International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(3s) 2026 pp. 594-605
https://doi.org/10.70917/ijcisim-2026-2338
Article

Golden Jackal Cost Optimized Zero Trust Security with Block-Chain for Intrusion Detection and Prevention in MANET with 5G and NxtG Technology

S. Kalaichelvi[1], K. R. Ananth[2]

[1]Department of Computer Science, Nandha Arts and Science College (Autonomous), Erode - 638 052, Tamilnadu, India. Email ID: sskalaichelvi06@gmail.com
[2]Department of Computer Science, Nandha Arts and Science College (Autonomous), Erode - 638 052, Tamilnadu, India. Email ID: sapujaa@gmail.com

Abstract: The usage of Fifth-Generation(5G) and Next-Generation(NxtG) technology within MANETs makes new opportunities for achieving reliable, high-speed, and low-latency connectivity. But, the absence of centralized management in MANETs, along with their exposure to security attacks and constrained resources, presents significant drawbacks. This paper proposes a Golden Jackal Cost Optimized Zero Trust Security with Block-Chain Technique (GJCOZTS-BCT) to provide robust and scalable security for MANETs operating under 5G and NxtG infrastructures. The GJCOZTS-BCT eliminates implicit trust within the network through enforcing a zero trust architecture where each node must continuously authenticate their identity and behavior of others before communication. A block-chain protocol is utilized in GJCOZTS-BCT to securely store trust metrics, authentication data, and policy logs, ensuring tamper-proof and transparent trust management. The GJCOZTS-BCT also incorporates a cost optimization engine that balances trust enforcement with resource usage by minimizing computational overhead during routing and access control decisions. By using the advanced capabilities of 5G and NxtG technology, proposed GJCOZTS-BCT ensures secure, real-time, and efficient operations across the MANET. The GJCOZTS-BCT is designed to effectively predict the cyber threats including Sybil, spoofing, and insider attacks in 5G and NxtG technology while maintaining scalability. The simulation of GJCOZTS-BCT is carried out using metrics such as packet delivery rate achieved approximately 95.98%, communication overhead reduced to 18ms, and scalability achieved 95.56% across dynamic MANET environments.
Keywords: 5G, Block-chain, Continuous Verification, Golden Jackal Optimization, MANET, Risk Function, Zero Trust Security

1. INTRODUCTION

The fast development of MANETs incorporated with 5G and NxtG communication technologies has facilitated flexible, low-latency, and infrastructure-less connectivity for applications such as emergency response, military communications, intelligent transportation, and satellite-assisted networking. Though, the decentralized and highly dynamic characteristic of MANETs formulates severe security problems such as node impersonation, insider attacks, routing manipulation, and DDoS attacks. The state-of-the-art techniques do not achieved higher security due to the absence of centralized control and continuously changing network topology. For example, Brown Boosted Expectation Maximization Ensemble Node Clustering (BBEMENC) Technique was implemented in [1] to provide enhanced routing performance in 5G and next technology. But, finding cyber threats in MANETs was remained open issue. An adaptive Zero Trust policy management framework called SecureChain-ZT was presented in [2] to overcome the limitations of static access control in 5G networks. However, computational overhead was higher.

Multi-Source Fast and Autonomous Zero-Trust Authentication (MUFAZA) was presented in [3] with aiming at performing autonomous authentication against a possible threats via accurate trust measurement. But, conventional MUFAZA computationally intensive and necessitates rich datasets. A secure handover authentication and key managing procedure was designed in [4] with the help of Chinese remainder theory. This method achieved

minimal communication overhead and computation overhead. However, 5G networks involve real-time processing of data, which affects the continuous monitoring and analysis performance. A novel scheme was intended in [5] for remote registration in 5G cellular system. With an increase in the quantity of associated devices, verification performance of the devices was not effectual. A Slice Specific Authentication and Access Control (SSAAC) method was introduced in [6]. Though, Scalability of SSAAC method was inadequate. An efficient verification and re-authentication procedures was implemented in [7] for 4G/5G heterogeneous networks to safeguard user identity and reduce the burden on the verification server during the sequential handovers. However, security level was poor.

Blockchain-enabled anonymous mutual authentication was planned in [8] to attain security and privacy for 5G networks. This algorithm protects privacy against various kinds of attacks. Though, communication overhead was very higher. Rapid and Universal Inter-Slice Handover validation with Privacy Preservation was presented in [9] for 5G with the support of block-chain, chameleon hash, and ring signature. This method decreases the overhead of the user side during the authentication process. However, multi-factor of user verification was not focused. Lightweight and Secure Authentication Model was introduced in [10] to render a more security in diverse vehicular communication with the application of lightweight cryptographic algorithms and securely access all messages. Though, authentication performance was insufficient when considering a larger 5G network. A Secure and Efficient Multi-Server Authentication Scheme was presented in [11] to find impersonation attack, password guessing attack in 5G Networks. But, this scheme required more time for accurate verification. Privacy-preserving authentication with device verification (PP-ADV) was planned in [12] for securing 5G networks with better data delivery ratio, authentication delay. However, false positive rate of device verification was higher.

