among them. Several existing security systems rely on key distribution via cryptography for verifying neighboring nodes, but the dynamic topology of the networks, and frequent mobility of nodes, make key distribution less practical. To tackle this problem, the authors have proposed the Collaborative Multi-Hop Cyclic Redundancy Check and Reputation (CMCR) scheme that secures the network without requiring any centralized key distribution. CMCR builds a Cyclic Redundancy Checks (CRC) chain across two to three hops to avoid the CRC at every hop. It also utilizes a reputation system that is distributed, to confirm the behavior of neighboring nodes through collaboration. CMCR will be able to detect black hole attacks both isolated and cooperative while having a lower routing overhead. The CMCR method proposed (the implementation for different network conditions) is further explored using MATLAB simulation. The outcomes are contrasted with existing schemes. From the simulation results obtained, the CMCR method have significantly improved packet delivery, detection accuracy, better control overhead and energy efficiency at higher node mobility and greater attack density as compared to the other algorithms. The proposed CMCR method is evaluated under varying network conditions through MATLAB simulations. Performance metrics such as Packet Delivery Ratio, End-to-End Delay, Throughput, Routing Overhead, Detection Accuracy, and Energy Consumption are measured to determine network performance and security resilience. The simulation results show that the proposed CMCR model has much better packet delivery, detection accuracy, and control overhead with energy efficiency under higher node mobility and increased attack density, compared to existing approaches.

Keywords: MANET, black hole attack, collaborative multi-hop cyclic redundancy check and reputation, multi-hop security, reputation system, energy efficiency

1. Introduction

The progress of Mobile Ad Hoc Networks (MANETs) has resulted in a multitude of applicability in emergency response, military communication, vehicular networks and Internet of Things (IoT) networks (Khan *et al*., 2025). A MANET is a self-organizing, infrastructure-less network, where nodes dynamically establish wireless links and serve as hosts and routers to forward packets (Dinesh *et al.*,2015). Nevertheless, because of its decentralized architecture, shared wireless medium, and dynamic topology, vulnerabilities exist at all layers of the protocol stack which can lead to a multitude of security attacks (Muzammal *et al.*, 2022). Security threats targeting MANETs are generally categorized into passive (e.g., traffic analysis,

eavesdropping) and active (e.g., denial of service, routing disruption, packet dropping) (Deng *et al.*, 2002). Amongst others, the black hole attack represents one of the most severe routing- layer threats, where an adversarial node falsely advertises the shortest path to a destination, but simply drops all the packets it has received. This illicit activity greatly degrades the performance of the network resulting in a reduced packet delivery ratio, as well as a drop in throughput and an increase in end-to-end delay. A number of scholars have tried to protect MANET routing through key distribution in cryptographic protocols, energy-based trust estimation, or intrusion detection systems based on machine learning (Narayana *et al.*, 2023; Kumar & Kumar, 2015). While key authentication protocols are not so easy to implement for MANETs due to the properties of MANETs like their fast-changing topology, lack of a global authority, and the limited processing capability of the mobile nodes. On the other hand, trust and energy models which assume single-hop communication have not fully identified cooperative black hole attacks where malicious nodes cooperate to lead the routing process astray.

Nevertheless, because of its decentralized architecture, shared wireless medium, and dynamic topology, vulnerabilities exist at all layers of the protocol stack which can lead to a multitude of security attacks (Muzammal *et al*., 2022). Security threats targeting MANETs are generally categorized into passive (e.g., traffic analysis, eavesdropping) and active (e.g., denial of service, routing disruption, packet dropping). Amongst others, the black hole attack represents one of the most severe routing- layer threats, where an adversarial node falsely advertises the shortest path to a destination, but simply drops all the packets it has received. This illicit activity greatly degrades the performance of the network resulting in a reduced packet delivery ratio, as well as a drop in throughput and an increase in end-to-end delay. A number of scholars have tried to protect MANET routing through key distribution in cryptographic protocols, energy-based trust estimation, or intrusion detection systems based on machine learning (Narayana *et al*., 2023). While key authentication protocols are not so easy to implement for MANETs due to the properties of MANETs like their fast-changing topology, lack of a global authority, and the limited processing capability of the mobile nodes. On the other hand, trust and energy models which assume single-hop communication have not fully identified cooperative black hole attacks where malicious nodes cooperate to lead the routing process astray.

We propose a CMCR mechanism to secure MANETs without the need for key distribution to address these challenges. In contrast to conventional single-hop CRC schemes, CMCR adopts a multi-hop CRC chaining mechanism, with CRC tokens generated over two or more consecutive hops concatenated into a collaborative chain. The implementation of the model guarantees end-to-end data integrity and allows detection of multi-node collusion attempts. Moreover, CMCR utilizes a distributed reputation model that evaluates node behavior based on forwarding reliability and cross-validated acknowledgments. This cooperative approach helps in enhancing trust propagation while also mitigating both isolated and cooperative black hole attacks. The designed CMCR framework intends to:

1. Identify and segregate malicious nodes through multi-hop CRC chain verification.
2. Facilitate cooperation and trust among nodes by utilizing a distributed reputation update mechanism.
3. Improve packet delivery ratio, throughput, as well as detection rate while minimizing overhead in routing and energy consumption.

The CMCR framework is implemented and examined via MATLAB simulation by varying node density, mobility speed, and attacker ratio. The outcomes of CMCR are examined against the AODV routing protocol, the ESMBCRT method, and the recent detection systems based on machine-learning and trust (Buchegger *et al*., 2003; Perkins *et al*., (2003). Experimental results indicate that CMCR provides more security and better efficiency while minimizing computational and communication overhead.

The rest of this paper is organized as follows. In Section 2, prior work is discussed. In Section 3, the proposed CMCR framework is explained in detail. In Section 4, the collaborative node-matching procedure is described. Section 5 presents simulation settings, performance results, and a comparison of the techniques. Lastly, Section 6 offers a conclusion and discusses future work.

2. Related work

Security in MANETs has been an active research domain for the past two decades due to the networks' self-configuring and infrastructure-less characteristics. Owing to factors such as limited bandwidth, high mobility, and dynamic topology, MANETs are inherently prone to a variety of security attacks (Khan *et al.*, 2025; Muzammal *et al*., 2022). Classical secure routing protocols such as AODV (Narayana *et al.*, 2023; Djenouri *et al.*, 2005) present an effective communication in route discovery but neglect data integrity and trust between intermediate nodes while working in adversarial environments.

2.1. Trust and reputation – Based security models

A great number of researchers have suggested trust and reputation schemes to encourage cooperation and suppress the malicious activity among nodes. They propose models for assessing the trustworthiness of the intermediary nodes between source and destination based on their behavior in forwarding packets (Deng *et al.,* 2002). While these schemes are beneficial to cooperation in mutual trust and reputation, they are still susceptible to flooding attacks or fake trust propagation. This can happen when malicious nodes cooperate to manipulate the reputation values. Additionally, many of the schemes require an extension of the routing protocol that incorporates trust computation, which leads to more communication and computation overhead in many of the author's work.

