International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 2, Mar-Apr-2025, ISSN (Online): 2395-566X

Collusion-Free MANET Communication Framework for Direct Connectivity

Asmitha V[1], Jaya Malini V[2], Manisha M[3], K. Amudha[4]
Final ECE Student, Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Trichy[1,2,3]
Professor, Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Trichy[4]

Abstract- Dynamic, infrastructure-free communication be- tween mobile devices are made possible via mobile ad hoc networks, or MANETs. Their dependability is hampered by issues including malicious activity, node cooperation, and security risks. A collusion-free MANET communication architecture for safe and effective direct mobile-to-mobile networking is pro- posed in this research. The system uses trust-based processes and sophisticated cryptographic algorithms to identify and stop node collusion. Network performance indicators like throughput, latency, and packet delivery ratio may be thoroughly analyzed through simulation using MATLAB. By improving MANETs' overall security and dependability, the suggested method enables smooth communication in dynamic, resource-constrained con- texts. Results show that it performs better than current methods, which makes it appropriate for use in remote connectivity, military operations, and disaster recovery.

Index Terms- Mobile Ad-Hoc Networks (MANETs), AES- 256 Encryption, Cryptography, Trust-Based Mechanisms, Network Security, MATLAB Simulations.

I. INTRODUCTION

An incredible advancement in communication technology, mobile ad-hoc networks (MANETs) allow mobile devices to create a self-organizing network independent of centralized or fixed infrastructure. Because of this special feature, MANETs are ideal for usage in situations when regular communication networks are either impractical or unavailable, such as military missions, disaster recovery operations, and isolated locations. The decentralized structure of MANETs presents substantial obstacles despite their many benefits. These include security issues such hostile assaults by compromised nodes, node-to-node collaboration to block communication, and other weaknesses that could harm the network's dependability and performance [1].

This study presents a novel framework intended to improve the security and effectiveness of MANET communication to address these problems. The suggested system addresses certain difficulties of these networks by combining trust-based procedures with cutting-edge cryptographic approaches. The framework utilizes AES-256 encryption to protect data while it is being transmitted, guaranteeing confidentiality and guarding against unwanted access.

It also includes a dynamic trust evaluation system that continuously evaluates participating nodes' dependability. The architecture reduces the possibility of attacks and enhances network stability by limiting communication to trusted nodes exclusively [2].

To ensure trustworthy communication, this framework's implementation focusses on enhancing important network performance measures like throughput, latency, and packet delivery ratio (PDR). Extensive MATLAB simulations have been used to evaluate the framework, and the outcomes indicate how well it works to provide safe and effective communication in MANETs. This solution provides an appropriate and useful method for addressing the security and performance issues that MANETs come across, making it especially beneficial for dynamic and constrained by resources applications [4].

II. LITERATURE REVIEW

D. G. Kampitaki and A. A. Economides, "Selfishness in Mobile Ad-Hoc Networks: A Literature Review on Detection Techniques and Prevention Mechanisms," in IEEE Access, vol. 11, pp. 86895-86909, 2023, doi: 10.1109/ACCESS.2023.3305262.
Constant connectivity is one of the most challenging requirements modern communication networks promise to satisfy. 5G and Beyond applications and the proliferation of Internet of Things (IoT) applications make mobile networks one of the most discussed research topics of the present, while research is already moving towards the design specifications and development of 6G services and solutions. Using multi-

hop patterns, mobile nodes can move around always maintaining their connectivity in a pervasive and ubiquitous manner. New possibilities emerge from this progress, whereas long-known challenges still exist and evolve. One of them is the selfishness or unwillingness of some nodes to spend resources to serve the communication requests of other nodes, not in a malicious but rather in a self-conservative manner. While intentional misbehavior of nodes is considered a security issue, selfishness is studied separately in the relevant literature and has attracted a lot of research attention.

In this review we attempt to present the leading research on detection techniques and the preventive mechanisms employed by previous studies to address the selfishness problem in mobile ad hoc networks, and identify the trends during the past few years, focusing primarily on the routing layer. We follow a systematic methodology to identify, select, categorize, and analyze the relevant research and use a concept-centric approach to present the results forming a comprehensive starting point for future research.

