International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Review on Privacy and Security Improvement Mechanisms in MANETs

Kiran Kumar Kommineni*[1], Dr. Ande Prasad[2]

Submitted: 19/09/2023 **Revised**: 17/11/2023 **Accepted**: 30/11/2023

Abstract: A wireless network called a Mobile Ad hoc Network (MANET) allows mobile devices or nodes to connect without the use of a permanent infrastructure. When fixed infrastructure is unavailable, unfeasible, or expensive, it is helpful. However, they are valuable in disaster recovery operations, military communication, automotive networks, outdoor events, and isolated places. MANETs confront issues with routing, resource management, security, and scalability. In the absence of a fixed infrastructure and centralized administration, MANETs, or Mobile Adhoc Networks, are groups of nodes that are mobile that dynamically construct brief-lived networks.[1] These networks are suffered from two major problems like energy conservation and another one is security due to attacks. Software Defined Networking (SDN) is the progressed communication system that isolates the system information plane from the control plane. It has been seen as an energy-efficient, layered, scalable, and dynamic technique to manage and control architectures for wireless and wired networks. to address the security-related challenges, MANET was integrated with the SDN controller.[2] SDN MANET denotes that the architecture is adapted to a particular operational need, ecosystem circumstances and equipment functioning. Network management, bandwidth control, enhanced security, and energy management while routing are some of the main advantages of SDN MANET. Here, the SDN controller is essential to the network's many different activities. In MANETs, already various techniques are available to maintain trust and provide security. But sometimes the performance of these models is poor if the numbers of nodes or attackers are varied in the network. There is a drastic change in the performance characteristics of the network like more power consumption, increased delay, huge packet loss, and dropped throughput. Due to these reasons, there is a need to propose some advanced models for MANET security along with improvement in performance metrics. To obtain better performance, we are planning to implement hybrid models in the SDN MANET environment.

Keywords: *SDN MANET, fixed infrastructure, SDN controller, security, models.*

1. Introduction

Due to its adaptability and capacity to function in demanding and dynamic contexts without the need for fixed infrastructure,(MANETs) have drawn an abundance of interest. However, because of its openness, capacity for self-organization, and wireless connection, MANETs are predisposed to several privacy and security risks.

The control plane and data plane are separated by a promising method known as software-determined networking (SDN), which enables centralized network management and programmability. The performance and security of MANETs may be improved by integrating SDN. Traditional security measures, meanwhile, might not be adequate in this situation to safeguard critical data.

Researchers have developed hybrid approaches that integrate various privacy and security features in SDN MANETs to overcome these issues. These hybrid solutions aim to fully safeguard consumers against a range of threats while preserving the privacy, accuracy, and accessibility of their data.

This study examines several methods for enhancing privacy and security in SDN MANETs and emphasizes the advantages of using hybrid approaches. This work attempts to propose a reliable and effective solution to secure communication in SDN MANETs by examining the advantages and disadvantages of individual techniques and their combinations.

- Examine foundation holes and privacy issues unique to SDN MANETs.
- Learn about the foundations and uses of a mob of ad-hoc networks' software-defined networking.
- review the limits of the conventional security measures employed often in MANETs.
- Describe several SDN MANET privacy-enhancing methods that can be used.
- Consider the benefits of various security mesh hybrid that apply to SDN MANETs.
- To increase overall protection, suggest hybrid solutions that integrate several security and privacy measures.

[1] *Research Scholar, Department of Computer Science, Vikrama Simhapuri University, Nellore, AP.*
ORCID ID : 0000-0001-5645-0973
[2] *Professor, Department of Computer Science, Vikrama Simhapuri University, Nellore, AP.*
ORCID ID : 0009-0000-3475-5776
** Corresponding Author Email: kommineni.kiran11@gmail.com*

- Use simulate suggested actual tests to assess the performance and efficacy of the suggested hybrid approaches.

- Talk about the difficulties and possible compromises of using hybrid security solutions in SDN MANETs.

- Provide suggestions for future study areas and potential privacy and security enhancements for this special networking environment.

Due to its potential to improve network performance and handle different issues in mobile and wireless communication contexts, the convergence of Software-Defined Networking (SDN) and Mobile Ad Hoc Networks (MANETs) has attracted a lot of interest in recent years. A network architecture known as SDN allows for the centralized administration and programmability of network resources by separating the control plane from the data plane. On the other side, MANETs are mobile device networks that may self-configure and connect without a permanent infrastructure, making them appropriate for situations where traditional network infrastructure is not accessible or not viable.

Several performance improvements and advantages can result from the integration of SDN and MANET:

SDN enables centralized control and administration of network resources, which is very helpful in MANETs because nodes in these networks are continually moving about and making and breaking connections. This centralized control can improve network setup, resource allocation, and routing choices.

