EXPLORING MANET SECURITY ASPECTS: ANALYSIS OF ATTACKS AND NODE MISBEHAVIOUR ISSUES

Burhan Ul Islam Khan[1*], Farhat Anwar[2], Farah Diyana Bt. Abdul Rahman[3], Rashidah Funke Olanrewaju[4], Miss Laiha B. Mat Kiah[5], Md Arafatur Rahman[6], Zuriati Janin[7]

[1,2,3,4]Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia (IIUM), Kuala Lumpur, 50728, Malaysia

[5]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya (UM), Kuala Lumpur, 50603, Malaysia

[6]Faculty of Computing, Universiti Malaysia Pahang (UMP), Pekan, Pahang, 26600, Malaysia

[7]Faculty of Electrical Engineering, Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, 40450, Malaysia

E-mail: burhan.iium@gmail.com[1*] (corresponding author), farhat@iium.edu.my[2], farahdy@iium.edu.my[3], frashidah@iium.edu.my[4], misslaiha@um.edu.my[5], arafatiium@gmail.com[6], zuriaty@uitm.edu.my[7]

DOI: https://doi.org/10.22452/mjcs.vol35no4.2

ABSTRACT

Mobile ad hoc networks are susceptible to various security threats due to their open media nature and mobility, making them a top priority for security measures. This paper provides an in-depth examination of MANET security issues. Some of the most critical aspects of mobile ad hoc networks, including their applications, have been discussed. This is followed by a discussion of MANETs' design vulnerability to external and internal security threats caused by inherent network characteristics such as limited battery power, mobility, dynamic topology, open media, and so on. Numerous MANET-related attacks have been classified based on their sources, behaviour, participating nodes, processing capability, and layering. The many different types of misbehaviour a node can exhibit and the various ways a node can behave were investigated. Two major types of MANETs misbehaviour have been evaluated, classified and analysed. Notably, mitigating node misbehaviour in MANET is a critical issue that must be addressed to ensure network node functionality and availability. Strategies for detecting network nodes that misroute packets are also examined. Finally, the paper emphasises the need for effective solutions to secure MANETs.

Keywords: Mobile Ad hoc Network (MANET), Intrusion Detection System, Node Misbehaviour, Incentive-based mechanisms.

1.0 INTRODUCTION

Mobile Ad Hoc Networks (or MANETs) are self-organising, infrastructure-free, self-configuring networks of mobile devices connected wirelessly via cellular, Wi-Fi, local Radio Frequency (RF) communication channels, etc. (depicted in Figure 1). As MANETs are self-organising and self-configuring, nodes are not constrained and are free to move around to form random and transient "ad hoc" network topologies. In MANETs, networking performance relies heavily on the cooperation of all member nodes. Due to its infrastructure-less nature, all the networking tasks, including management of nodal mobility, multi-hop packet delivery, and routing, must be done individually or collectively by the member nodes. Examples of MANET applications can be found in military wireless networks, large-scale civilian applications, rescue operations, and other emergencies [1].

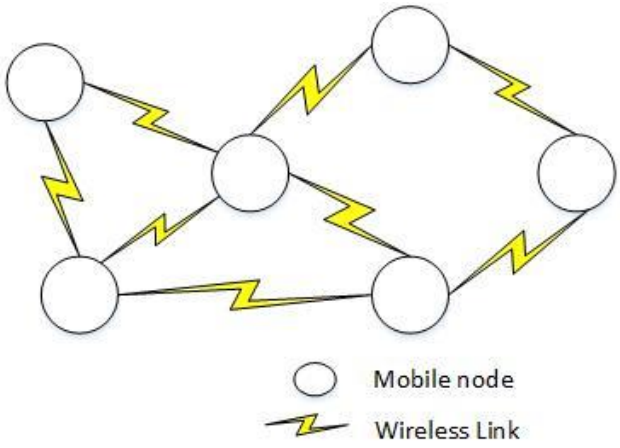

Fig. 1: A mobile ad hoc network

The MANETs can be categorised as either "closed MANETs" or "open MANETs" [2]. As in civilian applications, an open MANET comprises multiple users with diverse aims to share their resources to connect globally. Closed MANETs, being different from open MANETs, are governed by a single authority, share the same purposes, and work together to benefit the entire group. A MANET's open environment can lead to misbehaving nodes.

In MANETs, communication among nodes can occur either directly or indirectly. Thus, MANET offers two kinds of networks: single-hop and multi-hop [3]. In single-hop networks, all nodes lie within a range and may interact directly, referred to as direct communication. However, in a multi-hop network, nodes depend on neighbours to establish connections outside the transmission range, a process called indirect communication [4]. Communication in a network is based on mutual trust, and communication can only be successful if each node cooperates with another for data transfer. As more nodes cooperate to move traffic, MANETs become more powerful. However, maintaining a MANET is an expensive activity for a mobile node. Local CPU time, network bandwidth, energy, and memory are consumed while identifying routes and forwarding messages [5]. As a result, a node has a solid incentive to refuse packet forwarding to others, yet they expect to receive it when they want services from other nodes.

MANET has a lot of applications, but securing it remains a challenge. MANETs are more sensitive to physical security and information than permanently wired networks due to their mobility and wireless nature. In addition, security solutions designed for permanently wired networks are difficult to adapt to mobile wireless networks. This study seeks to identify and illustrate the inherent security difficulties of MANET and the existing and suggested solutions to these challenges.

The following is how the paper is sectioned: Section 1 provides an overview of MANET, including its intrinsic characteristics, application areas, and design restrictions that result from these characteristics. The classification and consideration of various types of security attacks that may be launched in MANET are described in Sections 2 and 3. Section 4 discusses node misbehaviour in mobile ad hoc networks and the causes and consequences. Section 5 provides a high-level overview of the various methodologies used to identify node misbehaviour in MANETs. Several strategies for detecting node misbehaviour in MANET are described in Section 6. Finally, in Section 7, the article finishes with some closing thoughts and future research directions.

1.1 Characteristics of MANETs

All MANETs share common traits with wireless networks in general, as well as ad hoc networks in specific [3], [6]:

- Wireless: Wireless links are used by network nodes to communicate through shared media such as radio or infrared.
- Ad hoc-based: When the need arises, a group of nodes in MANETs build a temporary network dynamically and randomly.
- Self-contained and infrastructure-free: In contrast to any current infrastructure or centralised management based technology, MANET is entirely self-contained. Each node communicates with others in a distributed peer-to-peer network, functions as a standalone router, and produces its data.

- Autonomous and infrastructure-less: MANET is entirely self-contained and does not require any additional infrastructure. Each node in a dispersed peer-to-peer network connects with the other nodes, serves as an independent router, and creates its information.
- Multi-hop routing: In a MANET, specialised routers are not required. Every node also functions as a router and forwards packets from other network nodes to allow mobile hosts to share information.
- Mobility: In a MANET, nodes can move around randomly, even if communication is active. As nodes move about, the topology changes. The ad hoc network is a fluid system. As a result, node-to-node transmission-reception patterns change.

1.2 Applications of MANETs

Mobile ad hoc networking is proliferating due to the rise in portable devices and advancements in wireless communication and its constantly growing area of possible applications [7]. Mobile ad hoc networking, with its customisable networks, allows users to connect anywhere and at any time. Mobile ad hoc networking allows nodes to maintain network connections while effectively adding and removing nodes from the network.

The development of smartphones and tablets over the last decade has resulted in them being versatile computing platforms that rely only on wireless connectivity. They have mostly replaced low-end mobile PCs and personal digital assistants. The ad hoc concept has played a crucial role in supporting this development. Many studies have looked at various aspects of mobile ad hoc networks, like routing methods, quality of service, and security concerns. However, there are a few research studies on existing and prospective mobile ad hoc communication.

The following briefly reviews some mobile ad hoc communications applications and areas of interest [8].

1.2.1 Vehicular Networking

A vehicular ad hoc network (VANET) provides several network services to vehicles and ensures information exchange between vehicles in this application area [9].

There are two fundamental communication techniques in VANETs. Vehicle-to-Vehicle (V2V) communication is the first communication method of VANETs, and it has applications in lane changes, convoy driving, and other safety services. For example, when a vehicle detects a new event (such as an accident), it tells other cars of the change in traffic conditions, assisting drivers in making decisions.

The second method is Vehicle-to-Infrastructure (V2I). During V2I, infrastructure performs a coordination function by receiving information about global or local traffic patterns and road conditions and then suggesting or enforcing specific driving behaviours on a group of automobiles. For example, ramp metering is a commonly used approach that requires only a few actuators and sensors to be effective.

Finally, VANETs provide convenient features by providing Internet access and directing cars to nearby parking places [10]. VANETs also incorporate Vehicle-to-Broadband Cloud communication (V2B), which entails short-range communication between passengers' devices and the vehicle using a variety of technologies, including Bluetooth [11], 3G cellular telephony [12], LTE [13], and WiMAX [14].

1.2.2 Urban Sensing

With wireless sensor networking, research is moving from static networks of special devices to network technologies that use robotic or other forms of restrained mobility to adapt to the people-centric approach and environmental conditions [15] that consider people's mobility.

In the area of Wireless Sensor Networks (WSN), initiatives are being proposed on one level to improve infrastructure efficiency. Still, on another level, citizens with sensing capabilities can make urban processes more efficient by monitoring their consumption patterns, transportation patterns, and energy consumption. A growing research community is devising techniques for very large-scale urban sensing using consumer devices such as smartphones that offer enhanced sensor capabilities. The data captured by these mobile sensors are used for exciting people-centric applications and projects, including MIT Senseable City Lab [16], the Intel Urban Atmospheres project [17], and the Google Street View [18].

1.2.3 Ubiquitous Computing

Ubiquitous, sometimes known as pervasive, refers to something that is "existing everywhere" [19]. Unlike desktop computing, ubiquitous computing may occur in any location, device, and format. This paradigm is the product of exponentially increasing computer technology to integrate computing into the environment.

At their core, all ubiquitous computing models have a vision of small processing devices dispersed across all scales in daily life. For example, a smart housing environment might connect heating controls with personal biometric monitoring woven into clothes, allowing for continuous and imperceptible modulation of room environment settings [20].

Another example is solutions that let a smartphone control a television set-top box via an Internet connection, even if the two devices are located several feet apart.

1.2.4 Network Extension

Ad hoc networks are utilised in this application to improve the performance of networks with insufficient coverage [21]. Both service providers and users will gain from the addition of an ad hoc extension to the access network. While some nodes connect directly to an Access Point (AP), others may connect to the Internet by sending and receiving data packets through those intermediate nodes. In this scenario, the most well-known method for network expansion and Internet access is Wireless Mesh Networks (WMNs) [22]. These networks provide stationary and mobile consumers with low-cost wireless broadband Internet access [23].

WMN nodes may interact with one another directly without requiring an Internet connection. Consequently, even if one node fails, the other nodes can still interact with one another, either directly or via one or more intermediary nodes. As a result, WMNs provide scalable coverage, high fault tolerance, and inexpensive installation costs, all of which can be used to expand network service coverage.

1.2.5 Wireless Body Area Network (WBAN)

The wireless body area network field is a multidisciplinary field where medical data may be updated in real-time through the Internet, allowing for continuous and low-cost health monitoring. Wearable health monitoring devices incorporated into a telehealth system are a new type of information technology that can help with the early diagnosis of aberrant situations and the prevention of significant repercussions [24]. By augmenting paper charts and back-end storage systems, patient data such as identity, medical history, and treatment can be stored in wearable sensor nodes. These networks can considerably increase first responders' ability to treat multiple casualties in a Mass Casualty Event (MCE). These networks can help first rescuers treat more patients with wearable wireless monitoring in an MCE [25].

1.2.6 Wireless Personal Area Network (WPAN)

Ad hoc networks allow a group of unconnected data devices to communicate without centralised management. WPAN communications are generally limited to a person or object up to 10 metres in all directions [26]. WPANs have the potential to connect all the communication nodes that many individuals have on their desks or in their pockets today.

Smart Phone Ad hoc Network (SPAN) is a peer-to-peer (P2P) network built using existing technology in commercially available smartphones to avoid the need for wireless access points or cellular carrier networks for personal use. These differ from conventional hub-and-spoke networks such as Wi-Fi Direct [27] in that it permits peers to enter and leave the network instantly without causing damage to the network.

The Near Field Communication (NFC) technology, which enables two NFC-enabled devices to converse and exchange information in an ad hoc manner [28], is another model of WPANs applications. This contactless technology enables devices to connect with a simple tap or touch, allowing them to perform various functions such as cashless payment, peer-to-peer data transfer, loyalty and membership identification, and other real-time applications.

Besides, MANETs can be deployed in [7]:

Emergency services:

- Ad hoc networks may be utilised as a replacement for permanent infrastructure in the event of a natural disaster.
- Emergency rescue operations.
- Firefighting and policing.
- Support for doctors and nurses in hospitals.

Tactical networks:

- Military equipment increasingly involves computers. Ad hoc networking allows the military to employ standard network technology to connect soldiers, vehicles, and command centres. The ad hoc network's core techniques came from here.
- Battlefields that are fully automated through mobile ad hoc networks.

Commercial, civilian and education environments:

- In airport visitor networks, MANETs are used to connect people.
- Asynchronous networking in virtual classrooms, institutions, and on-campus environments.
- On-the-fly communication during meetings or presentations.

1.3 MANET Design Issues and Constraints

MANETs are subject to a wide variety of assaults and threats in addition to most of the well-known attacks and threats that wired and wireless networks have faced. The following are the various open design and security issues for MANET [6], [29], [30]:

1.3.1 Infrastructure-less

MANETs are self-contained networks and do not need additional infrastructure. No centralised managerial authority exists. Administration and problem identification are difficult because a node's communication ability depends entirely on its willingness to participate.

1.3.2 Dynamically Varying Network Topologies

Because nodes in mobile ad hoc networks can move freely, the network topology frequently changes, causing network partitions, route unavailability, overall performance decrease and packet loss.

1.3.3 Physical Layer Restraint

Using the radio interface, every node broadcasts the transmitted packets. The radio interface has a limited wireless transmission range, which causes problems with mobile ad hoc networks like hidden and exposed terminals. Furthermore, when opposed to wired systems, the wireless channel is open and shared, which increases the chances of collisions and packet loss due to transmission faults.

1.3.4 Link Bandwidth and Quality Constraints

The communication environment for mobile nodes includes bandwidth limits, varied capacity for each node, open wireless channels, and greater error rates. Wireless networks have lesser capacity than traditional links, resulting in congestion.

1.3.5 Node and Link Capabilities Variation

Every node has one or multiple radio interfaces. Each interface operates in a distinct frequency band and has various transmission/receiving capabilities. Because each node's radio capabilities are different, asymmetric linkages are formed. In addition, each mobile node's software and hardware configurations vary, resulting in differing processing

capabilities for each node. As a result, it is challenging to develop network protocols and algorithms for heterogeneous networks because they must take into account a variety of variables throughout time, including traffic distribution/load variations, changing power and channel conditions, congestion, service environments, and load balancing.