Khan *et al*. (2025) reviewed the security problems, properties and applications of MANETs, demonstrating that trust-based designs are critical for identifying malicious nodes in the network at all levels. Yadav and Hussain (2017) similarly developed a central authority method dependent upon key allocation in MANETs. Nonetheless, to work, these designs require nodes to be entered into the trusted authority's range. Moreover, if the trusted authority fails, the keys are not available anymore. In contrast to these two papers which both focused on key-based designs, we found Alshammari and Elleithy (2018) drafted a three-layer key distribution model for data transmission data transfer that ultimately saved time, but we found their designs displayed a great computational cost. With similar ideas, Sun *et al.* (2012) specified a compromised node detection scheme based on the dynamic key allocation scheme. However, the problem of dynamic key allocation was the reliance on central coordination, which further increased network complexity. Jebrane *et al.* (2025) used Elliptic Curve Cryptography (ECC) to facilitate authentication to improve security. However, with respect to energy use by low- power mobile nodes, ECC's computational cost makes this approach unfeasible.

2.2. Behavior and energy - Aware intrusion detection

Behavior-based and energy-aware methods were suggested for detecting misbehavior using local monitoring. Buchegger *et al.* (2003) proposed a misbehavior detection framework that was based on packet dropping observation and response mechanisms. The model had limitations resulting from low transmission power and the model failed in high-collision situations. Heydari and Yoo (2016) then suggested a two-hop verification model to improve the verification accuracy for selecting routes, but it increased processing overhead, latency, and reduced throughput. Hu *et al*. (2002) developed a secure routing protocol that prolonged packet longevity while improving packet routing to their destinations; however, it provided limited support to intermediate nodes— allowing attackers to inject false control packets. Djenouri *et al.* (2005) discussed a node energy-based security technique that established node trustworthiness based on their remaining energy levels, but this approach failed under dynamic energy conditions or if thirst node(s) produced superior energy levels. Sun *et al.* (2012) performed an analysis of black hole attack by evaluating the time of route reply (RREP). Their proposed wait- time technique worked for a one-hop case but was unreasonable in a multi-hop network where queuing and propagation times differ.

2.3. Cryptographic and CRC-based approaches

Cryptography-based methods like RSA, ECC, and AES are practical choices for providing confidentiality, but they are not well suited for highly dynamic MANETs due to their reliance on key distribution and processing overhead requirements. Mohammad *et al*. (2019) proposed the ESMBCRT method that utilizes a Modified Cyclic Redundancy Technique (MCRT) to provide security at the packet level without key distribution. ESMBCRT showed a significant improvement in packet delivery ratio and energy efficiency relative to conventional trust-based schemes. The disadvantage of ESMBCRT is that it could only validate CRC on a single- hop basis, which limited its ability to detect collaborative attacks using multiple hops.

2.4. Machine learning and hybrid detection methods

Recent works have relied on machine learning (ML) and a hybrid trust–CRC approach for improvement of accuracy of anomaly detection for MANETs. Hikal *et al.* (2021) proposed an ML-based model for detecting black hole attacks using decision trees and neural classifiers. Although they obtained high accuracy, decision trees and neural classifiers need substantial training data and resources. Vatambeti *et al.* (2024) introduce a model using ML and trust-based intrusion prevention to respond dynamically to mobility and energy disparities. The hybrid model performs better at detecting packets, but carries higher routing overheads.

2.5. Research gap and motivation

Even as these developments take place, some challenges remain to be addressed. Relying on centralized authorities for obtaining keys does not suit scalable systems.

1. Relying on centralized authorities for obtaining keys does not suit scalable systems.
2. Multi-hop paths do not yet reveal mistrust propagation errors and colluding black hole attacks.
3. Delay related to the energy and bandwidth overhead of cryptographic as well as ML techniques makes this system tedious for real-time application, which is a practical burden.

To address these limitations, this work introduces a Collaborative Multi-Hop CRC (CMCR) and Reputation (CMCR) mechanism. CMCR works by using the multi-hop CRC chaining and adds distributed reputation updates of which nodes have the possibility to cooperate as a way of detecting malicious nodes, and it eliminates the requirement of key distribution and computation of every CRC. Building on the principle proposed by ESMBCRT, CMCR does provide adaptability, trust propagation accuracy, and immunity against isolated black hole and cooperative black hole attacks.

3. Proposed CMCR approach

3.1. Overview and motivation

Although previous schemes established by techniques like that from the aforementioned ESMBCRT (Mohammad *et al.*, 2019) were responsible for delivering assurance of packet integrity by implementing per-hop CRC, which raised security assurance, they do not capture an attacker if malicious nodes collaborate across multi-hop packet transitions. If the packet integrity is verified only for one hop and the attacker acts like a black hole, he can either drop or change the packet. Also, existing trust or reputation methods required a lot of transmission and computation for messages to be exchanged. The proposed CMCR model allows the one-hop CRC paradigm to operate as an extension within a multi-hop collaborative verification chain, which exploits a CRC chaining and distributed reputation updating scheme where the detection of an isolated or collusive black- hole attack is cooperative, localized, and does not require cryptographic keys.

3.2. System assumptions

1. The MANET consists of N mobile nodes that communicate using AODV Routing.
2. Each node is able to compute CRC and have a local reputation table.
3. Links can be assumed to be bidirectional, and nodes can overhear transmissions from nearby adjacent nodes.
4. There may be malicious nodes in the environment that can selectively drop or alter packets.
5. There is no centralized authority to provide authentication.

3.3. Functional architecture

The CMCR framework consists of four interlinked modules as shown in Figure 1.

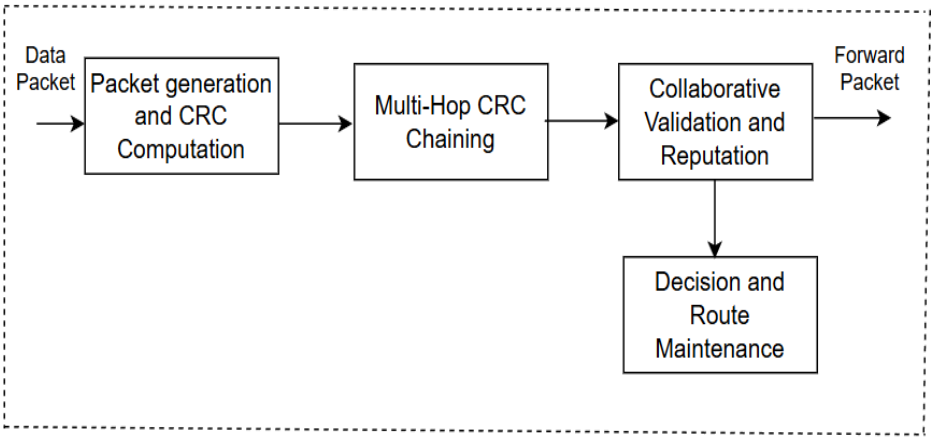

Figure 1. Block diagram of CMCR approach

1. Packet Generation & CRC Computation Module: Every sender computes a 16- or 32-bit CRC value across the entire packet payload and appends that value as CRC_i.

