P-ISSN 1991-8941
E-ISSN 2706-6703
Vol. 19, No. 2 (2025)

Journal of University of Anbar for Pure Science
(JUAPS)

journal homepage: juaps.uoanbar.edu.iq

Open Access

Review Paper

Mobile ad hoc network wireless security: problems, solutions, and application: state-of-the-art

Shahlaa Mashhadani [1*], Oday Ali Hassen [2], Iptehaj Alhakam [1]

[1]Department of Computer, College of Education for Pure Sciences Ibn Al-Haitham, University of Baghdad, 10071, Iraq

[2]Ministry of Education, Wasit Education Directorate, Kut 52001, Iraq

ARTICLE INFO

Received: 27/09/2024
Accepted: 19/11/2024
Available online: 21/11/2025
December Issue
10.37652/juaps.2024.153957.1323

Cite @ JUAPS

Corresponding author
Shahlaa Mashhadani
shahlaa.t@ihcoedu.uobaghdad.edu.iq

ABSTRACT

Dedicated mobile networks (MANETs) in wireless networks are prone to security issues because they are not regulated. They rely on a non-static infrastructure and do not have routers or fixed terminals to manage communication between devices. Networked devices, known as nodes, communicate directly with each other. Each node can act as a router and contribute to the transfer of data to other nodes. Therefore, the lack of regulation has several causes: (1) Network dynamics: devices in a MANET move continuously and frequently change location, altering established communication paths. (2) Decentralized architecture: there is no central point that manages data traffic; each node operates independently and is responsible for communication. (3) Devices are not always directly connected to each other, so data may need to pass through several hops to reach other nodes, which increases complexity and makes communication more difficult. This study examines MANET security challenges, suggests remedies, and proposes full security implementations. Security measures under investigation and potential implementation include attacks on the Domain Name System (DNS), distributed denial-of-service (DDoS), node abuse, energy-efficient security, trust management, intrusion detection systems, secure routing protocols, multilayer design, and machine-learning-based security. Implementing complete security methodologies, while addressing these issues, is necessary to enable effective wireless security for MANETs.

Keywords: *Communication system security, Mobile ad hoc networks, Mobile communication, Routing protocols*

1 INTRODUCTION

MANETs can be used for vehicle communications, disaster recovery, and military operations. They operate through direct or intermediary nodes, and a secure MANET is essential to protect communications from hostile nodes, denial-of-service attacks, and node misbehavior [1]. MANETs present unique security challenges due to their dynamic nature and lack of centralization. This article examines MANET security problems, proposes solutions, and assesses their effectiveness and the threats they pose, including routing, denial-of-service attacks, and misbehavior. We then propose security solutions for intrusion detection and mitigation, discussing artificial intelligence, collaborative security, game theory, and multi-layered planning. We evaluate these methods to identify ways to make MANETs more secure and reliable in demanding, constantly changing environments [2].

Ad hoc networks are self-configuring wireless networks of mobile nodes connected via routers or hosts. Mobile nodes can communicate with one another without an access point. This means there is no permanent infrastructure, and routers may move freely and position themselves as needed. Every mobile node has a

transmitter and a receiver. Thus, mobile ad hoc network (MANET) nodes self-organize dynamically. MANET nodes can communicate directly with other nodes within their radio range; if a destination is outside direct communication range, they relay data through intermediate nodes. Key characteristics of ad hoc networks include the following [3].

First, ad hoc networks use wireless links that can be unstable. Nodes also operate with limited power, and mobility is high. Second, node relocation can affect routing information. In a MANET, nodes can move within or beyond their radio range. Third, the frequent movement of MANET nodes increases their vulnerability to attacks. Therefore, routing takes node movement into account to help prevent attacks on mobile AD-HOC networks. Mobile AD-HOCs in MANETs are wireless networks of mobile nodes that dynamically organize themselves without a pre-defined or centralized structure. While they offer flexibility and resilience, they also present unique security challenges due to their dynamic nature and open wireless environment without centralized authority. This research outlines the security problems in MANETs, their solutions, and highlights effective methods for enhancing their security [4–6]. Figure 1: A mobile AD-HOC network without an access point [4].

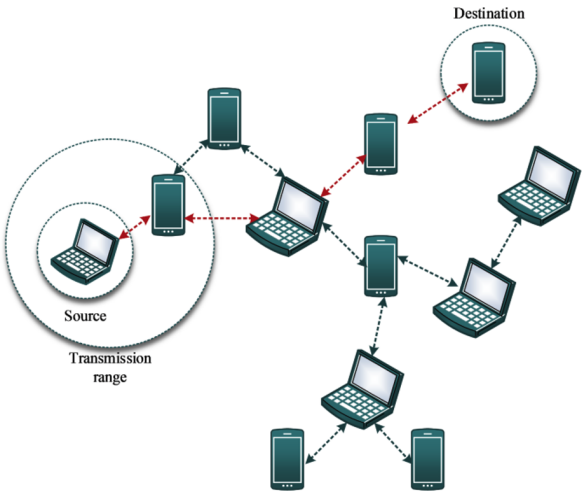

Fig. 1 Mobile Ad-hoc Network [5]

2 RELATED WORK

Research has addressed the problems of MANETs and their solutions. There are two main types of attacks on MANETs: active and passive. Passive attacks do not affect data transmission because their role is to monitor information traffic [7]. In a passive attack, legitimate nodes are compromised internally to steal information. In contrast, active attacks disrupt data transmission. Kaur et al. argue that active attacks are more dangerous because they interfere with data transmission between nodes [8]. Therefore, both types of attacks can be internal or external and are more vulnerable than wired networks because the nodes are self-organizing, which increases the difficulty of security. To protect users, MANETs must meet standard security goals. Confidentiality requires that only authorized devices and users access the network [9]. Each node should verify the identity of peers and users; network access requires valid credentials for both. Without authentication, impersonators cannot join the network. Other studies recommend edge cryptography for network security [10]. Reference [11] describes how nodes can authenticate one another and issue security certificates. Reference [8] presents a MANET routing system that uses covert information exchange to mitigate security risks. Reference [12] provides a broad model for MANET data transmission and connection security.

Security design and current practices in data-packet transmission are discussed in detail in [13]. Because MANETs are vulnerable, many security methods have been developed. In reference [14] proposes ARAN, a secure MANET routing mechanism. This protocol ensures network security with node certificates. It also states that certificates can defeat every MANET security threat. Supplementary works examine MANET multi-hop security challenges and risks.

Intrusion detection aims to identify threats early. One approach proposes a distributed and cooperative model for attack detection [15]. In such systems, all network nodes participate: when a node detects a hazard, it warns the others. However, limited node power may prevent wide alert distribution. For these cases, cluster-based IDS is used. A cluster-driven IDS divides the network into subgroups so member nodes can alert peers about attacks. A designated node watches over others and detects intrusions; when an attack is identified, it notifies the cluster. All nodes in a cluster share a single radio range.

Other MANET attacks include the wormhole. In a wormhole, an attacker impersonates a receiver to intercept data and forwards it to a colluding node before sending it on to the real receiver, potentially corrupting the message or disrupting communication. To counter wormhole attacks, packet leashing adds information to

limit transmission distance. Packet leashing may be temporal or geographic: geographic leashes use distance to restrict transmission, while temporal leashes use a maximum transmission time [16, 17][16, 17].

Research in Mobile Ad hoc Network (MANET) wireless security encompasses a wide range of studies, academic papers, and projects aimed at addressing these challenges. Here is a summary of key areas of related work:

2.1 Ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR) are two encryption protocols for safe routing

Numerous studies have sought to strengthen AODV and related protocols by adding authentication, cryptographic techniques, and trust-based routing. One example is Secure AODV (SAODV). Researchers have also worked to improve DSR, focusing on preventing routing attacks such as black-hole and gray-hole attacks and on securing route discovery and management [18].

2.2 Intrusion detection and prevention systems (IDPS)

Key Management and Authentication: Studies of anomaly-based MANET detection and prevention methods, and research related to node misbehavior for attacks, including proposed algorithms for detecting and preventing such behaviors, monitoring systems [19], and key generation protocols. These were also addressed with the aim of achieving efficiency, security, and biometric authentication to ensure protected communications in MANETs [20].

