STM JOURNALS

Journal of
Mobile Computing, Communications & Mobile Networks

ISSN: 2349-901X
Volume 13, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoMCCMN

https://journals.stmjournals.com/jomccmn

Review JoMCCMN

Privacy and Security Enhancement in Mobile Ad Hoc Network (MANET) Using Information Hiding Techniques Based on Man-In-The-Middle Attack: A Review

Ashish Kumar Soni[1,*] Rajendra Gupta[2], Ankur Khare[3]

Abstract

The mobile ad hoc network (MANET) is widely spread throughout the entire world for quick communication. MANET is a type of ad hoc network with specific features of independent direct connections between devices. The current MANET network is rapidly used in wireless communication in fast and easy access terms, but MANET has many weaknesses in privacy and security, which makes information leakage in unprotected communication. So, goals are the most important points for MANET to achieve maximum features during insecure communication. Many information hiding plans are presented in the world to find a better result for security features, but the entire existing hiding plan is mostly dependent on the particular application. The combined security plan, or an improved or newly designed plan, can prevent security problems. The Man-In-The-Middle attack technique is mostly used to attack the MANET network. The literature work introduced the general idea of security goals, their challenges, existing algorithms against attacks, information hiding plans, and MANET features against man-in-the-middle (MITM) attacks.

Keywords: Application, information hiding methods, MANETs, MITM attacks, security goals

INTRODUCTION

A mobile ad hoc network (MANET) is a collection of nodes that automatically create connections with each other, with special features such as distributed applications, flexibility, and node-to-node connections. MANETs are classified into two types: the first is an infrastructure network using wired and fixed network systems, and the second is an infrastructure-less network known as an ad hoc network with no fixed routers, where all nodes can create connections dynamically in a free manner, such as emergency connections or quick connections for immediately sharing information in undefined conditions. MANETs have many challenges and are also classified in different patterns by researchers in given papers, such as routing quality of services, routing, and packet loss during transmission, except for general MANET applications in the world. However, security remains the main problem in insecure communication [1].

MANETs are applied in many emergency services, including the quick connection of networks with many routing attacks, which are categorized as active and passive attacks. Active

***Author for Correspondence**
Ashish Kumar Soni
E-mail: ashish1989soni@gmail.com

[1]Research Scholar, Department of Computer Science, Rabindranath Tagore University, Raisen, Madhya Pradesh, India
[2]Associate Professor, Department of Computer Science, Rabindranath Tagore University, Raisen, Madhya Pradesh, India
[3]Assistant Professor, Department of Computer Science and Computer Science Engineering, Rabindranath Tagore University, Raisen, Madhya Pradesh, India

Received Date: January 22, 2026
Accepted Date: January 29, 2026
Published Date: April 24, 2026

Citation: Ashish Kumar Soni, Rajendra Gupta, Ankur Khare. Privacy and Security Enhancement in Mobile Ad Hoc Network (MANET) Using Information Hiding Techniques Based on Man-in-The-Middle Attack: A Review. Journal of Mobile Computing, Communications & Mobile Networks. 2026; 13(1): 35–50p.

attacks are classified into routing procedures and network flooding. Passive attacks are applied in packet silent discard and routing information hiding [2]. Wireless networks are also applied in vehicular networks for traffic management and emergency data sharing with a quick response of networks in unreachable network areas using cloud services, and mobile ad hoc networks are also helpful [3, 4].

Privacy and security represent the biggest challenges to creating a safe and shielded transmission. Federated studies define many solutions for this major challenge-based attack and promote global cybersecurity research in the whole world [5]. Many privacy models have been presented, modified, or improved, along with new concepts by researchers. Most privacy models compare and summarize protocols, attacks, and other points to describe the improved results of privacy protocols [6].

Security plans for MANETs have been introduced with better features, but the selection of better security, advantages, disadvantages, and attacks has been introduced [7]. MANET has many security issues arising in modern networks against worm-hole attacks with detection and prevention [8]. In recent years, many advanced protocols have been proposed for privacy and security applications [9].

Much research is presented with its limitations and limited features of privacy and security. A new attack technique is introduced based on the weaknesses of the old information hiding techniques. Thus, the literature is summarized in this paper.

The remainder of this paper is organized as follows. Section 2 explores the application of MANET. Section 3 defines the research challenges in MANETs. Section 4 describes the security goals of MANETs. Section 5 explores several attacks on the MANET. Section 6 describes the literature work in two subsections: first, a comparative analysis of the literature work, and second, a summary. Finally, Section 6 presents the conclusions and prospects of this study.

APPLICATION OF MANETS

MANETs have many application areas worldwide, as shown in Figure 1 and displayed graphically as MANET worlds.

RESEARCH CHALLENGES IN MANETS NETWORK

The MANETs network has some challenging research key areas before MANETs are accepted [1, 2], which are summarized as follows.

Dynamic Behavior

MANET has self-organizing features where nodes are free to move accidentally in the network, and behavior changes very normally and accidentally at any time. This behavior is used to route packets to the intended recipient. Therefore, there is no fixed route for the node because of its dynamic behavior.

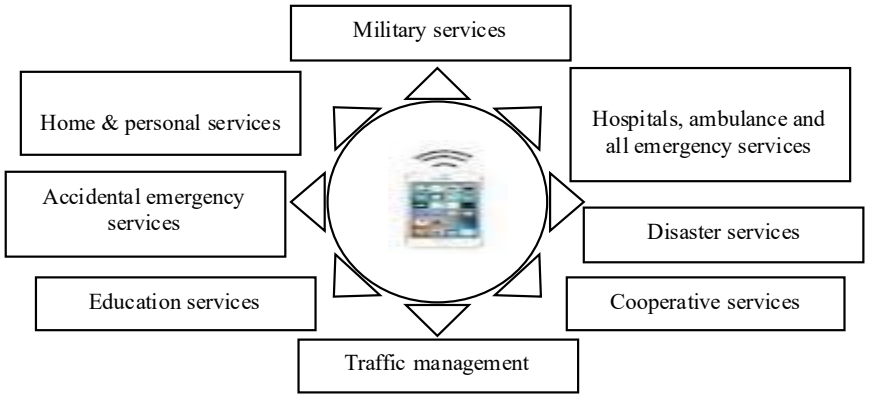

Figure 1. Mobile ad hoc network world.