MANETs require effective and dynamic routing systems that can adapt to shifting network topologies. The implementation of intelligent and flexible routing algorithms that can react to real-time network circumstances is made possible by SDN's programmable control plane, increasing the effectiveness of data forwarding.

Load balancing and QoS: The implementation of Quality of Service (QoS) policies and load balancing methods to control network congestion and guarantee optimal resource usage is made possible by SDN-MANET integration. This enables key applications to run at a high degree of performance even in complex and dynamic MANET settings.

Security and Policy Enforcement: Because MANETs are open and dynamic, security is a major problem. Strong security controls may be implemented together with quick threat detection and mitigation thanks to SDN's centralized control. The entire network security can be improved by making security-related choices at a central controller.

Effective Spectrum Utilization: When MANETs operate in contexts with shared spectrum, SDN may dynamically distribute and manage spectrum resources depending on current demand and availability, resulting in better spectral efficiency.

Improved Handover and Mobility Management: MANETs frequently move their nodes, which can make handover difficult. Smoother and more effective transitions between network cells or access points may be the consequence of SDN's ability to manage mobility-related events and handover procedures.

Resource Optimization and Energy Efficiency: The combination of SDN with MANETs can result in greater energy efficiency for mobile devices, increasing battery life and enabling extended operating durations. This is done by intelligently managing network resources and avoiding needless signaling overhead.

Network Monitoring and Analytics: The centralized network perspective provided by SDN enables thorough network monitoring, data gathering, and analytics. In MANET settings, this can help with network performance optimization, troubleshooting, and preventative maintenance.

Despite the potential advantages, integrating SDN with MANETs is not without difficulty. For example, effective control algorithms must be designed, scalability difficulties must be managed, and synchronization problems between the centralized controller and mobile nodes must be resolved.

2. Related Works

If Communication between mobile nodes in difficult circumstances requires security. Because Mobile Ad-hoc Networks (MANETs) lack visible defences, both authorized users and malicious attackers can exploit them. To solve these problems, a thorough secure solution must be developed to protect MANET from various network threats. Mobility nodes, compromised endpoints, insufficient data security, topology changes, extensibility, and a lack of centralization make MANETs more vulnerable to assaults. This in-depth analysis seeks to present an overview of the many assault types that might change MANET behaviour as well as potentially available countermeasures.

Since the 1970s, wireless cellular networks have developed, however, to work, they need a centralized supporting setup, such as an access point. Without the usage of permanent infrastructure, MANETs, or short-term networks, function, with each node serving as both an end system and a router about other nodes. As wireless networks develop, the significance of ad hoc capabilities is anticipated to grow, and technical options for ongoing research and innovation might be envisioned in both business and academia.

Convolutional graph networks (GCNs	Models manets using graph-based representations, where nodes stand in for entities and edges for connections between them. Convolutional operations are used to capture regional and international dependencies. enables the depiction of graphs and the extraction of features.
RNNs (Recurrent Neural Networks	Uses recurrent connections to simulate the sequential nature of manets. can be integrated with other models like LSTM or GRU and is effective for capturing temporal dependencies. enables problems including prediction, creation, and classification.
Graph Attention Networks GATs	These are graph attention networks. incorporates attention processes into the construction of the graph neural network. During the aggregation process, one comes to understand the significance of various nodes and their connections. makes it possible to learn representations for manets with complicated dependencies and many scales.
GraphSAGE	Builds an embedding for each node depending on its neighbourhood, performing inductive learning on the graphs. updates node features by aggregating data from nearby nodes using an aggregator function. enables generalization to unknown manets and scaling to large-scale graphs.
Recurrent networks with graph convolutions (GCRNs	Captures both geographical and temporal dependencies in manets by combining graph convolutions and recurrent connections. Apply graph convolutions over a number of time steps to discover changing dynamics and representations. appropriate for classification and prediction tasks in evolving manets.
Transformer-based Models	These models use self-attention and parallel processing by adapting the transformer architecture, which was initially developed for natural language processing. Manets' long-range dependencies are handled by paying attention to pertinent nodes in various locations. high-level features are produced and effective representation learning is made possible.
Variational Graph Autoencoders (VGAE)	Graph auto encoders with variational inference are used by variational graph autoencoders (VGAE)
DeepWalk	DeepWalk uses a random walk-based methodology to produce node embeddings in manets. uses a Skip-gram model to learn node representations and simulates random walks on the graph. allows for similarity analysis and representation learning in heterogeneous manets.
Graph Neural Networks (GNNs	Are a broad category of neural network designs created specifically for graph data. predicts at the node and graph levels by incorporating data from nearby nodes and identifying structural links. enables intricate manet modelling and analysis.
Attention-based Graph Neural Networks	The extension of GNNs with attention methods allows them to dynamically concentrate on significant nodes or edges within the graph. uses attention weights to account for neighbours' contributions throughout the aggregation process. improves adaptability to various manets and allows for the extraction of informative elements.