2.3 Designing and optimizing across layers

Cross-layer security protocols. Research has explored improving security by integrating mechanisms across multiple layers of the protocol stack, rather than only one or two. Resource optimization. Studies have examined how to maximize resource use in MANETs under acceptable security constraints, considering energy efficiency, bandwidth allocation, and QoS limitations .

Collaborative security and game theory. First, collaborative defense mechanisms: researchers have explored cooperative strategies among MANET nodes and broader collaborative security frameworks to share security information and strengthen networks against threats. Second, game-theoretic models: studies use game theory to analyze and improve MANET security measures, incentive systems, and decision-making, accounting for the rational behavior of selfish nodes and adversaries [21].

Clustering and vulnerability. MANET connectivity and data-packet transfer can rely on clusters of nodes (mobile devices) that form short-lived, ephemeral networks without central administration. In the absence of centralized control, links between mobile nodes must rely on trust. Because of their dynamic nature and rapid topology changes, MANETs are vulnerable to insider attacks. MANET attacks are characterized at the network layer [22], as shown in Figure 2.

3 SOLUTIONS THAT CONTRIBUTE TO IMPROVING THE SECURITY OF MOBILE WIRELESS AD HOC NETWORKS

In the security of mobile ad hoc networks (MANETs), the technologies used face many challenges, but there are also advanced solutions that improve protection. Key recent contributions include:

1. Public- and private-key encryption: Protects communications in wireless networks using asymmetric keys and is effective against eavesdropping.

2. Quantum-cryptography applications: Resist classical computing–based attacks that may penetrate existing systems.

3. Deep-learning–driven IDS: Uses modern neural networks to power intrusion detection systems (IDS) that detect attacks and learn new threat patterns, improving recognition of previously unseen threats.

4. Biometric authentication: Fingerprint, face, or voice authentication helps protect connected devices and prevents unauthorized access to network resources.

5. Blockchain technologies: Reduce the risk of data tampering within MANETs by protecting and recording transaction history without a third party.

6. Making smart decisions based on neural networks and potential threats to connected devices.

4 PROBLEM SOLUTIONS

MANETs pose unique security challenges because of their dynamic topology and lack of fixed infrastructure.

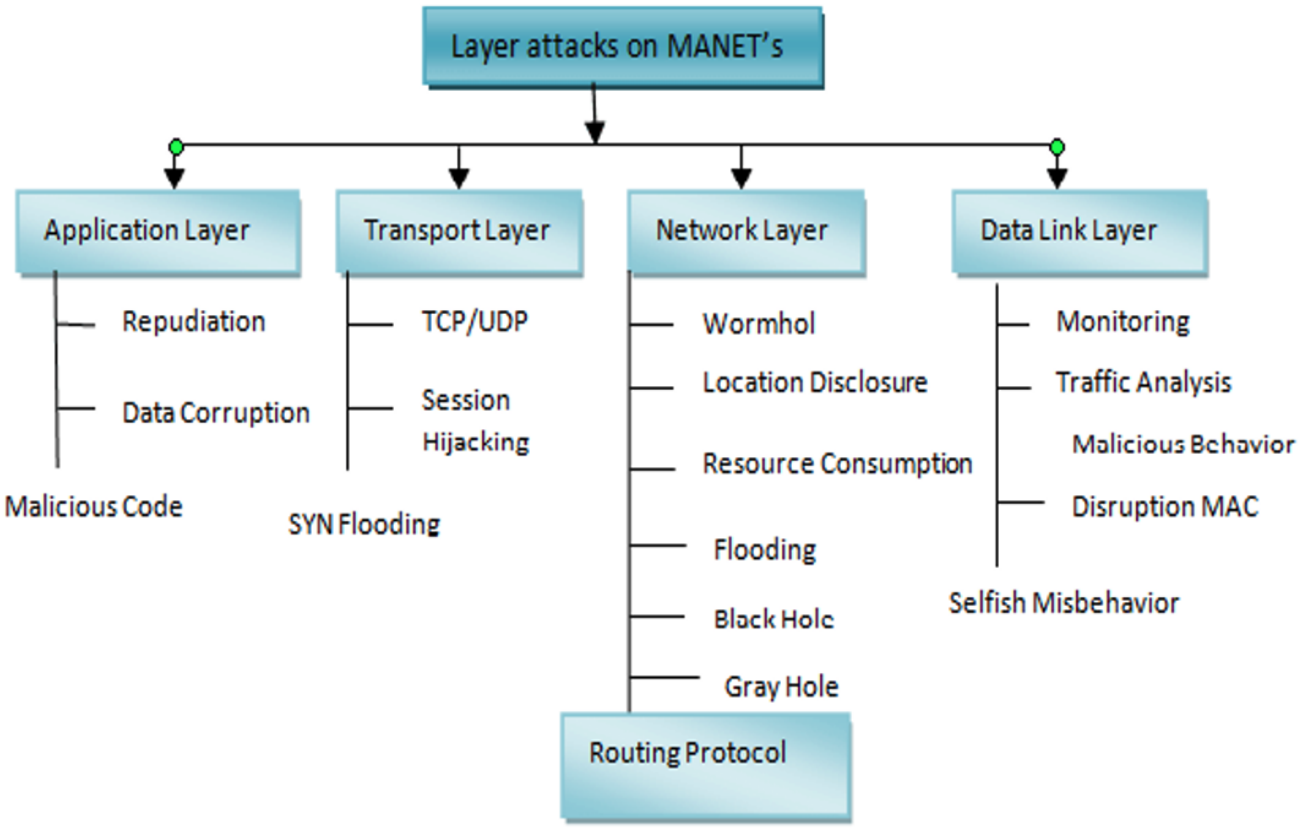

Fig. 2 Attacks in various layers of MANET [22]

Here we present the most common security issues resulting from mobile ad hoc networks and their solutions [23]:

1. In a denial-of-service attack, the attacker usually floods the network with traffic and exhausts all the available resources or even halts routing [24].
   - Objective: Security measures such as IDS, adaptive routing algorithms, and rate limiting should be employed to stop DoS assaults. Limiting the resource usage, as well as preventing unwanted access and using encryption with authentication are other practical solutions [24].

2. mobile ad hoc network node resources are often vulnerable and exposed to hacking, which can lead to illegal access, unwanted activities and data loss [25].
   - Objective: Limiting network activity to nodes with appropriate authorization is the aim of setting up an intrusion detection and prevention system also known as (IDPS). Strict authorization procedures may help with identifying vulnerable nodes in order to accomplish this [25].

3. In MANET communications there is a significant risk of data manipulation and eavesdropping attacks since they are frequently transmitted over unprotected wireless networks [26].
   - Objective: one way to encrypt the communication channels is to use encryption technologies like IPsec or SSL/TLS. A digital signature can also be used as an extra method to confirm the legitimacy of data transmissions in order to guarantee the confidentiality and integrity of data [26].

4. complex security operations are challenging to execute on MANET nodes due to their limited life along with the processing power and bandwidth [27].
   - Objective: To make up for the lack of resources,

lightweight security algorithms and protocols should be created to maximize performance as well. For instance, elliptic curve cryptography (ECC) offers greater and better security at a significantly lower computational resource cost compared to conventional cryptographic techniques [27].

5. Dishonest node behavior, such as failing to forward packets and using network resources without contribution can have a detrimental impact on MANET performance [28].
   -Objective: To develop reputation- based systems such as path monitors and classifiers, additionally to detect and eliminate malicious nodes in the network and promote cooperative behavior while also discouraging selfish nodes [28].

6. Physical layer attacks include things like jamming, eavesdropping and signal interference. MANETS could be compromised by these kinds of attacks [28]
   -Objective: to mitigate the impact of physically layer attacks, power management , frequency hopping and spread spectrum techniques are used [29].

It is important to use a combination of cryptographic techniques, intrusion detection systems, secure routing protocols as well as cooperative processes that can adapt to the particular characteristics and points of MANETS, this is in order to address these security concerns. This helps foresee potential security vulnerabilities in dynamic networks, which also require ongoing monitoring and adaptation.