Routing Behavior

The routing behavior of MANETs is an important research challenge for researchers regarding performance in multicasting, geocaching, and unicasting requirements by network nodes because of rapid changes in networks with different speeds.

Discovery of Gadgets

Optimization is a basic method for finding the route in a distributed system using dynamic updates, where the movement of the object is random; thus, it is a requirement.

Power Consumption

Mobile devices are designed for low battery power and storage. Thus, power consumption provides a limited time to access all processes of a mobile device.

Privacy and Security

The special widely used key point in MANETs is privacy and security during communication to transfer data safely, and other existing features of user requirements. However, this system weakness also motivates researchers to improve privacy and security protocols by providing a hybrid model for insecure MANET transmissions.

Efficient Service

Efficient service is the primary need of users to take reliable and future advantage of the devices. This provides a significant challenge and requirement for generating the best control system in combined applications to achieve efficient services with minimum resources in MANET wireless networks.

Congestion Control

Congestion control demands network capacity; in transmissions higher than this, congestion issues arise. The output is generated with low network performance due to congestion. The congestion problem is known as an overpopulation problem whenever packets are overloaded, and the loss of data generates lost delivery of data.

Route Selection

Accidentally generated disasters can break the route, and information delivery may be bounded on that route. Thus, route selection protocols should have multiple selection features for successful information delivery to achieve effective disaster management.

Directional/Unidirectional Link

Information traveling across a source may be directional or unidirectional. The utilization technique can improve the performance of the routing method to find the best link.

Quick Response on Demand Operation

Demanding operations are difficult to achieve with quick response protocols in the network for managing traffic distribution in low-power devices.

Distributed Protocols

Centralized dependency cannot refer to good communication in weak signals; therefore, distributed protocols must be used to create reliable connections between nodes to successfully share information in a poor network.

SECURITY GOALS IN MANETS

Security goals can be achieved by adding some main security key points, such as integrity goals, confidentiality of information, authentication protocols, and information availability, which are explored as follows [8, 9].

Integrity Goals

If integrity goals do not consider security protocols, the accuracy of the information must be weak, which is managed by advanced protocols to find accurate information in unsafe transmissions.

Confidentiality of Information

Information sharing must be confidential. It is the basic need of all users in open media for the right access between the sender and receiver. Information must be shielded with a strong security plan before it is transmitted in an unprotected wireless network.

Authentication Protocol

Authentication protocols can guarantee authorized senders and receivers in a trusted environment in many fields worldwide. If information is accessed by unwanted users, it can be dangerous and risky.

Availability of Information

The availability of information to users is always a major security goal of MANET. If information is not accessed by the user, then it is a big problem, and this should be solved as soon as possible.

OVERVIEW OF ATTACKS ON MANET NETWORK

Security and privacy attacks are introduced in some categories on different bases, like active or passive attacks, internal or external attacks, attacks on different network layers, cryptography or non-cryptography attacks, and stealthy or non-stealthy attacks classified by researchers. Attackers can attack based on their selection of finding weak points in privacy and security. The reporting place is categorized as internal, external, both, publicly viewed, or moving maximum time. Other selections of attacks may be in different natures: active, passive, or both; except for these, attackers can make selections based on presence, knowledge, behavior, and resources [6]. This section introduces various attacks in non-classified points [10–13].

Collaborative Attack

Attackers attack mobile ad hoc networks in groups, directly or indirectly. In indirect attacks, non-available attacker nodes fake legal nodes to point packets to specific malicious nodes. The routing method is affected by the overcrowding of routing data to circulate to nodes, packet forwarding, and release. A device is turned unnatural by disturbing the packet delivery, hostile to the programmed path in attacks such as Sybil or routing table overflow attacks. Direct collaborative attacks are performed by joining or staying in the network first, such as black hole or worm-hole attacks.

Routing Table Overflow Attack

The routing table overflow attack jams the entire network through extreme route advertisements to nonactive nodes. This attack generates a new direction and significant improvement in the protocol.

Flooding Attack

Network flooding is an example of a flooding attack, such as an route request (RREQ) message flooded in reactive routing methods and a proactive routing method flooded by topology control messages, where the route is uncontrolled. Flooding attacks are aimed at sending hoax messages to fake nodes to waste resources and capabilities, such as processor speed, memory, battery consumption, and bandwidth.

Impersonation Attack

Impersonation attacks mimic legal nodes and find the identity of legal nodes to join the network and express false route information. Attackers are available in the core of communication between two parties, covering IP addresses, and initiate impersonation attacks without visibility between active parties.

Node Isolation Attack

Node isolation attacks focus on the performance of nodes relative to the remaining nodes in the network. These attacks block route data about the exact node or class of nodes to be broadcast in the entire network; thus, the next node fails to receive link data about the continuity of these nodes and cannot create the next route to these nodes.

Location Disclosure Attack

A location disclosure attack occurs by discovering the position of nodes and finding outline information of the entire communication system using special traffic analysis or observed samples to create dangerous conditions for breaking special security terms of MANET.

Black-Hole Attack

Attacks are accessed by finding mistakes in the steps of route discovery of unconsidered methods and adding the wrong route to the next node to act as the optimum route. Whenever the route reply error (RRER) message is forwarded, the RREP message is transferred with a superior destination chain compared to the sent RREQ message, stating a trail to the goal. This was performed using a flood-based method. The black-hole attack is more harmful than the gray-hole attack.