1.3.6 Energy Constrained Operation

The mobile node runs on battery power, which is a finite resource. The processing power of a mobile node is restricted. As a result, each node offers services and applications that are constrained. In a MANET, a node faces a more significant problem because every node serves as an end system and a router. Extra energy is necessary for packet forwarding in the network.

1.3.7 Network Reliability and Robustness

In a MANET, nodes are accountable for network connectivity. Nodes are in charge of routing and forwarding. However, this does not eliminate the limitations of fixed infrastructure connectivity and presents design issues. An individual node might not succeed in forwarding the packet due to various factors such as overload, selfish behaviour, or broken links. Misbehaving nodes and unstable links can severely harm the performance of a network. Because there are no centralised monitoring and administration points, these misbehaviours are challenging to detect and isolate, making the protocol design further complex.

1.3.8 Network Security

Information and physical security threats are more common on mobile wireless networks than fixed-wire line networks. Because wireless broadcast channels are open and shared, nodes with insufficient physical protection are vulnerable to security attacks. Furthermore, since a MANET lacks infrastructure, it relies heavily on nodes. Some crucial security essentials in ad hoc networking comprise:

- Confidentiality: Only the intended receivers can see the information.
- Access control: Only authorised individuals have access to wireless transmission.
- Data integrity: Information cannot be tampered with. There is no way to access, change, or insert traffic.
- Malicious nodes launch Denial-of-Service attacks.

1.3.9 Network Scalability

Moving from a small network of nodes to an extensive network with restricted resources is difficult. It poses numerous challenges in areas like location management, routing, interoperability, addressing, and security, to name a few.

1.3.10 Quality of Service

For multimedia network traffic to be transmitted successfully, Quality of Service (QoS) assurance is a must. Jitter, packet loss, throughput, delay, and error rate are all examples of QoS requirements. The unique constraints and attributes of wireless and mobile ad hoc networks, for instance, restrained link bandwidth and quality, dynamically changing network topologies, and variation in node and link capabilities, exacerbate the difficulty of obtaining the required QoS in a MANET [6].

2.0 SECURITY ATTACKS

Since MANET is a short-lived network of nodes with no central management, the nodes should communicate with one another with total trust. Unfortunately, compared to other network types, this property means that MANET is more susceptible to attacks from within the network. In practice, MANET can be attacked in various ways using a variety of approaches; however, before delving deeper, it is obligatory to categorise security threats in the context of MANET.

The categorisation can be based on the attack’s behaviour (Active or Passive), the attack's source (Internal or External), the attacker's processing capacity (Mobile or Wired), and the number of attackers (Single or Multiple) [7], [31], [32], [33].

2.1 Based on the Behaviour of Attack

Passive attacks often try to steal users' useful information from no less than two communicating nodes (as shown in Figure 2(a)), if not the entire network. Passive attacks come in various forms, but there are two sorts in MANET: eavesdropping and traffic analysis. Depending on the circumstances, passive attacks might be judged acceptable or illegitimate in practice. Such as using tools to diagnose or account for the network is legitimate or to probe network traffic. Alternatively, if the goal is malicious, an attacker can take important information from network traffic, like credit credential emails and card information, and utilise it to unlawfully extract money from victims' bank accounts or blackmail them.

Passive attacks, on the other hand, do not seek to disturb the operation of a specific network; however, active attacks can affect the regular network operation [34]. Masquerade attacks, replay assaults, message manipulation (as seen in Figure 2(b)), and Denial-of-Service (DoS) attacks are all examples of active attacks.

The most effective approach to avoiding a passive attack is to employ robust network encryption technologies. Active attacks can be prevented by using intrusion prevention systems and effective firewalls.

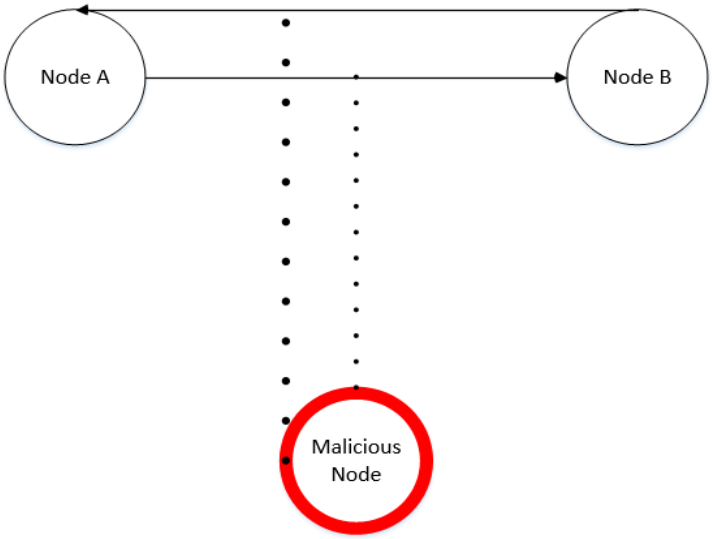

Fig. 2(a): Demonstration of passive attack

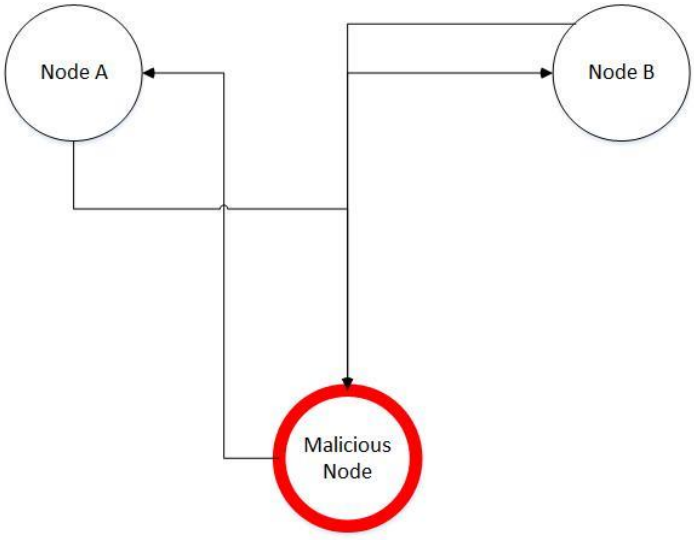

Fig. 2(b): Demonstration of active attack

2.2 Based on the Source of Attack

As the term implies, external assaults are launched by attackers who remain physically outside the attacked network. These attacks are typically designed to limit access to a particular network function (such as HTTP traffic), induce network congestion, or might even disturb the entire network. External assaults would be challenging to launch if the network was protected and set up correctly, but inside attacks are far more challenging to counter.

As shown in Figure 3, an exterior attack could become an interior attack with far more devastating consequences. As a result, internal attacker nodes have two types: the compromised node (described above) and the misbehaving node (discussed below), which is authorised to access system resources but fails to utilise them in the manner in which they should be used [34]. Internally malfunctioning node attacks are not detected easily, such as a selfish attack where the node is hesitant to expend network bandwidth, CPU cycles, or battery power to transmit irrelevant packets, even though it expects other nodes to do so.

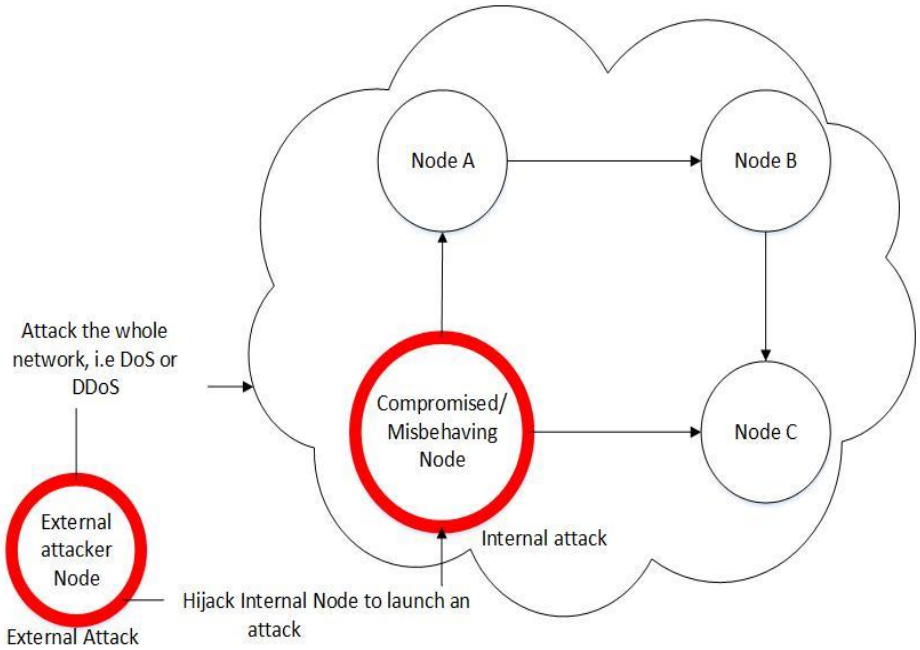

Fig. 3: Demonstration of internal and external attacks

2.3 Based on Processing Capability of Attacker

- Wired: Intruders utilise wired media to get illegal access.
- Mobile: The invaders employ a wireless medium to obtain unlawful access.

2.4 Based on the Number of Attackers

- Single Attacker: A single individual or malicious node disrupts the network's normal flow.
- Multiple Attackers: The network is under attack by a group of individuals or malicious nodes [35].

2.5 Based on the Network Layer Carried On

MANET attacks can also be classified by the networking layer on which they are carried out [36]. Figure 4 shows the attack classification by network layer.

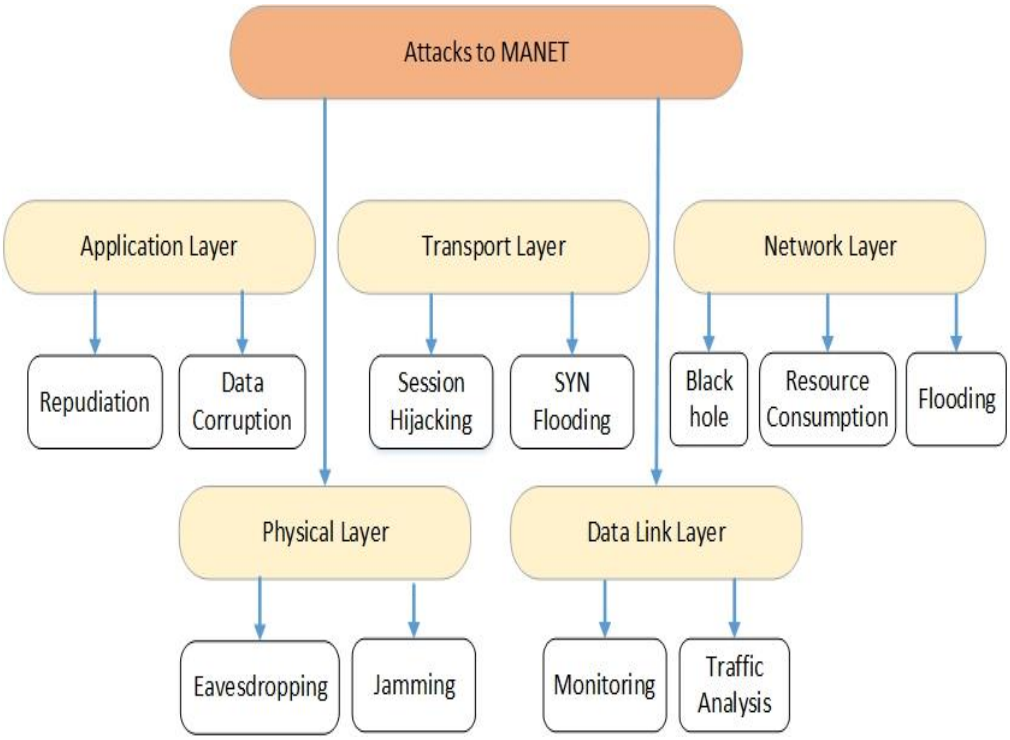

Fig. 4: Classification of MANET attacks

2.5.1 Physical Layer Attacks

Since MANET and all wireless networks broadcast network signals over the radio, hostile attackers can simply intercept them [37]. Eavesdropping is one of the physical layer attacks that can be carried out. Attackers can merely retrieve talks between target nodes by intercepting radio signals over the air. Furthermore, radio signals are susceptible to interference. A malicious signal can readily be generated to overpower the target signal and disrupt communications if the malicious attacker has a powerful transmitter. Jamming attacks are one of the most well-known examples of this type of attack.

Direct sequence (DSSS) and Frequency hopping (FHSS) can be employed to thwart eavesdropping attacks at this layer. It randomly fluctuates in frequency, making signal acquisition problematic. Additionally, it reduces the likelihood of interference from other electromagnetic and radio equipment.

2.5.2 Link Layer Attacks

Attacks on the link layer of a MANET can be made by distorting the cooperation of the link layer's protocols [38]. MANET is a peer-to-peer network architecture that is open and medium in size. Link-layer protocols are in charge of ensuring that communication between each pair of nodes is maintained. When it comes to MANET, traffic analysis is one of the most important assaults on the link layers. It allows the attacker to detect communication participants' functionality. In reality, this form of attack is commonly used across various network types. The use of traffic analysis attacks on Wireless Sensor Networks, for example, is described in [39].

The use of encryption at the data link layer precludes traffic monitoring. Wired Equivalent Privacy (WEP) has received much criticism. During message delivery, a dynamic mix mechanism is utilised to "mix" nodes in the network and mask the source and destination information. Wi-Fi Protected Access (WPA) and WEP are used to authenticate every node that wishes to join the network. The Link Layer Security Protocol (LLSP) is a data connection layer security protocol protecting data transmissions that utilises encryption to prevent attacks. A DoS attack or a Man-in-the-Middle attack can be prevented using Secure Link State Protocol (SLSP).

2.5.3 Transport Layer Attacks

In MANET, transport layer protocols are responsible for establishing an end-to-end connection, reliable transfer of packets from one end to the other, flow management, congestion control, and clearing an end-to-end connection

[38]. SYN flooding attacks [40] and session hijacking attacks [41] are therefore possible in MANETs transport layers, just as they are in a regular Transmission Control Protocol (TCP) network.

Encryption at the transport layer keeps messages between nodes private. Secure Socket Layer (SSL) safeguards a session from start to finish. Transport layer assaults include Denial-of-Service, impersonation, and Man-in-the-Middle. Countermeasures for these assaults must be deployed at several stages to be effective.

2.5.4 Application Layer Attacks

In the application layer, worms and computer viruses are the most frequent threats. Attackers can compromise mobile nodes, transmitting virus or worm payloads in the same way they do in a traditional TCP/IP network. These malicious applications can be spread to other mobile nodes through application-layer communications. By propagating malicious malware to other nodes in the network, attackers can bring the entire network down. Researchers have looked into worm attacks on MANETs that use both User Datagram Protocol (UDP) and TCP [42], [43].

Most assaults may be avoided using application layer firewalls. An Intrusion Detection System (IDS) may be quite effective as a second line of defence. A Multi-Layer attack is hard to spot because these attacks can occur at the data connection, network, or transport layers.