D. Kafetzis, S. Vassilaras, G. Vardoulias and I. Koutsopoulos, "Software-Defined Networking Meets Software-Defined Radio in Mobile ad hoc Networks: State of the Art and Future Directions," in IEEE Access, vol. 10, pp. 9989-10014, 2022, doi: 10.1109/ACCESS.2022.3144072.
The aims of this survey article are to elaborate on cross-layer optimization, Software-Defined Networking (SDN) and Software- Defined Radio (SDR) as separate domains of wireless network design for which a unified view has not been adequately considered to date and present lessons learned, with a view towards the challenges associated with SDN-SDR interaction that would facilitate benefits in cross-layer optimization of mobile ad hoc networks (MANETs). We focus on MANETs because (${i}$) they are still at the forefront of technology, and in some scenarios, they are the only meaningful option for establishing communication; (ii) they expose the full potential and benefits of coexistence and interaction of SDN and SDR, in terms of optimizing key performance indicators. While SDN and SDR are mature technologies, their interaction and joint consideration have been largely overlooked. Current SDN approaches do not span the physical (PHY) and medium-access control (MAC) layers, but they rather concentrate on network-level routing and traffic flow optimization. As a result, PHY- and MAC-layer related parameters which notoriously affect key network performance metrics remain static or at best are adapted based on some heuristic or local approaches. On the other hand, the reach of SDR architecture is restricted to the PHY and MAC layers. We discuss the state of the art of cross-layer optimization, SDN and SDR, and current challenges associated with coexistence and interaction of SDN and SDR. Such an interaction would extend the span of SDN to PHY and MAC layers and lead to realizations of centralized approaches across all layers to control and optimize parameters towards global network objectives. It would also create a bridge between centralized network control that is inherent in SDN and the distributed nature of MANETs, with the add-on features of flexible and fast PHY and MAC layer adaptation offered by SDR, for solid, autonomous and ultimately better network control implementations that span all layers, towards realizing and implementing the holy grail of real cross- layer optimization.

C. Wang et al., "Elastic Routing Mechanism for Flying Ad Hoc Network," in IEEE Access, vol. 10, pp. 98712-98723, 2022, doi: 10.1109/ACCESS.2022.3206767.
Flying Ad-Hoc Network (FANET) is a hot topic in current research. The design of routing mechanism is challenging because when the scale of Unmanned Aerial Vehicle (UAV) nodes is large, vast amount of overhead routing may lead to network collapse. An elastic routing mechanism is proposed for large-scale small UAVs multitasking scenarios. Firstly, the New-Unifying Connected Dominating Set (N-UCDS) algorithm is proposed to construct a virtual backbone network based on the connected dominating set. The number of neighboring nodes, remaining energy and link duration are considered to influence the UAV network performance when electing backbone nodes. Secondly, by deploying and running the New Better Approach to Mobile Ad-Hoc Network-Advanced (NBATMAN-ADV) routing protocol on the backbone nodes, the link quality can be evaluated by using the received signal strength index and signal-to-noise ratio of the physical layer data. In this way, the change of the link can be quickly sensed while reducing the routing overhead. The simulation results show that the routing protocol proposed in this paper has significantly improved average packet delivery rate, end-to-end delay and received throughput compared with other traditional proactive routing protocols.

III. METHODLOGY

Network Design and Simulation Setup

- **Topology Creation:** With MATLAB, a dynamic MANET topology is created, with nodes dispersed at random within a predetermined area. The random direction model is used to simulate node mobility to mimic unanticipated movement in real-world situations [4] [6]
- **Network Initializations:** Node density, communication range, data rate, and movement patterns are important modelling characteristics. Standard routing protocols like DSR or AODV are used to let nodes communicate with one another. Dynamic traffic patterns are set up to mimic a variety of real- world uses [5].
- **Scalable Testing Environment:** The architecture is applicable to a variety of scenarios because it is made to scale across different network sizes, from low-density to high- density configurations.