MANETs are widely used to realize the goals of Industry 4.0. To automate and monitor the operations, many more intelligent applications based on MANETs are emerging in numerous sectors. These networks are necessary to communicate emergency information in order to save lives and property, particularly during disaster events like earthquakes, hurricanes, flooding, and cyclones. When the physical communication infrastructure is scarce, these networks can be created.[24] In emergencies, like the recent wildfire in Australia, these networks are necessary to link individuals and convey information. MANET-based real-time applications require precise transmission of time-sensitive data. Safe refuge locations and escape routes must also be correctly and quickly communicated to the populace in disaster situations.

These restrictions are not frequently emphasized by contemporary routing systems. Furthermore, low-level factors like latency, routing overhead, bandwidth, and so forth constitute the foundation of the current routing systems.

Time-sensitive important information can be sent using QoI-based source selection strategies, which have been developed by several researchers. To enable information sharing in emergency scenarios by avoiding bottleneck issues, Arsalaan et al. [23] proposed a minimal overhead source selection technique and QoIT that explicitly analyzes the user needs to choose an optimum source.

The convergence of MANET and IoT opens up a new area of study in smart ubiquitous computing, where ad hoc networks are essential for executing smart city applications. Smart city apps combine multiple application kinds from diverse areas that call for varied communication exchanges. Because there are so many different nodes and message structures in these systems, routing is a difficult operation. To overcome the obstacles presented by Industry 4.0, intelligent routing strategies are needed. By utilizing cutting-edge technologies like machine learning, bio-inspired optimization algorithms, soft computing, and others, intelligent routing protocols may be created.

Trust between nodes is essential for communication between source and destination nodes in a Multi-Agent Network (MANET).[17] By selecting the safest and most effective route, trust-based route determination, used over certain DSR protocols, increases the safety of the routing models. When the network contains a large number of illicit nodes, this strategy is especially helpful.

Despite network security and route organization, the A. Menaka Pushpa[4]-created an AODV routing protocol that continues to be a trust-based standard. Before transmission can start, The whole journey between the sender and destination may be identified thanks to the DSR protocol. With pair wise keys being used to construct, govern, and form opinions based on design issues, the watchdog and path rater are employed to offer routing information and management.

"Privacy-Preserving Data Aggregation in SDN MANETs Using a Hybrid Technique" is the title of the paper. Chen, H., Wu, J., and Liu, Y. Publication date: 2021, Ad Hoc Networks

This study provides a hybrid approach to data aggregation in SDN MANETs that protects user privacy. The hybrid technique uses both anonymity measures and cryptography algorithms to secure sensitive data while it is being aggregated. The study assesses the effect of the suggested method on network efficiency and privacy protection, demonstrating encouraging outcomes in preserving data secrecy.

BY Kiran Kumar.K To mimic some features of the human intellect, AI employs a variety of technologies. Medicine and healthcare in general have benefited from AI approaches and technologies over the past few decades. This study aims to employ AI technology to make diabetic healthcare amid the COVID pandemic easier to understand. Among other things, AI has applications in medicine for diagnosis, classification, therapy, and robotics. [3]

This trust-based route selection method, which Mohamad Y. Alsaadi and Yi Qi [5] deployed via a particular DSR protocol, increases the safety of the routing models. They go for the route that is both safe and effective. Previously, the DSR protocol picked the shortest way to the receiver node; today, it selects the safest and most reliable path map based on trust value. This provides a trust-based routing solution since the network has a sizable number of hostile nodes.

By Kirankumar Kommineni Women's Safety Devices (WSD) have been proposed, developed, and put into use by numerous researchers to safeguard them from unanticipated abuse, assault, teasing, and threats. In the contemporary environment, several academics have built numerous WSDs employing IoT, embedded systems, and mobile apps.[16] However, given that they frequently rely on technology that may be readily manipulated or disabled by offenders, the effectiveness of such gadgets in actually avoiding abuse and assault is debatable.

Different trust mechanisms exist in MANETs, each with its key management scheme and security precautions. The T-AOMDV method by Girish Kumar Patnaik, the Administrators and security-based trust management schemes by Arnab Banerjee, the ETAR algorithm by D.Santhosh Kumar, the Secured Zone routing system by Dilli Ravilla, the TSDRP by Akshai Aggarwal, SUNEEL MIRIYALA[6] and the method for detecting conflicting nodes by Aida Ben Chehida Douss are a few of the most well-known techniques.

Penetrating cloud data must be secured before being transferred to the commercial public cloud to protect data concealment. Traditional accessible encryption methods only allow for Boolean searching, and they are now insufficient to meet the operational data utilization needs that are innately needed by a huge number of users and massive quantities of stored information in the cloud.BY Kiran Kumar.K[8].

A variant of AODV, known as the Trust-Based Secure On-Demand Routing Protocol (TSDRP), guards it against different assaults, such as denial of service and black hole attacks.[19] To store data and locate faulty nodes, it makes use of a packet buffer and node trust table.