2. RELATED WORKS

The DzTrust scheme was developed in [13] with the objective of providing better performance in predicting compromised nodes with higher computational and communication efficiency. But, dynamic identity authentication was not considered. SqueezeNet-based key generation was utilized in [14] for protecting device-to-device group verification in 5G wireless networks. Though, 5G networks are complex where it includes many unified constituents which formulate it hard to define clear boundaries for trust and to apply security management efficiently. A Blockchain-Based Authentication and Key Agreement (AKA) was implemented in [15] to defend user privacy and offers mutual authentication of the participants. But, 5G networks contain more number of devices and connections which formulate it complex to balance security controls without affecting their performance. Fast user verification was presented in [16] for 5G heterogeneous networks with the aid of the reinforcement learning and block-chain technology. However, strong authentication and authorization was not achieved.

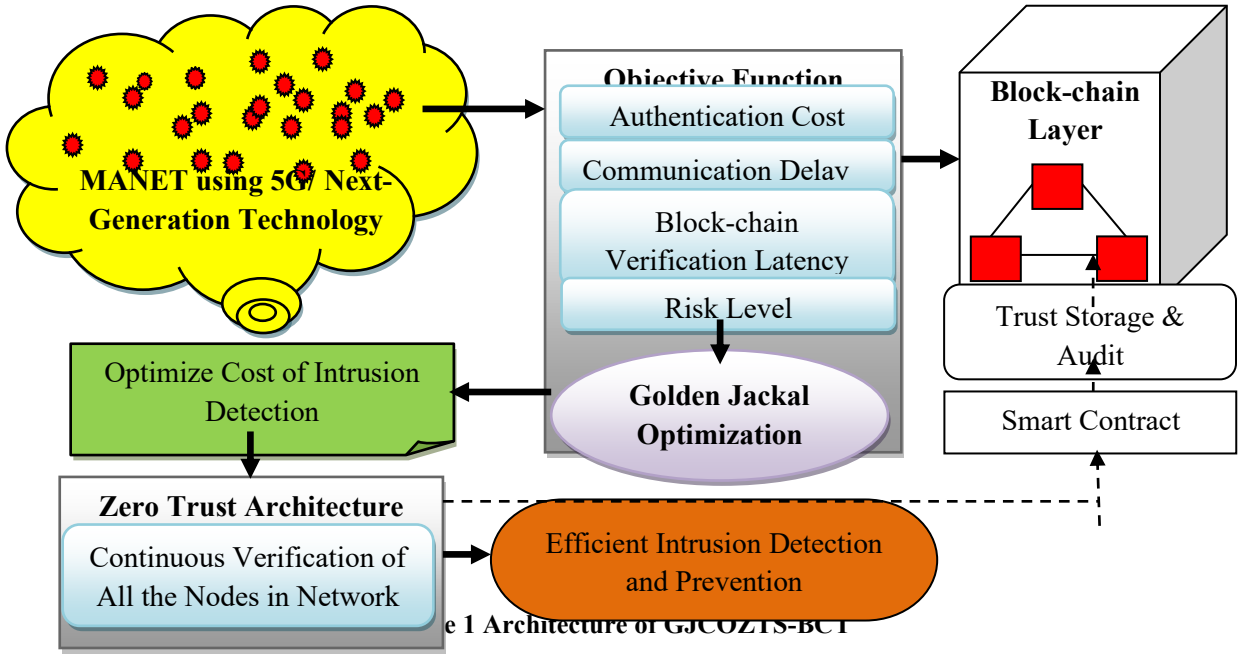
Lattice-Based Cryptography and Fog Computing Based Efficient Anonymous Authentication Scheme was constructed in [17] with the goal of minimizing processing cost for generating and verifying message signatures. Though, transmission cost was more. A 2-way identity authentication method (2WIAM) was intended in [18] with the assist of Physical Unclonable Function to enhance the users' privacy. But, authentication accuracy was not sufficient. Three-Factor Authentication Scheme was presented in [19] for 5G wireless sensor networks. However, the data lost rate was higher. Privacy Enhanced Fast Mutual verification was performed in [20] with the support of identity based encryption in 5G Network. But, the complexity involved during the mutual verification process was not reduced. Secure Secondary Authentication Framework was intended in [21] to boost efficiency of network via managing the traffic created during the mutual verification. However, predicting the abnormal behavior of network was not considered. In order to resolve the above problems, GJCOZTS-BCT is introduced in this paper. The key contributions of GJCOZTS-BCT is described as,

- A Zero Trust Security framework is integrated in GJCOZTS-BCT enforces the rule of never trust, always verify, while reducing the overhead associated with continuous authentication and monitoring. Thus, proposed GJCOZTS-BCT enables continuous verification of nodes while significantly reducing security overhead.
- The Golden Jackal Optimization algorithm is implemented in GJCOZTS-BCT to dynamically optimize security parameters where it ensures an effective balance between attack detection accuracy and resource efficiency, even under varying traffic loads and node mobility.
- Block-chain technology is combined in GJCOZTS-BCT to provide tamper-proof storage of risk scores, authentication costs, and intrusion decisions. From that, GJCOZTS-BCT enhances resilience against insider

attacks and enables collaborative intrusion prevention across MANET nodes in next-generation wireless networks.