Gray-Hole Attack

The gray-hole attack has two steps to break security: the first step is node spreading by discovering routes for routing methods for advertising in the entire network, as the legal route to the destination. Here, hateful nodes are captured as black-hole attacks, and in the second step, the node drops cached packets with an assured possibility.

Worm-Hole Attack

The worm-hole attack is a collaborative operation between two attacking nodes as a tunnel attack. First, a hacker searches for and captures routing packets at an exact location within the network and tunnel. These packets are transferred to the other hacker, bypassing intermediate nodes. In the second step, the hacker again produces captured packets in the network from that point onward. The tunnel spreads personal transmission links between hackers using in-band or out-of-band channels. A secret overlay tunnel built on the present medium is implemented using in-band channels via encapsulation. The out-band channel is used in external communication mediums, such as long-distance communication or personal rapid networks, to set quick connections between conspiring nodes. The routing steps may be interrupted whenever the routing control message is tunneled. These tunnels created between two colluding hackers are known as worm-hole attacks.

Rushing Attack

Nasty nodes spread a rushed RREQ message to arrive at every neighbor before the RREQ message of valid nodes, causing the valid RREQ message to become useless. Maker nodes during the route search fail to find any route with a maximum length of two hops, which excludes a route from end-to-end hackers' nodes. The RREQ message is delayed in reactive routing methods owing to dangerous movement and border spacing on the media access control (MAC) layer, as required by IEEE 802.11, and waits to solve crashes between receiving and resending an RREQ message to create an easy way for hackers. Hackers use the proposed method to generate a rushing attack by spreading the RREQ message at a superior level for an extended range transmission, by passing some midway hops to arrive at the destination first. Hackers perform this redirection.

Sybil Attack

The unique identity of each node is a routing property in a MANET. This generates confusion among the nodes. The hacker node supervises many identities in this Sybil attack and produces many virtual nodes with new identities using fresh arbitrary production or other applicable node identities to produce confusion in the routing steps or interrupt the entire network. Hackers especially focus on decentralized systems or authorization protocols in MANETs. There are two methods in sensitive terms: first, table-driven, and second, on-demand routing methods, in the Sybil attack.

Blackmail Attack

Weak authentication can generate a chance for hackers to damage the information of other valid nodes, and this chance makes reporting information possible with the help of a few routing methods. This advertised information blacklists a few spiteful nodes and blacklists legal nodes to detach them from other nodes.

Snare Attack

This is related to the special uses in military services. Some nodes are very special and are physically compromised. This technique is used to interrupt all active transmissions in the entire network. A hacker can link the vehicle identification number (VIN) by tracing and observing a few routes. This can lead to a kill strike to achieve success in a fight.

Invisible Node Attack

The unknown attack is considered an invisible attack. Invisible node attacks are performed in an invisible form, where nodes enter as participants without an open identity in any routing method, depending on the generated identity proof for any functionality. The invisible node attack (INA) conditions are accessed as the given types of node activity and outcomes of the routing method.

Denial of Service Attack

The denial of service (DoS) attack is used to generate and spread many packets in the entire network; after that, the server slows down in speed or generates a message for a user request for a resource that is not present. Such users cannot use this service. A hacker can perform a DoS attack using radio signals to jam networks and battery exhaustion techniques.

Replay Attack

A replay attack is used to break weak security by targeting the freshness of the route in the network. Hackers produce retransmitted signals for legal information, frequently repeated to insert network routing traffic that has been captured previously.

Jamming Attack

A jamming attack is performed by observing the wireless medium to decide the frequency at which the destination node is connected to signals from the sender and then broadcasting signals on that observed frequency; hence, the error-free receptor can be delayed.

MITM/MIM Attack

The MITM/MIM attack can be understood as a ball game where two people, such as the sender and receiver, play catch while a third unknown person tries to catch the ball, which is the same technique used by MITM or MIM attacks. This technique is also known as a fire brigade attack in mobile ad hoc networks.

IP Spoofing Attack

In this attack, hackers spoof IP addresses or produce IP packets with the wrong source IP address to cover the identity of the sender in the device's network.

Byzantine Attack

The Byzantine attack technique is preceded by a single intermediary node or clusters of intermediary nodes that act as horrible nodes and generate a routing loop or direct the message packets to the wrong path. Byzantine attacks are too complex to detect and prevent.

Selfish Attack

In this technique, hackers generate participation in active routes as selfish participants by discovering routes in the network. After participating in the active route, the hacker nodes initiate dropping message packets that are not associated with them to preserve the power used to transmit information packets associated with other nodes.

Jellyfish Attack

These attack techniques are separate from black-hole and gray-hole attacks, where data packets are not dropped blindly. The jellyfish attack announces non-invited delays that they previously transmitted in the network. This may challenge the sequence of packets in which they are delivered and transferred randomly. These interrupts are produced as a common flow control tool used by nodes for reliable communication.

Pseudorandom Number Attacks

The gathered keys are produced from random values. The generated random numbers are used to create solutions for replay attacks by generating fresh packets or accidental numbers. In public and private key structures, a secret key can produce many different random numbers to prevent attacks. The random number generator protocol is primarily used for statistical randomness. The best random numbers in wireless network security are generated in optimal cases based on physical sources of randomness that cannot be observed. Weak protocols of pseudorandom value generators can be easily detected by pseudorandom number attackers.

Key Management Attack

The key management method manages key creation, memory space, allotment, revocation, updates, and certification facilities. Hackers can initiate attacks to release the secret key at the local host or during the key-sharing steps. The weakness of a centrally reliable entity in MANETs makes it more susceptible to key management attacks. Key management methods require reliability in key-sharing centers or authorized authorities to prevent attacks.