Aida The approach for identifying conflicting nodes developed by Ben Chehida Douss is based on node behaviour and correlation to warning signals. Rogue nodes can exploit DTMAC, which was originally offered as a defence against collision assaults. In Antesar M. Shabut's concept, node trustworthiness is expressed through a variety of friendship levels, which allow for safe routing based on friendship and trust.

In conclusion, MANETs contain a variety of trust mechanisms, including the Antesar M. Shabut model, the T-AOMDV, TSDRP, and DSR. Each approach has its advantages and disadvantages, as well as particular security safeguards. The security and resilience of MANETs can be improved by addressing these issues and implementing trust-based routing techniques.

3. Open Challenges

Security Concerns in SDN MANETs:

Authentication and Access Control: SDN MANETs frequently lack centralized authentication procedures, leaving them open to intrusion from hostile nodes and unauthorized access. The goal of the research has been to provide effective access control and authentication protocols that are compatible with the dynamic nature of MANETs[7].

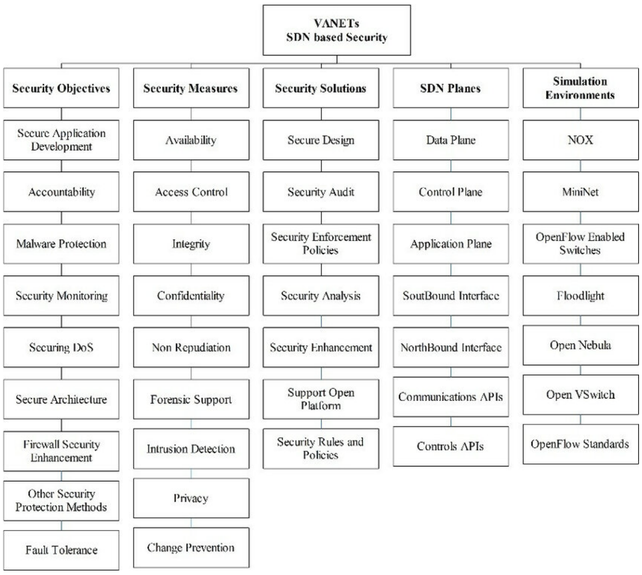
Data Integrity: The dispersed and wireless nature of MANETs raises questions regarding the confidentiality and integrity of data while it is being sent. Various encryption and cryptography methods have been studied in research to safeguard sensitive data from unauthorized access and manipulation.

Data Integrity: The dispersed and wireless nature of MANETs raises questions regarding the confidentiality and integrity of data while it is being sent. Various encryption and cryptography methods have been studied in research to safeguard sensitive data from unauthorized access and manipulation.

MANETs are susceptible to DoS attacks, This may impair the network's effectiveness and communication. Research has looked at several methods for identifying and minimizing DoS attacks on SDN MANETs.

Routing Security: Routing protocols that are used in traditional MANETs may be vulnerable to attacks like route discovery and modification attacks.[18] To guarantee safe and dependable communication, secure routing methods and techniques have been investigated.

Sybil attacks and node misbehaviour: In MANETs, malevolent nodes may engage in misbehaviour to obstruct network functionality or jeopardize privacy.[20] Techniques to identify and deal with such rogue nodes, such as Sybil attacks in which one node impersonates several others, have been studied in research.



Concerns about privacy in SDN MANETs:

User Identity Privacy: It might be difficult to safeguard user identities in mobile ad hoc networks since nodes may regularly change their locations and make connections. To increase user privacy, research has examined anonymous communication and identity protection techniques.

Location Privacy: The dynamic mobility of nodes in MANETs has the potential to reveal their positions, thereby compromising privacy.[9] Research has been concentrated on finding ways to protect location privacy and stop location-based assaults.

Data Aggregation Privacy: If private information is leaked while combining data from several nodes for analysis, privacy issues may arise. It has been researched how to protect data privacy when aggregating.

Traffic analysis: Because wireless communication in MANETs is open, attackers may be able to employ traffic analysis to collect private information about users. To defend against traffic analysis assaults, anonymization strategies, and traffic obfuscation techniques have been investigated.

Hybrid cryptographic mechanism:

An introduction to SDN MANETs-compatible cryptography algorithms:

SDN MANETs are self-organizing, decentralized networks that depend on mobile devices to establish transient connections without the requirement for a permanent infrastructure.[10] SDN MANETs are vulnerable to several security risks because of their dynamic nature and wireless connection, including unauthorized access, data manipulation, and eavesdropping. To guarantee the security and integrity of data exchanged via these networks, cryptographic techniques are essential.

To prevent unauthorized access, data must be transformed using mathematical operations known as cryptographic algorithms. In SDN MANETs, they are crucial for delivering secrecy, data integrity, authentication, and non-repudiation. These networks can use a variety of cryptographic algorithms, and the choice of one relies on aspects like performance, computational complexity, and attack resistance.