3. PROPOSED GJCOZTS-BCT

The GJCOZTS-BCT introduces a cost-optimized zero trust security architecture integrated with block-chain technology for intrusion detection and prevention in decentralized and dynamic networks. The GJCOZTS-BCT is designed to operate efficiently in MANET environments enhanced by 5G and Next-Generation (NxtG) communication technologies where high mobility, low latency, and massive connectivity significantly increase security challenges. The proposed GJCOZTS-BCT enforces continuous verification of all nodes without assuming implicit trust. To mitigate the high overhead associated with continuous authentication, the GJCOZTS-BCT employs the Golden Jackal Optimization (GJO) algorithm to dynamically minimize security cost while preserving strong intrusion detection performance. The architecture of GJCOZTS-BCT is presented in Figure 1.



e 1 Architecture of GJCOZTS-BCT

As shown in the above Figure 1, GJCOZTS-BCT initially considers a more number of mobile users in MANET using 5G/ NxtG technologies. The aim of the GJCOZTS-BCT is to minimize the overall security cost while maintaining effective intrusion detection. Therefore, GJCOZTS-BCT then defines objective function using authentication cost, communication delay, block-chain verification latency and risk level of users. Subsequently, the GJO algorithm is applied in GJCOZTS-BCT to find the solution for above objective function. Motivated by the hunting actions of golden jackals, GJO balances exploration and exploitation to predict optimal candidate solution that reduces the cost of reliable intrusion detection. Besides to that, Blockchain concept is used in GJCOZTS-BCT to present a tamper-proof trust management where risk scores, authentication costs, and access decisions are stored as immutable blockchain transactions. Smart contracts in GJCOZTS-BCT enforce access control policies and trigger attack prevention actions when a risk threshold are higher and also ensures transparent auditing of security events across the network. Hence, GJCOZTS-BCT provides scalable, and robust intrusion detection and prevention solution for next-generation mobile networks.

Problem Formulation

MANETs integrated with 5G and Next-Generation (NxtG) technologies facilitate ultra-low latency and high-mobility communication however it was affected by decentralized control, dynamic topology, and increased attack surfaces. The state-of-the-art security techniques are ineffective in such environments. Therefore, a novel

GJCOZTS-BCT is proposed by using a zero trust security framework integrated with block-chain concept for effective intrusion detection and prevention.

Objective Function (Overall Optimization Problem)

The main goal of GJCOZTS-BCT is to minimize the total system cost of zero trust 5G network and NxtG Technology under the following security constraints,

- Authentication Cost
- Communication Delay
- Block-chain Verification Latency
- Risk Level From User

Thus, objective function (OF) of zero trust 5G network and NxtG Technology is mathematically formulated as,

$$\min OF = a_1 C_A + a_2 Delay_C + a_3 Delay_{BCV} + a_4 R_i \qquad (1)$$

In equation (1), 'C_A' defines cost of continuous authentication, 'D_C' describes communication delay between nodes, 'D_B' represents delay due to block-chain consensus and verification and 'R' refers risk score (attack probability or trustworthiness). Here, 'a_i' indicates weighting factor.

Authentication Cost

In zero trust 5G network and NxtG Technology, each session or message is authenticated with the help of below equation,

$$C_A = \sum_{i=1}^{N} (\lambda_i . f(Trust_i, Reputation_i, Device_i)) \qquad (2)$$

In equation (2), λ_i indicates authentication frequency or intensity for user 'i' whereas $f(.)$ describes a function integrating user's trust score, reputation and device security state.

Communication Delay

The communication delay in zero trust 5G network and NxtG technology is mathematically formulated as,

$$Delay_C = \sum_{(i,j)\epsilon E} \frac{d_{i,j}}{B_{i,j}} + \mu_{ij} \qquad (3)$$

In equation (3), $d_{i,j}$ represent data size between node 'i' and 'j' and $B_{i,j}$ defines bandwidth between 'i' and 'j' whereas μ_{ij} describes propagation or queuing delay.

Block-chain Verification Latency

The block-chain verification latency in zero trust 5G network and NxtG technology is mathematically described as,

$$Delay_{BCV} = \tau_{tx} + \tau_{consensus} + \tau_{smart\_contract} \qquad (4)$$

In equation (4), τ_{tx} defines transaction creation and broadcasting time and $\tau_{consensus}$ refers time for reaching consensus whereas $\tau_{smart\_contract}$ indicates smart contract execution time for access control.

Risk Function

The risk function in zero trust 5G network and NxtG technology is mathematically defined as,

$$R_i = \sum_{i=1}^{N} P_{attack,i}.S_i \quad (5)$$

In equation (5), $P_{attack,i}$ represent probability that user 'i' is an attacker whereas S_i defines sensitivity or impact of attack from user 'i'.