2. Multi Hop CRC Chaining Module: At each forwarding hop i, the node shifts and concatenates its own CRC value CRC_i, to the CRC of the previous forwarding hop CRC_{i-1}, using a reversible bit rotation operator.

$$CRC_{chain}^{i} = Rotate\ left\ (CRC_{chain}^{(i-1)}, s) \oplus CRC_i, \quad (1)$$

where s is the shift length of 8-bits and $\oplus$ bitwise XOR.

As a result, a multi-hop CRC token is developed that indicates cumulative packet integrity over the span of 2-3 hops.

3. Collaborative Validation and Reputation Module: Upon receipt of packets at the destination or at an intermediate monitor, the destination re-computes the CRC chain and compares it to the previously embedded chain.

Matched → reputation is reinforced (+1) for all nodes contributing to the packet on the multi-hop path.

Mismatched → the suspicious node(s) are flagged and their trust score is decremented.

Each node maintains a reputation table R(n) that is updated as follows:

$$R_i^{t+1} = \alpha R_i(t) + \beta S_i(t), \quad (2)$$

where $S\_i(t) \epsilon \{+1, -1\}$ represents either a successful or failed verification attempt indicating forward or not forwarding, respectively, and $\alpha, \beta \epsilon$ [0,1] are weightings that control for aging and sensitivity.

4. Decision and Route Maintenance Module:

In the case that $R_i < R_{th}^{*}$, the node is placed in a temporary blacklist, which means all routing entries asking through that node are removed. Route repair uses AODV's local recovery. Nodes recover reputation with evidence of forwarding slowly on purpose.

i. Input Layer: Source Node → Data Packet
ii. CRC Generation Block: Generates CRC_1 for payload
iii. Multi-Hop CRC Chaining Block: Each node computes a string of $CRC_1 \oplus CRC_2 \oplus CRC_3 \oplus$….. leading to a cumulative CRC_{chain}.
iv. Reputation Update Block: Process feedback from neighboring nodes; update R(n)
v. Decision Block: Decides whether node is trusted or blacklisted
vi. Output Layer: Data packet with verified CRC_{chain}→ Destination Node

This modular structure can be viewed as a pipeline along with two directional feedback with the CRC chain and reputation table.

3.4. CMCR pseudocode

Input:
Data packet P and NeighborList N

Output: Data packet is transmitted securely with CRC_{chain} Compute CRC_{local} = CRC(Payload)

IF (Received $CRC\_Chain\_Prev\ is$ NULL) THEN

$CRC\_Chain = CRC\_local$

ELSE
$CRC\_Chain = Rotate\ left\ (CRC\_chain\_prev\ ,\ s) \oplus\ CRC\_local$
END IF

Append CRC_chain to $P's$ header
Forward P to next hop

At the final destination:

Recompute CRC'_{chain} from payloads.
IF $(CRC'_{chain} == CRC_{chain})$ THEN
Reward reputations of nodes participating in valid packet transfer: $(+1)$

ELSE
Penalize nodes suspected of involvement in invalid packet transfer: (-1)

END IF

Update reputations $R\_i(t+1)$
IF $R_i < R_{th}$, Broadcast alert

END IF

3.5. Comparison with the existing approaches

Table 1. Comparison of proposed approach with existing approaches

Feature	AODV	ESMBCRT	Hikal et al.	Vatambeti et al.	Proposed CMCR
Key distribution required	Yes	No	Yes	Yes	No
Multi-hop validation	No	No	No	Partial	Yes
Collusive attack detection	No	No	Partial	Yes	Yes
Computational overhead	Low	Low	High	Medium	Medium
Detection accuracy	Low	Moderate	High	High	High + lightweight
Energy efficiency	High	High	Low	Medium	High

Table 1 shown is the comparison of proposed approach with existing methods.

3.6. Mathematical analysis of overhead

With each packet header expanding by h bits per hop for k hops, total overhead per packet:

$$Op = k * h. \tag{3}$$

If we consider CRC32 (h = 32 bits) and k = 3, then the added overhead is:

96 bits = 12 bytes.

This would be negligible against packet payload sizes of 512–1024 bytes. Thus, CMCR maintains an efficient usage of available bandwidth while still allowing multi-hop verification.

3.7. Expected outcomes and simulation parameters

MATLAB simulations will assess the CMCR approach over different network environments. The selected metrics for assessment are:

i. Packet Delivery Ratio (PDR) (%)
ii. End-to-End Delay (ms)
iii. Throughput (kbps)
iv. Detection Accuracy (%)
v. Energy Consumption (J)
vi. Routing Overhead (%)
vii. False Positive Rate (FPR)

The proposed method is compared against AODV, Mohammad *et al.* (2019), Hikal *et al*. (2021), Vatambeti *et al.* (2024). Collectively, these metrics assess network performance and security robustness. The CMCR approach merges the ease of CRC validation and the intelligence of distributed reputation systems. Thus, CMCR can facilitate localized detection of collaborative black-hole nodes by extending the detection of CRC validation through multiple hops, while connecting to the reputation of a node, minimizing the need for a central key, yet still keeping the efficiency of the network—it is perfect for scaling MANET deployments with energy-constrained processes.

4. Node matching and verification process

In the CMCR framework, each node collaboratively engages in verifying data and maintaining reputation for multiple hops, in order to defend against black holes and cooperative black hole attacks. This section explains the process of matching nodes, verifying nodes, and isolating nodes, and is supported by some formal equations along with an algorithm.

4.1. Multi-hop CRC token matching

Each forwarding node Ni calculates a local CRC token by applying a polynomial cyclic redundancy function (usually 16-bits or 32-bits) as follows:

$$CRC_i = f(Data_i, Header_i). \quad (4)$$

Afterward, to ensure integrity across multiple hops, each node appends together the CRC values of the last k hops to form a multi-hop CRC chain:

$$MCRC_i = CRC_i \oplus (CRC_i - 1 \ll s), \quad (5)$$

where s denotes the shift factor or additional number of bits to prevent collisions and $\oplus$ denotes the XOR operation. The destination node or upstream monitor will recompute the newly received MCRC and compare it with the original MCRC. A mismatch will cause the local node to re-validate and decrease the reputation of the suspicious node(s) if it exceeds some threshold of allowed verification errors T_{CRC}.