2.5.5 Network Layer Attacks

The network layer in the Open Systems Interconnection (OSI) network model is responsible for extending network communication from one-hop neighbouring nodes to all other MANET nodes [36]. When multi-hop communication is required, nodes rely heavily on one another for data packet relay. As a result, the network layer protocols used by MANET are susceptible to various attacks. According to [44], the bulk of MANET routing strategies is based on the assumption that every network node is cooperative rather than malicious. As a result, attackers can carry out a variety of assaults during the data forwarding phase. Corrupting data content, quietly dropping packets, flooding data, or replaying data packets are all general attacks.

The Statistical Ad hoc On-Demand Distance Vector (SAODV) prevents black hole attacks but requires a complex encryption algorithm [8]. Search and Rescue (SAR) helps defend against black hole assaults. SAR involves a lot of encryption and decryption. Ad hoc Networks (ARAN) can defend against impersonation and repudiation attacks. This system may not protect against selfish nodes that have been authenticated. When it comes to preventing modification attacks, the Secure Efficient Ad hoc Distance Vector (SEAD) security protocol is employed.

The various attacks in MANETs and the respective solutions have been tabulated in Table 1.

Table 1: Attacks in MANET

Layer	Attacks	Countermeasures
Physical layer [37]	Flooding [50] Eavesdropping [52] Active Interference	Adopting Spread spectrum methods DHSS, FHSS
Data Link layer [38], [39]	Selfish node misbehaviour Malicious node behaviour Denial-of-Service Traffic diversion Assaulting neighbour sensing protocols	Securing link layer protocol such as LLSP utilising WPA
Transport layer [40], [41]	SYN Flooding [40] Session Hijacking [41]	Safeguarding End-to-End communication (SET, TLS, SSL)
Application layer [42], [43]	Impersonation, Worms, Virus, Man-in-the-Middle Attack, DoS	Firewall [42], [43]

Network layer [8], [44]	Black Hole Attack [48] Worm Hole Attack [46] Information Breaches Byzantine Attack [45] Consumption of resources Rushing Attack Routing Table Poisoning Routing Table Overflow Route Cache Poisoning Packet Replication Routing Attack	Securing routing protocols such as ARAN, SAR and SAODV [8] for countering impersonation attacks, SECTOR method [3] to ward off wormhole attack

3.0 PROMINENT ATTACKS IN MOBILE AD HOC NETWORKS

Many kinds of intrusions or attacks identified in MANETs have been discussed in this section.

3.1 Byzantine Attack

This assault targets a single or a group of mobile nodes to degrade or disrupt routing services using various means, including packet forwarding to non-optimal paths, routing loops, or selective packet dropping. From a node's perspective, the network shall continue to operate normally even in the presence of byzantine behaviour, making this attack one of the most difficult to detect. Other examples of byzantine behaviour include the advertisement of bogus links in topology control messages or hello packets. Additionally, a compromised node may include itself in a route update message to mediate between communicating nodes. When a compromised node receives packets sent over its path, it can modify the metrics, drop route requests without broadcasting them again, or suspend transmission of route requests [45].

It is possible to utilise a secure routing protocol that provides a technique for overcoming these attacks through public key cryptography. Adaptive probing approaches have the potential to lessen the occurrence of byzantine failures. Robust Source Routing (RSR) is a safe on-demand MANET routing mechanism developed. The RSR can protect against clever hostile agents that selectively discard or change packets they committed to deliver besides offering data origin authentication services and integrity checks.

3.2 Wormhole Attack

A node affected by this maliciousness receives packets at one network point, tunnels them to another, and then replays them (Figure 5). Although wormhole attacks might be used to optimise network performance by shortening paths, they can give the attacker a stronger position in the network against other nodes when used honestly and reliably. This violates mobile network standards, which implies node equality with no such thing as a superior node having more control features than others. A wormhole attack can prevent the detection of new paths if employed against on-demand routing protocols such as Ad hoc On-Demand Distance Vector (AODV) or Dynamic Source Routing (DSR); hence all routes will have to be through the wormhole [46].

TrueLink is a timing-based anti-attack countermeasure. Packet leashes may also be used to identify wormholes. A leash is any information provided to a packet to limit its maximum transmission distance. A geographical leash guarantees that the packet receiver is close to the source node. A temporal leash limits the packet's lifespan (restricts the maximum travel distance). The SECTOR mechanism [3] may also identify wormholes without synchronising clocks. Anti-wormhole antennas or Directional antennas are also proposed.

In the absence of authentication in the existing ad hoc routing protocol, a compromised node assumes the identity of (impersonates) a genuine node. This emulation can result in perplexing routes, partitioning or more complex routing loops [31], [45].

Equip nodes with GPS and test whether two nodes can truly connect. Another alternative is to include 2-hop neighbours in the hello message, giving every node a 3-hop network topology, which is countered by spoofing outside 3-hops.

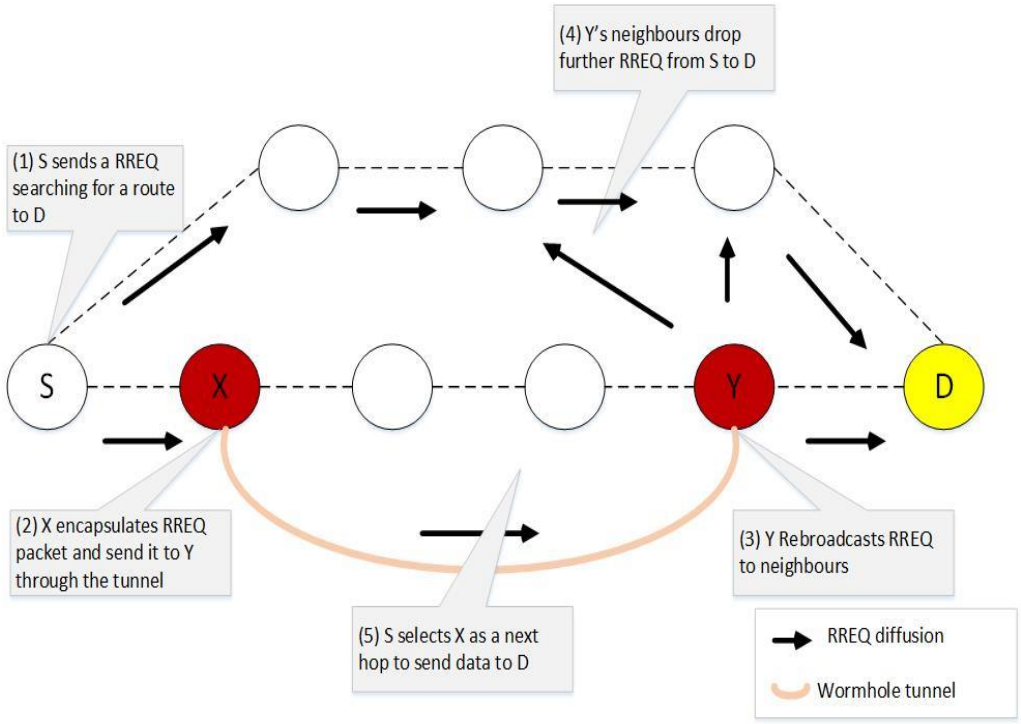

Fig. 5: Demonstration of wormhole attack

3.3 Spoofing Attack

In the absence of authentication in the existing ad hoc routing protocol, a compromised node impersonates (takes on the identity of) a valid node; this impersonation can lead to confusing routes or more troublesome routing loops or partitioning [45].

3.4 Sybil Attack

A Sybil attack occurs when a node assumes the identity of a non-existent node, resulting in the appearance of numerous malicious nodes working together. When a node has been penetrated by such an assault, the peer-to-peer network's reputation system will be compromised due to the creation of a massive number of imaginary nodes employed to gain a disproportionately large impact. Sybil attack mainly aims at networks where cooperative operation is a must; it can affect the auto-configuration schemes and the secure allocation schemes based on trust models. Defeating a Sybil attack can be challenging, especially if the network trust system is weak and the ID generation process isn't used correctly with the chain-of-trust concept. But Sybil attacks can be prevented by using a central authority for ID distribution or by employing mechanisms that use the connectedness features of social networks, among other measures [47].

A robust Sybil attack detection framework for MANETs is suggested based on cooperative network monitoring.

3.5 Black Hole Attack

It is regarded as one of the most common internal active attacks in MANETs and the most threatening misbehaviour leading to serious malfunction in the overall network operation. In a black hole attack, a malicious node advertises its routing protocol to claim the fastest path to the target node or packets it desires to intercept. Furthermore, the malicious node publicises the availability of new routes regardless of whether or not it has checked its routing database, which makes it constantly accessible to respond to routing queries and, as a result, intercept and keep the data packets they receive. Black Hole attacks exploit the vulnerabilities in reactive (on-demand) routing schemes such as DSR and AODV [48]. For example, AODV is a protocol based on flooding. Suppose a black hole attack compromises a node using AODV, then the malicious node advertisements will be received by sending the (Route Request initiator) node before any other Route Reply. Hence, the malicious node has already established its fraud route, and it's up to it whether to forward the packets to an unknown address or simply drop it (shown in Figure 6).

This attack is prevented by the Detection, Prevention, and Reactive AODV (DPRAODV) protocol. Using cryptographic hash functions, several black holes may be identified. A wait-and-check mechanism is also proposed for packet safety. The SAR protocol protects against black hole assaults. Requests for route confirmation (CREQ) and route confirms.

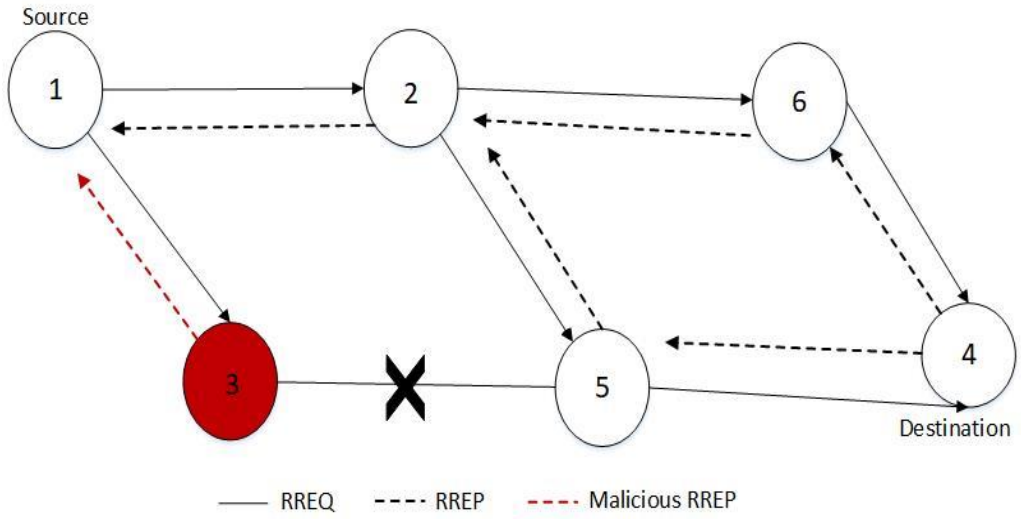

Fig. 6: Demonstration of black hole attack

3.6 Gray hole Attack

The attacker is selective in which packets it discards. Depending on the circumstances, the malicious node may modify its course of action from forwarding routing packets to rejecting other packets. The attacker's goal influences the decisions made by the network on its behaviour. A node in the established routing architecture drops packets on a selective basis, resulting in network disruption that might be difficult to notice at first glance (Figure 7). Detecting this attack might be difficult, depending on the type of data dumped and the pace at which data is dropped. A node that has been overloaded, despite no fault of its own, may begin to selectively discard packets, mimicking the behaviour of a gray hole [49].

A signature mechanism is presented as a countermeasure to the gray hole attack, which allows packet dumping nodes to be traced.

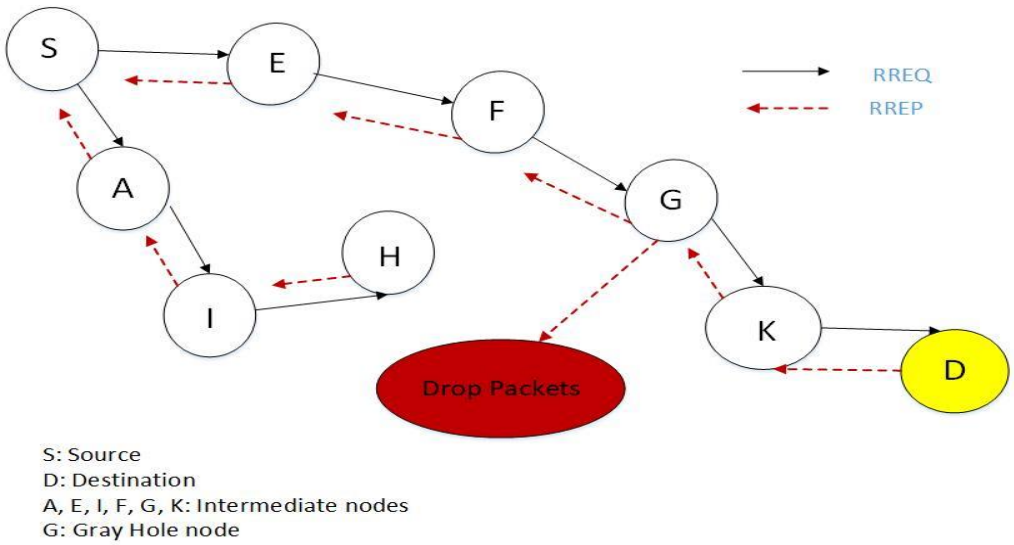

Fig. 7: Representation of gray hole node in a MANET

3.7 Flooding Attack

Several nodes launch this attack in the network, which generate an excessive number of malformed Route Request (RREQ) messages (shown in Figure 8). Data flooding attack occurs after a route is established between the attacker and one or more legitimate network nodes. After setting up a route to a legitimate node, the attacker forwards many useless data packets along the path to disrupt the normal packet processing of targeted nodes to exhaust their battery power and isolate them from the network [50].

Calculate the RREQs of your neighbours and block them if they reach a certain level. If A is spoofing actual nodes, it will not be able to halt flooding below the threshold and may even block valid nodes. Statistical analysis can be used to discover variations in the pace of flooding.