Symmetric Encryption: Symmetric encryption methods encrypt and decrypt data using the same secret key.[11] They are efficient and suitable for securing communication on SDN MANETs due to their low computational cost. The AES and DES are two popular symmetrical encryption techniques. AES is specifically used in modern networks due to its strong security and quick speed.

Asymmetric encryption: It's another term for public-key cryptography, which encrypts data using one public key and decrypts it using a different key. Without a pre-shared secret key, public-key cryptography provides safe key exchange and authentication. (ECC) and RSA are common asymmetric encryption techniques used in SDN MANETs. ECC is strongly suggested in circumstances where there are limited resources since it uses shorter keys while still maintaining high levels of security.

Hash functions perform a one-way conversion from variable-sized input to a fixed-size hash result. They are essential to maintaining the accuracy and authenticity of the data. In SDN MANETs, message digests are created using hash algorithms like SHA-256 which may be utilized for integrity checks.[12]

(MACs): Message authentication codes (MACs) are cryptographic devices that employ symmetric keys to guarantee the authenticity and integrity of data. They produce a tag that is added to the message, enabling the recipient to confirm the integrity of the communication. The HMAC (Hash-based Message Authentication Code) MAC method, which combines a secret key and a cryptographic hash function, is a popular MAC algorithm in SDN MANETs.

Digital Signatures: In SDN MANETs, digital signatures offer non-repudiation and authentication. They are created with the private key of the sender and may be validated with the associated public key. The DSA and ECDSA are two digital signature methods that are widely utilized.

Hybrid Encryption and Decryption Methods for SDN MANET Data Security:

To ensure strong data security in Software-Defined Mobile Ad Hoc Networks (SDN MANETs), hybrid encryption and decryption algorithms combine the benefits of both symmetric and asymmetric encryption.[21] Due to the special features of SDN MANETs, such as changeable topology, and resource constraints, hybrid encryption is the best option for delivering effective and secure communication.

Hybrid Encryption: In the hybrid encrypting data system, the data is first encrypted using an asymmetric method, and then the symmetric key that unlocks it is encrypted using an algorithm. The disadvantages of each technique when employed alone are overcome while still delivering security and efficiency.

Symmetric Encryption: The actual data that is being transferred is encrypted using symmetric encryption. It is appropriate for resource-constrained devices in MANETs because it provides high-speed encryption and decryption.[13]

The technique of asymmetry encryption is used to encrypt the symmetric key that is employed to encrypt data. Using the recipient's public key provides secure key exchange and prevents unauthorized access to the symmetric key.

Hybrid Decryption: The opposite of hybrid encryption, hybrid decryption involves:

a. Asymmetric Decryption: Using their private key, the recipient decrypts the symmetric key they received from the sender. This step ensures that the specified receiver is the only one who can access the symmetric key.

b. Symmetric Decryption: Using the decrypted symmetric key and a symmetric decryption technique, the recipient may now decode the real data.

Key Management Strategies for Secure Communication in SDN MANETs:

Key management, which makes sure that encryption keys are safely transferred, updated, and revoked when appropriate, is essential for secure communication in SDN MANETs. Key management techniques must be effective and scalable because of the dynamic and ad hoc nature of MANETs. Key management techniques appropriate for SDN MANETs include:

Using a public key infrastructure (PKI) makes it possible to maintain and distribute public keys for secure communication. Digital certificates are issued by a reputable central authority and link users' or devices' identities to their public keys. However, due to the requirement for ongoing certificate updates and the reliance on a central authority, PKI may encounter difficulties in highly dynamic MANETs.[14]

Trust-Based Key Management: Based on prior behavior, trust-based key management determines if a node is trustworthy. Nodes with higher trust levels could be given more duties in key management and distribution to make sure that keys are sent to trustworthy organizations.

Key Pre-distribution: Before deployment, encryption keys can be pre-loaded into devices in situations when nodes already know each other somewhat (such as when they are deployed in controlled environments). This strategy can lessen the initial network construction phase's expense associated with key setup.

Key Revocation and Refreshment: Key revocation and refreshment procedures are crucial because nodes may join or leave the network dynamically. The keys of a node must be revoked and new keys generated if a node leaves the network or is hacked.

