International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

MANET Security Appraisal: Challenges, Essentials, Attacks, Countermeasures & Future Directions

Rashidah F. Olanrewaju, Burhan Ul Islam Khan, Farhat Anwar, Bisma Rasool Pampori, Roohie Naaz Mir

Abstract*: Currently, Mobile Ad hoc Networks (MANETs) have evolved as one of the essential next-generation wireless network technologies. MANET comprises of mobile nodes that are self-configurable, and every mobile node behaves as a router for every other node allowing data to move by making use of multi-hop network routes. MANETs signify a networking class that is crucial and differs from conventional systems. Although MANETs are being popularly employed in commercial as well as academic fields, these were primarily designed for deployment in areas like military battlefields, emergency rescue and search operations, and other challenging or hostile environments. The distributed and wireless nature of MANETs paves the way for intruders to reduce MANET functionalities. MANET are susceptible to various attack at different layers since the majority of MANET routing protocols are designed with the assumption that no malicious intruder is present in the network. Therefore, recognizing those threats and finding solutions for their mitigation become essential. This study analyses various security attributes, challenges, attacks on multiple layers and countermeasures for thwarting attacks in MANETs.

Keywords*: Intrusion detection system, MANET security, secure MANET routing, MANET security attacks.

I. INTRODUCTION

In mobile communication technology, Mobile Adhoc Networks (or MANETs) are among the most topics discussed in the research community. MANET is formed of a group of mobile nodes that are devoid of a network infrastructure [1]. The MANET nodes interact with each other using radio waves. MANETs are distinguished by (a) wireless communication, (b) nodes having a dual job of acting as hosts and a router (c) decentralized control and lack of infrastructure. (d) dynamic change of network topology accompanied by regular routing updates, (e) easy deployment, (f) Scalable network, (g) Self-administration, self-configuration, and self-creation, (h) Cooperative and distributed nature of working, (i) Restriction on device size, (j) easy deployment, (k) constraint bandwidth utilization, (l) minimum human intervention for network configuration, (m) automatic reconfiguration, (n) device heterogeneity, and (o) multi-hop radio transmission [2], [3].

MANETs find extensive use in military operations, sensor networks, emergency relief and rescue missions, medical service, quarry site procedures, robot data acquirement, the commercial sector, personal area networks, etc. [4]-[6]. Contrary to the years of current research, there is an evolution in the area of mobile ad hoc networks representing the future trend of its services and applications, chiefly owing to new hardware development (smart vehicles, intelligent drones, UAVs, etc.) as well as evolving software (embedded platforms) [7]. Also, more application/service-oriented research issues integrated with the industrial as well as business-related services of Internet-of-Things (IoT) like smart home, smart vehicles, smart grid, etc. are emerging in the domain of sensor networks that is a chief component of MANETs. Undoubtedly, it is a new trend that is being faced and is typified by several unique challenges.

Delay-tolerant networking or DTN has been one of the most active research fields in MANETs in recent years. A DTN might be disintegrated into sub-networks temporarily due to insufficient transmission range, node movements, or hurdles in the environment. Pedestrian smartphone network, tactical network, or vehicular network exemplify a DTN [7].

The chief goal of MANETs is ensuring users access to mobile resources. MANETs are signified by dynamic topologies such that the mobile nodes keep moving randomly and assuming the next mobility point is not possible. Due to such a topology, MANET nodes should ensure to have highly stabilized routing since the chances of intermittent link increase as the nodes move. This shall also imply that mobile nodes have to perform constant listening mode with all the network nodes and their routing tables need to be updated regularly. Thus, enormous energy is depleted, leading to a reduction in node performance, thereby affecting the performance of the network gradually. As a result, it is observed that there are various issues related to MANET such as bandwidth consumption, inter-arrival time, energy drainage, routing, latency, unstabilized or intermittent links, etc. [1], [8].

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Burhan Ul Islam Khan*, Department of Elec. & Comp. Engin, Kulliyyah of Engineering, IIUM Malaysia. Email: burhan.iium@gmail.com
Rashidah F. Olanrewaju, Department of Elec. & Comp. Engin, Kulliyyah of Engineering, IIUM Malaysia.
Farhat Anwar, Department of Elec. & Comp. Engin, Kulliyyah of Engineering, IIUM Malaysia.
Bisma Rasool Pampori, Department of IT, CUK, Srinagar, Kashmir.
Roohie Naaz Mir, Department of CSE, NIT, Srinagar, Kashmir.