5 CHALLENGES

1. Enhancing MANETs security is extremely challenging and difficult due to the presence of dynamic, potentially malicious nodes and the lack of fixed infrastructure [25].

2. Designing efficient, secure routing protocols is challenging due to the fact that MANETs have limited resources, meaning they are susceptible to routing attacks, and undergo frequent topology changes [26].

3. MANETs are inherently unpredictable and heterogeneous, making consistent quality of service hard to guarantee, especially for bandwidth-intensive applications [26].

4. it is difficult to deploy MANETS without compromising speed or dependability, such networks with limited resources find it difficult to achieve such large energy and resource savings [27].

5. Interoperability among protocols and devices is another challenge in MANETs [28].

6 ADVANTAGES

Due to the fact that mobile MANETs are dispersed and have an unpredictable structure, a unique challenge such as wireless security will be present. There are several advantages to fixing security flaws in these networks, such as:

1. Dynamically, nodes in MANETs can join or leave the network at any time. The network can configure itself for flexibility and can quickly adapt to different conditions, making it difficult for attackers to create specialized attacks based on network topologies [30].

2. MANETs can reduce the reliance on central authority for implementation by distributing security measures among nodes in the network. The system's distributed design makes it more resilient to failures and reduces the impact of compromised nodes [31].

3. Battery life and bandwidth are two resource limitations for MANETs. For the reason that their limited resources, MANETs require lightweight moreover effective security solutions. Effective security procedures protect against security threats and optimize the use of network resources. [32].

4. Adaptive routing techniques are used by MANETs to handle network changes such as node mobility and connection loss. Routing decisions can be dynamically changed by security- enabled routing protocols according to perceived security.

5. When numerous nodes work together to accomplish shared goals and objectives, MANETs provide assistance. Solutions for group chat security may include confidentiality, integrity as well as authentication. These kind of techniques facilitate important group conversations. [33].

6. In MANETs, nodes can work together and pool resources to carry out network functions like data relaying and service delivery at the same time. To improve the use of network resources while shielding them from potentially harmful activities or unauthorized access, security solutions that enable nodes to operate safely together are highly required.

7. MANETs often employ cross-layer communication to optimize network performance in addition to efficiency. When security protocols are integrated across various network layers, the network infrastructure itself may be more resilient and better protected against a wide range of security threats. [33].

8. MANETs have built-in self-healing capabilities, so therefore they can recover when a node fails or the network is divided. Security mechanisms may autonomously detect and resolve those security breaches by employing self-healing features, improving the networks overall dependability and resilience [34].

7 DISADVANTAGES

1. Among other security concerns, MANETs are vulnerable to routing attacks, denial of service attacks and node misbehavior. This is due to their decentralized structure, open wireless medium and lack of centralized management [35].

2. The performance of real time applications is impacted by factors like dynamic topology, network congestion and varying connection quality, this makes it challenging to guarantee quality of service in MANETs [36].

3. The limited battery power, processing power and the memory of MANET nodes limit the implementation of complex protocols and security procedures.

4. Due to the routing and resource management becoming more expensive as the number of nodes increases, MANET scalability issues may occur [37].

5. Managing MANETs without a centralized administrator can be a difficult task that requires efficient setup, monitoring as well as maintenance procedures [38].

8 APPLICATIONS

Creating an application for mobile ad hoc network (MANET) wireless security would involve several steps and considerations. The second category includes decentralized mobile networks, which are wireless multihop network that operates autonomously. Neither the network's infrastructure nor its routers are permanently installed. There is complete mobility among the nodes, and they may all dynamically stay in touch with one another. Even if the terminal's wireless coverage is restricted, two users who are unable to contact directly can still work together by enlisting the assistance of other nodes to pass packets. The ability to locate and maintain routes to other nodes is essential for each node, which may be viewed as a router, Figure 3.

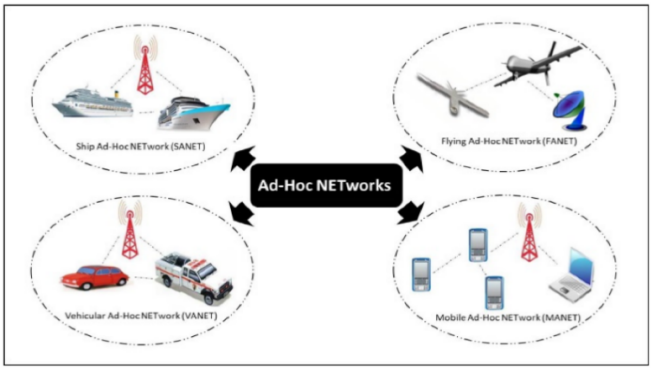

Fig. 3 Types of ad hoc networks [39]

Here's a basic outline of what you might include in such an application:

1. An application that has the ability to find other devices in the area and connect to them so that an ad hoc network may be formed. A possible protocol involved in this is the use of Bluetooth and IEEE 802.11 [40].

2. To prevent unauthorized devices from connecting to the network, establish authentication methods first. The next step is to set up a key exchange. Digital certificates, authentication via a username and password, and other methods are some examples of such procedures. To put the cherry on top of everything, you should establish encryption keys for secure communication by utilizing secure key exchange protocols [41].

3. Because of the inherent dynamic nature of MANNETs, secure routing protocols are absolutely necessary. Adaptable secure routing protocols should be put in place to guarantee the safe delivery of data [42].

4. To avoid eavesdropping on MANET traffic and keep data secure, encryption and preserving the integrity of encrypted data are crucial. It is easier to prevent tampering with transmitted data if procedures are in place to check its integrity [43].

5. Detecting and preventing intrusions by combining intrusion prevention and detection systems to find and lessen the impact of assaults on MANETs. Do what has to be done [44].

6. To fix security issues and make the program work better over time, make sure it can get patches, updates, and maintenance [45, 46].

7. Assistance and paperwork: Make sure the documentation is thorough and that users have access to all they need [47].

8. Verification and Testing: Verify that the software is working as it should and that the security mechanisms protect the MANET from a variety of threats by testing them at a comprehensive level [48].

9. Wi-Fi Inspector: A tool that provides users with the ability to scan neighboring Wi-Fi networks, even those operating in ad hoc mode, for security vulnerabilities. Although it was not designed with MANETs in mind when it was built, it can still be useful for identifying security vulnerabilities in a wireless network anyway [49].

10. If you are experiencing problems with your network or are interested in analyzing your Wi-Fi coverage, consider using NetSpot, a Wi-Fi analysis tool. It likely does not have security features specifically designed for MANETs; however, it can help make ad hoc networks operate more securely and efficiently. [50, 51]

11. With the assistance of Air cracking, a bundle of wireless security tools, it is possible to test the security of both ad hoc and standard Wi-Fi networks together. Furthermore, it is equipped with tools that can decipher encryption keys, intercept packets, and conduct various other types of attacks against networks [52].

Remember that although these techniques can improve MANET security, guarding ad hoc networks is different due to their dynamic and decentralized nature. The use of robust encryption, secure authentication procedures, and routine software and firmware updates to patch security holes is part of good network security practice, which must be supplemented with these technologies. If you need advice on how to secure your particular deployment, it's a good idea to consult with someone knowledgeable in network security and MANETs. [53]

9 VEHICULAR AD-HOC NETWORKS (VANET)

Wireless intravehicular communication between electronic devices and automobiles is enabled using various networks, including media players, GPS, cellphones, and Bluetooth, among others. Emerging technology for automobile ad hoc networks allows for communication between vehicles. As a subset of MANET and VANET differ in the following ways: Vehicles are the nodes available here. Because of this, the mobility of the vehicle, or nodes, is limited. Yet, VANET allows for a certain amount of permanent infrastructure. Because of its constraints, this infrastructure can only offer fixed network connectivity and support a subset of VANET services.