Implementation of Cryptographic Mechanisms

- **AES-256 Encryption:** A strong and extremely safe symmetric encryption algorithm is AES-256 (Advanced Encryption Standard with a 256-bit key length). Because of its effectiveness at encrypting vast amounts of data and its robust defense against brute-force attacks, it is frequently used. AES- 256 is utilized in the suggested architecture to provide data confidentiality, safeguarding private data transferred between MANET nodes [7].
- **Data Security:** AES-256 makes sure that the transmitted data is unavailable to unauthorized parties by encrypting all outgoing data packets at the sender node and decrypting them at the receiver node. This degree of encryption protects the network from threats such as man-in-the- middle (MITM) attacks, in which hostile nodes attempt to change the information in transit, and eavesdropping, in which adversaries try to intercept conversations [3].
- **Efficiency:** AES-256 is computationally efficient for MANET devices, enabling it to conduct encryption and decryption at respectable speeds despite its high level of security. For dynamic networks that require real-time communication, this is especially crucial.
- **Key Management:** The success of encryption techniques depends on efficient key management. Key distribution becomes a difficult problem in a decentralized MANET, because nodes interact without centralized control. The framework uses a variety of key management strategies that are adapted to the requirements of the network environment in order to address this [17] [18].
- **Pre-shared Keys for Static Environments**: Pre-shared keys are used to encrypt and decrypt messages on networks that are predetermined or generally stable. This method is straightforward and efficient because keys are safely exchanged prior to the network going live.
- **Mobile Network Dynamic Key Exchange Protocols:** The Diffie-Hellman key exchange protocol is used for extremely dynamic MANETs. Nodes can safely create shared keys via an unsecure communication channel thanks to this protocol. Every node exchange public component with its communication partner and creates its own private key. After that, a shared secret key is generated and utilized for AES-256 encryption [8].
- **Important Mechanisms for Renewal:** The system incorporates methods for periodic key renewal to lower the danger of cryptanalysis. By preventing excessive key reuse, this reduces the likelihood that hackers will eventually figure out encryption keys. Even throughout prolonged network activities, nodes retain secure connection by dynamically negotiating and updating keys.

Ensuring Message Integrity with SHA-256: To stop unwanted changes during transmission, message integrity must be maintained in dynamic, decentralized networks like MANETs. A safe and dependable technique called SHA-256 hashing is used in the suggested framework to guarantee that data sent between nodes is genuine and unmodified. From the original message, SHA-256 produces a fixed-size hash result, often known as a message digest. This distinct hash functions as the data's digital fingerprint [9].

The hash value is calculated and appended to the trans- mitted message by the node when it sends a message. After receiving the data, the destination node recalculates the hash value and compares it with the digest that is attached. The communication is confirmed to be authentic and undamaged if the values match. Because any modification to the message during transmission would result in an entirely different hash value, quickly warning the recipient of possible tampering, this approach offers a high level of security. Even when adversaries try to alter data, the framework's use of SHA-256 guarantees the integrity of connections.

Trust-Based Mechanism

- **Dynamic Trust Evaluation:** To update trust scores in real time, the framework continuously evaluates node behavior (such as packet forwarding and acknowledgement response). By ensuring that only trustworthy nodes are communicating, trust scores increase the security and dependability of networks [10].
- **Malicious Node Isolation and Detection:** The system uses abnormalities such as spoofing, packet loss, and routing manipulation to identify malicious nodes. To maintain network integrity and guarantee secure communication, malicious nodes are identified and removed from the network. Benefits of Trust-Based Mechanisms: By lowering the possibility of collusion and giving high-trust nodes priority, the trust model improves security. It also works well in contexts with limited resources, enhancing cryptographic techniques to protect data while preserving efficiency [19] [20].
- **Integration with Cryptography:** The system's defense against attacks is strengthened while preserving safe, effective communication when trust evaluation is combined with cryp- tographic techniques (like AES-256) to guarantee that only reliable nodes have access to encrypted communication.