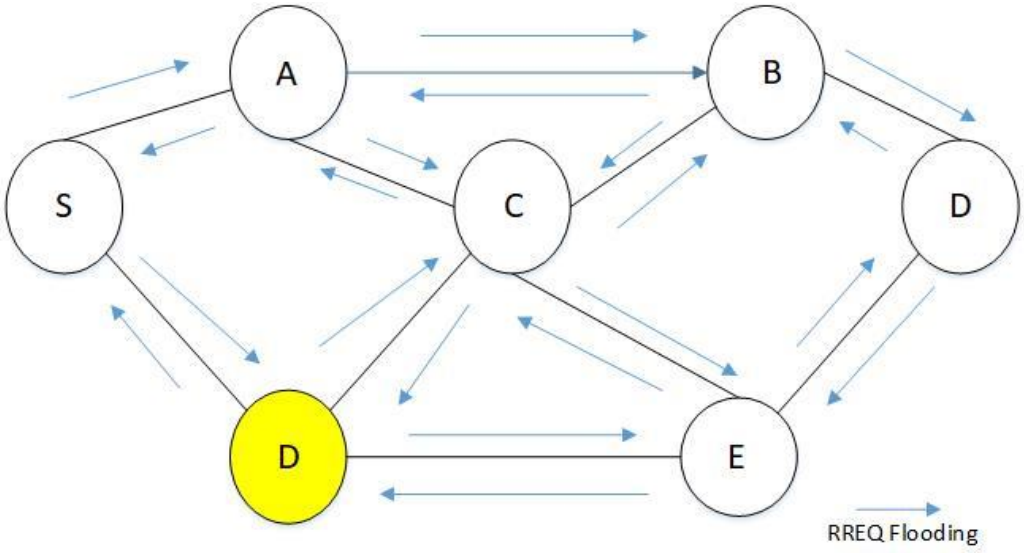

Fig. 8: Representation of flooding attack in a MANET

3.8 Sleep Deprivation Attack

It is another method that can be performed by an attacker to disable the routing services provided at a legitimate node. An attacker can launch a sleep deprivation attack by communicating with the targeted node in a manner that seems genuine. Nevertheless, these communications prevent the attacked node from staying in power conserving sleep mode [51].

Timeout media access protocol (MAC), Berkley MAC, Sensor MAC, Clustered Adaptive Rate Limiting (CARL), and Hash-based scheme are some techniques used as a countermeasure to sleep deprivation attacks.

3.9 Sinkhole Attack

A malicious node can attract traffic by advertising itself as the best possible node with a route towards some destination to deceive other nodes and force them to use that route more frequently for packet forwarding (Figure 9). Such misbehaviour is known as a sinkhole attack, which can be established by a malicious insider or a resourceful outsider. For instance, in the case of the AODV routing protocol, an attacker can modify or create a Route Reply (RREP) message that announces a sequence number larger than that in a received RREQ. Therefore, the new route provided by the malicious node guarantees that other nodes will select it as the next hop to forward packets toward the requested destination [8].

Mutual understanding among nodes is used to identify sinkholes, and a cooperative sinkhole detection method is developed. A cross-layer tool to detect sinkhole attacks in MANET is also developed, as is a Sinkhole Intrusion Indicators Technique (SIIT).

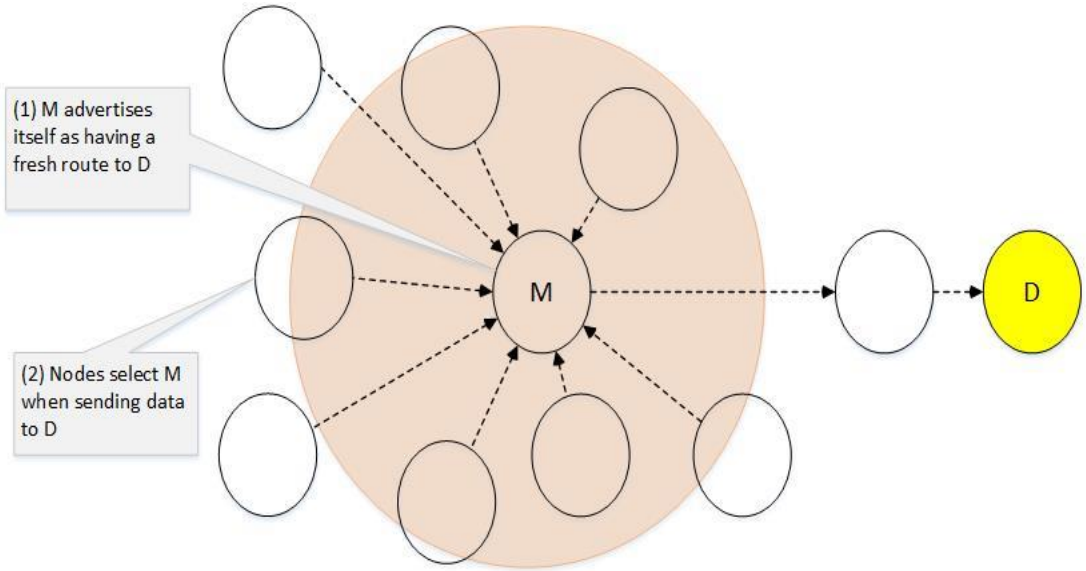

Fig. 9: Representation of sinkhole attack

3.10 Rushing Attack

A malicious node can dominate the route discoveries launched by a legitimate node by forcing the routing protocol to malfunction. A flooding-based routing protocol, AODV limits the number of broadcast RREQ packets using a Back-off waiting period, which an attacker may exploit to launch a Rushing attack [8]. In this case, if the RREQs sent by a malicious node reach the neighbours of a requested destination first, then any route discovered towards this destination will include that malicious node (shown in Figure 10).

RAP (Rushing Attack Prevention) is a type of attack prevention in which a threshold value is set to a specific level for the reaction time. This approach may be further enhanced by incorporating a threshold value and an average time calculation into the mix to identify the source of fake requests.

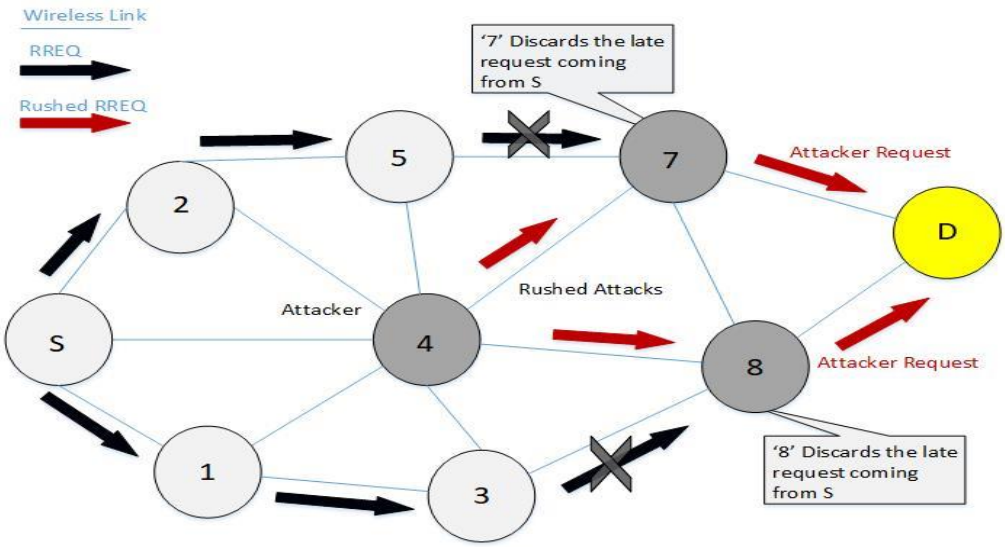

Fig. 10: Representation of rushing attack

3.11 Eavesdropping

Wireless communication is a significant flaw in these attacks. Any device with a transceiver within the transmission range can intercept communication. Encryption can prevent attackers from acquiring valuable data. Without encryption, the attackers can simply obtain the information [52].

An eavesdropping attack can be prevented using SSL spread spectrum technologies, such as frequency hopping (FHSS) and direct sequence (DSSS). It haphazardly fluctuates in frequency, making signal acquisition problematic. Additionally, it reduces the likelihood of interference from other radio and electromagnetic equipment.

3.12 Traffic Analysis and Location Disclosure

Less intrusive methods like eavesdropping can identify node locations by analysing the communication pattern, frequency, and volume [52]. For example, a controlling centre will receive and transmit more messages than usual in an emergency. An attacker can quickly pinpoint the controlling centre by studying traffic patterns.

It is possible to prevent such an attack by employing geometric restrictions and heuristics to identify node placements as efficiently as possible. Because such an "omniscient" attacker can achieve such high localisation precision, it is possible to evaluate the quality of future, more realistic attack models based on their accuracy.

3.13 Denial-of-Service

The node cannot reach clients or access points because it has been a victim of overwhelming traffic [6].

A firewall can stop DoS attacks. To mitigate DoS threats, a digital signature mitigation approach is presented.

4.0 NODE MISBEHAVIOUR IN MANETS

The term "misbehaviour" refers to a node that does not operate in a regular manner and exhibits aberrant behaviour in wireless networks [3]. The node is misbehaving if its behaviour deviates significantly from its definition or set of behaviours [53]. Nodes can be malicious or selfish; the entire categorisation is depicted in Figure 11. Misbehaviour takes place in the following ways:

- Deferring packets
- Deferring acknowledgements
- Dropping acknowledgements
- Dropping packets and changing routing information
- Forwarding control packets but dropping data packets
- Restraining from packet forwarding to save its resources

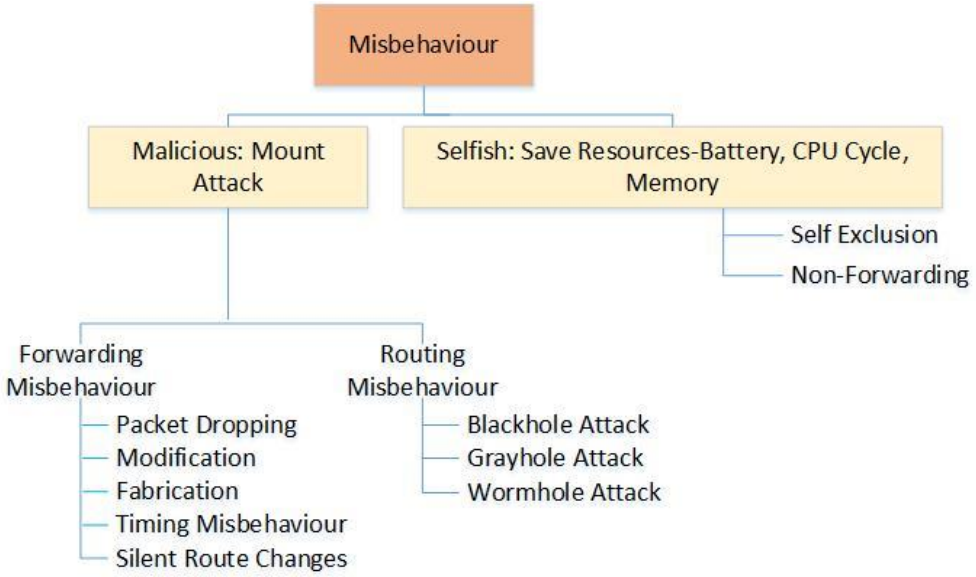

Fig. 11: Node misbehaviour in MANET

4.1 Types of Node Misbehaviour

Node misbehaviour in MANET is a serious issue that can severely impact network performance. A node might misbehave by not transmitting data packets from other nodes or executing routing procedures incorrectly. There are

several possible misbehaviours within these two categories. For example, 'selfishness' may prevent packets from being sent, whereas 'maliciousness' may launch various assaults and create misleading reporting [3], [29].

Packet forwarding misbehaviour includes the selective and complete discarding of packets and misrouting packets. Routing misbehaviour includes route capture, tunnelling, misleading reporting, and not being a part of any path. We shall now demonstrate how nodes in MANETs might behave incorrectly [30]. Figure 12 represents MANET misbehaviour categorisation.

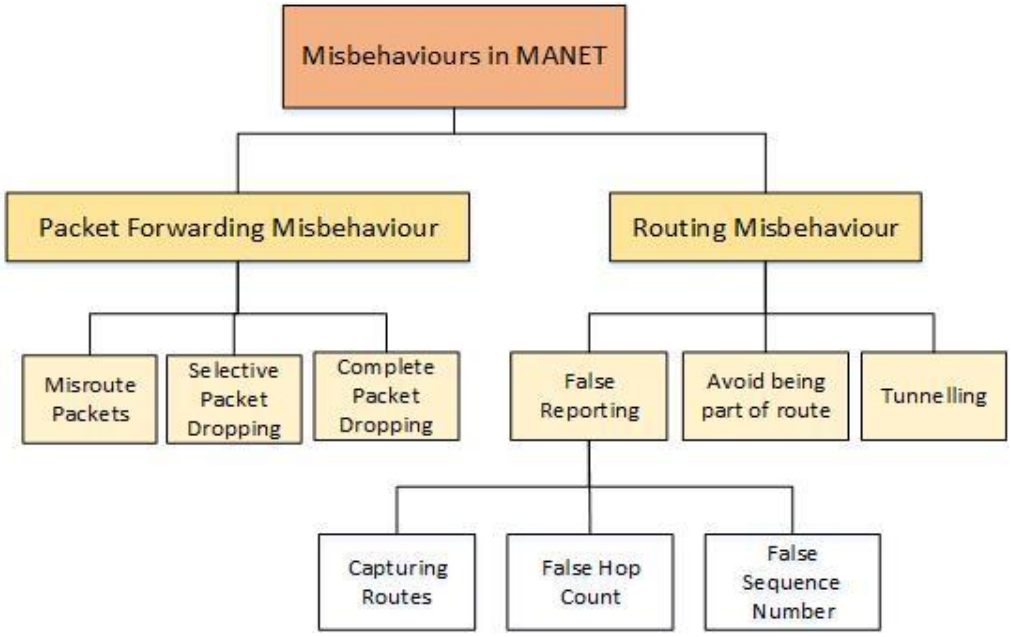

Fig. 12: Classification of node misbehaviour in MANET

4.1.1 Packet Forwarding

Authors define misrouting packets in [30], [54]. A malicious node can drop and misroute packets to alternative pathways instead of the intended destination. Figure 13 shows how node G misroutes packets intended for node I.

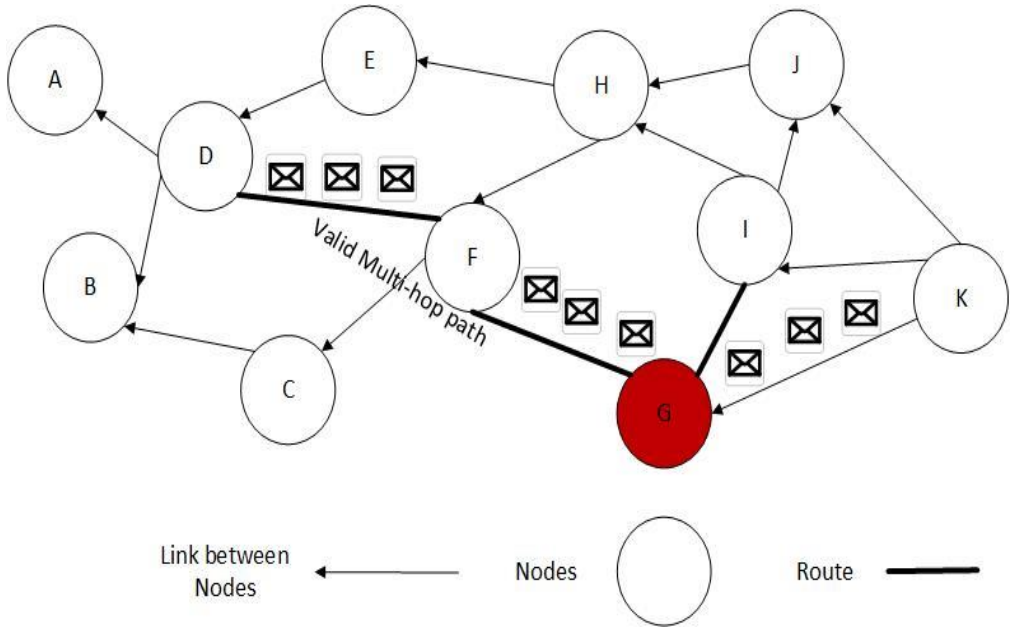

Fig. 13: Representation of node G misrouting packets

The authors in [55] characterise complete packet dropping as a black hole attack in MANET. Figure 14 represents the scenario of complete packet dropping as discussed in [56]. In a Gray hole attack, the node drops packets randomly or selectively for specified nodes [57].