9.1 Architecture of vanets

Communication operators, content producers, and government organizations can all implement the VANET network, or they can cooperate to build a hybrid wireless communication network. The VANET architecture has been expanded to cover more ground, with the in-vehicle domain housing in-vehicle communication, the ad-hoc domain housing workshop communication, and the infrastructure domain housing vehicle-to-road communication, as defined by the European Car Communication Consortium (2C-CC). In-vehicle communication refers to the exchange of data between the user terminal and the On-Board Unit (OBU). A physical device or an OBU-integrated virtual module can serve as the user terminal. Both wired and wireless communication modes are available. Figure 4 is an example of OBU-to-OBU (V2V) and OBU-to-RSU (V2R) communication, both of which fall under the ad hoc area of workshop communication. There are two possible modes of communication, single-hop

and multi-hop. The connection between the on-board unit (OBU), remote service unit (RSU), and infrastructure (e.g., satellites, hotspots, and 3G and 4G networks) is known as vehicle-to-road communication (DSRC) [10]. A wired connection is an option for RSU [11].

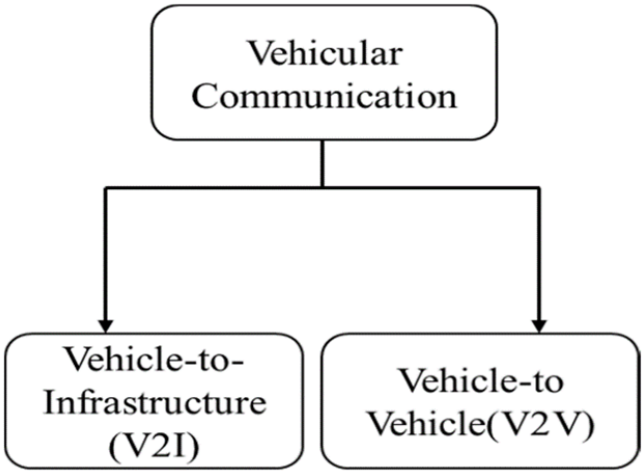

Fig. 4 VANET Communication [54]

When it comes to ITS (such as electronic toll collection systems), DSRC is a technological standard that was designed for ITS. The ISO/TC204 Intelligent Transportation System Committee is in charge of developing DSRC standards on an international level. The worldwide DSRC standard formulation is divided into three main lines: Europe, the US, and Japan [12]. The DSRC standard was begun in 1994 by the ninth working group of the European DSRC standardization working group CEN/TC278, which went on to pass the ENV12253 "5.8 GHz DSRC physical layer" standard in 1997, the ENV12795 "DSRC data link layer" standard in 1998, and the ENN12834 "DSRC application layer" standard in 1999. The work on the DSRC standard formulation was ended in 1997 by the TC204 Committee of the Japanese DSRC Standardization Working Group. Two standards, ARIB STD-T75 in 2001 and ARIB STD-T88 in 2004, were issued by them. The 5.850 5.925 GHz (75 MHz) frequency band was designated for short-range communications in the transportation services industry by the US Federal Communications Commission in 1998 [13]. Two versions of the DSRC standard, E2213-02 and E2213-03, were approved by ASTM in 2002 and 2003, respectively. The E2213-03 standard, IEEE 802.11p, and IEEE 1609 working groups started to develop standards for wireless communication in the automotive setting. Standardization for the IEEE 1609.1–1609.4 family of devices was accomplished in 2006. The official publication of the IEEE 802.11p standard occurred in July 2010. The DSRC standard consists of the physical and media access control layers that are implemented as an enhancement to the IEEE 802.11 standard; it caters to ITS-related uses [14].

Wireless local area networks (WLANs) based on 802.11a/g/n/ac can be utilized in either the infrastructure domain or the in-vehicle domain, cellular networks such as 2G, 3G, or 4G for the ad hoc domain, Bluetooth for the in-vehicle domain, and so on [15]. Applications like eCall, which utilize both a 2G network and GPS location, are examples of VANETs that may leverage several communication methods. If an eCall device detects a critical sensor signal, such as an airbag deployment, it will immediately activate the communication module and contact 112 for the agent. It will immediately begin voice contact with the nearby rescue squad and transmit the vehicle's GPS locations, accident time, license plate number, and other pertinent details. Figure 5 illustrates a typical communication in a VANET.

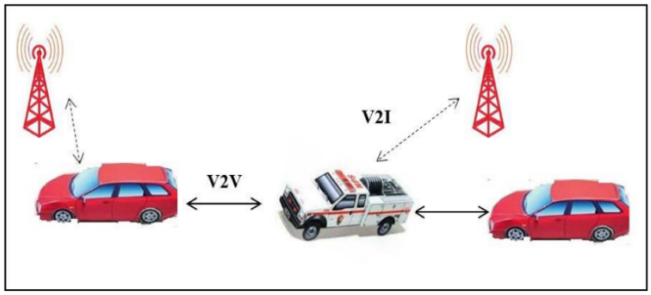

Fig. 5 typical communication in a VANET [55]

Whether it's a simplified layer consideration or a cross-layer consideration, the protocols of each layer in in-vehicle communication might vary substantially depending on the application. The most authoritative protocol architecture currently provided by IEEE is the WAVE protocol stack. It consists of the following layers: physical, data link, network, and safety. At the physical layer are IEEE 802.11p, IEEE 1609.4, and IEEE 802.2. At the network and transport layers are two sets of protocols, the traditional TCP/IP and the safety-focused IEEE 1609.3. At the application layer, safety-related applications are differentiated from non-safety applications. At the application layer, the SAE protocol is introduced as a message sublayer for safety

applications. Lastly, there is a cross-layer safety protocol, IEEE 1609.2. Figure 6 shows the characteristics of VANETs.

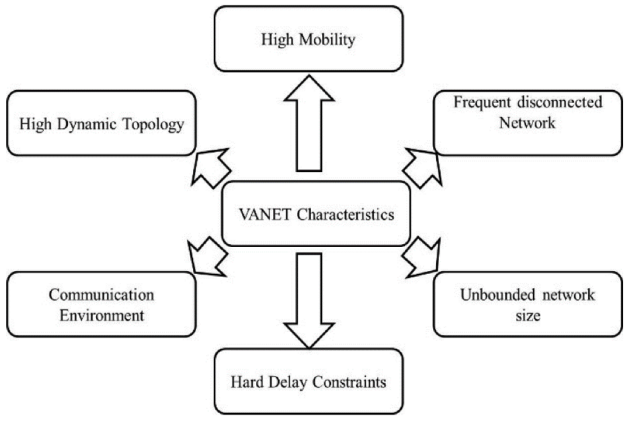

Fig. 6 Characteristics of VANET [56]

- The communication link between two vehicle nodes has a very short life period due to the fast changes in the topological structure of the onboard self-organizing network caused by the vehicles' rapid movement. Increasing the transmission power is the standard method for making a link last longer. Although doing so reduces network performance due to both the increased power consumption and the increased communication distance.

- Each node finds it impractical to acquire and preserve the global topological structure of the whole network due to the topology's fast evolution, which makes it difficult to build an accurate neighbor node list. Thus, the self-organizing network installed on the vehicle is not a good fit for the protocol that relies on the topology of the network.

9.2 Potential applications of vanets

New VANET technologies are defining a plethora of potential uses in areas such as driver assistance, efficient traffic, and safety. In VANET, there are a number of possible uses, including V2V and V2I (vehicle-to-infrastructure) communication. These applications are being examined based on whether they are safety-related or not, or on the communication techniques used (Vehicle-to-Vehicle and Vehicle-to-RSU).

- Security: The application of VANET technology aims to reduce injuries, save lives, and decrease the frequency of accidents. Warnings of impending collisions, accidents, lane departures, obstacles, vehicle breakdowns, work zones, and similar situations are all part of this category.

- Periodic Messages: So that vehicles may make decisions to attempt to avoid dangerous situations, information connected to them, such as their position, speed, and direction, is to be known to them from another environment. Accordingly, periodic messages are considered a crucial message type that aids decision-making in safety applications; yet, they may lead to undesired bandwidth usage, particularly in expansive environments, increasing the likelihood of a storm problem.

- Messages that are sent only when a harmful scenario occurs: event-driven messaging. They won't be sent unless you take that step. Priority will likely be given to communications that are based on events. Sending these messages with a higher degree of certainty to every known vehicle is the biggest issue.