LITERATURE WORK

Information hiding protocols achieve better results for generating a strong shield to create secure and private communication in MANETs. Different information hiding protocols are introduced, including advanced encryption standard (AES), RSA, data encryption standard (DES), 3DES, Blowfish, and Two-fish, with a comparative table of block sizes, mathematical operations, speed, structure, security, attacks, and other key points [14]. The secure homomorphic encryption plan can create complex conversions of information in a cloud environment where many digital attacks or cybercrimes are stealing information in several sectors. Cloud services require secure data communication between users through strong encryption plans with complex key management, which are investigated using different standard homomorphic encryption security plans with their security results 15].

The session key management plan can manage security in the cluster sensor network instead of using long keys. Elliptic curve cryptography with Diffie-Hellman key exchange and hash chains was introduced for mutual authentication, MITM, and other attacks; energy cost, computational cost, and other parameters were analyzed and compared [16]. Wireless networks are open, and broadcasting features are added with the provided open applications for attacks. The traditional plan does not perform well in physical layer security problems, which are classified, and researchers have analyzed the pros and cons of recent security research to create a direction for a better research area [17].

MANET suffers from many cyberattacks. MITM attacks are mostly used in MANET between two users. These attacks examine and change the information inside the network system. The introduced problem is observed in most cryptographic security plans that are attacked by malware known as MITM or MIM attacks [18]. MITM attacks are solved by quantum cryptography using two-way quantum key transmission, ping-pong, and copying all information in an unreadable form using the LM05 method [19].

The authentication plan Hopper–blum (HB) is introduced as an OOV-MIM attack, and its performance and complexity create a strong security concept [20]. The Internet key exchange can detect round-trip time and 90% accuracy against MITM attacks using a normal distribution based on IPsec protocols [21].

An artificial neural network can detect and prevent MITM attacks by achieving a better detection rate [22]. A strong framework can protect against MITM attacks for multiple nodes in a cloud environment. The RSA-CP-IDABE framework can protect both users and owners against MITM attacks [23].

Efficient and secure authentication can solve most problems of privacy and security against attacks. Fair exchange protocols and transaction security by near field communication (NFC) communication are proven for MITM attacks and replay attacks [24]. The security protocol blockchain is used as a game-changer security protocol with a big capability of non-repudiation for all participants in cloud communication. One-time security keys are used by physical unclonable functions with the logistics function of the additively manufactured operation. All these schemes are used to prevent MITM attacks [25]. Quantum identification protocols are modern, fair, and efficient exchange protocols. The semi-quantum authentication plan is accessed against double controlled NOT gate (CNOT) attacks and MITM attacks. Cross-comparison and measurement of security protocols can provide valuable results against both attacks [26].

Comparative analysis can help select security and privacy protocols for the optimal shielding methodology. The biometric application with the AES methodology can ensure reliable biometric key generation against network security attacks in MANETs [27]. Wireless security in MANETs is based on sequence distance vector routing and curve cryptography [28].

Elliptic curve cryptography is a high-speed protocol that achieves lightweight access and complex terms [29]. Lightweight protocols can achieve quick authentication key management in slow applications and for wireless devices [30].

Cloud services are already overloaded in distributed networks for safe driving; thus, the modified DES cryptography protocol achieves better results for overloaded objects [31]. Chaotic systems are widely used to create strong security protocols with lightweight speed and complexity for generating pseudorandom numbers. The combined hybrid algorithm for encryption introduces encryption based on a hyperchaotic function produced by a tri-valued memristor and a hash table used to generate initial values based on a hyperchaotic sequence [32]. The two-layer chaotic encryption protocol achieves a maximum entropy of 7.99, and other analyzed parameters are more effective for brute force attacks, coping attacks, and noise attacks prevented by achieving a hybrid chaotic protocol [33].

Significant security and privacy applications are achieved using hybrid advanced encryption standards with a biometric authentication scheme based on chaotic functions for the Internet of Things [34]. Secure communication with neural network chaotic encryption generates hybrid coding and dynamically sensitive keys with a better avalanche effect [35]. The new concept of chaotic function is used for encryption and decryption operations based on cipher block chaining protocols to prevent statistical and cryptographic attacks [36].

A substitution box plan is defined as a loose security protocol. This can be improved with better cryptanalysis attacks [37]. Improved identity-based encryption introduced a hybrid chaotic mapping protocol that provides better performance results for wireless networks [38].

Location privacy attacks can leak a user's location in a wireless network; their prevention is more essential in MANETs. The analysis of specific results on pseudonym and cryptographic protocols using digital signatures can improve user privacy and security with fifth-generation technology [39]. Public key encryption with keyword search is used with many different patterns of security and privacy protocols, such as identity-based, attribute-based, and other protocols, with their functionality and prevented attacks summarized [40].

Authorization and authentication plans are mostly used worldwide and are helpful protocols for mobile gadgets. This is the most common research area in insecure wireless communication for many applications, such as application security, disaster recovery, quick response, and other applications related to privacy and security [41]. The study of quantum cryptography can be more helpful against

modern fifth-generation technology attacks. Random number generation protocols based on ciphers were studied, and quantum-based cryptography with its attacks and many security and privacy parameters to improve quantum cryptography were summarized [42]. Quantum cryptography also helps in fog computing against edge, end, and cloud layer attacks performed by analyzing results [43].

Network traffic is rapidly improving in the world. This network traffic is fully open for hackers to leak through unauthorized access or break weak identities in the communication network. This problem motivates the use of identification protocols to create identified user access. Diffie-Hellman introduced identification key exchange protocols using the public key to create secure communication [44]. Two methods are used together for improving more complex shielded information in the MANETs network: first, AES, and second, the Diffie-Hellman key exchange plan [45]. Both protocols are also helpful in ensuring the security of medical records against cyberattacks [46].

Information confirmation should be performed using reliable key exchange protocols to ensure receiver confirmation. The real-or-random model is used to generate session key security. It can also defend against MITM and replay attacks. This is also proven by an informal security analysis [47]. The signed Diffie-Hellman protocol is performed as a random oracle model to generate tight security, which is briefly described against attacks and privacy and security parameters [48].