In the recent past, there were substantial research efforts where the chief goal was the enhancement and design of routing protocols. Though there are several MANET routing protocols [9], 98% of the research works conducted so far, focus only on protocols like DSDV (Destination Sequence Distance Vector), OLSR (Optimized Link State Routing),

AODV (Adhoc On-Demand Distance vector) and DSR (Dynamic Source Routing). These protocols have their respective pros and cons that prompt the researchers to design a new routing protocol or enhance the existing ones. Besides the performance issue of MANETs, security is another issue that is yet to be solved [10]. Some works such as [11]-[17] have discussed several security threats and techniques for mitigating the same. The diverse security threats and attacks that have been analysed so far comprise Sybil attack, cloning attack, black hole attack, flooding or Denial-of-Service attack, sinkhole attack, rushing attack, packet dropping, etc. [18]. To provide secure MANET communication, understanding the variety of attacks possible at various MANET layers is essential. This study aims to present a comprehensive and structured review of the well-known security attacks, threats and security approaches in MANETs.

The paper is organized into various sections with Section II discussing the security vulnerabilities in MANETs. A discussion on multiple MANET security attributes has been given in Section III, and Section IV deliberates about trust as an essential security feature in MANETs. The various type of attacks frequently observed in MANETs have been put in detail in Section V, and the consequences of those attacks on MANETs have been given in Section VI. This is followed by detailed information about the preventive and reactive security solutions in MANETs in Section VII. Finally, the paper is concluded with an elucidation on future research direction in MANETs and concluding remarks in Section VIII and IX, respectively.

II. SECURITY CHALLENGES IN MANET

MANETs comprise of the most exciting networks. MANETs are exposed to a variety of active as well as passive attacks since it makes use of air and hostile environments as a medium. Active attacks are conducted by opponents that are fully equipped with high-tech tools. They can modify data transmitted through the network as well as corrupting the functionality of the system by making alterations in link-related updates, topology and routing. Examples of active attacks include Blackhole attack, impersonation, DoS, Byzantine attack, Distributed DoS, wormhole attack, etc. On the other hand, passive attacks are performed by opponents that have insufficient abilities. Passive attacks are exemplified by traffic analysis, eavesdropping, etc. Some open issues and fundamental limitations of MANET security aspects have been discussed in this section.

A. Distributed Management

No centralized management can be established in MANETs owing to its adhoc installation and peer-to-peer characteristic of nodes. Due to the absence of this centralized control and distributed nature of the network, maintenance of new node generations, loss of control in topology changes, authenticating new nodes and secure data distribution as well as keying information are affected. Furthermore, it also makes attack detection complex since no central point monitors the traffic in such a large-scale and very dynamic adhoc network [2].

B. Limited Resource

There is a shortage of bandwidth, power resources, and computational constraints in adhoc networks due to temporal and adhoc deployment in harsh environments with limited resources. Adhoc networks have become a playground for both developers and attackers owing to the restricted resources, and its solution space has also been significantly affected [19].

C. Cooperativeness

MANETs have transformed from client-server networks to cooperative networks owing to the absence of a central manager and peer-to-peer architecture. This collaborative nature seeks trust among the network nodes during routing or any data exchange. A change in this cooperative nature results in compromised or selfish nodes establishing necessitates forced cooperation among MANET nodes and customized MANET security solutions [20], [21].

D. Dynamic topology

Energy depletion in nodes, node mobility, physical hurdles, and node revocation due to actions against selfish and malicious nodes and node compromises, due to the dynamic nature of MANET necessitates adaptive security solutions.

E. Wireless medium

The free access provided to the wireless medium in MANETs makes it vulnerable to various attacks like active interference and eavesdropping. Malicious nodes can make use of this wireless medium for injecting spoofed packets or modifying other mobile node transmissions.

F. Infrastructure-less

No specific infrastructure is available in MANETs to address security services like certificates, key distribution, etc.

G. Threats from compromised nodes within the network

The risks from the nodes compromised within the network can be more threatening when attackers possess the valid decryption as well as encryption keys and utilise them to perform malicious actions. Also, such attackers attempt to conduct new attacks not known to the secure system [2].

H. Absence of secure boundaries

MANETs fail to provide safe boundaries from the outside surroundings for securing against undesirable access to the network, thereby making it vulnerable to passive attacks.

III. SECURITY REQUIREMENTS IN MANET

The domain of security is vast, and the network can be considered to be secure if the attributes described below hold good. Systems that deal with the exchange of sensitive information should make use of some model to ensure security from attacks. The complementary attributes should be taken into consideration to characterize the various security needs of adhoc networks.

Retrieval Number: E6537018520/2020©BEIESP
DOI:10.35940/ijrte.E6537.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Since nodes are connected to MANETs for a limited time, real-time restraints need to be maintained to achieve the goal of controlled access to limited resources. The critical requirements for networks are as follows [22]:

Confidentiality – In MANET, every node or application is allowed to access only a specific set of services of the applications that are being used currently. Confidentiality is required to prevent an opponent from traffic analysis and to protect the data.