To minimize the security cost of zero trust 5G network and NxtG technology, Golden Jackal Optimization algorithmic concept is utilized in this research work where Zero Trust Security is applied for continuous verification and block-chain concept is used for tamper-proof authentication and trust management. In GJCOZTF-BCT, Golden Jackal Optimization is a bio-motivated algorithm which depends on golden jackal hunting approaches such as tracking, surrounding, and attacking prey.

Step 1: Initialization:

Considered an initial population of candidate solutions using below mathematical expression,

$$X = \{x_1, x_2, .. x_N\} \quad (6)$$

In the equation (6), each x_i represents authentication frequency, trust threshold, consensus timeout, node role assignment (e.g., validator).

Step 2: Fitness Measurement:

Fitness for each candidate solutions is estimated based on the objective function which obtained mathematically as,

$$J(x_i) = a_1 C_A + a_2 Delay_C + a_3 Delay_{BCV} + a_4 Risk \quad (7)$$

Step 3: Alpha Jackal Selection:

Find the best solution (alpha jackal) with the lowest cost using mathematically as,

$$x_{alpha} = \arg\min_{x_i} J(x_i) \quad (8)$$

Step 4: Exploration:

Each jackal's position (solution) is mathematically updated as,

$$x_i^{t+1} = x_i^t + r_1.(x_{alpha} - |r_2.x_i^t|) \quad (9)$$

In the equation (8), r_1, r_2 indicates random coefficients for exploration.

Step 5: Exploitation:

Optimize the solution as jackals surround the best prey using following equation,

$$x_i^{t+1} = x_{alpha} - r_3.\left|tan\,h\,(F).\,x_{alpha} - x_i^t\right| \quad (10)$$

In the equation (10), F describes convergence factor which decreased with iterations and $\tan h$ defines controls balance between exploration and exploitation. From that, golden jackal optimization algorithm efficiently reduces the cost of zero trust security architecture in 5G network and NxtG technology while using the black-chain concept.

Each candidate solution in the GJO population indicates a specific configuration of Zero Trust parameters. The fitness of each solution is determined using the risk function and authentication cost of users. Through iterative tracking, surrounding, and attacking phases, GJO converges toward a globally optimal configuration that reduces security cost while achieving robust intrusion detection accuracy. From that, attack detection and prevention is mathematically performed as,

$$Y = \begin{cases} \text{If } R_i < R_{th} \text{and } C_A < C_{th}, \text{then user is normal/trusted} \\ \text{If } R_i < R_{th} \text{and } C_A \geq C_{th}, \text{then user is suspect} \\ \text{f } R_i \geq R_{th} \text{and } C_A \geq C_{th}, \text{then user is attacker/intrusion} \end{cases} \quad (11)$$

In the equation (11),$R_{th} = 0.6$ defines the risk threshold and $C_{th} = 0.5$ refers the cost threshold. By using the above equation, each user in 5G network and NxtG technology is significantly identified as normal or suspect or 5G network and NxtG technology with respect to their risk and cost function.

Table 1 Prediction Result

Detection Output Y	**Action**
Normal user	Allow full access to get all the services
Suspect	Trigger multi-factor authentication
Attacker	Block

The algorithmic steps of GJCOZTS-BCT is represented as follows,

// Golden Jackal Cost Optimized Zero Trust Framework with Block-Chain Technique
Input: Number of mobile users $u_1, u_2, .., u_N$;
Output: Improves the security of inter-satellite communication with better latency
Step 1:Begin
Step 2: Consider number of users $u_1, u_2, .., u_N$
Step 3: **For** each users u_i in 5G network and NxtG technology
Step 4: Define objective function using (1)
Step 5: Measure authentication cost using (2)
Step 6: Determine communication delay using (3)
Step 7: Evaluate block-chain verification latency using (4)
Step 8: Estimate risk function using (5)
// Apply Golden Jackal Optimization
Step 9: Initialize population of candidate solutions using (6)
Step 10: Measure Fitness for each candidate solutions using (7)
Step 11: Find alpha jackal solutions with the lowest cost using (8)
Step 12: Update each jackal's position using (9)
Step 13: Find optimal candidate solutions to reduce cost of intrusion detection
Step 14: **If** $R_i < R_{th}$ and $C_A < C_{th}$ **then**
Step 15: User u_i is identified as Normal or Trusted user
Step 16: **Else If** $R_i < R_{th}$ and $C_A \geq C_{th}$ **then**
Step 17: User u_i is detected as Suspect
Step 18: **Else If** $R_i \geq R_{th}$ and $C_A \geq C_{th}$), **then**
Step 19: User u_i is predicted as intrusion
Step 20: **End If**
Step 21: End For
Step 22:End

Algorithm 1 Golden Jackal Cost Optimized Zero Trust Security with Block-Chain Technique

Algorithm 1 represents the process of GJCOZTS-BCT. With the help of above algorithmic procedures, GJCOZTS-BCT attained enhanced attack detection and prevention performance in 5G/ next technology with better communication overhead and scalability as compared to existing works.