Multiple system controls can be achieved using a single log known as a single sign-on (SSO) method for achieving domain-free access for separate access for every user, which is possible by the SSO protocol, a verifiable encryption-based authentication protocol to prevent MITM attacks [49]. Denial of service attacks are spreading widely in wireless networks; a summarized analysis presents various areas of these attacks [50]. The avalanche effect protocol can ensure a strong encryption enhancement to generate unbreakable codes against attacks. Better results were shown for the DES security protocol in a modified form as the triple DES, and the analysis of avalanche effects achieved better output in comparison to the traditional DES [51].

Complex pseudorandom numbers can generate high performance in a wireless network with fast and easy-repeating unpredictable protocols [52]. The reversible encryption plan AES-CTR is used for hiding information that is based on a multi-key encryption plan and embedded steps used to achieve recovered information [53]. Mixed cryptography can achieve better output. The Mutual entity wireless authentication cryptography (MEWAC) protocol is performed in the microcontroller unit (MCU) and Wi-Fi modules. High-security protocols are used to create advanced high-performance security methods to reduce authentication and high-security parameters of the wireless network by using AES, RSA, and SHA-1 protocols [54]. The regenerated self-healing protocol achieved better results in generating capability against attacks [55].

Chaotic mathematical functions have been applied in different cryptographic schemes and improved to award better and stronger encryption schemes [56, 57].

Comparative Analysis of Literature Work

Security and privacy protocols are accessed using information hiding techniques. These protocols are becoming the first essential service for many application areas worldwide in every multimedia digital tool, such as audio, video, text, and image-forming data. Many information hiding patterns, copyright protection, and advanced-level security patterns are directed worldwide. Information is shared in an encrypted form in a public network to ensure confidentiality for both the sender and receiver. Cyberattacks violate the confidentiality, integrity, and availability security goals through different attack techniques in MANETs.

A literature survey of privacy and security in mobile ad hoc networks can help select the required security and privacy protocols for information hiding techniques to solve attack problems during communication in affected environments. The categorized information hiding techniques are illustrated in Figure 2.

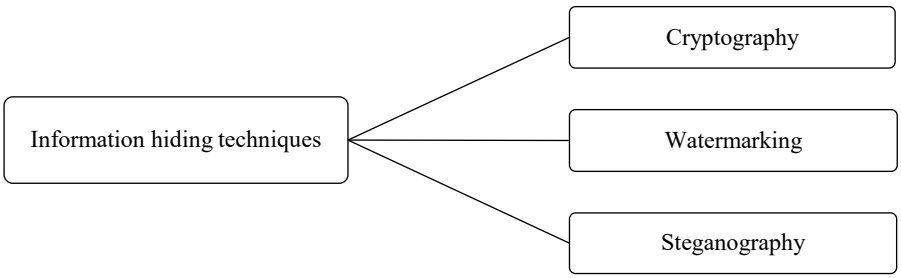

Figure 2. Classified information hiding techniques.

The cryptography technique is a complex encryption pattern to convert unreadable information without allowing hackers or unwanted objects to extract information. It is designed from mathematical ideas as special writing patterns to create complex code for attackers. Methods are designed for secret encryption key generation, digital signatures, password protection, identification, web surfing, confidential communication, etc. The cryptography technique has two types based on the key property, known as symmetric and asymmetric key cryptography. The symmetric key cryptography pattern uses the same key for both the sender and receiver. That same key is also used for the encryption and decryption of information. The second type of cryptography pattern is an asymmetric key pair with a public key and a private key. Both keys are different from each other; even the public key is used for public encryption, but the private key is accessed only by the receiver, which is completely secret. That cryptographic pattern can achieve CIA security goals in the network during transmission.

Watermarking techniques help verify user identity, copyright protection, and authentication of the owner by being embedded into many applications, such as digital signals, pictures, audio, video, or text. Watermarking protection is mostly used for copyright in different areas, such as document authentication, websites, watermarked certificates, articles, poems, emails, books, SMS, and other demanded applications.

The steganography technique is an advanced and complex algorithm of information hiding concepts that covers information between two nodes. Nobody can access and decrypt the covered information without leaving a significant track on the real data, such as video, audio, and picture data. The covering process may be possible with lightweight speed using many software tools and obtaining confidential transmission, strong privacy, and security features.

Summary

Various attacks are used in MANET to steal user-sensitive information during communication in these networks. Various solutions have been proposed for privacy and security to provide better advanced solutions for generating strong shields and identification methods. The latest research methodologies are presented in Table 1 for selecting the required techniques.

Various types of research are introduced to stop MITM attacks through different information hiding techniques. The two-way ping-pong and LM05 method [15] are applied with high complexity. Some operations are added like arithmetic, exponentiation, S-box, transformation, XOR gate, etc. in different methods like OOV [16], IPsec [17], ANN [18], RSA-CP-IDAEB [19], PUFs and Blockchain [21], SQA [22], ECC [24], AKMS [26], SSO [45], chaotic function [39], SSO [45], AES [49], and RESH [51] against MITM, DoS, CNOT, typical eavesdropping attacks, channel attacks, theoretical, classical, collusion attacks, and brute force attacks. The chaotic function is used to create high speed and better hybrid security [39] and combined with highly complex algorithms like hash functions [28], explored chaotic cryptosystems [29], AES [30], Aihara Neural Network [31], block ciphers [32], against plain text attacks, differential attacks, occlusion attacks, noise attacks, matrix cracking attacks, and statistics-based brute force attacks, etc. The DES method is improved, like 3DES [47] and DES-3L [27], with better results. Combined features are applied like Diffie-Hellman and AES [42] and signed Diffie-Hellman [44].

Table 1. Compared the properties of information hiding techniques.