10 MEASURES TO PREVENT SPOOFING IN SECURITY PROTOCOLS

Protocol Security Elements Communication integrity, secrecy, and availability can be jeopardized in a Wi-Fi Mobile Ad hoc Network (MANET) due to spoofing and relay attacks, which are major security concerns. To counter these threats, let's explain the characteristics of security protocols, attacks using Spoofing. In order to get unauthorized access or disrupt communication, an attacker can launch a spoofing attack by pretending to be a valid node in the network.

1. **Digital certificates:** Nodes have their identities verified before they can join the network using digital certificates, pre-shared keys, or biometric verification, all of which are strong authentication methods. Because of this, malicious nodes can't pose as legitimate ones [57].

2. **Secure Neighbor Discovery**: A Piece of advice is to use secure neighbor discovery methods to make sure that nodes can verify each other's identities before establishing communication links. This prevents spoofing attacks that imitate adjacent nodes from taking place [58].

3. **Intrusion Detection Systems (IDS), nodes, exchange authentication, and tracking:** Monitoring any sudden changes in network traffic to quickly thwart spoofing attacks [59], and Public Key Infrastructure (PKI) protects malicious actors from impersonating legitimate nodes [60]. When two people communicate, the identity of the other must be verified [61]. Also, it includes relay attacks between legitimate nodes and prevents tampering or disruption of the connection [62].

11 SECURITY PROTOCOL FEATURES TO MITIGATE RELAY ATTACKS

1. **Secure Channel Establishment:** if secure communication channels are created using authentication and encryption, attacks are unable to intercept or modify data packets while they are in transit. Therefore, transport layer security protocols such as DTLS or TLS can prevent relay attacks by encrypting communication channels [63].

2. **Authentication Based on Location:** By employing location-based authentication methods, nodes can conform to each other's identities just by being in close proximity to one another. As a result, attackers outside the communication range cannot launch relay attacks [64].

3. **Verifying Timestamps:** nodes can detect suspicious and unknown packet delivery delay that may indicate relay attacks by implementing protocols to verify timestamps. If timestamps are verified as recent, hence the attackers are unable to replay intercepted packets [65].

4. **Using Hop-by-Hop Authentication:** a packet is forwarded by first sending an authentication request to each intermediary node. Then by stopping unauthorized nodes from intercepting and forwarding traffic, this protects the network [56].

5. **Using Cryptographic Message Authentication:** Digital signatures or codes (MACs) guarantee that the data being sent is authentic and that its in good shape as well. This protects and shields the system against such relay attacks, in which malicious actors could insert harmful payloads or change the contents of packets [66].

By incorporating these security protocols and measure features into Wi-Fi MANETs, businesses can decrease their susceptibility to spoofing and relay attacks, and thrive towards safeguarding the networks availability, confidentiality, and communication integrity. Even though new threats and vulnerabilities can arise at any time possible so therefore it is essential to update and modify security measures on a regular basis to address them.

12 WIRELESS SECURITY IN MOBILE AD HOC NETWORKS FOR A FORMAL VERIFICATION

In order to guarantee the security of wireless (MANETs), comprehensive analysis as well as validations of security protocols, procedures and systems must be carried out using formal methodologies and mathematical models. Adding on, a mobile ad hoc network with four linked devices is shown in (figure 7). Communication between devices must first pass through the first device and this will imply that any device in the network, including devices 2,3,4 and 5 may establish a connection with the first device.

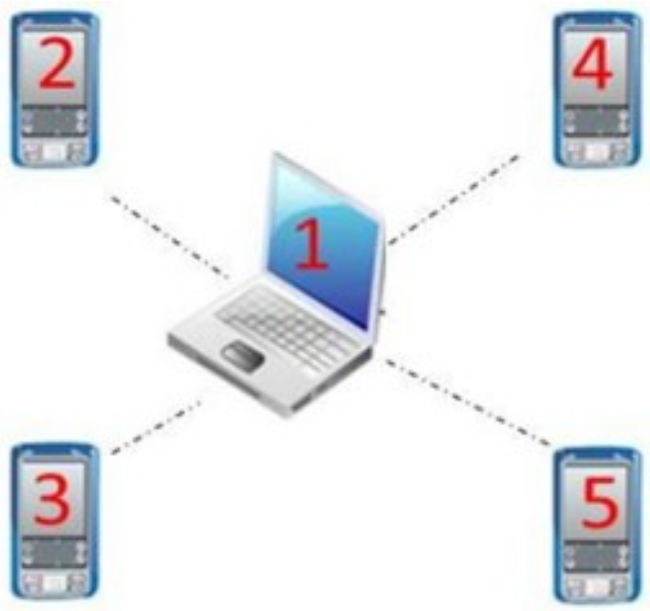

Fig. 7 Infrastructure-less Network [50]

1. **Formal Modeling:**
Specification:clearly state the MANET systems security features as well as the requirements needed for availability, integrity, secrecy and authentica-

tion. [67].
Language for Modeling: to model the security features, choose a formal language such as temporal logic (examples stating CTL,LTL), process algebra (CSP, π-calculus) or theorem proving (like Isabelle/HOL, Coq) [68].
Nodes: the MANET system needs to be modeled, this includes the communication channels with the protocols and adversaries [69].

2. **Protocol Analysis:**
Verification of Protocols: use formal techniques to assess the security protocols of the MANETS system to ensure they satisfy specific security requirements. [70].
Model checking is indeed crucial to make sure the system model has the necessary security features in every possible state and transition [71].
Equivalence Checking: verify that the formal model with the intended security features is equivalent to the original implementation [72].

3. **Theorem Proving:**
Proof Construction: create mathematical proof to show that security protocols and mechanisms are corrected in relation to certain security properties [73].
Interactive Theorem Proving: create and verify formal proof of security properties using interactive theorem proving tools [74].
Automated Theorem Proving: To automatically obtain proof or counterexamples for particular security properties, use automated theorem proving techniques [75].

4. **Model Analysis:**
To begin with Security Analysis: determine which security flaw needs to be fixed, where the MANET system model may be vulnerable, and how attacks could possibly enter the system [76]. Then comes Risk Assessment: consider how the security risks that are associated with the identified and known vulnerabilities could impact the MANET system [77].
Then Countermeasure Design: to strengthen the MANET systems defenses and address known vulnerabilities recommend security upgrades and countermeasures [78].

5. **Tool Support:** For formal verification, the following: model checking, theorem proving and security research utilize MANET-specific frameworks along with tools [79]. Now to aid with analysis and verification: modeling tools that can specifically express MANET system models in formal languages are useful for analysis and verification [80]. Finally, tools for security analysis: usage of security analysis tools helps assess how well security protocols and mechanisms guard against known security threats [81].

6. **Ensuring Accuracy and Validity:**
Starting off with Validation Testing: in order to verify the formal model and security analysis findings, use simulation testing and experimentation in real or simulated MANET environments [82]. Adding onto that is Guaranteeing accuracy and dependability: conduct expert and peer assessments of the formal model with the security features as well as the verification results to ensure accuracy and reliability is there [83]. Lastly, Ongoing Improvement: it is crucial to make constant improvements to the formal model and security verification procedure by the following: utilizing feedback, insights and lessons learnt from validation operations [84].

13 MOBILE AD HOC NETWORK WIRELESS SECURITY: A PERFORMANCE EVALUATION

Wireless security in Mobile Ad hoc Networks (MANETs) is evaluated by testing various security techniques, protocols, and systems in both real-world and simulated MANET settings. The procedure is outlined here:

1. **Selecting Metrics:**

   - **KPIs for Security:** Measurements pertaining to security should be defined. These may include packet delivery ratio, energy consumption, throughput, processing time, and bandwidth use, among others [85].
   - **Standards for Quality of Service:** When establishing security measures, it is essential to keep quality of service metrics such as dependability, jitter, and latency in mind. This is done to prevent a significant decrease in network performance [86].

- **Utilization of Resources:** In order to assess the impact that security measures have on the resources of MANET nodes, it is necessary to examine metrics such as the amount of CPU utilization, memory consumption, and battery life [87].