4. SIMULATION SETUP

The GJCOZTS-BCT is implemented in NS-3 simulator where MANET comprising 50–250 mobile nodes is considered as input to emulate realistic 5G and NxtG communication scenarios. Nodes are randomly considered within a 1000 m × 1000 m region and utilize Random Waypoint Mobility Model with node speeds ranging from 1 to 20 m/s. Each node is connected with 5G/NxtG radio interfaces supporting high-data-rate, low-latency communication. The metrics assumed for simulation is shown in Table 2.

Table 2 Simulation Constraints

Metrics	Values
Network Simulator	NS-3
Simulation Area	1100 m × 1100 m
Number of Mobile Nodes	250
Node Deployment	Random
Mobility Model	Random Waypoint
Speed of Nodes	0 – 20 m/s
Pause Time	5 s
Simulation Time	250 s
Traffic Type	CBR / VBR
Packet Size	64, 128, 256, 512, 1024 bytes
Queue Type	DropTail
Queue Size	50 packets
Initial Battery Energy	100 J
Transmission Range	250 m
MAC Protocol	IEEE 802.11g / 5G NR (emulated)
Communication Technology	MANET with 5G / NxtG support
Routing Protocol	DSR
Attack Types	Blackhole, Grayhole, Flooding, Impersonation
Security Model	Zero Trust Security
Optimization Algorithm	Golden Jackal Optimization (GJO)
Blockchain Functionality	Risk Storage, Auth Cost Logging, Access Control
Risk Threshold	0.6
Authentication Cost Threshold	0.5

The result of proposed GJCOZTS-BCT is compared against with conventional BBEMENC)Technique [1] and SecureChain-ZT [2]. The performance of proposed GJCOZTS-BCT is tested using the following metrics,

- Packet Delivery Rate
- Communication Overhead
- Scalability

4. RESULTS AND DISCUSSION

5.1 Packet Delivery Rate (PDR)

It determines the number of packets efficiently get by the destination to the number of packets sent by the source in MANET using 5G and next generation technology which obtained mathematically as,

$$PDR = \left(\frac{Number\ of\ data\ packets\ \text{efficiently}\ received}{n}\right) * 100 \qquad (12)$$

In equation (12), 'n' indicates a total packets sent by source node. The data delivery rate is determined in percentage (%).

Table 3 Simulation Performance of PDR

Number of data packets	PDR (%)		
	BBEMENC	SecureChain-ZT	GJCOZTS-BCT
25	90.88	89.05	92.14
50	91.56	89.96	93.54
75	92.13	90.51	94.28
100	93.41	91.62	95.34
125	94.55	92.11	95.98

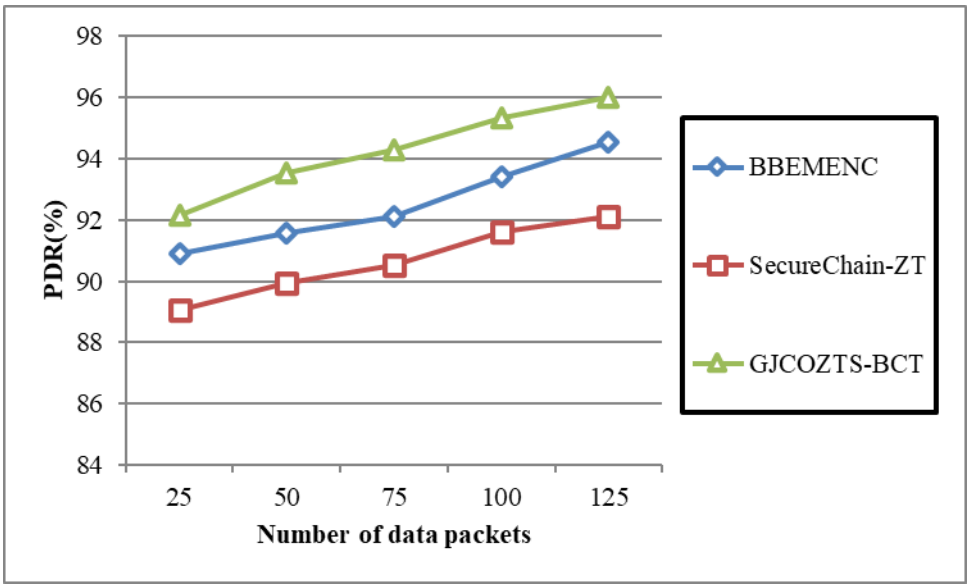


Figure 2 Graphical Results of Packet Delivery Ratio

Table 3 and Figure 2 describes the testing results of PDR versus dissimilar number of data packets for three frameworks i.e. BBEMENC, SecureChain-ZT, and the proposed GJCOZTS-BCT. As the number of data packets increases from 25 to 125, all three frameworks display a gradual enhancement in PDR which represents better network reliability under higher traffic loads. Among the compared approaches, proposed GJCOZTS-BCT consistently attained highest PDR, starting at around 92% for 25 packets and reaching approximately 96% at 125 packets. This enhancement emphasizes the efficiency of Golden Jackal cost optimization integrated with Zero Trust and blockchain concepts in ensuring secure and efficient packet forwarding. The existing BBEMENC model illustrates moderate performance, with PDR values ranging between approximately 91% and 94.5% whereas existing SecureChain-ZT records the lowest PDR, varying from about 89% to 92%. The better performance of proposed GJCOZTS-BCT reveals its ability to reduce packet loss through dynamically optimizing authentication cost and risk-aware access decisions in increasing network traffic conditions.