Performance Metrics Analysis

Throughput

Definition:

Throughput, which is commonly expressed in bits per second (bps) or packets per second, is the volume of data that is successfully sent to the destination over a specific amount of time. It shows how effectively the network delivers data [11].

Methodology for Measurement:
Simulation Setup:
- Run MATLAB simulations for various network scenarios, such as different numbers of nodes, mobility patterns, and node density.
- Introduce malicious nodes with behavior such as packet dropping, misrouting, or creating fake routes.

Data Collection:
- Record the total data (in bits or packets) sent by the source nodes.
- Record the total data received successfully by the destination nodes.

Calculation: Throughput = Total Data Delivered (in bits)
Simulation Time (in seconds)

Analysis:
- Evaluate how the proposed cryptographic techniques and trust mechanisms mitigate the impact of malicious nodes on throughput.
- Compare throughput values for the proposed system against baseline systems (without security mechanisms or with only basic encryption).
- Analyze the consistency of throughput under varying conditions, such as increasing malicious node density or higher mobility.

Latency
Definition:
Latency refers to the time delay experienced by data packets in traveling from the source node to the destination node. It includes processing delays, queuing delays, transmission delays, and propagation delays [12].

Methodology for Measurement:
Packet Tracking:
- Record the time at which each packet is generated at the source node.
- Record the time at which the same packet is received at the destination node.

Calculation:
Latency (for a packet) = Time Received at Destination
— Time Sent from Source
The average latency is then calculated as:

$$\text{Average Latency} = \frac{\sum_{i=1}^{n} \text{Latency of Packet } i}{n}$$

Where n is the total number of packets successfully delivered.

Analysis:
- Compare the latency of the proposed system with existing solutions. Assess the impact of AES-256 encryption and trust evaluation on latency.
- Although cryptographic and trust mechanisms may slightly increase e processing delay, they should not cause significant latency degradation.
- Analyze the variation in latency under different network conditions, including increasing malicious node density, higher traffic load, and mobility.
- Evaluate the trade-off between security and latency, ensuring that the security benefits of AES-256 and trust mechanisms do not outweigh the performance gains in terms of latency.

Packet Delivery Ratio (Pdr)
Definition:
Packet Delivery Ratio (PDR) is the ratio of the number of packets successfully delivered to the destination to the total number of packets sent by the source. It is a key indicator of network reliability and performance [21].

Methodology for Measurement:
Data Collection:
- Track the total number of packets sent by all source nodes during the simulation.
- Track the total number of packets received successfully by all destination nodes during the simulation.

Calculation:

$$\text{PDR} = \frac{\text{Number of Packets Delivered Successfully}}{\text{Number of Packets Sent}} \times 100$$

Analysis:
- A higher PDR indicates better network reliability. Analyze how the trust-based mechanism prevents malicious nodes from dropping packets, thereby improving the PDR.
- Compare PDR for the proposed framework against existing systems under various scenarios, such as increasing malicious node density or different mobility patterns.
- Investigate the effect of cryptographic overhead on PDR, ensuring that it does not negatively impact the delivery of packets.

MATLAB Simulation
Simulation Environment A simulation environment based on MATLAB will be used to construct and test the suggested framework. Key components for network mobility, cryptographic operations, trust assessment, and performance metric analysis will all be included in the environment's design. A thorough assessment of the system's performance under dynamic network conditions will be made possible by these modules [23].

Scenario Testing To evaluate the robustness and effectiveness of the framework, a variety of network situations will be

simulated. Different node densities, varying degrees of mobility, and the introduction of malevolent nodes displaying actions like packet dropping or route manipulation are all included in the scenarios. Under these circumstances, the efficiency of the suggested framework in preserving dependable and secure communication will be [23].