References	Hiding method	Mathematical function	Speed	Security goals	Complexity	Based attack	Future work	Encryption effect
Mladen Pavicic et al. [15]	Two-way ping-pong and LM05 QKD	Conditional, Arithmetic and Other Operations	Good	Confidentiality	High	MITM attack	Need Improvement	Good
Milica Knezevic et al. [16]	OOV	XOR	Better	Integrity	Medium	MITM attack	Extract Probability	Medium
Yunxiao Sun et al. [17]	IPSec	Arithmetic	Medium	Integrity	Medium	MITM attack	Required Implementation	Medium
Robert A et al. [18]	ANN	-	Average	Availability	Good	MITM attack	Future Attacks	Average
Sonali Chandel et al. [19]	RSA-CP-IDAEB	Exponential and Arithmetic	Good	Confidentiality and Integrity	High	MITM attack	Integrity and Privacy	High
Bertrand Cambou et al. [21]	PUFs and Blockchain	XOR	Better	Confidentiality, Nonrepudiable, and Integrity	Average	MITM, DoS, and Brute Force Attack	Third Party Identification	Advance
Chun-Wei Yang et al. [22]	SQA	XOR		Confidentiality	Good	MITM, Controlled NOT gate (CNOT), and Typical Eavesdropping Attacks	QUnit Efficiency	Average
N. Sridevi et al. [24]	ECC	Arithmetic	High	Confidentiality	High	External Attack	Improve more reliable	High
Danyang Qin et al. [26]	AKMS	Arithmetic	High	Confidentiality and Integrity	Advance	Static and Mobile Attack	Resist Various Attacks	Average
S. Jerald Nirmal Kumar et al. [27]	DES-3L	Exponentiation and modulo arithmetic	Good	Confidentiality	Average	Brute Force Attack	More Reliable	Average
Xiaoyuan Wang et al. [28]	Chaotic and Hash Function	Arithmetic	Advance	Confidentiality	Medium	Plain Text Attack, Differential Attack, Occlusion Attack, and Noise Attack	Privacy Improvement	Medium
Hemalatha Mahalingam et al. [29]	Chaotic Cryptosystem	Arithmetic	Medium	Confidentiality	Average	Brute Force Attack	Speed Improvement	Average
Ayman Altameem et al. [30]	Chaotic Function and AES	Arithmetic, substitute Bytes, Shift Rows (Srows), HC transformation, and key transformation	Advance	Confidentiality, Availability, and Integrity	High	Brute Force Attack and Differential Attack	More Prevention of Attacks	High

Chen Liang et al. [31]	Aihara Neural Network and Chaotic Function	Arithmetic	Good	Confidentiality	Average	Matrix Cracking Attack and Statistics-Based Brute Force Attack	More Enhancement of the method	Average
Fethi Dridi et al. [32]	Block Cipher, Chaotic Function	Average, S-Box	Average	Confidentiality	Medium	Statistical and Cryptographic Attack	More Reliable Security	Not Better
Cherry Mangla et al. [39]	Hybrid Chaotic Function	XOR, exponentiation, and arithmetic	Good	Confidentiality and Integrity	High	-	Improve Performance in Image and Video	High
Prastyo et al. [42]	Diffie-Hellman, AES	Substitution-permutation, arithmetic, and exponentiation	Medium	Confidentiality, Availability, and Integrity	Good	MITM Attack and Side Channel Attack	Proof Attacks and Algorithm Modification	Good
Jiaxin Pan et al. [44]	Signed Diffie-Hellman	Arithmetic and Exponentiation	Good	Confidentiality and Integrity	Not Better	MITM Attack and Active Attack	Testing In Different Media	Not Better
Maki Kihara et al. [45]	SSO	XOR, exponentiation, and arithmetic	Average	Confidentiality and Integrity	Good	MITM, Theoretical and Classical Attack	Improve More Reliability	Good
Meixi Chen et al. [47]	3DES	Transportation and substitution	Good	Confidentiality	Medium	Brute Force Attack	Modification Of DES	Better
Zhaohui Li et al. [49]	AES	XOR, exponentiation, and arithmetic	Average	Confidentiality and Integrity	Good	Side Channel Attack	AES Improvement	Good
Wei Liang et al. [51]	RESH	XOR and arithmetic	Not good	Confidentiality	Not Better	Collusion Attack	Effective Distribution and Security	Good

CONCLUSION AND FUTURE WORK

Privacy and security can help achieve a better, safer, and more secure output in affected networks. These are the primary key points worldwide. Many researchers have found enhanced or new techniques for various types of attacks. This study explores various works, applications, security and privacy challenges, security goals, and different kinds of attacks with their solutions using information hiding techniques. Many key points are presented in tabular form to facilitate the selection of better information hiding techniques. The future scope must be grateful to select and research points from this paper to create hybrid solutions in the modern world for advanced new attacks. This literature work can be more helpful for users to select a safe and secure environment in affected tools during the communication of information in MANET.

New research will introduce better information hiding techniques in various fields according to new attack techniques. Combined features explore reports of privacy and security in tabular or graphical forms. The ad hoc network summarizes the properties of better strong connections for weak or jammed signals. Prospects will contribute to new research concepts for new and better improvements of information hiding techniques against attacks.