5.2 Communication Overhead

Communication Overhead (CO) is determined based on time the data packets required to effectively reach their destination in MANET using 5G and next generation technology. From that, CO determines the difference

among the transmitting and receiving time of data packets in MANET while utilizing 5G next generation technology which obtained mathematically as,

$$CO = (d_{re} - d_{se}) \quad (13)$$

In equation (13), d_{re} describes receiving time of data packets, d_{se} defines sent time of data packet. The overhead is involved during the data communication in MANET is measured in milliseconds (ms).

Table 4 Simulation Performance of Communication Overhead

Number of data packets	Communication Overhead (ms)		
	BBEMENC	SecureChain-ZT	GJCOZTS-BCT
25	11	12	10
50	14	15	12
75	15	19	13
100	17	21	15
125	20	25	18

Table 4 and Figure 3 shows the experimental results of communication overhead versus number of data packets considered as input using three approaches: BBEMENC, SecureChain-ZT, and the proposed GJCOZTS-BCT. As the traffic load raises from 25 to 125 data packets, communication overhead increases for all schemes owing to increased control signaling, authentication exchanges, and security operations. Among the compared methods, proposed GJCOZTS-BCT gets better communication overhead where it increasing modestly from about 10 ms to 18 ms. This is because of usage of Golden Jackal cost-optimized Zero Trust mechanism which reduces redundant authentication and blockchain interactions through optimal policy selection.

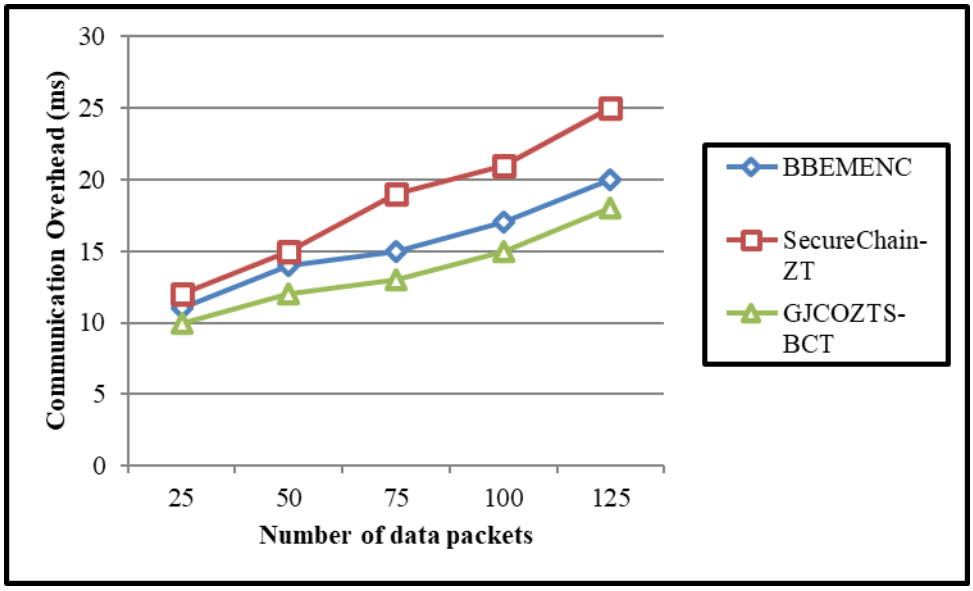


Figure 3 Graphical Results of Communication Overhead

The conventional BBEMENC demonstrates moderate overhead, ranging from approximately 11 ms to 20 ms whereas existing SecureChain-ZT shows the highest overhead, ranging from nearly 12 ms to 25 ms as packet volume increases. Overall, the results designate that proposed GJCOZTS-BCT attains an improved balance between security enforcement and communication efficiency, formulating it more suitable for high-traffic and resource-constrained MANET environments integrated with 5G and next-generation technologies.

4.3 Scalability

Scalability measures the capability of a network to manage efficiently a raise in users, devices, or data and also guarantee that performance remains secure and reliable. The scalability is measured in percentages (%).