2. **Security Mechanism Integration:**

- The incorporation of proper security measures is the first step in the process of establishing a secure MANET simulation or emulation environment. Methods of authentication, encryption strategies, and intrusion detection systems are some examples of these [88].
- Based on your security goals and needs, configure the following parameters: key sizes, authentication timeouts, and intrusion detection levels [89].

14 CONCLUSION

Mobile ad hoc networks (MANETs) show strong potential for adaptive, real-time communication when fixed infrastructure is unavailable. At the same time, their decentralized, self-organizing design introduces significant risk. Protecting availability, confidentiality, integrity, and authenticity demand robust, well-tested defenses.

From the reviewed literature, MANETs face a broad set of threats: denial-of-service, node misbehavior, tight resource limits, rapid topology changes, spoofing, and relay/wormhole attacks. Effective responses combine secure collaboration frameworks, sound key-management practices, intrusion detection, and hardened routing. Recent work has produced distributed IDS designs, lightweight key-management protocols, and strengthened routing (e.g., AODV/DSR variants), all aimed at improving resilience and reliability in unpredictable or hostile conditions.

Security mechanisms must be validated, not assumed. Formal modeling, protocol analysis, proof when feasible, and careful performance evaluation help confirm that systems behave as intended and at acceptable cost. Equally important are simulation and experiment: realistic scenarios and attack models allow researchers to measure effectiveness, scalability, and overhead, compare alternatives fairly, and expose gaps that need correction.

Progress depends on coordination. Researchers, practitioners, industry partners, and public agencies all have roles in advancing MANET security, sharing datasets, tooling, and evaluation practices so results are reproducible and actionable.

In sum, protecting MANETs is an ongoing effort. Continued innovation, rigorous verification, and active collaboration are needed to meet evolving threats and keep ad hoc networks dependable across demanding environments.

ACKNOWLEDGEMENT

N/A

FUNDING SOURCE

No funds received.

DATA AVAILABILITY

N/A

DECLARATIONS

Conflict of interest

The authors declare that they have no known competing of interests.

Consent to publish

All authors consent to the publication.

Ethical approval

N/A

REFERENCES

[1] Brar MK, Singh S, Singh S. Security boundaries of mobile adhoc network: A systematic literature review and future aspects.In: RECENT ADVANCEMENTS IN COMMUNICATION, COMPUTING, AND ARTIFICIAL INTELLIGENCE (RACCAI-2023). vol. 3121. AIP Publishing; 2024. p. 020002. 10.1063/5.0221557

[2] Baird I, Wadhaj I, Ghaleb B, Thomson C. Impact Analysis of Security Attacks on Mobile Ad Hoc Networks (MANETs). Electronics. 2024;13(16):3314. 10.3390/electronics13163314

[3] Alyoubi AA. Enhancing Data Security in Mobile Ad-hoc Network (MANETs) Using Trust-Based Approach with RSSI and Fuzzy Logic. Mobile

Networks and Applications. 2024;29(6):2030–2046. 10.1007/s11036-024-02336-6

[4] Joshi K, Kumar K. Security Breaches Of Mobile Ad-Hoc Networks (MANET) - A Review. Educational Administration Theory and Practices. 2024. 10.53555/kuey.v30i4.1912

[5] Mukhedkar MM, Thorat VV, Mukhedkar BA, Jadhav SV, Dawande NA, Thorat CV. A Review on Development of Farmers Disease Diagnostics and Reporting Using Machine Learning Techniques. In: 2025 International Conference on Visual Analytics and Data Visualization (ICVADV). IEEE; 2025. p. 997–1000. 10.1109/icvadv63329.2025.10961552

[6] Dharani G, Prasanth N, Vasanth P, Vignesh S. A true and private security monitor for wireless ad hoc networks. Naturalista Campano, 28(1), 2951–2957.; 2024.

[7] Ahmed HA, AL-Asadi HAA. An Optimized Link State Routing Protocol with a Blockchain Framework for Efficient Video-Packet Transmission and Security over Mobile Ad-Hoc Networks. Journal of Sensor and Actuator Networks. 2024;13(2):22. 10.3390/jsan13020022

[8] Raza N, Umar Aftab M, Qasim Akbar M, Ashraf O, Irfan M. Mobile Ad-Hoc Networks Applications and Its Challenges. Communications and Network. 2016;08(03):131–136. 10.4236/cn.2016.83013

[9] Deepika S, Nishanth N, Mujeeb A. An Assessment of Recent Advances in AODV Routing Protocol Path Optimization Algorithms for Mobile Ad hoc Networks. In: 2021 Fourth International Conference on Microelectronics, Signals & Systems (ICMSS). IEEE; 2021. p. 1–6. 10.1109/icmss53060.2021.9673632

[10] Sreenivasulu K, Gayatri K, Kundana K. In: A Secure AOMDV Protocol's Design and Implementation in Mobile Adhoc Network Cryptography. CRC Press; 2024. p. 16–21. 10.1201/9781032665535-4

[11] Safari F, Savic I, Kunze H, Ernst J, Gillis D. The Diverse Technology of MANETs: A Survey of Applications and Challenges. International Journal of Future Computer and Communication. 2023:37–48. 10.18178/ijfcc.2023.12.2.601

[12] Vargheese M, Bhatia S, Basheer S, Dadheech P. Improved Multi-Path Routing for QoS on MANET. Computer Systems Science and Engineering. 2023;45(3):2521–2536. 10.32604/csse.2023.031476

[13] Soomro AM, Naeem AB, Senapati B, Bashir K, Pradhan S, Ghafoor MI, et al. In MANET: An Improved Hybrid Routing Approach for Disaster Management. In: 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T). IEEE; 2023. p. 1–6. 10.1109/icest56843.2023.10138831

[14] Korir FC, Cheruiyot W. A survey on security challenges in the current MANET routing protocols. Global Journal of Engineering and Technology Advances. 2022;12(1):078–091. 10.30574/gjeta.2022.12.1.0114

[15] Sangheethaa S. A Comparative Study for Block Chain Applications in the MANET. International Journal on AdHoc Networking Systems. 2023;13(03):1–7. 10.5121/ijans.2023.13301

[16] Deebak B, Al-Turjman F. A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Networks. 2020;97:102022. 10.1016/j.adhoc.2019.102022

[17] Barman MR, Chakraborty D, Das JK. In: Reactive and Proactive Routing Protocols Performance Evaluation for MANETS Using OPNET Modeler Simulation Tools. Springer Nature Switzerland; 2023. p. 285–293. 10.1007/978-3-031-34622-4_22

[18] Hassen OA, Ibrahim H. Preventive Approach against HULK Attacks in Network Environment. International Journal of Computing and Business Research. 2017;7(3)

[19] Jain R. Ant Colony Inspired Energy Efficient OLSR (AC-OLSR) Routing Protocol in MANETS. Wireless Personal Communications. 2022;124(4):3307–3320. 10.1007/s11277-022-09514-3

[20] Bhuvaneswari R, Ramachandran R. Denial of service attack solution in OLSR based manet by varying number of fictitious nodes. Cluster Computing. 2018;22(S5):12689–12699. 10.1007/s10586-018-1723-0

[21] Wheeb AH, Al-jamali NA. Performance Analysis of OLSR Protocol in Mobile Ad Hoc Networks. International Journal of Interactive Mobile Technologies (iJIM). 2022;16(01):106–119. 10.3991/ijim.v16i01.26663

[22] Haridas S, Prasath DAR. Bi-Fitness Swarm Optimizer: Blockchain Assisted Secure Swarm Intelligence Routing Protocol for MANET. Indian Journal of Computer Science and Engi-

neering. 2021;12(5):1442–1458. 10.21817/indjcse/2021/v12i5/211205158

[23] Venkatasubramanian S, Suhasini A, Hariprasath S. Detection of Black and Grey Hole Attacks Using Hybrid Cat with PSO-Based Deep Learning Algorithm in MANET. International Journal of Computer Networks and Applications. 2022;9(6):724. 10.22247/ijcna/2022/217705

[24] Ghodichor N, V RT, Sahu D, Borkar G, Sawarkar A. Secure Routing Protocol to Mitigate Attacks by using Blockchain Technology in MANET. International journal of Computer Networks & Communications. 2023;15(2):127–146. 10.5121/ijcnc.2023.15207