REFERENCES

1. Raza N, Aftab MU, Akbar MQ, Ashraf O, Irfan M. Mobile ad-hoc networks applications and its challenges. Commun Netw. 2016;8(3):131–136. doi:10.4236/cn.2016.83013.
2. Chitra P, Ranganayaki T. A study on MANET: applications, challenges and issues. Int J Eng Res Technol. 2020;8(03 Special Issue):1–4.
3. Sheikh MS, Liang J, Wang W. Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey. Wireless Commun Mob Comput. 2020;2020:1–25. doi:10.1155/2020/5129620.
4. Khelifi H, Luo S, Nour B, Shah SC. Security and privacy issues in vehicular named data networks: an overview. Mobile Inf Syst. 2018;2018:1–11. doi:10.1155/2018/5672154.
5. Gosselin R, Vieu L, Loukil F, Benoit A. Privacy and security in federated learning: a survey. Appl Sci. 2022;12:9901. doi:10.3390/app12199901.
6. de Fuentes JM, González-Manzano L, Mirzaei O. Privacy models in wireless sensor networks: a survey. J Sensors. 2016;2016:1–18. doi:10.1155/2016/4082084.
7. Nithyapriya J, Anandha Jothi R, Palanisamy V. Securing data with selective encryption based DAC scheme for MANET. In: Pandian AP, Senjyu T, Islam SMS, Wang H, editors. Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI 2018). Lecture Notes on Data Engineering and Communications Technologies. Vol. 31. Cham: Springer; 2020. p. 133–139. doi:10.1007/978-3-030-24643-3_15.
8. Sharma PK, Sharma V. Survey on security issues in MANET: wormhole detection and prevention. 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India. 2016. p. 637–640. doi:10.1109/CCAA.2016.7813799.
9. Yu F, Chang CC, Shu J, Ahmad I, Zhang J, de Fuentes JM. Recent advances in security and privacy for wireless sensor networks 2016. J Sensors. 2017;2017:1–3. doi:10.1155/2017/3057534.
10. Panda N, Patra B, Hota S. MANET routing attacks and their countermeasures: a survey. J Crit Rev. 2020;7(13):2777–2792.
11. Prashar L, Kapur RK. Performance analysis of routing protocols under different types of attacks in MANETs. 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India. 2016. p. 405–408. doi:10.1109/ICRITO.2016.7784989.
12. Rajkumar K, Prasanna S. Complete analysis of various attacks in MANET. Int J Pure Appl Math. 2018;119(15):1721–1727.
13. Goyal M, Poonia SK, Goyal D. Attacks finding and prevention techniques in MANET: a survey. Adv Wirel Mob Commun. 2017;10(5):1185–1195.

14. Kumar K, Sasikala K. Comparative study of cryptographic algorithms. Int J Eng Res Technol. 2020;9(11). doi:10.5281/zenodo.18655114.
15. Devi P, Sathyalakshmi S, Venkata Subramanian D. A comparative study on homomorphic encryption algorithms for data security in cloud environment. Int J Electr Eng Technol. 2020;11(2):129–138.
16. Kim J, Moon J, Jung J, Won D. Security analysis and improvements of session key establishment for clustered sensor networks. J Sensors. 2016;2016:1–17. doi:10.1155/2016/4393721.
17. Fang W, Li F, Sun Y, Shan L, Chen S, Chen C, Li M. Information security of PHY layer in wireless networks. J Sensors. 2016;2016:1–10. doi:10.1155/2016/1230387.
18. Khadam U, Iqbal MM, Alruily M, Al Ghamdi MA, Ramzan M, Almotiri SH. Text data security and privacy in the Internet of things: threats, challenges, and future directions. Wireless Commun Mob Comput. 2020;2020:1–15. doi:10.1155/2020/7105625.
19. Pavičić M. How secure are two-way ping-pong and LM05 QKD protocols under a man-in-the-middle attack? Entropy. 2021;23:163. doi:10.3390/e23020163. PubMed: 33573044.
20. Knežević M, Tomović S, Mihaljević MJ. Man-in-the-middle attack against certain authentication protocols revisited: insights into the approach and performances re-evaluation. Electronics. 2020;9:1296. doi:10.3390/electronics9081296.
21. Sun Y, Wang B, Liu H, Wei Y, Wu D, Wang J. Detecting IKEv1 man-in-the-middle attack with message-RTT analysis. Wireless Commun Mob Comput. 2022;2022:2605684. doi:10.1155/2022/2605684.
22. Sowah RA, Ofori-Amanfo KB, Mills GA, Koumadi KM. Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in artificial neural networks (ANN). J Comput Netw Commun. 2019;2019:1–14. doi:10.1155/2019/4683982.
23. Chandel S, Yang G, Chakravarty S. RSA-CP-IDABE: a secure framework for multi-user and multi-owner cloud environment. Information. 2020;11(8):382. doi:10.3390/info11080382.
24. Thammarat C. Efficient and secure NFC authentication for mobile payment ensuring fair exchange protocol. Symmetry. 2020;12:1649. doi:10.3390/sym12101649.
25. Cambou B, Gowanlock M, Heynssens J, Jain S, Philabaum C, Booher D, et al. Securing additive manufacturing with blockchains and distributed physically unclonable functions. Cryptography. 2020;4(2):17. doi:10.3390/cryptography4020017.
26. Yang CW, Wang HW, Lin J, Tsai CW. Semi-quantum identification without information leakage. Mathematics. 2023;11:452. doi:10.3390/math11020452.
27. Srividya R, Ramesh B. A comparative analysis of DES and BAES for MANET. Int J Adv Res Eng Technol. 2020;11(6):816–825. doi:10.34218/IJARET.11.6.2020.073.
28. Sridevi N, Nagarajan V. A curve based cryptography for wireless security in MANET. Cluster Comput. 2019;22:4017–4025. doi:10.1007/s10586-018-2612-2.
29. Xiao Y, Lin W, Zhao Y, Cui C, Cai Z. A high-speed elliptic curve cryptography processor for teleoperated systems security. Math Probl Eng. 2021;2021:6633925. doi:10.1155/2021/6633925.
30. Qin D, Jia S, Yang S, Wang E, Ding Q. A lightweight authentication and key management scheme for wireless sensor networks. J Sensors. 2016;2016:1547963. doi:10.1155/2016/1547963.
31. Kumar NS, Goel AK. Detection, localization and classification of fetal brain abnormalities using YOLO v4 architecture. Int J Performability Eng. 2022;18(10):720–729. doi:10.23940/ijpe.22.10.p5.720-729.
32. Wang X, Zhang X, Gao M, Tian Y, Wang C, Iu HHC. A color image encryption algorithm based on hash table, Hilbert curve and hyper-chaotic synchronization. Mathematics. 2023;11:567. doi:10.3390/math11030567.
33. Mahalingam H, Veeramalai T, Menon AR, S S, Amirtharajan R. Dual-domain image encryption in unsecure medium – a secure communication perspective. Mathematics. 2023;11:457. doi:10.3390/math11020457.
34. Altameem A, P P, T S, Poonia RC, Saudagar AKJ. A hybrid AES with a chaotic map-based biometric authentication framework for IoT and Industry 4.0. Systems. 2023;11:28. doi:10.3390/systems11010028.