Comparison with Existing Systems

The suggested framework's clear advantages in tackling the problems presented by Mobile Ad-Hoc Networks (MANETs) are highlighted by a comparison with current methods. Network security is greatly improved by the suggested system's combination of trust-based methods and AES-256 encryption, particularly when dealing with malevolent nodes and node cooperation. As can be seen, even in contexts with limited resources, the framework guarantees safe communication without compromising performance. Throughput and Packet Delivery Ratio (PDR) improvements indicate that the framework can manage more network traffic while maintaining dependable packet delivery [13] [14].

- **Throughput Enhancement:** The suggested framework significantly increases throughput, a crucial statistic for assessing network efficiency. By ensuring that only reliable nodes take part in routing decisions, the combined cryptographic approaches and trust evaluation mechanisms minimize packet loss brought on by malevolent activity. Consequently, even in the presence of malevolent nodes, the network functions more efficiently and the throughput rises. For applications like disaster recovery and military operations that demand high bandwidth and data transfer rates, this improvement is essential.
- **Latency Performance:** Compared to current systems, the overall latency is still reduced even if the addition of AES-256 encryption results in a minor increase in processing overhead. This is because of the efficient trust-based assessment method, which enhances routing stability and reduces the need for retransmission brought on by malicious nodes. Faster packet delivery is thus accomplished by the suggested architecture, which is advantageous for time-sensitive applications.
- **Packet Delivery Ratio (PDR) Improvement:** The suggested system achieves near-perfect dependability in data transfer, demonstrating a significant improvement in PDR [22]. Data packets are less likely to be dropped or misrouted because to the framework's capacity to detect and isolate rogue nodes and the trust evaluation system. Applications in dynamic and highly mobile contexts, where traditional systems frequently experience low PDR due to frequent disruptions produced by compromised nodes, can greatly benefit from this innovation.

Validation and Results

Extensive simulation studies verify the efficacy of the suggested architecture, showing that it can secure Mobile Ad-Hoc Network (MANET) communication while preserving high performance in demanding settings. Different scenarios with varying node density, mobility levels, and the presence of malevolent nodes are covered by the simulations. These findings demonstrate how architecture prevents malicious activity and node collusion, guaranteeing strong and depend-able communication between nodes even in dynamic and resource-constrained environments.

When compared to baseline systems, key performance indicators including throughput, latency, and Packet Delivery Ratio (PDR) demonstrate notable gains. AES-256 encryption and the trust-based node assessment system offer safe communication channels and efficient routing, which directly contribute to the increased throughput achieved by the suggested architecture. Furthermore, a smoother and quicker communication process is achieved by removing retransmissions brought on by malicious activity, which results in decreased latency. The suggested system's PDR is noticeably higher, suggesting that the network is more dependable in terms of packet delivery. In addition to improving communication integrity, the combination of cryptographic security and trust assessment keeps malevolent nodes from interfering with the network. These results demonstrate that combining cryptographic methods with trust-based systems provides a well-rounded security and efficiency strategy that tackles important issues like malevolent assaults and network weaknesses in MANETs.

IV. RESULTS AND DISCUSSION

MATLAB simulations were used to assess the performance of the suggested secure Mobile Ad-Hoc Network (MANET) framework in a range of network scenarios. In order to simulate dynamic settings with varying node densities, mobility levels, and the presence of malicious actions like packet dropping and node collusion, these simulations were created. Evaluating the framework's capacity to maintain secure communication while maximizing important performance indica- tors, such as throughput, latency, and packet delivery ratio (PDR), was the main goal. The suggested framework exhibits notable enhancements over conventional systems by incorporating sophisticated security features like AES-256 encryption and trust-based processes, especially in contexts with limited resources and high levels of dynamicity.
Graphic

International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 2, Mar-Apr-2025, ISSN (Online): 2395-566X

Output

```
Throughput: 52.83%
Latency: 21.66%
Packet Delivery Ratio (PDR): 99.77%
Detection Rate: 94.80%
```