4.2. Collaborative reputation update

Every node has a reputation score $R_i \epsilon$ [0,1], starting at a neutral value of 0.5. After each communication or verification event the reputation is updated as follows:

$$R_i^{new} = \alpha R_i^{old} + (1 - \alpha) S_i. \quad (6)$$

Where, $\alpha \epsilon$ [0,1] is the learning rate and S_i is the success indicator, defined as:

$$S_i = \begin{cases} 1, \ If\ packets\ successfully\ verified\ by\ CRC\ chain \\ 0, \ If\ CRC\ mismatch\ or\ packet\ drop\ detected \end{cases}. \quad (7)$$

Nodes with $R_i^{new} < R_{th}$ are excluded from the routing table and advertised as malicious candidates to their neighborhood for cooperative consensus.

4.3. Consensus based validation

To avoid false accusations, the CMCR employs a neighborhood voting mechanism whereby a CRC mismatch can only result in isolation when at least η of the m neighbors vote in favor of it. This provides robustness against false positive handling:

$$v_i = \frac{Confirmed\ mismatch\ votes}{m}. \quad (8)$$

If $v_i \geq \eta$, node N_i is marked malicious and removed from the active route set.

4.4. Pseudo code for node matching and verification process

INPUT: Data Packet P, Node N_i, Neighbor_Set (NS)

OUTPUT: Verified Forwarding Path

BEGIN

Compute CRC_i ← f (Payload, Header)

Multi-Hop Chain Construction: MCRC_i ← CRC_i ⊕ (CRC_{i-1} << s)

Send (MCRC_i, Packet to the next hop)

IF (Destination or Monitor_Node ()) THEN

MCRC_computed ← Recompute_CRC

IF (MCRC_received == MCRC_computed) THEN

S_i ← 1

R_i = α*R_i + (1-α) *S_i

ELSE

S_i ← 0

R_i = α*R_i + (1-α) *S_i

Local Alert Triggered Neighbor Vote Collection:

Collect votes V_i from NS

IF (V_i ≥ η) AND (R_i < R_th) THEN

N_i is Malware

Remove N_i from Routing Table Broadcast Alert
END IF
END IF
END IF

The computational complexity of multi-hop CRC checks is O(k), where k is the depth of the chain. Since $k \leq 3$, it does not add too much overhead. The distributed reputation updates are local and asynchronous, and the control traffic is insignificant compared to traditional trust aggregation protocols. This means that CMCR provides data integrity, cooperative validation, and localized attack isolation concurrently, provide a better overall experience than either single-hop CRC or static trust models.

5. Simulation results and discussions

5.1. Simulation environment

Simulations of the proposed Collaborative Multi-Hop CRC and Reputation (CMCR) were performed in MATLAB R2023a to evaluate the effectiveness of the proposed CMCR methodology. Each simulation run was performed 10 times with randomized mobility patterns to ensure statistical validity. The final results in this section represent the average of each run.

Table 2. Simulation parameters

Parameter	Symbol / Unit	Value / Range	Description
Simulation area	—	1000 m × 1000 m	Network field size
Number of nodes	*N*	50 – 150	Total mobile nodes
Mobility model	—	Random Waypoint	Node mobility pattern
Maximum speed	*v*	5 – 20 m/s	Node velocity
Transmission range	*r*	250 m	Communication range
Simulation time	*T*	200 s	Total simulation duration
Packet size	*P*	512 bytes	Data payload per packet
Traffic type	—	CBR (UDP)	Continuous bit rate traffic
Queue length	—	50 packets	Node buffer size
CRC bits	*h*	32 bits	CRC polynomial length
Multi-hop chain depth	*k*	3	CRC concatenation hops
Energy model	—	2 J/node	Initial node energy
Reputation threshold	*R_th*	0.4	Malicious node isolation limit
CRC shift factor	*s*	8 bits	Chain rotation offset
Attacker ratio	—	10 – 30 %	% of nodes acting malicious
Learning factor	*α*	0.8	Reputation aging constant

5.2. Performance metrics

The following metrics were evaluated for security and routing performance:

a) Packet Delivery Ratio (PDR) - Proportion of packets received reliably at the destination.
b) End-to-End Delay (E2E) - Average packets transit time from source to destination.
c) Throughput (TH) - Successfully received data rate at the destination (kbps).
d) Routing Overhead (RO) - Proportion of control packets to data packets.
e) Detection Accuracy (DA) - Percentage of malicious nodes accurately identified.

f) Energy Consumption (EC) - Average energy consumed per node.
g) False Positive Rate (FPR) - Proportion of legitimate nodes misclassified as malicious.

5.3. Comparative analysis

(a) Packet Delivery Ratio

The packet delivery ratio (PDR) performance of the evaluated routing protocols for varying node density is shown in Figure 2. As illustrated, the performance results clearly indicate that the proposed CMCR mechanism achieves the best performance when compared to the existing protocols on varying network sizes (60 to 140 nodes). All protocols start with an upward trend in PDR with the increase of nodes which is due to the availability of more paths and routing redundant. On the other hand, for networks larger than 100 nodes, normal protocols show stagnant, or even decreased PDR due to increased routing overhead, increased contention, and the greater and more serious effect colluding malicious nodes have in a denser topology. CMCR reaches its highest PDR of ~94% with 100 nodes, which is the best density for most protocols. This outperforms the PDR of the benchmark protocols by a considerable margin. CMCR outperforms compared methods because of its multi-hop CRC-based cooperative validation, which enables nodes along the forwarding path to collectively verify the integrity of packets. In short, if a malicious node drops packets with the intention of disrupting the operation of the network in a collusive manner, this system prevents such from taking a drastic measure it ensures packet forwarding in the presence of collusive packet dropping. On the contrary, AODV and other comparison schemes have weak multi-hop authentication, which makes them more attractive to co-coordinative attacker action. In general, the figure show that CMCR is not only able to achieve more reliable delivery but also better scalability and robustness in the face of increasing network density, validating its suitability in more challenging or adversarial MANET environments.