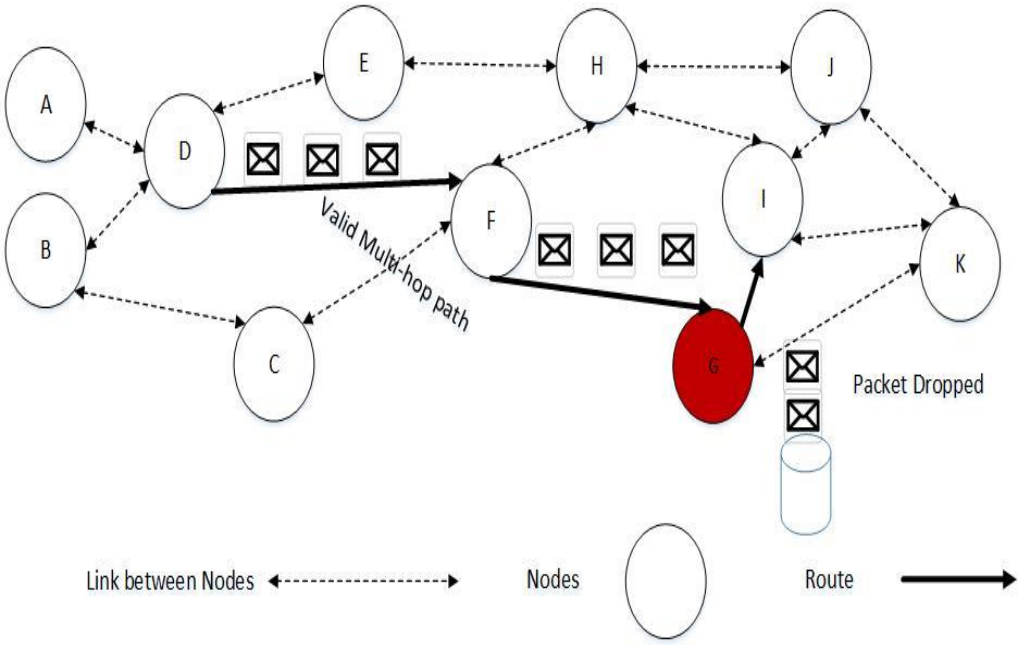

Fig. 14: Representation of node G dropping packets completely

Figure 15 demonstrates packet dropping by node G, targeted for node K and forwarding packets meant for another node I [30].

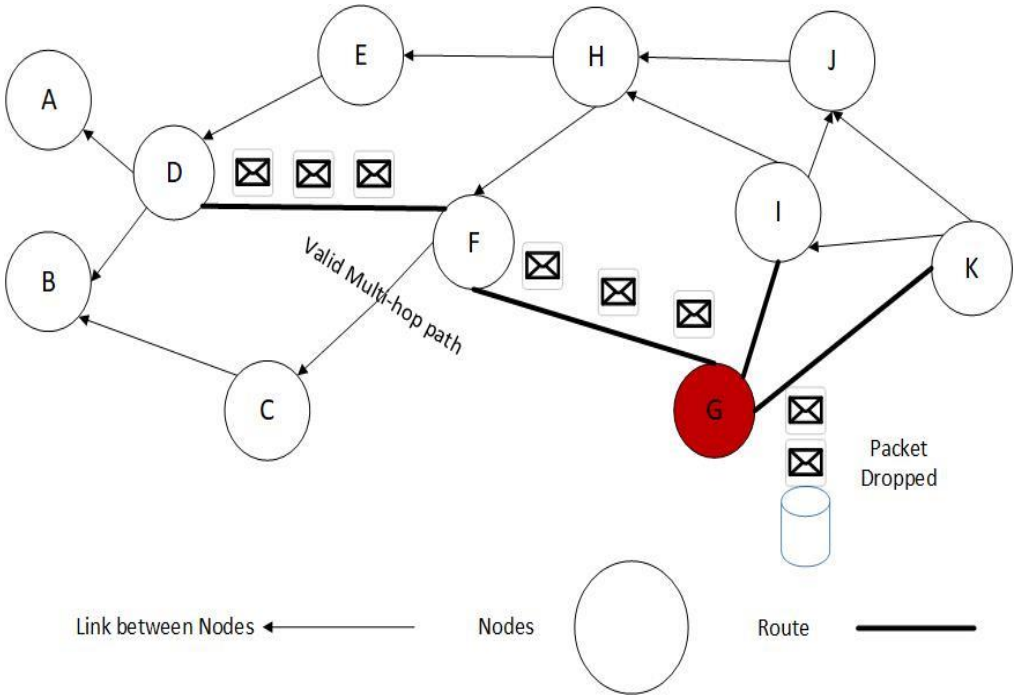

Fig. 15: Demonstration of selective packet dropping

4.1.2 Routing Misbehaviour

As seen in [58], altering various control fields of message headers, such as sequence numbers, can cause network traffic to be redirected. In AODV, any node can redirect traffic by publicising a false route to a node with a better

destination sequence number. False reporting of hostile nodes alters the hop count field in packet headers. Tunnelling attacks are a flaw in multipath routing in which at least two nodes collaborate to enclose messages (Figure 16).

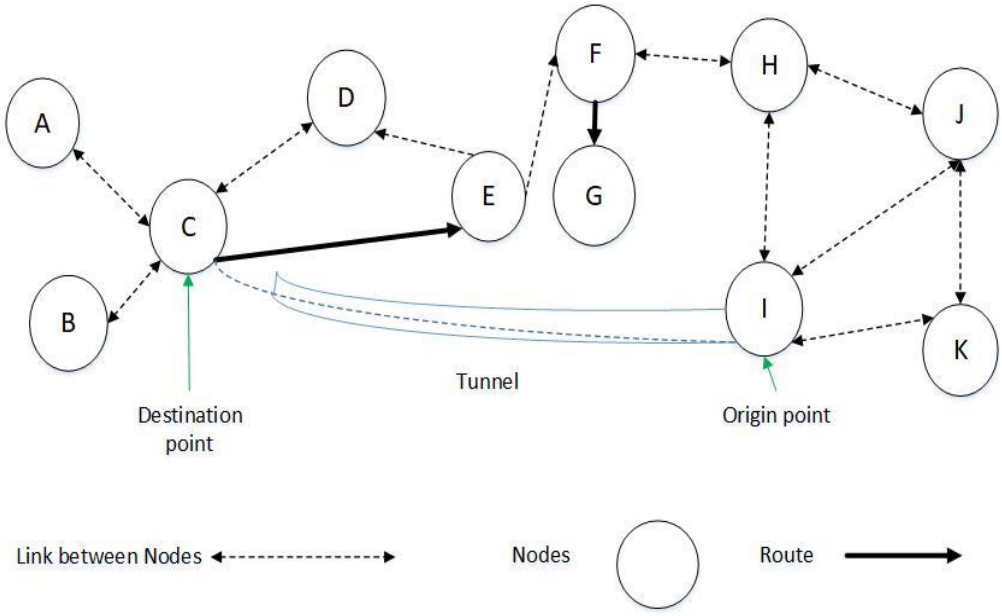

Fig. 16: Demonstration of tunnelling

According to [59], nodes do not engage in route discovery activities in the network owing to resource constraints. Sometimes they want to avoid any path which might be misbehaviour.

The invader advertises himself as having a new route when the node submits a Route Request to become a part of each route and grab the majority of routes in the network. Afterwards, identify an intermediary node that will discard packets rather than forward them.

Selfishness is commonly defined as non-cooperative conduct, distinct from malicious behaviour. Selfish nodes utilise the network for their communication without allowing other nodes to forward messages to preserve battery life. A selfish node would gain from other nodes' resources but not provide its own. They have no desire to harm the network. However, malicious nodes introduced by opponents will aggressively consume battery power to destroy the entire network. Therefore, giving nodes incentives to cooperate (either by rewarding active collaboration or penalising non-cooperation) becomes an attractive study topic.

Three distinct types of selfish nodes are identified in [10] in relation to routing protocols like DSR [60].

- Selfish Node Type 1 (SN1) – Such nodes participate in the Route Maintenance and Route Discovery phases of DSR. Still, they decline forwarding data packets that are often significantly bigger in size than the routing control packets.
- Selfish Node Type 2 (SN2) – They don't participate in the Route Discovery phase or forward data packets. Such nodes only require energy for transmitting their own packets.
- Selfish Node Type 3 (SN3) – Based on their energy levels, such nodes may behave (or misbehave) differently. The node functions appropriately when the energy is between total energy E and a threshold T1. It acts as a node of type SN1 for an energy level between T1 and another lower threshold, T2. Lastly, when the energy level is less than T2, it functions like an SN2 node. T1, T2, and E are related as $T2 < T1 < E$.

The routing protocol just ignores the SN2 nodes. So, while these nodes may reduce network connection, they do not constitute a substantial danger to the routing system. However, SN1 and SN3 nodes pose a more significant threat to routing systems [2]. As a result, the routing protocol must resume the route discovery process or choose another route if one is available. The revised routes may still contain some SN1 nodes, causing them to fail. This procedure shall continue till the traffic source determines data transmission is impossible. This work solely detects and mitigates SN1 misbehaviour. SN3 nodes are recognised when they act like SN1 nodes.

According to studies in [61], nodes in a MANET tend to become greedy over time. Selfish nodes are reluctant to share resources like memory and battery power with others. Selfishness is generally linked to decreasing resources like battery power and the desire for nodes to save resources for themselves. In a MANET, a node's selfishness is strongly encouraged. Authors in [61] characterised selfish node behaviour as follows:

No participation in routing: A selfish node ignores packets or corrupts the Route Reply packets and route discovery by altering the Time to live (TTL) parameter to a tiny value, so preventing them from reaching their destination

No response to hello messages: Selfish nodes may fail to acknowledge hello messages, concealing their presence and preventing other nodes from detecting them for packet forwarding purposes.

4.2 Causes/Reasons of Node Misbehaviour

In multi-hop communication, the source node relies on intermediate nodes to relay packets to the destination node. The network connectivity might be easily lost if the intermediary nodes do not cooperate. In MANET, there are a variety of reasons for node misbehaviour. They can be categorised into two major groups [36].

Unintended misbehaviour: When mobile nodes are overburdened in terms of memory space and computational power, packets may be dropped. This misbehaviour could also result from an unstable network or a network collision because wireless channels are highly unpredictable.

Intended misbehaviour: Selfish or malicious nodes usually cause this sort of misbehaviour. Due to mobile nodes' restricted energy and network bandwidth, selfish nodes engage in such misbehaviour to conserve their resources. They accept routing but decline to forward data packets to other nodes. Malicious nodes have the goal of disrupting network communication and limiting network connectivity. Black hole and Gray hole assaults are examples of such attacks.

Figure 17 depicts a general categorisation of node misbehaviour causes.

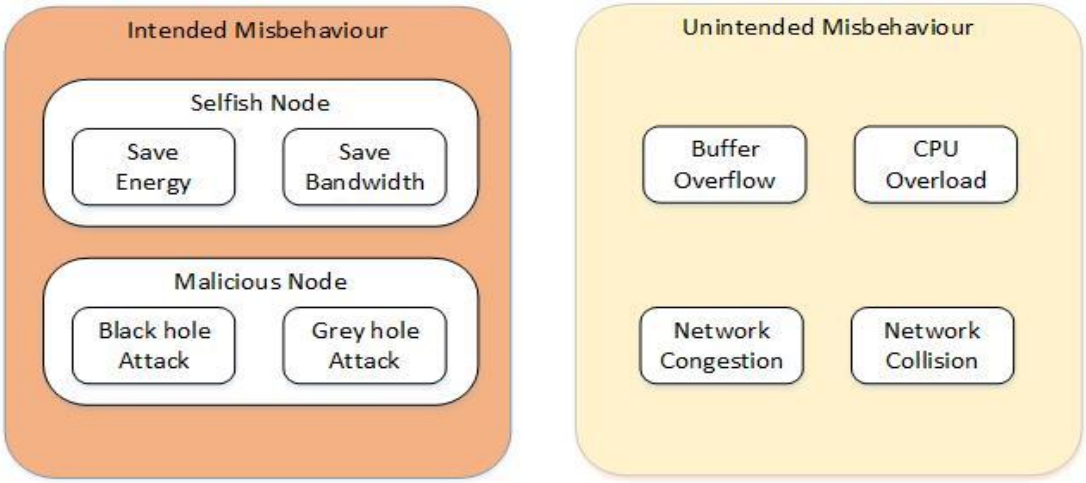

Fig. 17: Causes of node misbehaviour

When an ad hoc network node is programmed with intelligence or regulated by another intelligent entity, it might become selfish. Another gadget, module, program, or human can be an intelligent entity. Selfishness is widespread in human-operated personal devices such as personal digital assistants and cell phones [62]. A node can be sufficiently configured to become independent of other network nodes and determine its functionalities. For a variety of reasons, a smart node can change its behaviour. The primary reason is to conserve energy. The following are the motivating elements for smart nodes to change their cooperative behaviour [63].

4.2.1 Energy

The nodes in almost all wireless ad hoc networks rely solely on batteries for power. In most WSNs and comparable networks, these batteries are usually non-rechargeable and disposable. In such networks, nodes are randomly placed into a field and kept unattended. As a result, battery replacement or recharge is impossible, even though operators

recharge these batteries in some circumstances, such as in VANETs and MANETs. However, in ad hoc networks, the energy source is always considered scarce and finite [64].

A node's energy is consumed via a variety of functions. The most critical functions are data transmission, reception, processing, and sensing. The utilisation of energy can be classed as either beneficial or wasteful. Control messaging, data processing, data transmission, and data reception are examples of useful energy expenditure, whereas generation of control packets, retransmission of lost packets, overhearing idle listening, and processing of control packets are examples of wasteful energy expenditure. If a node disables or lowers any of these functions, it might cause problems in various ways. Nodes might decline forwarding data packets from other nodes to save energy. Forwarding nodes typically require more energy when data is received and then retransmitted. To preserve their battery, selfish nodes refuse to relay.