Table 5 Simulation Performance of Scalability

Number of Mobile users	Scalability (%)		
	BBEMENC	SecureChain-ZT	GJCOZTS-BCT
50	91.45	89.38	93.57
100	92.03	90.15	93.89
150	92.93	91.42	94.87
200	93.56	91.99	95.12
250	94.44	92.54	95.96

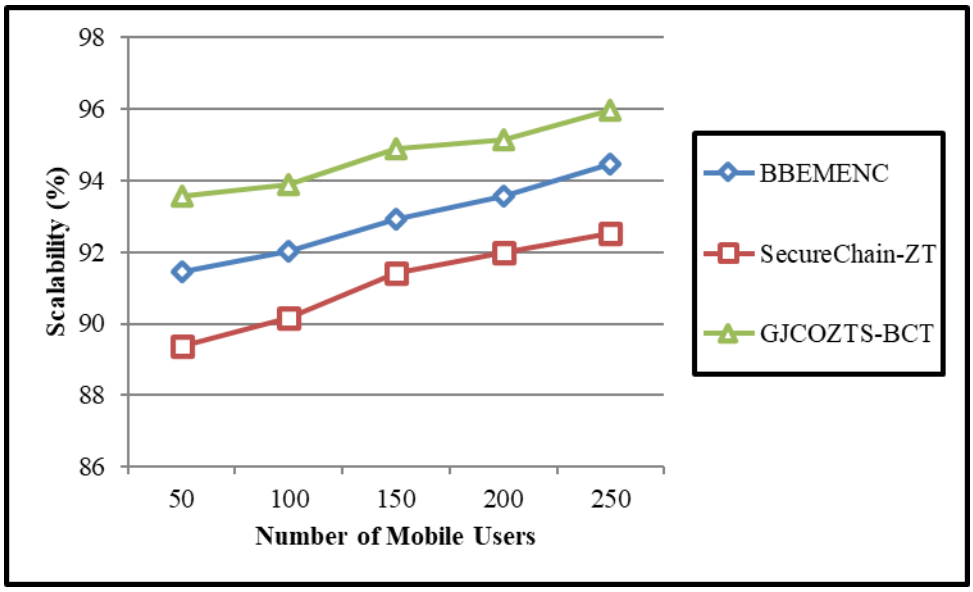


Figure 4 Graphical Results of Scalability

Table 5 and Figure 4 display the scalability outputs of three techniques i.e. BBEMENC, SecureChain-ZT, and the proposed GJCOZTS-BCT with respect to the number of mobile users in the network. As the number of users increases from 50 to 250, all techniques show enhanced scalability, indicating their ability to accommodate upward network sizes. Among the compared methods, proposed GJCOZTS-BCT achieves the better scalability, increasing from approximately 93.5% to 96%. This better performance emphasizes the effectiveness of the Golden Jackal cost-optimized Zero Trust model combined with blockchain technology, which efficiently manages authentication, access control, and trust estimation in a decentralized manner. The state-of-the-art BBEMENC demonstrates moderate scalability, ranging from about 91.5% to 94.5% whereas conventional SecureChain-ZT shows the lowest scalability where it ranging from 89.5% to 92.5%. Overall, the results exhibit that proposed GJCOZTS-BCT scales more effectively in dense MANET environments, making it compatible for large-scale deployments integrated with 5G and next-generation communication technologies.

6. CONCLUSION

This paper introduced a GJCOZTS-BCT for intrusion detection and prevention in dynamic MANET environments integrated with 5G and next-generation communication technologies. The GJCOZTS-BCT combines

continuous Zero Trust authentication, and blockchain-based trust management, while utilizing the GJO to decrease authentication and communication costs without compromising security. By considering security enforcement as a cost–risk optimization issue, GJCOZTS-BCT selects optimal security policies depends on real-time network conditions, node behavior, and threat levels. Blockchain concept in GJCOZTS-BCT ensures tamper-resistant storage of risk scores, authentication decisions, and access logs, enabling decentralized trust establishment and eliminating dependence on centralized authorities. The integration of GJO drastically decreases redundant authentication operations and optimizes resource consumption, which is critical in highly mobile and resource-constrained MANET scenarios. Simulation output reveals that the proposed GJCOZTS-BCT outperforms conventional techniques in terms of packet delivery rate is based on the number of data packets from 25 to 125, which is increased from 92.14% to 95.98%. The communication overhead is minimized to approximately 18ms compared with the conventional methods BBEMENC and SecureChain-ZT. The scalability is achieved in the dynamic MANET environment based on the number of nodes (from 25 nodes to 250 nodes), approximately from 93.57% to 95.56%. Thus, the proposed GJCOZTS-BCT presents a robust and cost-effective solution for intrusion identification and prevention in 5G and next-generation environments.