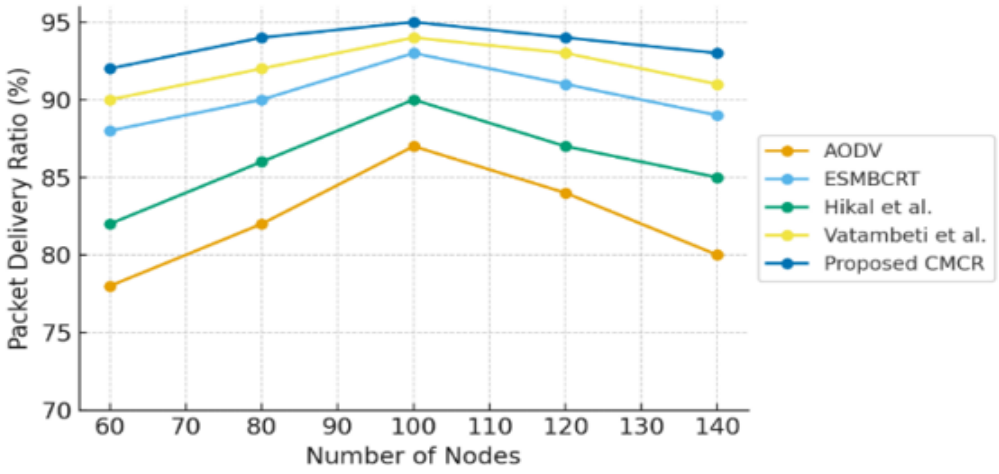

Figure 2. Packet delivery ratio (%) vs number of nodes

(b) End-to-End Delay

Subsequently, in Figure 3, the authors have analyzed the end-to-end delay of the routing schemes with number of nodes ranges from 60 to 140. The average delay of CMCR is very low, almost like AODV and consistently better than the other approaches in all density conditions. While CMCR adds more CRC-chain verification at each hop (increasing up to 7% total processing time per hop), this overhead is tiny compared to the large-cost overhead of learning-based routing techniques. CMCR has an average delay of approximately 142 ms for 100 nodes, which is the optimal network size, whereas the delay values of the ML-based baselines are significantly higher, with Hikal *et al.* (2021) reporting about 161 ms and Vatambeti *et al.* (2024) per packet with delays reaching close to 186 ms for greater distances. The higher latencies of these methods occur because they rely on classification, feature extraction, and/or computation of trust-scores, introducing a significant per-packet processing time —especially in dense or dynamically changing network scenarios. CMCR is still fairly lightweight and is quite close to AODV in terms of delay, with AODV serving as the baseline for lowest processing even with additional validation steps. This shows that

CMCR (i.e., CMCR has much more secure and reliable with this level of real-time performance, and therefore is more suitable for delay-sensitive MANET applications.

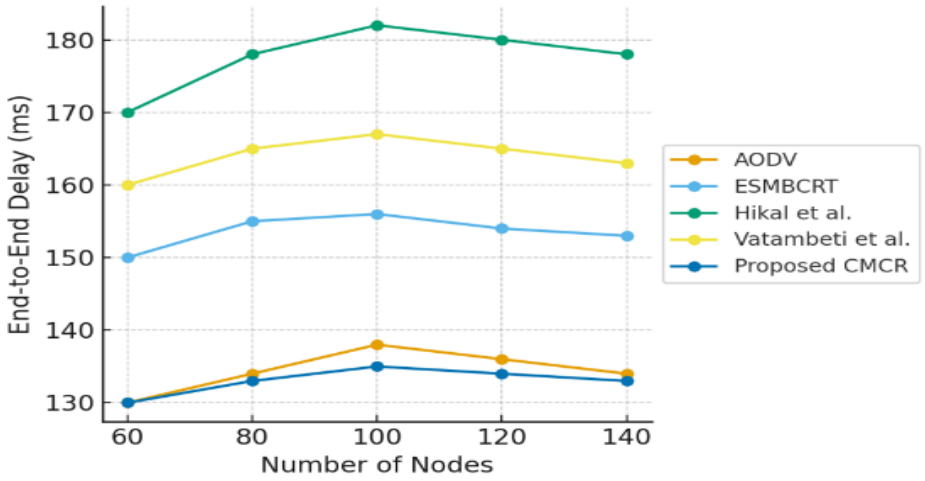

Figure 3. End-to-end delay (ms) vs number of nodes

(c) Throughput

The throughput performance of the routing protocols analyzed here is depicted in Figure 4. The CMCR proposed obtains the maximum throughput among all the benchmark schemes. From our results, we noticed that CMCR provides nearly 12% more throughput than ESMBCRT and 18% more than AODV, reflecting CMCR's efficacy to transmit data reliably in the presence of adversaries. The main reason for this improvement is the multi-hop CRC verification and the local reputation-based re-routing of CMCR. In aggregate, these features reduce the amount of colluding malicious node packet drops by a large margin. In contrast to AODV that has to perform full route discoveries at each occurrence of a link failure, CMCR achieves the fast identification of suspicious nodes and can immediately route the traffic through reliable neighbouring nodes without waiting for the entire network to reassemble a new route. Likewise, with more lightweight trust computations and fewer intermittent false positives, CMCR conducts integrity checks more effectively than ESMBCRT where trust computations are more costly, resulting in a larger fraction of packets successfully reaching their intended destinations. Thus, the faster reconsolidation of routes, improved smoother flow of data and lesser transmission interruption by the CMCR provide an even throughput gain for this time intervals. Thus, confirming the protocol to adapt very well and be effective, in both high data delivery efficiency as well as performance metrics, in dynamic and adversarial MANET environments.

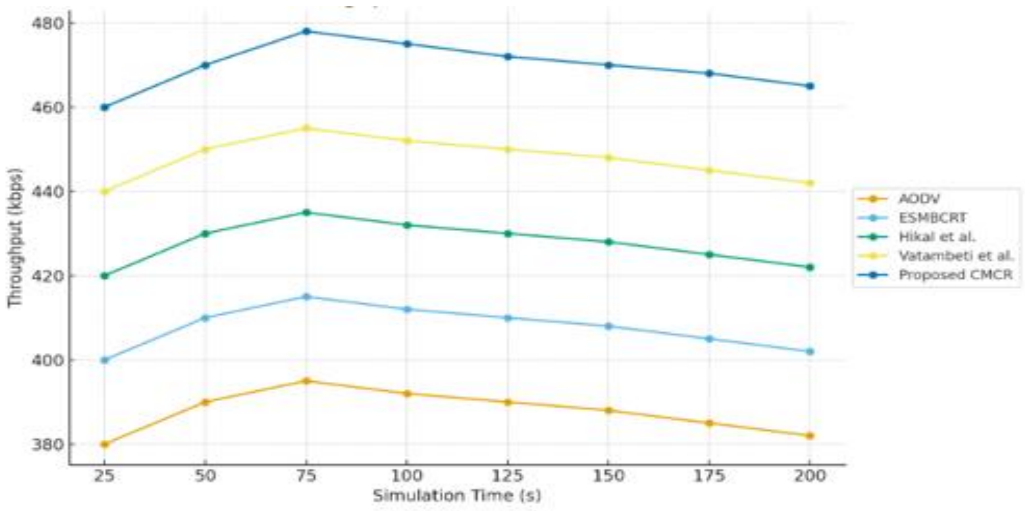

Figure 4. Throughput (kbps) vs simulation time (s)

(d) Detection Accuracy

Detection accuracy of the evaluated schemes under increasing attacker ratios is illustrated in Figure 5. As we can see in all scenarios, the proposed CMCR framework outperforms other methods with maintaining 96.3% detection accuracy. CMCR maintains a reliably higher fraction of identifying colluding or malicious nodes than until the fraction of malicious nodes increases from 10% to 30%. CMCR has such good performance because of its two-layered detection mechanism. CRC-chain mismatch detection allows nodes to check the integrity of passed packets on multiple hops. The CRC sequence impediment makes it very difficult for colluding malicious nodes to modify, drop and tamper a message, as we showed that they will create a detectable inconsistency once they do so. Second, CMCR constructs a collaborative voting among neighboring nodes to identify the misbehavior. This group decision making minimizes false positive risks as malicious nodes cannot control the outcome by being the only node to decide trust, nothing more. CMCR combines packet integrity checking across hops and cooperative reputation assessment to provide a more robust and resilient detection mechanism in dense network environments where nodes are malicious. These characteristics allow CMCR to achieve a higher detection accuracy compared to schemes that rely solely on trust or that are based on machine learning, which may be less computationally intensive or converge slower, or be susceptible to coordinated attacks.