Assume a node uses ax amount of energy to transmit a single bit and expends bx amount of energy to receive the same bit. The value of a must be bigger than b in wireless communication principles, i.e., $a > b$ [65]. $ax + bx$ amount of energy will be expended by a typical node for forwarding a single bit. An energy-saving strategy for a selfish node is to just hear a single bit with bx amount of energy and not retransmit the same bit. Most researchers [66], [67] use sensor nodes with disposable batteries in their case studies. On the other hand, any sort of ad hoc network with nodes powered by a finite power source can be expected to have a non-cooperative environment among the nodes. The selfishness of nodes has been cited by some authors as the most effective method for reducing energy consumption and extending node life [66].

4.2.2 Storage Buffer

Ad hoc networks have limited storage space available to them. Therefore, the nodes must temporarily store the data they receive before transmitting them to the following hops. Nodes may need to pick which data content to hold in their storage buffers. The majority of nodes attempt to keep their storage buffer for their acquired data full, which prevents another node from being entertained. Until they get connectivity with their following hops, all nodes preserve the relayed data they have received. The nodes may discard the received data before transmitting it to free up their storage buffer for their data [68]. Because of the restricted buffer size, it is necessary to develop effective buffer management solutions. The buffer management strategy outlines which messages to store and delete in ad hoc networks. Delay Tolerant Networks (DTNs) believe that prioritising messages for the data buffer is a particularly effective policy. Due to their limited buffer capacity, nodes in DTN can adopt a selfish behaviour that benefits them for their data transfer. A significant amount of damage is done to source nodes that must go via multiple hops to reach their destinations. In such cases, selfish nodes do not bother to request relay service with buffer utilisation; therefore, their data is never transmitted. Routing misbehaviour [68] is another term for selfish node behaviour. During data transfer, some nodes use their restricted storage buffers.

4.2.3 Social Likeness

Users of Internet-based social networks have formed many interwoven links. Such networks impact many facets of our everyday lives and allow us to connect with people who share similar beliefs. In many ways, the user's selfishness cannot be neglected in social networks. Likeness and dislike are the most common reasons for selfishness [69]. Similarly, in an ad hoc network, smart or human-controlled nodes can consider the issue of social similarity during communication. In practice, intermediate nodes may drop packets if they ignore the sender node. The DTNs networks, in which the majority of the nodes are either managed by humans or mounted in cars, are often connected with social selfishness [70]. The nodes with no social relationships fail to cooperate to conserve resources. A mobile social network may be used as an example in this scenario. People build communities by sharing shared interests via mobile phones. Each community member prefers to support only other community members and avoid spending energy on stranger nodes. Furthermore, previous connectedness and behavioural records might influence a node's social liking or hatred of individuals.

4.2.4 Bandwidth

In a network where nodes transmit large amounts of data, nodes' allocated bandwidth may need to be used. In nature, the amount of bandwidth available is always restricted. Depending on the magnitude of their given bandwidth, the nodes may adopt specific cooperative or non-cooperative behaviours. Due to their bulky data, nodes may be unable to accommodate any other relay requester for data transmission [70]. Bandwidth constraint is a significant issue in most ad hoc networks, and it has been the subject of numerous studies. Sensor nodes in WSNs have a relatively limited bandwidth because their lower energies and processing capabilities prevent them from

handling a larger data spectrum. Many writers recommended node-level processing to lessen the impact on communication bandwidth [63]. As a result, if the nodes are intelligently programmed, they will choose to use their own communication route for their data.

4.2.5 Mobility Rate

Due to the mobility of nodes in most MANETs, topological connectivity alters over time. When a node changes locations, it may disrupt some connections and create new ones. It is undeniable that more mobility nodes can significantly reduce network performance. A relay node may be unable to modify its network location to prevent data loss at the source node. It is also likely that a source node instructs the relay nodes not to migrate till the data transmission has been completed. Because each smart node is only concerned with its own interests, it can act selfishly and alter its location without favouring any source node. The fault tolerance system can also include mobility control [71]. In the 1970s, the concept of cooperative movement and communication first appeared in the literature. This means that each network node can function in one of two ways: (a) selfish, in which it does not move for others but chooses to optimise itself, or (b) cooperative, in which it looks after the whole network and attempts to achieve the collective goal.

4.2.6 Privacy Concern

Some nodes may request private data from others when connecting with them. Generally, it can be said that a network of mobile phones exists and that every phone communicates its location with others via various applications. It's feasible that a phone can read the positions of all linked devices but never disclose its location. Such selfishness might be classified as privacy or revealing personal info. According to a system presented by authors in [72] for WSNs, clusters may be able to share common data, whereas some nodes within clusters may be required to share their private data with one another.

4.3 Impact/ Effects of Node Misbehaviour

We examine the impact of two basic categories of misbehaviour - routing and packet forwarding misbehaviour. Misbehaving nodes might cause network failure by not performing adequate routing and packet forwarding functions.

In the AODV routing protocol [73], the selfish node in an ad hoc network can do the following probable actions:

- Turn off its power when it is not in active contact with other nodes.
- Does not re-broadcast RREQ.
- Re-broadcasts RREQ without forwarding RREP on the reverse path, resulting in the source not knowing the route to the destination and having to re-broadcast an RREQ.
- Participate in routing but decline forwarding any data packets.
- Route Error (RERR) packets are not unicast or broadcasted when data packets are received, but there is no route to send them to.
- Drop data packets selectively. This may combat existing approaches for detecting selfish nodes in particular.

Based on the above risks, the detrimental selfish nodes in MANET can be seen, particularly in lowering the delivery rate by discarding packets and not forwarding them, resulting in MANET inefficiency. Furthermore, the existence of selfish nodes in a MANET might impair the network's proper operation (shown in Figure 18), and the deterioration intensifies with the number of selfish nodes; therefore, increasing the proportion of well-behaved nodes leads to increased node trust. This shall increase security and thus improve the operation of MANET. As a result, there is a huge incentive to address this issue.

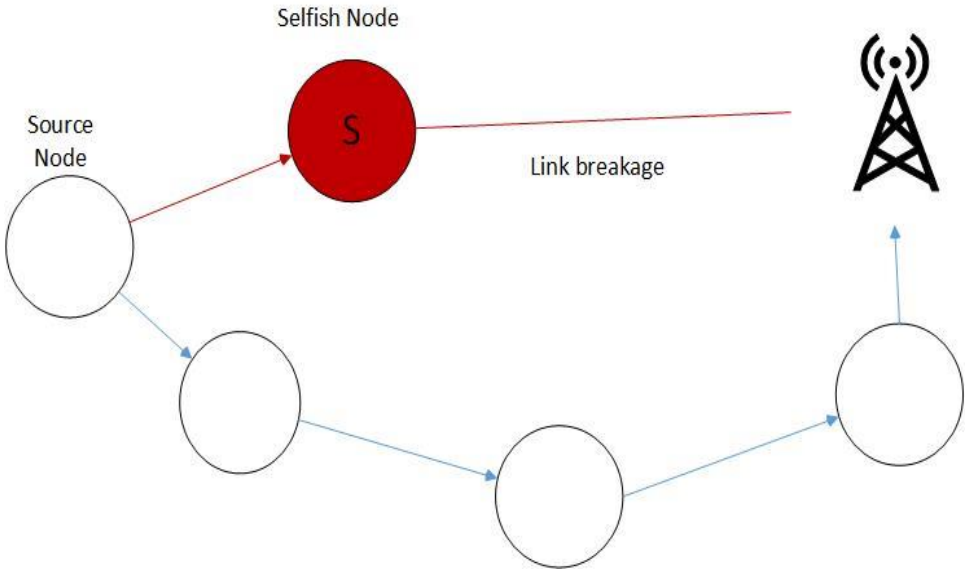

Fig. 18: Impact of a selfish node on routing

5.0 TECHNIQUES TO DETECT NODE MISBEHAVIOUR/MITIGATION OF NODE MISBEHAVIOUR

5.1 Audit-based

A system that isolates both selective and continuous packet droppers using an audit-based approach. Yu Zhang and Loukas Lazos [74] introduced Audit-based Misbehaviour Detection (AMD), a comprehensive approach for detecting and isolating selective and continuous packet droppers. The AMD system combines reputation management, reliable route discovery, and behavioural audits to identify problematic nodes. Resource-Efficient Accountability (REAct) is a revolutionary misbehaviour identification system presented by authors in their work [75]. This efficiently accounts for node misbehaviour. REAct discovers faulty nodes through random audits.

5.2 Credit-based

The central concept behind the suggested credit-based strategy for MANET is to reward mobile nodes for dependable network operations [76]. Virtual currency or a comparable electronic payment system is used to create incentives. Nodes earn money by offering services to other nodes. Whenever they request packet forwarding assistance from other nodes, they use the same payment system as before. Credit-based schemes have a significant disadvantage in virtual money or electronic payment systems because they typically necessitate the use of tamper-resistant hardware or additional protection. The principal contribution of the credit-based approach is to remove misbehaving nodes from routing paths, as follows:

- Typically, nodes receive credit for packet operations.
- The credit system is based on virtual currency.
- Nodes are the buyers and sellers of packets, and they require credits to forward their packets.

The credit-based strategy can be enhanced even further by taking into account the following factors:

- Because of the central electronic payment system or a bank, this approach is not scalable.
- Requires additional hardware on each node to prevent tampering.
- The cost of safeguarding virtual money or an electronic payment system.

5.3 Reputation-based

The fundamental goal of a reputation-based MANET solution is to identify problematic nodes through the monitoring process [77], [78], [79]. Every node in a network observes and recognises the behaviour of its neighbours in real-time, a technique known as direct or first-hand experience of reputation information. Furthermore, nodes can get reputation information from their neighbours, referred to as indirect or second-hand

reputation experience. The direct experience of reputation is given more weight in this method. However, a node's computed trust value is heavily influenced by its monitoring component.

The reputation-based method has a better chance of succeeding than the credit-based approach due to the following reasons:

- It does not necessitate using a virtual bank or network's central electronic payment system.
- At the node, it does not require any additional hardware, such as tamper-proof hardware.

This technology is more suited for use in a MANET since it can boost the network's scalability by implementing it in a distributed manner. This system collects, retains, and spreads reputation information from the network's nodes. A node with a good reputation can use the services, and a node with a bad reputation cannot. The promiscuous monitoring strategy is used by the majority of reputation-based systems. Each node keeps an eye on its neighbour for packet operations in a network.

5.4 Acknowledgement-based

On the successful reception of data packets, the acknowledgement provided by the destination node to the source node can be used to identify misbehaving nodes [80]. The fundamental premise of an acknowledgement-based strategy is that it is acknowledged when a source transmits data packets to a destination node. An acknowledgement is sent back from the receiving node in the reverse direction to show that the data packets have been successfully received. Only a percentage of received data packets are acknowledged to reduce further routing overhead. The reputation of the acknowledgements is used in this method. Protocol requirements determine whether acknowledgement packets are transmitted hop to hop or end-to-end.

Because they have less overhead in terms of memory and processing, acknowledgement systems are more promising than reputation-based systems.

5.5 Collaboration-based

A new technique for detecting selfish nodes, Collaborative Contact-based Watchdog (CoCoWa), was proposed by authors in [81] to combine local Watchdog detections with the distribution of this information across the network. When contact occurs, if one node has formerly discovered a selfish node, it can pass this information on to other nodes. This provides nodes with second-hand information about the network's selfish nodes.

5.6 Intrusion Detection Systems

Signature-based, specification-based IDS and anomaly-based models are used [82]. The specification-based IDS is utilised for MANETs, whereas the other two are meant for wired networks. In specification-based IDS, some security requirements are preserved by the node's correct behaviour. When any erroneous behaviour is seen, it is weighed against the stored specifications, and a detection decision is taken based on the comparison.

5.7 Cooperative Intrusion Detection System

Similar to the system presented in [83], the authors in [84] suggested a Cooperative Intrusion Detection System based on clustering methods. In this strategy, an intrusion is not only detected but the type of attack and the perpetrator is also identified. Statistical anomaly identification makes this feasible. Statistical formulae can be used to create attack detection criteria—these guidelines aid in determining the attack type and, in certain situations, the attacker node. IDS architecture is hierarchical in this approach, and every node has a fair chance of becoming the cluster leader. The data gathered from traffic would be monitored and evaluated for suspected intrusions. Monitoring the data collected from traffic, which is then examined for probable incursions, consumes energy. As a result, the cluster head is solely responsible for calculating traffic-related information rather than each node recording all characteristics. The cluster head is only one hop away, so it can hear all incoming and outgoing traffic (a clique: a group of nodes in which pairs of members can communicate over direct wireless links). As a result, member node energy consumption is lowered, although detection accuracy is marginally worse than when clusters are not employed. Furthermore, the total network performance has improved due to lower CPU consumption and network overhead.

5.8 Distributed Cooperative Mechanism (DCM)

To tackle the collaborative black hole assault, authors in [85] offer a Distributed and Cooperative technique called DCM. The nodes can evaluate, identify, and mitigate many black hole attacks since they work together. There are four sub-modules in the DCM. During the local data collection phase, each network node keeps an estimation table and examines the information in the overhearing packet to see whether any malicious nodes are present. The identified node initiates the local detection phase to determine if there is a potential black hole node, regardless of whether or not one suspicious node is discovered. The check packet is sent by the first detection node to the cooperating node. Whenever the inspection value is positive, it is assumed that the suspect node is normal. Or else, the initial detection node will initiate the cooperative detection method, which involves broadcasting and informing all one-hop neighbours so that they may participate in the decision-making process. The network traffic is raised since the notified mode uses the broadcasting approach. A restricted broadcasting technique is utilised to keep the notification range within a specified hop count. The maximum hop count range of cooperative detection messages is represented by a threshold. The global reaction phase is completed to construct a notification system and send a warning message throughout the network. In the global reaction phase, there exist reaction modes. When different threshold values are used, the notice delivery ratio ranges from 64.12 per cent (threshold 1) to 92.93 per cent (threshold 3). When these values are compared to those of the widely used AODV MANET routing protocol, simulation results show that DCM has a higher detection rate and data delivery ratio, even when there are multiple black hole nodes in the network. Because the distributed design technique DCM wastes little overhead, the control overhead may be decreased.

5.9 Snooping Packets Technique

Snooping protocols include two intrinsic properties in most MANET protocols [86]. The first feature is that each network node retains a list of nearby or routed nodes. The second is 802.11 and the Multiple Access with Collision Avoidance for Wireless (MACAW) link layer protocol, which allows a node to "hear" its neighbours' RTS / CTS transmissions. As a result, each node "snoops" on its neighbour's transmission during intrusion detection to verify that it is not distorted or misrouted. The Snooping nodes in this scheme, suitable for DSR and other routing protocols, listen to all nodes in their vicinity, unlike DSR's Watchdog and (CONFIDENT) Neighbourhood Watch, which only monitor the next node on the path. A node can detect a malicious node and initiate an isolation mechanism by monitoring neighbour transfers.