[25] Vivekananda GN, Reddy PC. Efficient video transmission technique using clustering and optimisation algorithms in MANETs. International Journal of Advanced Intelligence Paradigms. 2023;25(3/4):248–263. 10.1504/ijaip.2023.132371

[26] Sharma RS, Keswani B, Goyal D. Hybrid model for Protocol Independent Secure Video Transmission using improvised OSLR with optimized MPR and DYDOG. Journal of Algebraic Statistics. 2022;13(2):1669-79

[27] Qin R, Li X. In: Parameter Optimization for Neighbor Discovery Probability of Ad Hoc Network Using Directional Antennas. Springer Nature Singapore; 2022. p. 523–536. 10.1007/978-981-16-8656-6_47

[28] Trofimova Y, Tvrdík P. Enhancing Reactive Ad Hoc Routing Protocols with Trust. Future Internet. 2022;14(1):28. 10.3390/fi14010028

[29] Khalfaoui H, Farchane A, Safi S. Review in authentication for mobile ad hoc network. In: Advances on Smart and Soft Computing: Proceedings of ICACIn 2021. Springer; 2021. p. 379-86

[30] Malnar M, Jevtic N. An improvement of AODV protocol for the overhead reduction in scalable dynamic wireless ad hoc networks. Wireless Networks. 2022;28(3):1039–1051. 10.1007/s11276-022-02890-5

[31] Thirumurugan S, Gnanadurai JB. In: Cloud Computing Model on Wireless Ad Hoc Network Using Clustering Mechanism for Smart City Applications. Springer International Publishing; 2021. p. 123–145. 10.1007/978-3-030-66607-1_7

[32] Sorribes JV, Lloret J, Peñalver L. Analytical models for randomized neighbor discovery protocols based on collision detection in wireless ad hoc networks. Ad Hoc Networks. 2022;126:102739. 10.1016/j.adhoc.2021.102739

[33] Li Q, He D, Yang Z, Xie Q, Choo KKR. Lattice-Based Conditional Privacy-Preserving Authentication Protocol for the Vehicular Ad Hoc Network. IEEE Transactions on Vehicular Technology. 2022;71(4):4336–4347. 10.1109/tvt.2022.3147875

[34] Nourildean SW, Mohammed YA, Salih AM. Mobile Ad Hoc Network Improvement against Jammers for Video Applications Using Riverbed Modeler (v17.5). Webology. 2022;19(1):1446–1459. 10.14704/web/v19i1/web19096

[35] Kaur M, Prashar D, Rashid M, Khanam Z, Alshamrani SS, AlGhamdi AS. An Optimized Load Balancing Using Firefly Algorithm in Flying Ad-Hoc Network. Electronics. 2022;11(2):252. 10.3390/electronics11020252

[36] Singh S, Saini HS. Intelligent Ad-Hoc-On Demand Multipath Distance Vector for Wormhole Attack in Clustered WSN. Wireless Personal Communications. 2021;122(2):1305–1327. 10.1007/s11277-021-08950-x

[37] Ravindranath B, Murthy BRN, Ramu HC, Nambiar S S. Process Parameters Optimization of Pin and Disc Wear Test to Minimize the Wear Loss of General-Purpose Aluminium grades by Taguchi and simulation through Response Surface Methodology. Engineered Science. 2021. 10.30919/es8d605

[38] Anand R, Singh J, Pandey D, Pandey BK, Nassa VK, Pramanik S. In: Modern Technique for Interactive Communication in LEACH-Based Ad Hoc Wireless Sensor Network. Springer International Publishing; 2022. p. 55–73. 10.1007/978-3-030-91149-2_3

[39] Al-Absi MA, Al-Absi AA, Sain M, Lee H. Moving Ad Hoc Networks—A Comparative Study. Sustainability. 2021;13(11):6187. 10.3390/su13116187

[40] Li S, Hu X, Jiang T, Zhang R, Yang L, Hu H. Hop Count Distribution for Minimum Hop-Count Routing in Finite Ad Hoc Networks. IEEE Transactions on Wireless Communications. 2022;21(7):5317–5332. 10.1109/twc.2021.3139350

[41] Rani P, Kavita, Verma S, Kaur N, Wozniak M, Shafi J, et al. Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks. Sensors. 2021;22(1):251. 10.3390/s22010251

[42] Liu B, Shen M. Some geometrical and topological properties of DNNs' decision boundaries. Theoretical Computer Science. 2022;908:64–75. 10.1016/j.tcs.2021.11.013

[43] Kafetzis D, Vassilaras S, Vardoulias G, Koutsopoulos I. Software-Defined Networking Meets Software-Defined Radio in Mobile ad hoc Networks: State of the Art and Future Directions. IEEE Access. 2022;10:9989–10014. 10.1109/access.2022.3144072

[44] Zhang S, Li X, Liu Y. In: Analysis of Scheduling Delay and Throughput of Multiple Radio Multiple Access Protocols in Wireless Ad Hoc Networks. Springer Singapore; 2021. p. 5419–5428. 10.1007/978-981-15-8155-7_447

[45] Han L. Wireless ad-hoc networks. Wireless Personal Communication Journal of mobile communication and computing. 2004;4

[46] Liu R, Li X. In: Research on Reliability Assurance Mechanism of MAC Layer Control Messages in Wireless Ad Hoc Networks. Springer Singapore; 2021. p. 5301–5310. 10.1007/978-981-15-8155-7_437

[47] Chauhan K, Yadav K, Singh A. Review on secure ad-hoc networks for wireless sensor network. In: ICT with Intelligent Applications: Proceedings of ICTIS 2021, Volume 1. Springer; 2021. p. 145-53

[48] Srilakshmi U, Alghamdi SA, Vuyyuru VA, Veeraiah N, Alotaibi Y. A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access. 2022;10:14260-9

[49] Ergenç D, Onur E. Plane-separated routing in ad-hoc networks. Wireless Networks. 2022;28(1):331-53

[50] Vitalkar RS, Thorat SS, Rojatkar DV. In: Intrusion Detection for Vehicular Ad Hoc Network Based on Deep Belief Network. Springer Nature Singapore; 2021. p. 853–865. 10.1007/978-981-16-3728-5_64

[51] Sahu SR, Tripathy B. In: A Survey on AGPA Nature-Inspired Techniques in Vehicular Ad-Hoc Networks. Springer Nature Singapore; 2023. p. 729–740. 10.1007/978-981-19-5936-3_68

[52] Kharchenko V, Grekhov A, Kondratiuk V. Traffic Simulation in SAGIN Air Segment Containing Ad Hoc Network of Flying Drones. 2022. 10.20944/preprints202201.0161.v1

[53] Li H, Li X, Jing T. In: Design and Analysis of Low Signaling Overhead Multiple Access Protocol for Wireless Ad Hoc Networks. Springer Singapore; 2021. p. 5325–5336. 10.1007/978-981-15-8155-7_439

[54] Kumar A, Sharma N, Kumar A. End-to-end authentication based secure communication in vehicular ad hoc networks (VANET). Journal of Discrete Mathematical Sciences and Cryptography. 2022;25(1):219–229. 10.1080/09720529.2021.2014147

[55] Hamdi MM, Jassim SA, Abdulhakeem BS. Successful Delivery Using Stable Multi-Hop Clustering Protocol for Energy Efficient Highway VANETs. In: 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). IEEE; 2023. p. 1–6. 10.1109/ismsit58785.2023.10304927

[56] Pandey MR, Mishra RK, Shukla AK. An improved node mobility patten in wireless ad hoc network. In: Applied Information Processing Systems: Proceedings of ICCET 2021. Springer; 2021. p. 361-70

[57] Nagpal S, Aggarwal A, Gaba S. In: Privacy and Security Issues in Vehicular Ad Hoc Networks with Preventive Mechanisms. Springer Nature Singapore; 2022. p. 317–329. 10.1007/978-981-16-7136-4_24

[58] Santhi S, Udayakumar E, Gowthaman T. In: SOS Emergency Ad Hoc Wireless Network. Springer International Publishing; 2018. p. 227–234. 10.1007/978-3-030-02674-5_15