Integrity – It is the property of the authorized network nodes to edit, delete or create packets. Such a feature ensures that messages or data are not modified by the assailants while in transit. Otherwise, the modified crucial data may directly affect the users.

Authentication – There should be trustable communications between two different nodes. Nodes should respond to only those messages that are transmitted by authentic network members. Therefore, it is essential that the message sender is authenticated, and another node be authorized to update information or to receive information.

Non-Repudiation – This feature makes sure that the source or destination do not deny having sent or received any data. It assists in isolating the malicious nodes. At any point of time, when there is an investigation on the identity of a node, the sender must not deny the message transmission.

Availability – One of the features of the network is ensuring that authorized nodes can provide services and data despite all threats or attacks. Even if the system is attacked, it should be accessible through alternate methods without any effect on its performance.

The certainty of discovery – It makes sure that the source node acquires the destination node address by employing a route discovery process before dispatching the packets to the destined node.

Lightweight computations – Computations on route discovery can be performed with ease.

Isolation – This property prevents a particular network node from communicating with any other network node.

Data Verification – After validating the sender, the destination node performs verification to ascertain if the message received contains the undermined or right information.

Attack Resilience – It is needed for supporting the functionalities of the system in case some nodes are crushed or traded off.

Privacy – It prevents the individual's private information data against unapproved or unauthorized access.

Freshness – It guarantees that the malicious nodes refrain from sending the received packets beforehand.

IV. TRUST IN MANET

Trust is considered, by a basic description, to be a measure of subjective opinion that one party or person uses to evaluate the probability that another person or party will execute a favourable action when the opportunity presents itself and to observe whether that motion has occurred [22]. Whenever intended to facilitate with high-probability, the activities one person or party are expected to execute will be done advantageously. When making trust associations among the participating nodes, it is crucial to enable collaborative optimization of program metrics. This notion is vital for the development of communication and network functionalities by the designers. A key consideration that outlines the importance of the subject concerning the security of MANETs is that trust is always required in developing relationships when there is uncertainty. This is in line with the problem of MANETs, where unforeseen behaviour is the chief concern. Trust is defined as the behaviour of a group of associations among things contributing in a process, with the associations based on the proof created by the earlier communications of entities. A trust may occur between these entities in the event the interactions happen to be true to the process afterwards. In another way, trust is the amount of faith in regard to the behaviour of new things (representatives). In MANETs, the trust may be described as a level of belief as per node/agent/entity behaviour. The probability value of trust can be either 0 to1, with 0 signifying DISTRUST and 1 signifying TRUST [23].

A. Features of trust in MANETs

Attributable to the wireless medium of MANETs, characteristics and the theory, trust must be cautiously defined [22]. The essential features of MANET trust are:

- A decision technique to verify trust toward an entity has to be wholly spread because the being of a trusted third party (e.g., a trusted central certification authority) may not be supposed.
- Trust must be confirmed in a well-customized way without too much communication load and computation, even while apprehending the intricacies of the belief association.
- Decision support for MANETs must not believe that the node(s) are co-operative. In selfishness and resource-constrained environments, it is possible to be widespread above collaboration [23].
- Trust can't be static. It is dynamic.
- Trust is subjective.
- Trust is not transitive. The reality is that A trusts B and B trusts C does not conclude that A trusts C.
- Trust is considered as asymmetric, but mostly it is not reciprocal.
- Trust is dependent on context. A may trust B in one aspect but, not in the other.

In MANETs, most of the node(s) participating in routing, require high computational power. Thus, the nodes with high battery power are considered to be trusted while the nodes with low battery power although genuine (not malicious) are not trusted.

B. Centralized Versus Decentralized Trust

Centralized trust refers to the state in which for each additional node in the system trust values are calculated by a common trusted node. All user node(s) of the method request this trusted node to provide them with advice about the additional node(s). The state explained here has two main implications. First, it's reasonable to suppose that a distinct user node(s) is likely to have divergent opinions regarding the same target node. Secondly, since every other user node is dependent upon the trustworthiness of this distinct node, it leads to a single point of failure. This fact is covered up in a decentralized scheme of the trust issue where a node communicates to every user node, thus being the centre of its world. i.e., user node(s) are accountable for computing their very own trust values for almost any target node they desire. This "bottom-up" approach is the most widely implemented [22].

V. CLASSIFICATION OF MANET ATTACKS

The attacks in mobile adhoc networks can be grouped based on various criteria such as source/domain, nature/behaviour of attack, the number of attackers involved and processing capacity.