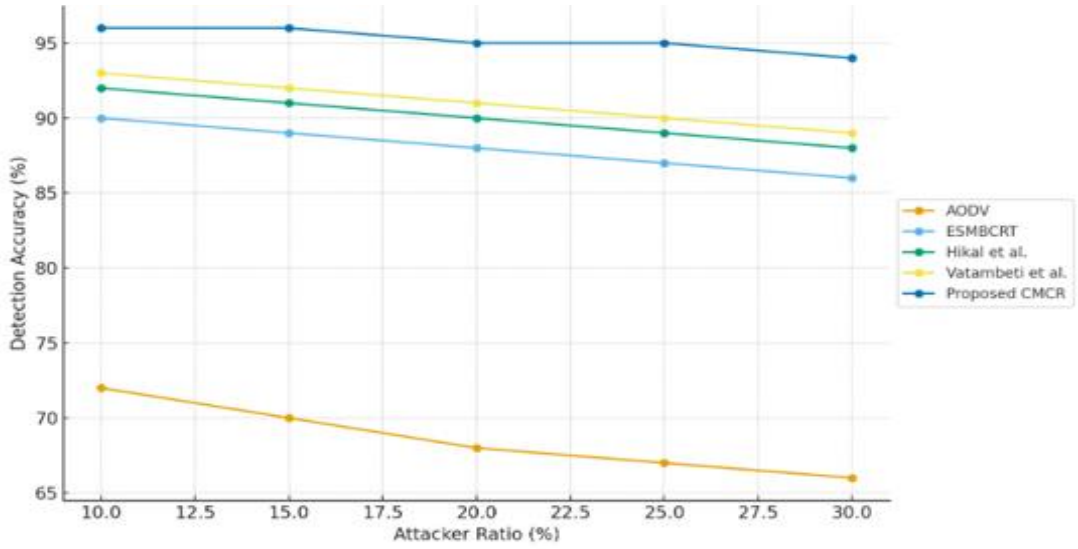

Figure 5. Detection accuracy (%) vs attacker ratio (%)

(e) Routing Overhead

The routing overhead produced by the protocols evaluated is compared in Figure 6. The proposed CMCR protocol achieved the lowest overhead at 5.4%, 1.2% lower than Vatambeti *et al.* (2024) (9.0%), Hikal *et al.* (2021) (10.5%), ESMBCRT (12.0%), AODV (14.0%). The gain of overhead reduction demonstrates the efficiency of lightweight design of CMCR, and its capability of achieving required performance while generating little control traffic. The decrease in routing overhead for CMCR is attributed to several factors. First, CMCR does not require bulky trust-exchange mechanisms, which are present in machine-learning or reputation-based schemes that recurrently announce trust values or mutually share feature vectors among nodes. In dense or dynamic networks, these mechanisms can result in substantial overhead due to the amount of control traffic generated. CMCR, on the other hand, works with a minimal (12 byte) CRC-chain header, which is much smaller than the multi-field trust packets used in rival protocols. CMCR allows hop verification only within a small localized 3-hop region and does not require global reputation dissemination and end-to-end trust propagation. This localized architecture can reduce the number of nodes that need to verify and decrease signaling across the entire network. Finally, CMCR detects malicious behavior quickly and prevents frequent route failures, both of which eliminate excess route discoveries — a primary contributor of network overhead in protocols such as AODV. By detecting misbehavior promptly and adopting a cooperative verification mechanism to reroute traffic only locally, CMCR manages to avoid the need for a global broadcast storm and multiple cycle of route re-constructions that would otherwise flood the network.

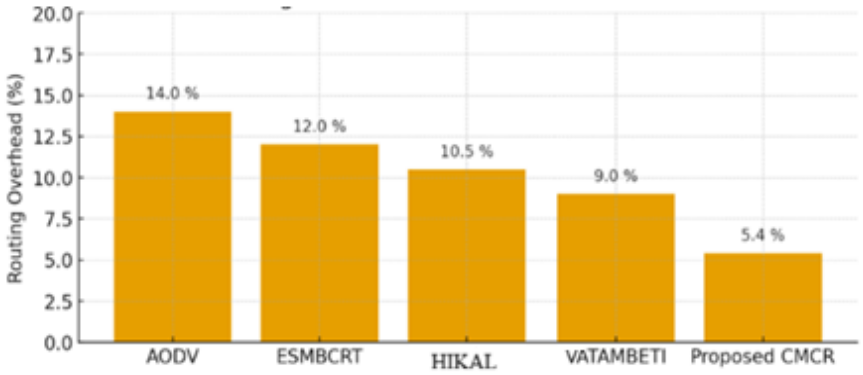

Figure 6. Routing overhead (%)

(f) Energy Consumption

Figure 7 shows the per-node energy consumption of different protocols for different network sizes. Our proposed CMCR always has the smallest energy consumption among others; it is less than 1.60 J in even higher node density cases. On average, CMCR consumes approximately 7% less energy compared with ESMBCRT and much less than Hikal *et al.* (2021), Vatambeti *et al.* (2024), and AODV. This overhead demonstrates the efficiency of CMCR's light-weight security and routing mechanisms. CMCR upgraded energy is mainly due to reduction of unneeded retransmissions. Due to CMCR's multi-hop CRC-chain checking and early suspicious packet behavior detection, malicious or untrusted nodes are not allowed to forward packets multiple times. This helps in elimination of duplicate transmission which is waste of node energy specially in case of dense networks where collision or attack probability are high. Furthermore, CMCR eliminates the need for broadcasting heavyweight network-wide trust and instead issues a localized alert. Rather than disseminating trust values, warnings, or diagnostic packets to everyone in the network—as is performed by ESMBCRT and other trust-based solutions —CMCR confines its verification process and warning dissemination mechanisms to a small vicinity (usually 3 hops). Such a mechanism significantly reduces the level of control packets disseminated, which leads to radio energy saving as one of the least efficient operations in MANET-nodes. In addition, CMCR's rapid recovery of routes and low overhead restrict the number of route discoveries and control-packet flooding. Classic protocols (e.g., AODV) cause the discovery of new routes when packets are dropped or links go down, and this results in wasting extra energy for both transmission and reception. By stabilizing routes and also by breaking the chain failures through allotted CRC-checking among the nodes, CMCR minimizes these energy consuming activities.