References

1. S. Kalaichelvi, K. R. Ananth, “Brown Boosted Expectation Maximization Ensemble Node Clustering Based Energy Efficient And Reliable Data Routing In Manet With 5g And Nxtg Technology”, Journal of Neonatal Surgery, Volume: 14, Issue: 28s, 2025
2. Alnaim, Abdulrahman K. "Adaptive Zero Trust Policy Management Framework in 5G Networks." *Mathematics* 13, no. 9 (2025): 1501.
3. Y. Ge and Q. Zhu, "MUFAZA: Multi-Source Fast and Autonomous Zero-Trust Authentication for 5G Networks," *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, Rockville, MD, USA, 2022, pp. 571-576, doi: 10.1109/MILCOM55135.2022.10017839
4. J. Huang and Y. Qian, "A Secure and Efficient Handover Authentication and Key Management Protocol for 5G Networks," in Journal of Communications and Information Networks, vol. 5, no. 1, pp. 40-49, March 2020, doi: 10.23919/JCIN.2020.9055109
5. emangi Goswami, Hiten Choudhury, “Remote Registration and Group Authentication of IoT Devices in 5G Cellular Network”, Computers & Security, Volume 120, 2022, 102806, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2022.102806
6. Shanay Behrad, Emmanuel Bertin, Stéphane Tuffin, Noel Crespi, “A new scalable authentication and access control mechanism for 5G-based IoT, Future Generation Computer Systems, Volume 108, 2020, Pages 46-61, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.02.014
7. Alezabi, K.A., Hashim, F., Hashim, S.J. et al. Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks. J Wireless Com Network 2020, 105 (2020). https://doi.org/10.1186/s13638-020-01702-8
8. Zaher Haddad, “Blockchain-enabled anonymous mutual authentication and location privacy-preserving scheme for 5G networks”, Journal of King Saud University - Computer and Information Sciences, Volume 35, Issue 6, 2023, 101458, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.11.018
9. Zhe Ren, Xinghua Li, Qi Jiang, Qingfeng Cheng, Jianfeng Ma, “Fast and Universal Inter-Slice Handover Authentication with Privacy Protection in 5G Network”, Security and Communication Networks, Volume 2021, Issue 1, 6694058, https://doi.org/10.1155/2021/6694058
10. Meriem Houmer, Safaa Laqtib, Siham Eddamiri, “Lightweight and Secure Authentication Model for Vehicle to Everything (V2X) Communication Based on 5G Networks”, Journal of Mobile Multimedia, Volume 18, Issue 5, September 2022, Pages 1399 – 1424
11. Azeem Irshad; Mohammed Alreshoodi, “SEMS-5G: A Secure and Efficient Multi-Server Authentication Scheme for 5G Networks”, IEEE Access, Volume: 12, Pages 49062 – 49077, April 2024
12. Patruni, M.R., Humayun, A.G. PPAM-mIoMT: a privacy-preserving authentication with device verification for securing healthcare systems in 5G networks. Int. J. Inf. Secur. 23, 679–698 (2024). https://doi.org/10.1007/s10207-023-00762-3
13. Wang, K., Hong, Y., Li, Y. et al. A distributed zero-trust scheme for airborne wireless sensor networks using dynamic identity authentication. Sci Rep 15, 8036 (2025). https://doi.org/10.1038/s41598-025-91957-2
14. Chandran, K.P., Dharmaraju, G., Misra, A. et al. SqueezeNet-based key generation for secure device-to-device group authentication in 5G wireless networks. Wireless Netw (2025). https://doi.org/10.1007/s11276-025-03951-1

15. M. Hojjati, A. Shafieinejad and H. Yanikomeroglu, "A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks," in *IEEE Access*, vol. 8, pp. 216461-216476, 2020, doi: 10.1109/ACCESS.2020.3041710
16. Manjaragi, S.V., Saboji, S.V. Fast user authentication in 5G heterogeneous networks using RLAC-FNN and blockchain technology for handoff delay reduction. *Wireless Netw* **29**, 3187–3205 (2023). https://doi.org/10.1007/s11276-023-03371-z
17. Z. G. Al-Mekhlafi et al., "Lattice-Based Cryptography and Fog Computing Based Efficient Anonymous Authentication Scheme for 5G-Assisted Vehicular Communications," in IEEE Access, vol. 12, pp. 71232-71247, 2024, doi: 10.1109/ACCESS.2024.3402336
18. Ali Darch Abed Dawa, "Enhancing Wireless Security and Privacy: A 2-Way Identity Authentication Method for 5G Networks", International Journal of Mathematics, Statistics, and Computer Science, Vol. 2, 2024
19. Q. Xie and Q. Xie, "Security Analysis on a Three-Factor Authentication Scheme of 5G Wireless Sensor Networks for IoT System," in *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 15038-15042, 15 April15, 2024, doi: 10.1109/JIOT.2023.3334708
20. M. Khan and V. Niemi, "Privacy Enhanced Fast Mutual Authentication in 5G Network Using Identity Based Encryption," in *Journal of ICT Standardization*, vol. 5, no. 1, pp. 69-90, 2017, doi: 10.13052/jicts2245-800X.514.
21. Gong, Seonghyeon, Abir EL Azzaoui, Jeonghun Cha, and Jong Hyuk Park. 2020. "Secure Secondary Authentication Framework for Efficient Mutual Authentication on a 5G Data Network" *Applied Sciences* 10, no. 2: 727. https://doi.org/10.3390/app10020727