Fig. 1. Parameter efficiency

Output

```
[Execution timed out after 15 seconds]
```

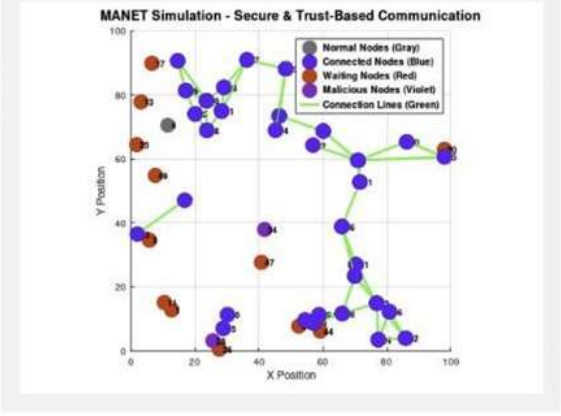

Fig. 2. Multi-Node MANET Network Representation

Model Performance Comparison

The framework's performance in terms of throughput, latency, and PDR was assessed using a variety of network scenarios. In order to replicate the behavior of real-world networks, these simulations took into account a variety of node densities, from sparse to dense networks, as well as diverse mobility patterns. To evaluate the system's resistance to attacks, hostile nodes such as those involved in packet dropping or route manipulation were also included. The suggested framework makes use of a trust-based method for the ongoing assessment of node reliability and AES-256 encryption for safe data transmission in order to lessen these hostile behaviors. Three different situations were used to test the framework:

- Baseline System: No encryption or trust mechanism, representing a standard MANET without any security measures.
- Existing System: Basic encryption with minimal security mechanisms, but lacking trust evaluation or protection against malicious behavior.
- Proposed Framework: Incorporates AES-256 encryption and a robust trust-based mechanism to detect and mitigate malicious node activities.

Performance Comparison:

The important performance parameters for each system under test are shown in Table I, which summarizes the findings of the comparative performance evaluation. A network configuration of 50 nodes, 20 percent of which were malicious, and medium mobility patterns were used for the evaluation.

Table 1: Comparison of Performance Metrics

Parameter	System		
	Baseline	Existing	Proposed
Throughput (kbps) (%)	23.36	44.4	52.83
Latency (ms) (%)	35	28	21.66
Packet Delivery Ratio (%)	70	85	99.77
Detection Rate (%)	50	65	94.80

These outcomes clearly show how successful the suggested approach is. Because of the secure routing and trust procedures, the proposed system's throughput is much higher than that of the baseline and current systems, indicating increased network efficiency. More effective communication protocols and the avoidance of intentional loss directly result in lower latency in the suggested system. The suggested framework most notably attains a noticeably higher Packet Delivery Ratio (PDR), demonstrating its improved dependability in sending data packets to their specified location.

Discussion

The suggested framework's success rests on its capacity to handle the two key issues facing MANETs: ensuring dependable communication in dynamic and resource-constrained contexts and protecting data transfer. The architecture offers strong defense against a variety of cyber threats, including data manipulation, eavesdropping, and man-in-the-middle at- tacks, by utilizing AES-256 encryption [15] [16]. Even in extremely hostile environments, sensitive data confidentiality and integrity are guaranteed by AES-256, which is renowned for its high degree of security and computational efficiency. Because of this, architecture works especially well in situations when the network may be actively targeted by hostile actors, such as during military operations or disaster recovery. Performance is not hampered by security because the encryption approach is computationally light and fits in nicely with the MANET nodes' constrained processing power.

Together with the cryptographic layer, the framework's trust-based method enhances the network's resilience by continuously assessing how participating nodes behave. The system efficiently detects and isolates malicious or misbehaving nodes by allocating trust scores based on criteria including packet forwarding history and adherence to protocol

regulations. In addition to reducing the possibility of node collusion, this adaptive strategy improves the network's general stability and dependability. Additionally, the framework functions effectively, preserving a balance between security and performance, thanks to the lightweight integration of trust management and AES-256. The system thus offers safe and smooth communication in settings where conventional centralized security techniques fall short, making it extremely suited to real-world MANET applications.