5.10 Backbone Nodes (BBN) Scheme

The technique to detect and eliminate the black hole and Gray hole attacks is addressed in the work [87]. This technique can locate the collaborating malicious node that causes huge packet drops. This strategy is used to break into their system model, and they also include a unique scheme to evade collaborative Gray and black attacks. In this technique, a backbone network is built from a collection of powerful backbone nodes (BBNs) spread over an ad hoc network. These trustworthy nodes can be given authority to allocate Routing Information Protocol (RIP) when a new node joins. When a node receives a RIP, it signifies it has been assigned a routing authority. Before transmitting data packets, the originating node asks for a RIP from the nearby BBN and then sends RREQ to the destination node with the RIP address. If the source node only receives RREP from the destination node, there isn't any indication of a black hole. When the source gets the RREP packet from RIP in this situation, it indicates that the adversary may be present in the network. The RIP neighbouring nodes convert to promiscuous mode due to the source node issuing monitor signals to alert them. This neighbourhood monitors not just the selected node's packets but also suspicious nodes. In addition, the source nodes transmit a few false data packets to the malicious node to test it. If the packet loss rate surpasses the typical threshold, the adjacent nodes flag it as a black hole and warn the source node of a hostile attacker. The neighbouring node adds the malicious nodes to the black hole list, which sends a warning message to the whole network. Finally, the attacker's authorisation will be removed, and all nodes will stop responding to nodes on the black list. Because its technique does not rely on trust, the suggested system identifies black holes and Gray hole attacks. However, because there is no experiment or simulated outcome, it is difficult to understand how the improved performance was achieved.

6.0 COMPARISON OF NODE MISBEHAVIOUR DETECTION METHODS

A comparison of various classical node misbehaviour detection schemes that are considered benchmarks for developing new node misbehaviour management methods has been displayed in Table 2.

Table 2: Pros and cons of node misbehaviour detection schemes

Methods	Pros	Cons
Audit-based technique [74], [75]	The probability of detecting an attacker is 93 per cent.	When attackers collaborate to forge fake reply packets, it fails.
Reputation-based technique [77], [78], [79]	SAODV detection rates range from 90 to 100 per cent, while AODV detection rate is about 70 per cent.	End-to-end delay increases if the malicious node is distant from the source node.
Acknowledgement-based technique [80]	Communication overhead is reduced; however, there is an increase in the identification delay.	A few more delays.
Distributed Cooperative Mechanism [85]	An increase in throughput performance.	Raised control overhead.
Backbone Nodes Scheme [87]	The rate of packet loss can be reduced.	Proves unsuccessful at a collaborative black hole attack.
Watchdog [81]	An increase in network throughput by 17-27 per cent.	False behaviour, receiver collisions, ambiguous collisions, low transmission power and partial drops make it difficult to detect misbehaviour.
Ex-Watchdog [3]	Throughput is up 11 per cent over Watchdog.	Partial dropping reduced transmission power and receiver collision.
2ACK [88]	Package delivery ratio increases to 90 per cent when just 40 per cent of nodes are misbehaving.	False misbehaviour and a 7 per cent increase in overhead.
IDS [82]	Increase in system efficiency.	Unable to identify DoS attempts and agents disconnect owing to link failure.
CONFIDANT [89]	Evade nodes that misbehave.	False misbehaviour and reduced transmission power.
CONFIDANT2 [90]	Ten per cent increase in throughput.	False behaviour, low transmission power and receiver collision.
Fast Random key scheme [91]	Faster and more accurate than 2ACK in detecting misbehaving nodes.	False misbehaviour.
Record and Trust-Based Detection (RTBD) Method [92]	An increase in packet delivery ratio by 18 per cent.	No neighbour node security.
Cooperative Bait Detection Scheme (CBDS) [52]	The packet delivery ratio improves by 95 per cent when the network size changes and by 90 per cent when mobility changes.	Less randomness when the next neighbourhood's address is used as bait.

7.0 CONCLUSION AND FUTURE WORK

MANETs are a collection of self-contained mobile devices that can function both as hosts and routers. No centralised controller is needed for this network, and it can be created or dismantled on-the-fly without relying on any fixed infrastructure. However, because of its changing topology, lack of centralised monitoring, and open medium, these qualities also render MANET vulnerable to passive and active attacks. This study began with a quick introduction to mobile ad hoc networks before delving into specific design constraints and limitations. Next, the

major security threats and solutions have been covered. Then we looked at the numerous ways a node might misbehave. This paper examines and compares existing strategies for controlling and mitigating misbehaving nodes in MANETs. Incentive-based detection, Trust-based detection, and Intrusion detection systems are all discussed in this study. A primary concern is that mobile devices are battery-operated and have restricted computational capabilities. So, researchers must consider this when devising security methods. A complete model of all known assaults would assist researchers in assessing protocol security. Additionally, such a model would enable the use of formal methods to test a security mechanism. Furthermore, it would aid researchers in developing a more comprehensive security solution rather than building specific security methods for dealing with specific security vulnerabilities. Another major challenge is to provide security systems that are both highly secure and high-performing on networks.

The investigation of security vulnerabilities and the development of defences against various attacks in MANET has occupied a substantial amount of research time. There is still a lot of work to be done in this field. The basic premise is that present security solutions have proven beneficial in protecting against recognised attacks but fail to defend against unexpected or combined attacks. Because of their unpredictable behaviour, there is always a small number of nodes (less than 5 per cent) in the network, which cannot be recognised using our technique. Monitoring time and threshold configurations considerably influence the number of nodes that are not discovered, and more research is needed in this area. Recent research shows that dropping attacks by several nodes can interrupt routing services for a long time without being discovered. An essential direction for future study would be to design a mitigation scheme capable of guarding against various collaborative attacks.

ACKNOWLEDGMENT

This research was funded by IIUM-UMP-UiTM Sustainable Research Collaboration Grant 2020 (SRCG) under Grant ID: SRCG20-013-0013.

The authors express their personal appreciation for the effort of Ms Gousia Nissar and Ms Manasha Saqib in proofreading, editing, and formatting the paper.

REFERENCES

[1] M. G. El-Hadidi, and M. A. Azer, "Traffic Analysis for Real Time Applications and its Effect on QoS in MANETs", in *2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, Cairo, Egypt, 26-27 May 2021, pp. 155-160, doi: 10.1109/miucc52538.2021.9447611.

[2] N. Priyanka, and N. Bhagirathi, "An Efficient and Secure Algorithm to Eliminate the Routing Misbehavior in MANETs", *International Journal of Scientific & Engineering Research*, Vol. 6, No. 5, 2015, pp. 117-122.

[3] R. Mali, and S. Bagade, "Techniques for Detection of Misbehaving Nodes in MANET: A Study", *International Journal of Scientific & Engineering Research*, Vol. 6, No. 8, 2015, pp. 1405-1411.

[4] O. Bushehrian, "Model-Based Service Selection for Reliable Service Access in MANET", *Malaysian Journal of Computer Science*, Vol. 27, No. 4, 2014, pp. 294-306.

[5] B. U. I. Khan, R. F. Olanrewaju, and M. H. Habaebi, "Malicious Behaviour of Node and its Significant Security Techniques in MANET-A Review", *Australian Journal of Basic and Applied Sciences*, Vol. 7, No. 12, 2013, pp. 286-293.

[6] B. U. I. Khan, N. F. Zulkurnain, R. F. Olanrewaju, G. Nissar, A. M. Baba, and S. A. Lone, "JIR2TA: Joint Invocation of Resource-Based Thresholding and Trust-Oriented Authentication in Mobile Adhoc Network", in *Proceedings of SAI Intelligent Systems Conference*, London, UK, 2016, pp. 689-701, doi: 10.1007/978-3-319-56991-8_50.

[7] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, A. R. Najeeb, and M. Yaacob, "A Survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 12, No. 2, 2018, pp. 832-842, doi: 10.11591/ijeecs.v12.i2.

[8] M. Rmayti, Gaïti Dominique, and R. Khatoun, "Misbehaviors Detection Schemes in Mobile Ad Hoc Networks", Ph.D. dissertation, Université de Technologie de Troyes, 2016.

[9] T. Yeferny, and S. Hamad, "Vehicular Ad-hoc Networks: Architecture, Applications and Challenges", *IJCSNS International Journal of Computer Science and Network Security*, Vol. 20, No. 2, 2020, pp. 1-7, doi: 10.48550/arXiv.2101.04539.

[10] L. Balico, A. A. Loureiro, E. F. Nakamura, R. S. Barreto, R. W. Pazzi, and H. A. Oliveira, "Localization Prediction in Vehicular Ad Hoc Networks", *IEEE Communications Surveys & Tutorials*, Vol. 20, No. 4, 2018, pp. 2784-2803, doi: 10.1109/COMST.2018.2841901.

[11] H. Fouchal, "Enhancing Coverage for Secure Communications over VANET", in *2018 IEEE Symposium on Computers and Communications (ISCC)*, Natal, Brazil, 25-28 June 2018, pp. 01132-01136, doi: 10.1109/ISCC.2018.8538767.

[12] D. Yue et al., "Cooperative Content Downloading in Hybrid VANETs: 3G/4G or RSUs Downloading", in *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY, USA, 18-20 November 2016, pp. 301-306, doi: 10.1109/SmartCloud.2016.24.

[13] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in Internet of Vehicles: A Review", *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16, No. 5, pp. 2339-2352, 2015, doi: 10.1109/TITS.2015.2423667.

[14] P. Tiwari, and R. S. Kushwah, "Traffic analysis for VANET using WAVE and WiMAX", in *2015 International Conference on Communication Networks (ICCN)*, Gwalior, India, 2015, pp. 343-346, doi: 10.1109/ICCN.2015.65.

[15] B. Rashid, and M. H. Rehmani, "Applications of Wireless Sensor Networks for Urban Areas: A Survey", *Journal of Network and Computer Applications*, Vol. 60, pp. 192-219, 2016, doi: 10.1016/j.jnca.2015.09.008.

[16] M. Diao, Y. Zhu, J. Ferreira, and C. Ratti, "Inferring individual Daily Activities from Mobile Phone Traces: A Boston Example", *Environment and Planning B: Planning and Design*, Vol. 43, No. 5, 2016, pp. 920-940, doi: 10.1177/0265813515600896.

[17] E. Paulos, and T. Jenkins, "Urban Probes: Encountering our Emerging Urban Atmospheres", in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Portland Oregon USA, 2-7 April 2005, pp. 341-350, doi: 10.1145/1054972.1055020.

[18] A. Rzotkiewicz, et al., "Systematic Review of the Use of Google Street View in health Research: Major Themes, Strengths, Weaknesses and Possibilities for Future Research", *Health & Place*, Vol. 52, 2018, pp. 240-246, doi: 10.1016/j.healthplace.2018.07.001.

[19] K. Chandrasekaran, *Essentials of Cloud Computing*, Boca Raton, Florida, United States, CRC Press, December 2014.

[20] N. Skeledzija, J. Cesic, E. Koco, V. Bachler, H. N. Vucemilo, and H. Dzapo, "Smart Home Automation System for Energy Efficient Housing", in *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 26-30 May 2014, pp. 166-171, doi: 10.1109/MIPRO.2014.6859554.

[21] A. Gupta, P. Verma, and R. S. Sambyal, "An Overview of MANET: Features, Challenges and Applications", *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, Vol. 4, No. 1, 2018, pp. 122-126, doi: 10.32628/CSEIT411820.

[22] S. Pandi, S. Wunderlich, and F. H. P. Fitzek, "Reliable Low Latency Wireless Mesh Networks — From Myth to Reality", in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 12-15 January 2018, pp. 1-2, doi: 10.1109/CCNC.2018.8319326.

[23] S. Ray, S. Saha, G. Roy, S. Sutradhar, R. Guhathakurta, R. Ghosh, S. Chowdhury, R. R. Chowdhury, S. Patra, C. Das, and P. Adhikary, "An Efficient Association of a Mobile Client in Wireless Mesh Network", in *2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada, 3-5 October 2017, pp. 497-500, doi: 10.1109/IEMCON.2017.8117225.

[24] K. Masroor, V. Jeoti, and M. Drieberg, "Improving the Energy Efficiency of a Wireless Body Area Network Using a Redundant Coordinator for Healthcare Applications", in *2018 International Conference on Intelligent and Advanced System (ICIAS)*, Vancouver, BC, Canada, 3-5 October, 2018, pp. 1-5, doi: 10.1109/ICIAS.2018.8540624.

[25] M. Cuka, "IoT Device Selection in Opportunistic Networks: Implementation and Performance Evaluation of Fuzzy-based Intelligent Systems and a Testbed", Doctoral Dissertation, Fukuoka Institute of Technology Japan, 2020.

[26] S. Xin, W. Ben-yuan, G. Li, and A. M. Liton, "Low Delay and Low Overhead Terahertz Wireless Personal Area Networks Directional MAC Protocols", in *2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP)*, Xi'an, China, 9-11 April 2021, pp. 687-691, doi: 10.1109/ICSP51882.2021.9408779.

[27] D. S. Teotia, "A Review on Mobility and the Routing Protocols in Mobile Ad-Hoc Networks", 2020, doi: 10.2139/ssrn.3579888.

[28] K. Kwan and B. Greaves, "FileLinker: Simple Peer-to-Peer File Sharing Using Wi-Fi Direct and NFC", in *2019 IST-Africa Week Conference (IST-Africa)*, Nairobi, Kenya, 2019, pp. 1-9, doi: 10.23919/ISTAFRICA.2019.8764840.

[29] M. Rath, et al., "Network Security: Attacks and Control in MANET", *Handbook of Research on Network Forensics and Analysis Techniques*, Pennsylvania, United States, IGI Global, 2018, pp. 19-37, doi: 10.4018/978-1-5225-4100-4.ch002.

[30] S. Azfar, A. Nadeem, K. Ahsan, and M. Sarim, "Impact Analysis and a Detection Method for Misbehaving Nodes in Mobile Ad-hoc Networks", *Journal of Basic and Applied Scientific Research*, Vol. 4, No. 8, 2019, pp. 26-35.

[31] R. F. Olanrewaju, B. U. I. Khan, F. Anwar, B. R. Pampori, and R. N. Mir, "MANET Security Appraisal: Challenges, Essentials, Attacks, Countermeasures & Future Directions", *International Journal of Recent Technology and Engineering*, Vol. 8, No. 6, 2020, pp. 3013-3024, doi: 10.35940/ijrte.e6537.038620.

[32] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs", in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, Amman, Jordan, 2019, pp. 28-33, doi: 10.1109/JEEIT.2019.8717449.

[33] P. Tonane, and S. Deshpande, "Trust Based Certificate Revocation and Attacks in MANETs", in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, India, 2018, pp. 1089-1093, doi: 10.1109/ICICCT.2018.8473238.

[34] R. Meddeb, B. Triki, F. Jemili, and O. Korbaa, "A Survey of Attacks in Mobile Ad Hoc Networks", in *2017 International Conference on Engineering & MIS (ICEMIS)*, Monastir, Tunisia, 8-10 May 2017, pp. 1-7, doi: 10.1109/ICEMIS.2017.8273007.

[35] R. F. Olanrewaju, F. Anwar, R. N. Mir, M. Yaacob, and T. Mehraj, "Bayesian Signaling Game Based Efficient Security Model for MANETs", in *Future of Information and Communication Conference*, San Francisco, USA, 2019, pp. 1106-1122, doi: 10.1007/978-3-030-12385-7_75.