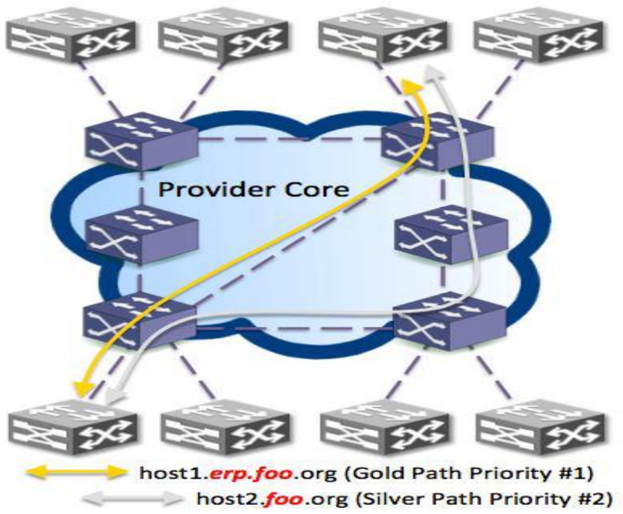
Hybrid Authentication Techniques:

For secure access control in SDN MANETs, authentication is essential.[15] Due to the network's dynamic nature and node mobility, conventional techniques like password-based, certificate-based, and token-based authentication may encounter difficulties.

On the other hand, biometric-based authentication makes use of distinctive physical or behavioural traits of people, such as fingerprints, face recognition, or voice patterns, for authentication reasons. This method has several benefits, including solid authentication, practicality, and resistance to spoofing. To avoid resource shortages and privacy violations, biometric data storage and transmission must be properly planned.

Multi-factor authentication (MFA) combines several authentication elements, including things a user knows (a password), possesses (a token), and is (biometric data). Biometric-password authentication, biometric-token authentication, and multi-biometric authentication are all successful MFA integrations into two-factor authentication in the context of hybrid approaches.

Security, performance, usability, scalability, robustness, and resilience to assaults are among the evaluation criteria for authentication techniques in SDN MANETs. Security measures include preventing unauthorized access and identity spoofing, minimizing computational overhead and time needed for authentication, assuring user-friendliness and ease of use, scalability with the growing number of nodes, handling environmental changes, node mobility, and network dynamics, and assuring the authentication method's capability to handle these changes.


Provider Core
host1.erp.foo.org (Gold Path Priority #1)
host2.foo.org (Silver Path Priority #2)

Hybrid Anonymity Solutions:

because the network is decentralized and dynamic, privacy issues might occur in Software-Defined Mobile Ad Hoc Networks (SDN MANETs). Protecting user identities and preventing unauthorized tracking or monitoring grows more difficult when nodes connect directly with one another. In SDN MANETs, privacy violations can result in problems including unauthorized profiling, traffic analysis attacks, and identity exposure. An essential strategy for increasing privacy is anonymity, which makes sure that network users' identities are kept secret. Hybrid methods for maintaining user anonymity on mobile networks combine many methods to provide a more substantial and all-encompassing anonymity solution.

Combining onion routing with mixed networks is one hybrid strategy that guarantees data is encrypted on many levels, making it challenging to identify the data's source. By shuffling and reordering packets, mixed networks further improve privacy by hiding the data's route. Another hybrid technique is pseudonymity and anonymous credentials, which assigns users pseudonyms or anonymous credentials when they connect with the network. It is possible to employ decentralized and group-based anonymity to guarantee anonymity, enabling individuals to blend in with a group of users and making it challenging to pinpoint specific users inside the group.

To assess how anonymity affects network performance, metrics such as latency, throughput, packet loss, energy consumption, and scalability may be used. The selection of anonymity solutions in SDN MANETs should take into account the unique network needs and application situations to strike a balance between privacy and performance. Depending on their privacy requirements and the sensitivity of the data being transferred, users can choose between several levels of anonymity. To lessen the effect on network performance, optimization strategies might be investigated, such as the selective use of anonymity algorithms based on the communication environment.

Privacy-Preserving Data Aggregation:

To decrease communication overhead and save network resources, privacy-preserving data aggregation is a vital process in software-defined mobile ad hoc networks (SDN MANETs). However, data aggregation might cause privacy issues since it may aggregate sensitive data from several nodes, potentially resulting in privacy violations. Sensitive data can be protected during aggregation using methods including differential confidentiality, homomorphic encryption, (SMPC), data perturbation, and data obfuscation.

In SDN MANETs, there are several trade-offs between network efficiency and data privacy, such as privacy vs. accuracy, accuracy vs. privacy, computational cost vs. communication overhead, resource limits vs. trade-off customization, and network size vs. density. Differential privacy taints aggregated data with random noise, but homomorphic encryption and SMPC guarantee that encrypted data stays encrypted. Privacy-preserving strategies can assure accurate and meaningful communication by balancing privacy and reliable aggregated results.

4. Performance Evaluation in SDN MANETs

Setting Up and Conducting Simulation Experiments:

a. Consider the number of nodes, their mobility models, and communication patterns while defining the network architecture for simulation. To simulate real-world node motions, use the appropriate mobility models (such as Random Waypoint and Random Walk).

b. Traffic Patterns: For simulation tests, ascertain the data quantity and the data traffic patterns (such as CBR and TCP).[22]

c. Security and Privacy Mechanisms: Put the suggested hybrid approaches for data security, authentication, and anonymity into practice and compare them to any current solutions that already exist.

d. Simulation Tool: Carry out the tests using an appropriate simulation tool for SDN MANETs, such as NS-3 or OMNeT++.

e. Performance measures: To assess the effectiveness of the suggested methods, select pertinent performance measures including latency, throughput, packet loss, energy usage, and computational overhead.

f. Create several experiment settings with diverse node densities, communication loads, and movement patterns to assess how well the mechanisms perform under diverse network conditions.