In summary, by reducing number of retransmissions, localized control messaging, limit the amount of verification and minimize route-recovery operations together allow CMCR to provide much lower energy consumption comparing with existing routing and trust-based protocols.

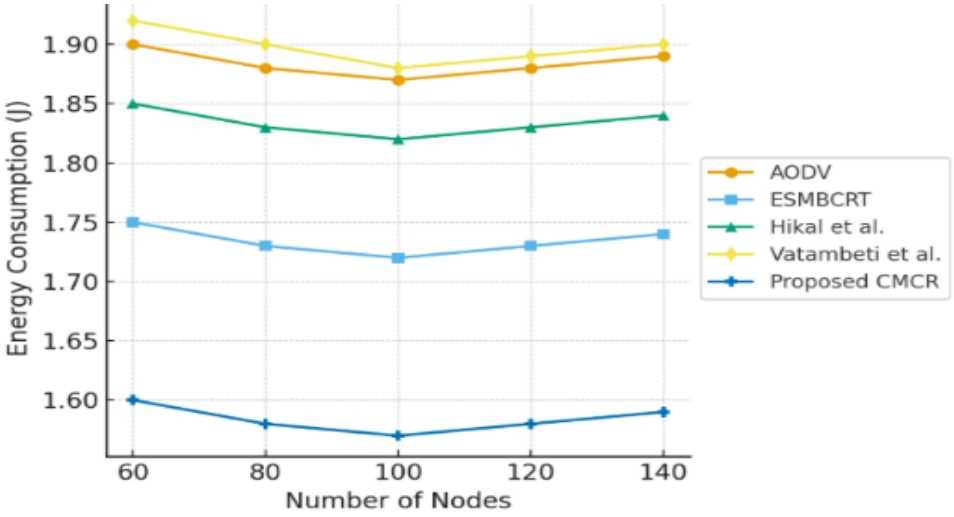

Figure 7. Energy consumption vs number of nodes

(g) False Positive Rate

Figure 8 presents the False Positive Rate (FPR) of the evaluated schemes with different attacker ratios. In all the settings, our CMCR protocol always attains the minimum FPR of around 2.1% which also remains unchanged when we increase the attacker ratio. On the other hand, existing methods —e.g. by Hikal *et al*. (2021) and Vatambeti *et al*. (2024) —achieve much higher FPR figures, often around 5%, and AODV and ESMBCRT present a similar trend. The reason that CMCR's FPR can be so low is the use of deterministic, packet-integrity-based detection rather than a statistical or model-based classification. CMCR employs multi-hop CRC-chain verification to identify packet corruption errors that are directly caused by malicious tampering or dropping. This results in a clear binary indication of malicious activity, so the detection mechanism is significantly more robust to changes in mobility, network density and traffic patterns. Machine-learning methods, however rely on feature vectors that represent the node behavior over time such as number of packets forwarded, delay in packet delivery, mobility patterns or trust metrics. In scenarios where the mobility of sensors is high with network topology changing fast, these features may fluctuate dynamically and unpredictably, which might lead the ML classifier to misclassify good as bad. It results in mis-classifications which are directly related to a high false positive rate. Furthermore, ML models may need to be retrained or tuned when the mobility level is varied in order to use them effectively in these levels that would not be feasible on real-time such as MANET scenarios. The CMCR circumvents these using cooperative cross-verification based detection, where the nodes in vicinity cross-checks to ensure that packet flow is valid. This multi-node verification also decreases the chance that a benign node is incorrectly marked as a malicious, since observations from a single node cannot prompt a false alarm.

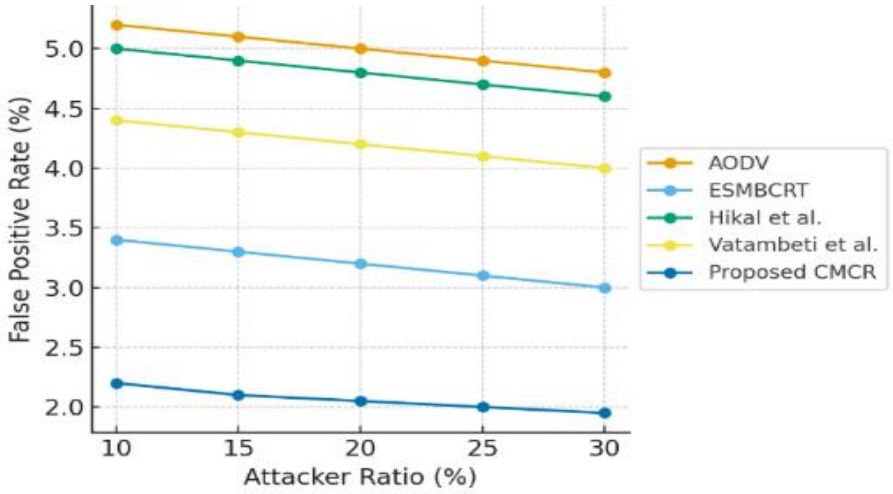

Figure 8. False positive rate (%) vs attacker ratio (%)

5.4. Results summary

Table 3. Summary of results obtained for the proposed CMCR approach with respect to the existing approaches

Metric	**AODV**	**ESMBCRT**	**Hikal *et al.* (2021)**	**Vatambeti *et al.* (2024)**	**Proposed CMCR Approach**
Packet Delivery Ratio (PDR)	77.3	88.4	91.2	92.1	94.6
E2E Delay (ms)	130	145	161	186	142
Throughput (Kbps)	411	455	480	472	512
Routing Overhead (%)	14.0%	12.0%	10.5%	9.0%	5.4%
Detection Accuracy (%)	71.5	83.4	91.2	88.5	96.3
Energy Consumption (J)	1.82	1.67	1.92	1.88	1.56
False Positive Rate (FPR) (%)	4.8	3.1	5.0	4.3	2.1

From the results obtained, it is clear that CMCR enhances security while allowing operational efficiency compatible with resource-limited MANET applications like battlefield communication, disaster recovery, and vehicular ad-hoc networks. The method shows fast adaptability as well as lightweight processing requirements and resilience to mobility variability and can be used as an alternative choice in next generation ad hoc networks.

6. Conclusion and future scope

6.1. Conclusion

In this paper, the authors have proposed a CMCR, which ensures a strong guard against black hole attacks for MANETs. We focus on CMCR as an alternative approach to security mechanisms such as AODV, ESMBCRT and ML based approaches that provide for a distributed, collaborative verification system that does not rely on centralized key management or static trust anchors. The improvement follows a novel CMCR methodology that uses multi-hop CRC chaining and trust-based reputation assessment to add a second layer of resilience in security and protection from malicious nodes (even in scenarios with significant node mobility). Our simulations show that CMCR has much better delay, delivery ratio, throughput, detection accuracy as well as energy efficiency with a low false positive rate. This lightweight system allows it to be implemented in MANETs of wide configurations without increasing routing complexity. Multiple hops of CRC validation chains mean that attacks will require coordinated collusion among multiple nodes, greatly reducing the chance of a single node being compromised.