[59] Shantaf AM, Kurnaz S, Mohammed AH. Performance Evaluation of Three Mobile Ad-hoc Network Routing Protocols in Different Environments. In: 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE; 2020. p. 1–6. 10.1109/hora49412.2020.9152845

[60] Sarkar D, Choudhury S, Majumder A. Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network. Journal of King Saud University - Computer and Information Sciences. 2021;33(10):1186–1201. 10.1016/j.jksuci.2018.08.013

[61] Khudair Madhloom J, Abd Ali HN, Hasan HA, Hassen OA, Darwish SM. A Quantum-Inspired Ant Colony Optimization Approach for Exploring Routing Gateways in Mobile Ad Hoc Networks. Electronics. 2023;12(5):1171. 10.3390/electronics12051171

[62] Darch Abed Dawar A. Enhancing Wireless Security and Privacy: A 2-Way Identity Authentication Method for 5G Networks. International Journal of Mathematics, Statistics, and Computer Science. 2024;2:183–198. 10.59543/ijmscs.v2i.9073

[63] Gurumekala T, Indira Gandhi S. Toward in-flight Wi-Fi: a neuro-fuzzy based routing approach for Civil Aeronautical Ad hoc Network. Soft Computing. 2022;26(15):7401–7422. 10.1007/s00500-021-06677-2

[64] Shang J, Liu Y, Tong X. In: Research on Network Overhead of Two Kinds of Wireless Ad Hoc Networks Based on Network Fluctuations. Springer Nature Singapore; 2022. p. 584–595. 10.1007/978-981-16-8656-6_52

[65] Elaryh Makki Dafalla M, Mokhtar RA, Saeed RA, Alhumyani H, Abdel-Khalek S, Khayyat M. An optimized link state routing protocol for real-time application over Vehicular Ad-hoc Network. Alexandria Engineering Journal. 2022;61(6):4541–4556. 10.1016/j.aej.2021.10.013

[66] Alzahrani E, Bouabdallah F, Almisbahi H. State of the Art in Quorum-Based Sleep/Wakeup Scheduling MAC Protocols for Ad Hoc and Wireless Sensor Networks. Wireless Communications and Mobile Computing. 2022;2022(1):6625385

[67] Katiyar A, Singh D, Yadav RS. Advanced multi-hop clustering (AMC) in vehicular ad-hoc network. Wireless Networks. 2021;28(1):45–68. 10.1007/s11276-021-02822-9

[68] Wheeb AH, Nordin R, Samah AA, Alsharif MH, Khan MA. Topology-Based Routing Protocols and Mobility Models for Flying Ad Hoc Networks: A Contemporary Review and Future Research Directions. Drones. 2021;6(1):9. 10.3390/drones6010009

[69] Benjbara C, Habbani A, Mouchfiq N. New multipath OLSR protocol version for heterogeneous ad hoc networks. Journal of Sensor and Actuator Networks. 2021;11(1):3

[70] Vijayalakshmi P, Nguyen TN, Abraham Dinakaran J, Cengiz K. Towards sustainable energy efficient routing for dynamic ad-hoc communications in smart cities. Measurement. 2022;189:110623. 10.1016/j.measurement.2021.110623

[71] Jeyaram G, Madheswaran M. In: Message Propagation in Vehicular Ad Hoc Networks: A Review. Springer Nature Singapore; 2022. p. 207–218. 10.1007/978-981-16-4863-2_18

[72] Khankhour H, Abdoun O, Abouchabaka J. In: A New Design of an Ant Colony Optimization (ACO) Algorithm for Optimization of Ad Hoc Network. Springer Singapore; 2021. p. 231–241. 10.1007/978-981-16-3637-0_16

[73] Srinivas M, Patnaik MR. Clustering with a high-performance secure routing protocol for mobile ad hoc networks. The Journal of Supercomputing. 2022;78(6):8830–8851. 10.1007/s11227-021-04258-6

[74] Ponnusamy V, Humayun M, Z Jhanjhi N, Yichiet A, Fahhad Almufareh M. Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks. Computer Systems Science and Engineering. 2022;40(3):1199–1215. 10.32604/csse.2022.018518

[75] Chaubey NK, Yadav D. Detection of Sybil attack in vehicular ad hoc networks by analyzing network performance. International Journal of Electrical and Computer Engineering (IJECE). 2022;12(2):1703. 10.11591/ijece.v12i2.pp1703-1710

[76] Sarikonda S, Shyamala K, Nigam P. Test bed implementation of energy efficient load balanced AOMDV routing protocol in wireless sensor networks. SSRN 4015626.; 2022.

[77] Khezri E, Zeinali E, Sargolzaey H. A Novel Highway Routing Protocol in Vehicular Ad Hoc Networks Using VMaSC-LTE and DBA-MAC Protocols. Wireless Communications and Mobile Computing. 2022;2022(1). 10.1155/2022/1680507

[78] Suo W, Wang M, Zhang D, Qu Z, Yu L. Formation Control Technology of Fixed-Wing UAV Swarm Based on Distributed Ad Hoc Network. Applied Sciences. 2022;12(2):535. 10.3390/app12020535

[79] Lee B, Lee IG, Kim M. FIT: Design and Implementation of Fast ID Tracking System on Chip for Vehicular Ad-hoc Networks. Wireless Personal Communications. 2022;124(2):1645–1659. 10.1007/s11277-021-09424-w

[80] Fayaz M, Mehmood G, Khan A, Abbas S, Fayaz M, Gwak J. Counteracting Selfish Nodes Using Reputation Based System in Mobile Ad Hoc Networks. Electronics. 2022;11(2):185. 10.3390/electronics11020185

[81] Temene N, Sergiou C, Georgiou C, Vassiliou V. A Survey on Mobility in Wireless Sensor Networks. Ad Hoc Networks. 2022;125:102726. 10.1016/j.adhoc.2021.102726

[82] Michoagan SG, Mali S, Gore S. Salient features selection techniques for instruction detection in mobile ad hoc networks. Tehnički glasnik. 2022;16(1):40-6

[83] Rao RS, Das S, et al. Fog computing environment in flying ad-hoc networks: concept, framework, challenges, and applications. Cloud computing enabled big-data analytics in wireless ad-hoc networks. 2022:31-48

[84] Chiejina E, Xiao H, Christianson B, Mylonas A, Chiejina C. A Robust Dirichlet Reputation and Trust Evaluation of Nodes in Mobile Ad Hoc Networks. Sensors. 2022;22(2):571. 10.3390/s22020571

[85] Nawej CM, Owolawi PA, Walingo T. In: Enhanced AODV Routing Protocol for Intelligent Attack Mitigation in Vehicular Ad-Hoc Networks. Springer Singapore; 2021. p. 733–744. 10.1007/978-981-16-2102-4_66

[86] Kanthimathi N, Roshini Roy J, Saranya N, Sandhya P. In: Trust-Based Security Scheme Using Fuzzy Clustering for Vehicular Ad Hoc Networks. Springer Singapore; 2021. p. 425–436. 10.1007/978-981-16-5301-8_32

[87] Kurumbanshi S, Rathkanthiwar S, Patil S. Packet Arrival Analysis using Pareto and Exponential Distribution in Wireless Adhoc Networks. In: 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC). IEEE; 2021. p. 338–343. 10.1109/icsccc51823.2021.9478159

[88] Yoshikawa T, Komura H, Nishiwaki C, Goto R, Matama K, Naito K. Evaluation of new CYPHONIC: Overlay network protocol based on Go language. In: 2022 IEEE International Conference on Consumer Electronics (ICCE). IEEE; 2022. p. 1–6. 10.1109/icce53296.2022.9730323

[89] Rajendran A, Balakrishnan N, P A. Deep embedded median clustering for routing misbehaviour and attacks detection in ad-hoc networks. Ad Hoc Networks. 2022;126:102757. 10.1016/j.adhoc.2021.102757

How to cite this article

Mashhadani S , Hassen OA, Alhakam I. Mobile ad hoc network wireless security: problems, solutions, and application: state-of-the-art. Journal of University of Anbar for Pure Science. 2025; 19(2):134-150. doi:10.37652/juaps.2024.153957.1323