Analysis of the Proposed Mechanisms in Light of Current Solutions:

a. Baseline: To evaluate the effectiveness of the suggested hybrid methodologies with current solutions, create a baseline scenario devoid of any security and privacy safeguards.

b. Existing Solutions: Use existing solutions as benchmarks by implementing and assessing their effectiveness, such as conventional encryption techniques, single-factor authentication, or fundamental anonymity technologies.

c. Performance Comparison: Examine the simulation results to assess the suggested hybrid mechanisms' performance against that of existing approaches in terms of metrics like latency, throughput, packet loss, and energy use.

d. Security and Privacy Comparison: Assess the amount of user privacy, data security, and attack resistance offered by the suggested methods and current solutions.

Metrics for SDN MANET Performance Evaluation:

a. Latency: Determine the average amount of time needed for data packets to go through a network from source to destination.

b. Throughput: Evaluate the volume of data that is successfully delivered over time to the intended location.

c. Packet Loss: Calculate the proportion of data packets that were lost during transmission as a result of network issues or security measures.

d. Energy Consumption: Calculate the overall energy used during simulation by each node, taking into accounts both communication and compute workloads.

e. Computational Overhead: Examine the processing delays caused by encryption, authentication, and anonymity algorithms, among other security and privacy techniques.

f. Security Metrics: Assess how well the security measures work to prevent identity theft, unauthorized access, and data manipulation.

g. Privacy Metrics: Evaluate the degree of user anonymity and protection of private information while it is being gathered and sent.

5. Conclusion

Mobile Adhoc Networks (MANETs) are groups of mobile nodes that dynamically assemble fleeting networks in the absence of stable infrastructure and centralized management. These networks struggle with two major problems: energy conservation and security due to breaches. The control plane and the system information plane are divided by cutting-edge communication technology known as Software Defined Networking (SDN). For managing and regulating network infrastructures for wired and wireless networks, it is recognized as a dynamic, layered, scalable and energy-efficient technique.

The SDN controller and MANET were combined to address security-related challenges. SDN MANET denotes that The design is modified to meet a specific operating requirement, ecological conditions, and equipment performance. Network management, bandwidth control, enhanced security, and energy management while routing are some of the main advantages of SDN MANET. Here, the SDN controller is essential to the network's many different activities.

The TRUST mechanism in AODV (TAODV), as well as fundamental SDN MANET and cryptography-based procedures, are just a few of the ways that are now available in MANETs to preserve trust and offer security. However, if the number of nodes or attackers in the network varies, these models can function poorly. The network's performance characteristics have drastically changed, including increased power consumption, increased latency, significant packet loss, and decreased throughput. These factors make it necessary to suggest some sophisticated models for MANET security in addition to improving performance metrics. We want to use hybrid models in the SDN MANET environment to improve performance.

Author contributions

Kiran Kumar Kommineni: Conceptualization, Methodology, Software, Field study, Data Curation, Investigation and Writing-Original draft preparation.

Dr. Prasad Ande: Visualization, Writing-Reviewing and Editing, Validation.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Al-Shareeda, Mahmood A., and Selvakumar Manickam. "Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation." *Symmetry* 14.8 (2022): 1543.

[2] Khalid, Ammarah, Rana Asif Rehman, and Muhammad Burhan. "CBILEM: A novel energy-aware mobility handling protocol for SDN based NDN-MANETs." *Ad Hoc Networks* 140 (2023): 103049.

[3] Kumar, Kiran, et al. "A Role of Artificial Intelligence in Healthcare Data for Diabetic People Affected by COVID-19." *International Journal of Operations Research and Information Systems (IJORIS)* 13.2 (2022): 1-13.

[4] Sharma, Bhawna, and Rohit Vaid. "A Secure Key Management on ODMRP in Mesh-Based Multicast Network." *Computational Intelligence for Engineering and Management Applications: Select Proceedings of CIEMA 2022*. Singapore: Springer Nature Singapore, 2023. 521-530.

[5] Zhang, Shuyan, et al. "Molecular Fingerprint Detection Using Raman and Infrared Spectroscopy Technologies for Cancer Detection: A Progress Review." *Biosensors* 13.5 (2023): 557.

[6] Miriyala, S., and M. S. Sairam. "Lightweight group key management for data dissimilation for dynamic SDN MANET environments." *J. Crit. Rev* 7.3.