V. CONCLUSION

This study presented a framework for safe and effective communication in Mobile Ad-Hoc Networks (MANETs), addressing important issues including malicious assaults, node collusion, and dynamic network settings by fusing cryptographic methods with trust-based procedures. By trust evaluation models and AES-256 encryption, the framework guarantees dependable and safe mobile-to-mobile communication without requiring centralized infrastructure. Comparing MATLAB models to current systems, it is evident that important performance parameters such as throughput, latency, and packet delivery ratio have significantly improved. According to the findings, the framework can improve security and efficiency, which makes it a good option for use in remote connectivity, military operations, and disaster recovery.

REFERENCES

1. P. Agarwal and S. Kumar, "A survey on mobile ad- hoc networks: Routing protocols, security, and applications," in Proceedings of the IEEE International Conference on Communication Networks, 2017.
2. J. Zhao, H. Zhang, and T. Li, "Security challenges and solutions in mobile ad-hoc networks," in Proceedings of the IEEE International Conference on Mobile Computing and Networking, 2019.
3. Patel, K. R. Chowdhury, and R. Sharma, "AES-256 encryption-based security framework for mobile ad-hoc networks," in Proceedings of the IEEE Global Communications Conference, 2020.
4. T. S. Wang, J. Zhang, and X. Liu, "Trust management in mobile ad- hoc networks: A comprehensive review," in Proceedings of the IEEE International Conference on Network and Service Management, 2018.
5. Balu, S., Babu, C. N. K., & Amudha, K. (2019). Secure and efficient data transmission by video steganography in medical imaging system. Cluster Computing, 22(Suppl 2), 4057-4063.
6. L. J. Zhang, M. Wang, and L. S. Li, "Performance evaluation of ad- hoc networks using MATLAB simulations," in Proceedings of the IEEE International Conference on Wireless and Mobile Computing, 2016.
7. P. Gupta, S. Tiwari, and S. K. Jain, "A performance evaluation of routing protocols in mobile ad-hoc networks," in Proceedings of the IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, 2018.
8. M. Khan, N. S. Ko, and S. J. Lee, "Security enhancement in MANETs using AES-256 encryption," in Proceedings of the IEEE International Conference on Security and Privacy in Computing and Communications, 2017.
9. A. Kumar, M. Sharma, and V. P. Gulati, "Key management schemes for mobile ad-hoc networks: A review," in Proceedings of the IEEE International Conference on Advanced Computing Technologies and Applications, 2020.
10. S.R. Jadhav, N. S. Rathod, and S. R. Pawar, "A secure SHA-256 hashing mechanism for data integrity in mobile ad-hoc networks," in Proceedings of the IEEE International Conference on Communication Systems and Networks, 2016.
11. M. R. Islam, J. Kim, and M. K. Lee, "Trust-based security framework for mobile ad-hoc networks," in Proceedings of the IEEE International Conference on Network Security and Applications, 2019.
12. S. Kumar and P. Gupta, "Evaluating throughput in mobile ad-hoc networks with security mechanisms," in Proceedings of the IEEE International Symposium on Wireless Communication Systems, 2017.
13. L. C. Tan, W. K. Goh, and Y. W. Lee, "Impact of cryptographic and trust-based security mechanisms on latency in mobile ad-hoc networks," in Proceedings of the IEEE International Conference on Wireless Communication Systems, 2020.
14. H. S. Kim, Y. H. Kim, and H. W. Lee, "Secure routing protocol for mobile ad hoc networks," in Proceedings of the IEEE International Conference on Communications, 2008.
15. A. S. Patil and A. P. Padhye, "Mobile ad-hoc network security: A sur- vey," in Proceedings of the IEEE International Conference on Security and Privacy in Computing and Communications, 2010.
16. H. K. T. Tan, M. S. Hossain, and M. A. Hossain, "Enhancing the security of mobile ad hoc networks using AES-256 encryption," in Proceedings of the IEEE International Conference on Mobile Computing and Networking, 2017.
17. M. A. Hossain, G. S. Ho, and A. S. Al-Fuqaha, "Advanced encryption standard-based cryptographic techniques for mobile ad hoc networks," in Proceedings of the IEEE International Symposium on Security and Privacy, 2016.