35. Liang C, Zhang Q, Ma J, Li K. Research on neural network chaotic encryption algorithm in wireless network security communication. EURASIP J Wirel Commun Netw. 2019;2019:151. doi:10.1186/s13638-019-1476-3.
36. Dridi F, El Assad S, El Hadj Youssef W, Machhout M, Lozi R. Design, implementation, and analysis of a block cipher based on a secure chaotic generator. Appl Sci. 2022;12:9952. doi:10.3390/app12199952.
37. Munir N, Khan M, Shah T, Alanazi AS, Hussain I. Cryptanalysis of nonlinear confusion component based encryption algorithm. Integr. 2021;79:41–47. doi:10.1016/j.vlsi.2021.03.004.
38. Zhou H, Bi H. Wireless sensor network security based on improved identity encryption. Sci Program. 2022;2022:2308825. doi:10.1155/2022/2308825.
39. Ahmed N, Deng Z, Memon I, Hassan F, Mohammadani KH, Iqbal R. [Retracted] A survey on location privacy attacks and prevention deployed with IoT in vehicular networks. Wireless Commun Mob Comput. 2022;2022:6503299. doi:10.1155/2022/6503299.
40. Noorallahzade MH, Alimoradi R, Gholami A. A survey on public key encryption with keyword search: taxonomy and methods. Int J Math Math Sci. 2022;2022:1–10. doi:10.1155/2022/3223509.
41. Kumar VB. Authorization and authentication in mobile devices. Int J Res Appl Sci Eng Technol. 2022;10(4):1733–1738. doi:10.22214/ijraset.2022.41610.
42. Saini A, Tsokanos A, Kirner R. Quantum randomness in cryptography – a survey of cryptosystems, RNG-based ciphers, and QRNGs. Information. 2022;13:358. doi:10.3390/info13080358.
43. Mangla C, Rani S, Atiglah HK. Secure data transmission using quantum cryptography in fog computing. Wireless Commun Mob Comput. 2022;2022:3426811. doi:10.1155/2022/3426811.
44. Mishra MR, Kar J. A study on Diffie-Hellman key exchange protocols. Int J Pure Appl Math. 2017;114:179–189. doi:10.12732/ijpam.v114i2.2.
45. Manjula T, Anand B. A secured multiplicative Diffie Hellman key exchange routing approach for mobile ad hoc network. J Ambient Intell Humaniz Comput. 2021;12:3621–3631. doi:10.1007/s12652-019-01612-8.
46. Ermatita, Prastyo YB, Pradnyana IWW, Adrezo M. Diffie-Hellman algorithm for securing medical record data encryption keys. 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia. 2020. p. 296–300. doi:10.1109/ICIMCIS51567.2020.9354297.
47. Lee J, Yu S, Kim M, Park Y, Lee S, Chung B. Secure key agreement and authentication protocol for message confirmation in vehicular cloud computing. Appl Sci. 2020;10:6268. doi:10.3390/app10186268.
48. Pan J, Qian C, Ringerud M. Signed (group) Diffie–Hellman key exchange with tight security. J Cryptol. 2022;35:26. doi:10.1007/s00145-022-09438-y.
49. Kihara M, Iriyama S. Security and performance of single sign-on based on one-time pad algorithm. Cryptography. 2020;4:16. doi:10.3390/cryptography4020016.
50. Mazur K, Ksiezopolski B, Nielek R. Multilevel modeling of distributed denial of service attacks in wireless sensor networks. J Sensors. 2016;2016:5017248. doi:10.1155/2016/5017248.
51. Yao L, Jin M. Research on accounting data encryption processing system based on artificial intelligence. Procedia Comput Sci. 2023;228:373–382. doi:10.1016/j.procs.2023.11.043.
52. Levina A, Mukhamedjanov D, Bogaevskiy D, Lyakhov P, Valueva M, Kaplun D. High performance parallel pseudorandom number generator on cellular automata. Symmetry. 2022;14:1869. doi:10.3390/sym14091869.
53. Li Z, Wang Y, Wang Z, Liu Z, Zhang J, Li M. Reversible information hiding algorithm based on multikey encryption. Wireless Commun Mob Comput. 2020;2020:8847559. doi:10.1155/2020/8847559.
54. Lu Y, Zhai J, Zhu R, Qin J. Study of wireless authentication center with mixed encryption in WSN. J Sensors. 2016;2016:9297562. doi:10.1155/2016/9297562.
55. Liang W, Ruan Z, Wang Y, Chen X. RESH: a secure authentication algorithm based on regeneration encoding self-healing technology in WSN. J Sensors. 2016;2016:2098680. doi:10.1155/2016/2098680.

56. Khare A, Shukla P, Rizvi M, Stalin S. An intelligent and fast chaotic encryption using digital logic circuits for ad-hoc and ubiquitous computing. Entropy. 2016;18:201. doi:10.3390/e18050201.
57. Shukla P, Khare A, Rizvi M, Stalin S. Applied cryptography using chaos function for fast digital logic-based systems in ubiquitous computing. Entropy. 2015;17:1387–1410. doi:10.3390/e17031387.