[36] S. N. Mohammad, "Security Attacks in MANETS (Survey Prospective)", *International Journal of Engineering and Advanced Technology (IJEAT)*, Vol. 6, No. 3, 2017, pp. 93-96.

[37] Y. Lin, and J. Chang, "Improving Wireless Network Security Based on Radio Fingerprinting", in *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion*, Sofia, Bulgaria, 22-26 July 2019, pp. 375-379, doi: 10.1109/QRS-C.2019.00076.

[38] V. Singh, D. Singh, and M. M. Hassan, "Survey: Black Hole Attack Detection in MANET", in *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*, Sultanpur, India, 2019, pp. 522-525, doi: 10.2139/ssrn.3351016.

[39] E. Shakshuki, N. Kang, X. Xing, and T. Sheltami, "Tracking Anonymous Sinks in Wireless Sensor Networks", in *IEEE 23rd International Conference on Advanced Information Networking and Applications*, Bradford, UK, 26-29 May 2009, pp. 510-516, doi: 10.1109/AINA.2009.61.

[40] K. Hussain, S. J. Hussain, N. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET", in *2019 International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia, 2019, pp. 1-4, doi: 10.1109/ICCISci.2019.8716416.

[41] G. Paliwal, A. P. Mudgal, and S. Taterh, "A Study on Various Attacks of TCP/IP and Security Challenges in MANET Layer Architecture", in *Proceedings of Fourth International Conference on Soft Computing for Problem Solving*, pp. 195-207. Springer, New Delhi, 2015, doi: 10.1007/978-81-322-2220-0_16.

[42] P. Kaneria, and A. Rajavat, "Detecting and Avoiding of Worm Hole Attack on MANET Using Trusted AODV Routing Algorithm", in *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, Indore, India, 18-19 March 2016, pp. 1-5, doi: 10.1109/CDAN.2016.7570907.

[43] M. Abdelhafez, G. Riley, R. Cole, and N. Phamdo, "Modeling and Simulations of TCP MANET Worms", in *Proceedings of the 21st International Workshop on Principles of Advanced and Distributed Simulation*, San Diego, CA, USA, 12-15 June 2007, pp. 123-130, doi: 10.1109/PADS.2007.25.

[44] A. M. Kurkure, and B. Chaudhari, "Analysing Credit Based ARAN To Detect Selfish Nodes in MANET", in *2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014)*, Unnao, India, 1-2 August 2014, pp. 1-5, doi: 10.1109/ICAETR.2014.7012851.

[45] H. M. I. M. Zain, "A Proposed Method to Detect Misbehaving Nodes During Route Discovery Phase in MANET's", Ph.D. dissertation, University of Science and Technology, 2017.

[46] S. Tripathi, "Performance Analysis of AODV and DSR Routing Protocols of MANET under Wormhole Attack and a Suggested Trust Based Routing Algorithm for DSR", in *2019 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)*, Bangalore, India, 2019, pp. 1-5, doi: 10.1109/WIECON-ECE48653.2019.9019971.

[47] R. John, J. P. Cherian, and J. J. Kizhakkethottam, "A Survey of Techniques to Prevent Sybil Attacks", in *2015 International Conference on Soft-Computing and Networks Security (ICSNS)*, Coimbatore, India, 25-27 February 2015, pp. 1-6, doi: 10.1109/ICSNS.2015.7292385.

[48] D. Khan, and M. Jamil, "Study of Detecting and Overcoming Black Hole Attacks in MANET: A Review", in *2017 International Symposium on Wireless Systems and Networks (ISWSN)*, Lahore, Pakistan, 19-22 November 2017, pp. 1-4, doi: 10.1109/ISWSN.2017.8250039.

[49] P. Roshani, and A. Patel, "Techniques to Mitigate Grayhole Attack in MANET: A Survey", in *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, India, 2017, pp. 1-4, doi: 10.1109/ICIIECS.2017.8276064.

[50] S. Gurung, and S. Chauhan, "A Novel Approach for Mitigating Route Request Flooding Attack in MANET", *Wireless Networks*, Vol. 24, 2018, pp. 2899-2914, doi: 10.1007/s11276-017-1515-0.

[51] T. Jamal, and S. A. Butt, "Malicious Node Analysis in MANETS", *International Journal of Information Technology*, Vol. 11, 2019, pp. 859-867, doi: 10.1007/s41870-018-0168-2.

[52] M. Umar, A. Sabo, and A. A. Tata, "Modified Cooperative Bait Detection Scheme for Detecting and Preventing Cooperative Blackhole and Eavesdropping Attacks in MANET", in *2018 International Conference on Networking and Network Applications (NaNA)*, Xi'an, China, 2018, pp. 121-126, doi: 10.1109/NANA.2018.8648739.

[53] B. U. I. Khan, R. F. Olanrewaju, R. N. Mir, A. Baba, and B. W. Adebayo, "Strategic Profiling for Behaviour Visualization of Malicious Node in MANETs Using Game Theory", *Journal of Theoretical & Applied Information Technology*, Vol. 77, No. 1, 2015, pp. 25-43.

[54] Mahdavi, B. Najafpour, S. Nejhad, M. Sardarpour, and N. L. Navid, "Application of Artificial Immune System for Detection of Misbehaviour Nodes in MANET", *Journal of Basic and Applied Scientific Research*, Vol. 3, No. 1s, 2013, pp. 160-164.

[55] S. Kurosawa, and A. Jamalipor, "Detecting Black Hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", *International Journal of Network Security*, Vol. 5, No. 3, 2007, pp 338-345.

[56] J. Sen, M. G. Chandra, S. G. Harihara, H. Reddy and P. Balamuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", in *2007 6th International Conference on Information, Communications & Signal Processing*, Singapore, 10-13 December 2007, pp. 1-5, doi: 10.1109/ICICS.2007.4449664.

[57] S. Dhende, S. Musale, S. Shirbahadurkar and A. Najan, "SAODV: Black Hole and Gray Hole Attack Detection Protocol in MANETs", in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2017, pp. 2391-2394, doi: 10.1109/WiSPNET.2017.8300188.

[58] N. Garg, and R. P. Mahapatra "MANET Security Issues", *International Journal of Computer Science and Network Security*, Vol. 9, No. 8, 2009, pp. 241-246.

[59] D. B. Roy, and R. Chaki, "MADSN: Mobile Agent Based Detection of Selfish Nodes in MANET", *International Journal of Wireless & Mobile Networks (IJWMN)*, Vol. 3, No. 4, 2011, pp. 225-235, doi: 10.5121/ijwmn.2011.3416.

[60] K. R. Abirami, and M. G. Sumithra, "Preventing the Impact of Selfish Behavior Under MANET Using Neighbor Credit Value Based AODV Routing Algorithm," Sādhanā, Vol. 43, No. 60, 2016, pp. 1-7, doi: 10.1007/s12046-018-0803-4.

[61] L. E. Jim, and M. A. Gregory, "Improvised MANET Selfish Node Detection using Artificial Immune System based Decision Tree", in *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, Auckland, New Zealand, 27-29 November 2019, pp. 1-6, doi: 10.1109/ITNAC46935.2019.9077968.

[62] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, and R. N. Mir, "ECM-GT: Design of Efficient Computational Modelling Based on Game Theoretical Approach Towards Enhancing the Security Solutions in MANET, "*International Journal of Innovative Technology and Exploring Engineering (IJITEE)*", Vol. 8, No. 7, 2019, pp. 506-519.

[63] M. A. Khan et al., "A Survey on the Noncooperative Environment in Smart Nodes-Based Ad Hoc Networks: Motivations and Solutions", *Security and Communication Networks*, Vol. 2021, 2021, pp. 1-17, doi: 10.1155/2021/9921826.

[64] G. S. Brar, S. Rani, V. Chopra, R. Malhotra, H. Song, and S. H. Ahmed, "Energy Efficient Direction-Based PDORP Routing Protocol for WSN", *IEEE Access*, Vol. 4, 2016, pp. 3182-3194, doi: 10.1109/ACCESS.2016.2576475.

[65] X. Wu, G. Chen, and S. K. Das, "Avoiding Energy Holes in Wireless Sensor Networks with Nonuniform Node Distribution", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 19, No. 5, 2008, pp. 710-720, doi: 10.1109/TPDS.2007.70770.

[66] M. M. Umar, S. Khan, R. Ahmad, and D. Singh, "Game Theoretic Reward Based Adaptive Data Communication in Security and Communication Networks Wireless Sensor Networks", *IEEE Access*, Vol. 6, No. 1, 2018, pp. 28073-28084, doi: 10.1109/ACCESS.2018.2833468.

[67] M. Manjula, and P. Elango, "A Survey of Selfish Nodes Behaviour in Mobile Adhoc Network", *International Journal of Computer Trends and Technology (IJCTT)*, Vol. 4, No. 6, 2013, pp. 1848-1851.

[68] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission with Optimised Network Operations in Futuristic Mobile Adhoc Networks", *IEEE Access*, Vol. 8, 2020, pp. 124097-124109, doi: 10.1109/ACCESS.2020.3006043.

[69] C. Sinha, "Providing social likeness within a messaging context", U.S Patent 8600901, 3 December 2013.

[70] J. Wu, Y. Zhu, L. Liu, B. Yu and J. Pan, "Energy-Efficient Routing in Multi-Community DTN with Social Selfishness Considerations", in *2016 IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, USA, 2016, pp. 1-7, doi: 10.1109/GLOCOM.2016.7841809.

[71] D. Wu, D. I. Arkhipov, E. Asmare, Z. Qin and J. A. McCann, "UbiFlow: Mobility Management in Urban-Scale Software Defined IoT", in *2015 IEEE Conference on Computer Communications (INFOCOM)*, Hong Kong, China, 2015, pp. 208-216, doi: 10.1109/INFOCOM.2015.7218384.

[72] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: Privacy-Preserving Data Aggregation in Wireless Sensor Networks", in *Proceedings of the INFOCOM 2007, 26th IEEE International Conference on Computer Communications*, Anchorage, AK, USA, 6-12 May 2007, pp. 2045-2053, doi: 10.1109/INFCOM.2007.237.

[73] K. S. Patel, and J. S. Shah, "Study the Effect of Packet Drop Attack in AODV Routing and MANET and Detection of Such Node in MANET", in *Proceedings of International Conference on ICT for Sustainable Development*, pp. 135-142, Singapore, Springer, 2016, doi: 10.1007/978-981-10-0129-1_15.

[74] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, Vol. 15, No. 8, 2016, pp. 1893-1907, doi: 10.1109/TMC.2012.257.

[75] W. Kozma, and L. Lazos, "REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits", in *WiSec '09: Proceedings of the Second ACM Conference on Wireless Network Security*, Zurich Switzerland, 16-19 March 2009, pp. 103-110, doi: 10.1145/1514274.1514290.

[76] M. M. Ghonge, P. M. Jawandhiya, and V. M. Thakare, "Selfish Attack Detection in Mobile Ad Hoc Networks", in *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, India, 17-18 March 2017, pp. 1-4, doi: 10.1109/ICIIECS.2017.8276136.

[77] S. N. Shah, and R. H. Jhaveri, "A Trust-Based Scheme Against Packet Dropping Attacks in MANETs", in *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, Bangalore, India, 21-23 July 2016, pp. 68-75, doi: 10.1109/ICATCCT.2016.7911967.

[78] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, M. Kiah and R. Mir, "Game Theory Analysis and Modeling of Sophisticated Multi-Collusion Attack in MANETs", *IEEE Access*, Vol. 9, 2021, pp. 61778-61792, doi: 10.1109/access.2021.3073343.

[79] N. Bhalaji, and C. Selvaraj, "Comprehensive Trust Based Scheme to Combat Malicious Nodes in MANET Based Cyber Physical Systems", in *Proceedings of International Conference on Communication and Networks*, Singapore, Springer, 2017, pp. 534-550, doi: 10.1007/978-981-10-2750-5_56.

[80] A. Bansal, A. Varshney, R. Matta, and A. Khanna, "Acknowledgement Based Approaches for Detecting Routing Misbehaviour in MANETs", in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 16-18 March 2016, pp. 835-840.

[81] E. Hernandez-Orallo, M. D. S. Olmos, J. C. Cano, C. T. Calafate, and P. Manzoni, "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes", *IEEE Transactions on Mobile Computing*, Vol. 14, No. 6, 2015, pp. 1162-1175, doi: 10.1109/TMC.2014.2343627.

[82] S. Smys, A. Basar, and H. Wang, "Hybrid Intrusion Detection System for Internet of Things (IoT)", *Journal of ISMAC*, Vol. 2, No. 4, 2020, pp. 190-199, doi: 10.36548/jismac.2020.4.002.

[83] H. Al-Hujailan, M. Al-Rodhaan, and A. Al-Dhelaan, "A Cooperative Intrusion Detection Scheme for Clustered Mobile Ad Hoc Networks", in *2011 7th International Conference on Information Assurance and Security (IAS)*, Melacca, Malaysia, 5-8 December 2011, pp. 179-185, doi: 10.1109/ISIAS.2011.6122816.

[84] T. S. Bharati, and R. Kumar, "Secure Intrusion Detection System for Mobile Adhoc Networks", in *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 11-13 March 2015, pp. 1257-1261.

[85] C. W. Yu, T. K. Wu, R. H. Cheng, and S. C. Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", in *Emerging Technologies in Knowledge Discovery and Data Mining*, Berlin, Heidelberg, Springer, 2007, pp. 538-549, doi: 10.1007/978-3-540-77018-3_54.

[86] S. Padiya, R. Pandit, and S. Patel, "Survey of Innovated Techniques to Detect Selfish Nodes", *Elixir Network Engineering*, Vol. 75, 2014, pp. 27887-27891.

[87] K. Vishnu, and A. J. Paul, "Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile AdHoc Networks", *International Journal of Computer Applications*, Vol. 1, No. 22, 2010, pp. 40-44, doi: 10.5120/445-679.

[88] W. Li, A. Joshi, and T. Finin, "Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-dimensional Trust Management Approach", in *2010 Eleventh International Conference on Mobile Data Management*, Kansas City, MO, USA, 2010, pp. 85-94, doi: 10.1109/MDM.2010.57.

[89] S. Mittal, and S. Dahiya, "Identification Technique for All Passive Selfish Node Attacks in a Mobile Network", *International Journal of Advance Research in Computer Science and Management Studies*, Vol. 3, No. 4, 2015, pp. 46-51.

[90] S. Buchegger, and J. Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol", in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, Lausanne, Switzerland, 2002, pp. 226-236, doi: 10.1145/513800.513828.

[91] J. Indhumathi, and T. P. Jacob, "Identification of Misbehaviour Activities in Mobile Adhoc Networks", *International Journal of Computer Science and Information Technologies*, Vol. 5, No. 2, 2014, pp. 1200-1203.

[92] S. Subramaniyan, W. Johnson, and K. Subramaniyan, "A Distributed Framework for Detecting Selfish Nodes in MANET using Record- and Trust-Based Detection (RTBD) Technique", *EURASIP Journal on Wireless Communications and Networking*, Springer, Vol. 2014, No. 1, 2014, pp. 1-10, doi: 10.1186/1687-1499-2014-205.