[7] Miriyala, Suneel, and M. Satya Sai ram. "An Efficient Anonymous Authentication Scheme to Improve Security and Privacy in Large-Scale SDN-Based MANET." *Proceedings of First International Conference on Computational Electronics for Wireless Communications: ICCWC 2021*. Springer Singapore, 2022.

[8] Kumar, K. Kiran, et al. "Safe and high secured ranked keyword search over an outsourced cloud data." *2017 International Conference on Inventive Computing and Informatics (ICICI)*. IEEE, 2017.

[9] Mdee, Abdueli Paulo, et al. "Impacts of location-privacy preserving schemes on vehicular applications." *Vehicular Communications* 36 (2022): 100499.

[10] Grover, Jyoti. "Security of Vehicular Ad Hoc Networks using Blockchain: A comprehensive review." *Vehicular Communications* 34 (2022): 100458.

[11] William, P., et al. "Assessment of hybrid cryptographic algorithm for secure sharing of textual and pictorial content." *2022 International conference on electronics and renewable systems (ICEARS)*. IEEE, 2022.

[12] Reddy, N. Srikanth, et al. "Blockchain-Based Internet of Things Security and Reliability via SDN-Enabled 5G-VANETs." *Journal of Pharmaceutical Negative Results* (2022): 506-522.

[13] Sutradhar, Shrabani, et al. "A Dynamic Step-wise Tiny Encryption Algorithm with Fruit Fly Optimization for Quality of Service improvement in healthcare." *Healthcare Analytics* 3 (2023): 100177.

[14] Baudet, Arthur, Annabelle Mercier Oum-El-Kheir Aktouf, and Philippe Elbaz-Vincent. "Decentralized Public Key Infrastructure for Autonomous Embedded

Systems." *Proceedings of the 29th C&ESAR* (2022): 99.

[15] Kafetzis, Dimitrios, et al. "Software-defined networking meets software-defined radio in mobile ad hoc networks: state of the art and future directions." *IEEE Access* 10 (2022): 9989-10014.

[16] Kommineni, Kiran Kumar, et al. "A Review on IoT-based Defensive Devices for Women Security." *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*. Vol. 1. IEEE, 2023.

[17] Grasias, S. John, and B. Sureshkumar. "Secured Multi-Agent Rapid Trusty Adhoc On-Demand Distance Vector (Smart-Aodv) Routing Protocol for Service Discovery Process in Manet." *Journal of Survey in Fisheries Sciences* 10.1S (2023): 5395-5411.

[18] Reddy, Bhaskar, and B. Dhananjaya. "The AODV routing protocol with built-in security to counter black hole attack in MANET." *Materials Today: Proceedings* 50 (2022): 1152-1158.

[19] Sirajuddin, Mohammad, Ch Rupa, and Ande Prasad. "A trusted model using improved-AODV in MANETS with packet loss reduction mechanism." *Advances in Modelling and Analysis B* 61.1 (2018): 15-22.

[20] Sirajuddin, M. D., Ch Rupa, and A. Prasad. "An innovative security model to handle blackhole attack in MANET." *Proceedings of International Conference on Computational Intelligence and Data Engineering: ICCIDE 2017*. Springer Singapore, 2018.

[21] D.J.Samatha Naidu, Dr.Ande Prasad**.** "SAMRAM adversary model to prevent security attacks and network degradation problems in wireless sensor networks "

[22] Sirajuddin, M. D., Ch Rupa, and A. Prasad. "Advanced congestion control techniques for MANET." *Information Systems Design and Intelligent Applications: Proceedings of Third International Conference INDIA 2016, Volume 1*. Springer India, 2016.

[23] A. ShakaybArsalaan and H. Nguyen, "Andrew coyle and MahrukhFida, " quality of information with minimum requirments for emergency communications," *Adhoc Networks*, vol. 111, pp. 1570–8705.

[24] Mohammad Sirajuddin, Ch. Rupa, Celestine Iwendi, Cresantus Biamba, "TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network", *Security and Communication Networks*, vol. 2021, Article ID 5521713, 9 pages, 2021. https://doi.org/10.1155/2021/5521713.

Kiran Kumar Kommineni is a Part Time Research Scholar at Department of Computer Science, Vikrama Simhapuri University, Nellore, Andhra Pradesh. He completed his B.Tech in JNTU Hyderabad and M.E in Anna University. He has 15 years of Teaching experience at various positions. His areas of interests include Mobile Adhoc Networks and Information Security.

Dr.Ande Prasad is working as a Professor in the Department of Computer Science, Vikrama Simhapuri University, Nellore, Andhra Pradesh. He completed his Ph.D from Andhra University, Vishakhapatnam. Under his guidance four scholars have been awarded doctorate so far. His areas of interest are Artificial Intelligence, Machine Learning, Speech Processing, Pattern Recognition, Image Processing, Computer Networks. He has published more than 50 research articles in various international journals till now.