6.2. Future scope

The CMCR framework also has much to offer in future research and development directions:

1. Cross-Layer Security Models: Future research may develop the possibility of integrating CMCR with the physical and MAC layer defenses to develop a complete cross-layer protection.
2. Adaptive CRC Optimization: Adaptive CRC chain length at different nodes depending on the network density and node mobility can be investigated in future work to optimize the trade-offs between delay and detection accuracy.
3. AI-Driven Reputation Learning: Real-time optimization on trust and reputation updates using federated learning or reinforcement learning approaches can enhance the source scalability through large MANET networks.
4. Blockchain-based Distributed Trust Ledger: Recording the CRC validation results and node reputation in a blockchain can give immutable evidence of node behavior without relying on a central authority.
5. Real-time Implementation: Future work can implement CMCR in NS-3 or OMNeT++ testbeds and extend it to vehicular ad hoc networks (VANETs) and IoT based MANET environments for greater applicability.

In summary, the CMCR approach offers a sustainable, decentralized, and cooperative infrastructure for the purposes of data integrity, access security, and trust management in MANETs. The CMCR both merges cryptographic security with trust-based verification, and represents an important step towards self-secured, efficient, energy, and adaptive MANET architectures.

Acknowledgements

The authors would like to acknowledge their parent university and college for providing all the relevant resources and facilities to complete this research work.

Declaration of Generative AI and AI-assisted technologies in the writing process:

During the preparation of this manuscript the author(s) did not used Generative AI and AI-assisted technologies and take(s) full responsibility for this declaration.

References

1. Alshammari, M. R., Elleithy, K. M. (2018) Efficient and secure key distribution protocol for wireless sensor networks. *Sensors*, 18(10), 3569. DOI:10.3390/s18103569.
2. Buchegger, S., Tissieres, C. and Le Boudec, J. Y. (2004) A test-bed for misbehavior detection in mobile ad-hoc networks - how much can watchdogs really do? In: *Proceedings of the Sixth IEEE Workshop on Mobile Computing Systems and Applications*, Windermere, December 2004. IEEE, 102-111. DOI: 10.1109/MCSA.2004.5.
3. Deng, H., Li, W. and Agrawal, D.P. (2002) Routing security in wireless ad hoc networks. *IEEE Communications Magazine*, 40(10), 70-75. DOI: 10.1109/MCOM.2002.1039859.
4. Dinesh, K., A., Singh, J. (2015) Security attacks in mobile Adhoc networks (MANET): A literature survey. *International Journal of Computer Applications*, 122(20), 31-35. DOI: 10.5120/21818-5148.

5. Djenouri, D., Khelladi, L. and Badache, A.N. (2005) A survey of security issues in mobile ad hoc and sensor networks. *IEEE Communications Surveys & Tutorials*, 7(4), 2-28. DOI: 10.1109/COMST.2005.1593277.
6. Heydari, V., Yoo, S.M. (2016) E2EACK: An end-to-end acknowledgment-based scheme against collusion black hole and slander attacks in MANETs. *Wireless Netw*, 22, 2259–2273. DOI: 10.1007/s11276-015-1098-6.
7. Hikal, N.A., Shams, M.Y., Salem, H., Eid, M.M. (2021) Detection of black-hole attacks in MANET using adaboost support vector machine. *Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology*, 41(1), 669-682. DOI:10.3233/JIFS-202471.
8. Hu, Y.C., Perrig, A. and Johnson, D.B. (2005) Ariadne: A secure on-demand routing protocol for Ad Hoc networks. *Wireless Netw*, 11, 21–38 (2005). DOI:10.1007/s11276-004-4744-y.
9. Jebrane, J., Chhaybi, A., Lazaar, S., and Nitaj, A. (2025) Elliptic curve cryptography with machine learning. *Cryptography*, 9(1), 3. DOI:10.3390/cryptography9010003.
10. Khan, N. R., Ahmad, G. F., Barskar, R., and Shukla, P. K. (2025) Mobile Adhoc networks: Protocols and its challenges. *IETE Journal of Research*, 1–31. DOI:10.1080/03772063.2025.2549521.
11. Kumar, V. and Kumar, R. (2015) An adaptive approach for detection of blackhole attack in mobile ad hoc network. *Procedia Computer Science*, 48, 472–479. DOI: 10.1016/j.procs.2015.04.122.
12. Mohammad, S.N., Singh, R.P., Dey, A., Ahmad, S.J. (2019) ESMBCRT: Enhance security to MANETs against black hole attack using MCR technique. In: Saini, H., Singh, R., Patel, V., Santhi, K., Ranganayakulu, S. (eds) Innovations in Electronics and Communication Engineering. Lecture Notes in Networks and Systems, vol. 33. Springer, Singapore. DOI:10.1007/978-981-10-8204-7_32.
13. Muzammal, S. M., Murugesan, R. K., Jhanjhi, N. Z., Humayun, M., Ibrahim, A. O., and Abdelmaboud, A. (2022) A trust-based model for secure routing against RPL Attacks in internet of things. *Sensors*, 22(18), 7052. DOI:10.3390/s22187052.
14. Narayana, M. V., Kumar, V. P., Nanda, A. K., Rao, H., and Chavva, S. R. (2023) Enhanced energy efficient with a trust aware in MANET for real-time applications. *Computers, Materials and Continua*, 75(1), 587–607. DOI:10.32604/cmc.2023.034773.
15. Perkins, C. E. and Belding-Royer, E. M. (1999) Ad-hoc on-demand distance vector routing. In: *Proceedings of the 2nd Workshop on Mobile Computing Systems and Applications (WMCSA '99),* New Orleans, February 1999. IEEE, pp. 90-100. DOI:10.1109/MCSA.1999.749281.
16. Sun, H.-M., Chen, C.-H. and Ku, Y.-F. (2012) A novel acknowledgment-based approach against collude attacks in MANET. *Expert Systems with Applications*, 39(9), 7968–7975. DOI:10.1016/j.eswa.2012.01.118.
17. Vatambeti, R., Mantena, S. V., Kiran, K. V. D., Chennupalli, S., and Gopalachari, M. V. (2024) Black hole attack detection using Dolphin echo-location-based machine learning model in MANET environment. *Computers and Electrical Engineering*, 114, 109094. DOI:10.1016/j.compeleceng.2024.109094.
18. Yadav, P. and Hussain, M. (2017) A secure AODV routing protocol with node authentication. In: Proceedings of *2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, April 2017. IEEE, 489-493, DOI: 10.1109/ICECA.2017.8203733.