A. Based on source/domain

a) Internal attack – The attackers, in this case, are present inside the network; therefore, any node in the system is malicious.

b) External attack – The attacker is present external to the network peripheries and attacks the unknown node or entity.

B. Based on nature/behaviour

a) Active attack – Active attacks are attempts at modifying or altering data without legal permission. Injecting false packets into the actual data stream to gain authorization is also included in such attacks. Such type of attacks can further be external or internal.

b) Passive attack – Passive attacks try to gain confidential information after monitoring network traffic without interfering in the functioning of the routing protocol.

C. Based on processing capacity

a) Wired – The intruders employ a wired medium to gain unauthorized access.

b) Mobile – The intruders utilise a wireless medium to gain unauthorized access.

D. Based on the number of attackers

a) Single – Only a single person or malicious node disrupts the usual flow of the network.

b) Multiple – More than one person or malicious node get together to disrupt the normal network functioning.

E. Attacks corresponding to different MANET layers

The description of various attacks based on distinct layers of MANET is given in Table I.

Table- I: Attacks on various MANET layers

Layer	Attack
Physical	Jamming, interceptions, eavesdropping, active interference, malicious message injecting
Data Link	Traffic analysis, monitoring, SYN flooding, TCP ACK storm
Network	Spoofing, wormhole, grey hole, Byzantine, blackhole, resource consumption, flooding, location disclosure attacks, Sybil, routing attacks, sinkhole
Application	Repudiation, malicious code, data corruption
Transport	Session hijacking, TCP ACK storm, SYN flooding, jellyfish
Multi-Layer	DoS, replay, man-in-the-middle, impersonation

These attacks have been summarized below:

1) Black-Hole Attack

The attacker establishes a path to a specified destination via itself and transmits false routing packets. When the data packets reach the point, those packets are dropped away (as shown in Fig. 1), thus outlining a black hole (or dark gap) where information keeps entering without leaving [24].

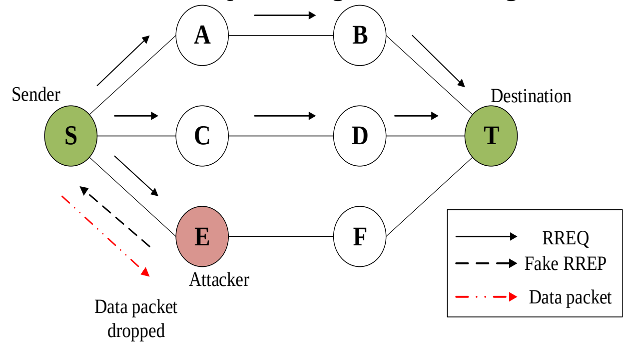


Fig. 1. Demonstration of blackhole attack.

2) Cooperative Black-Hole Attack

This is a sophisticated kind of attack which is done by two or more colluding nodes. The invisible colluding nodes participate in the attack and make the source node believe that there is a reliable route [22].

3) Grey-Hole Attack

In this attack, the packet is purposely entirely dropped or dropped for some specific time by the malicious node (Fig. 2). The state of the malicious node is reversed back to conduct itself as a normal node. The malicious node that receives the packet to be forwarded is dropped off after the route discovery process [24].

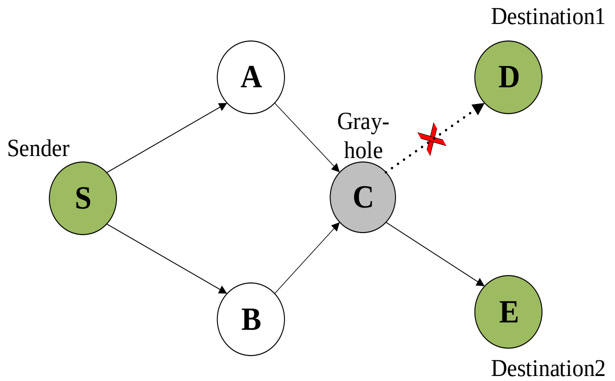


Fig. 2. Demonstration of grey-hole attack.

4) Jellyfish Attack

In Jellyfish attack, the attacker accesses the system, intrudes into the group and turns into a part of the system for forwarding the packets. Once it becomes a part of the system, it delays the packets and increases the performance factor End-to-End value to very high, before passing on the data packets. The overall network communication is impacted due to high delays [25].

5) Worm Hole Attack

In cosmology, a wormhole links two remote positions in space by a shortcut path. Similarly, in MANETs, one or more attacking nodes may interrupt routing by short-circuiting the network (as shown in Figure 3), thus disrupting the normal flow of packets [24].

Retrieval Number: E6537018520/2020©BEIESP
DOI:10.35940/ijrte.E6537.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

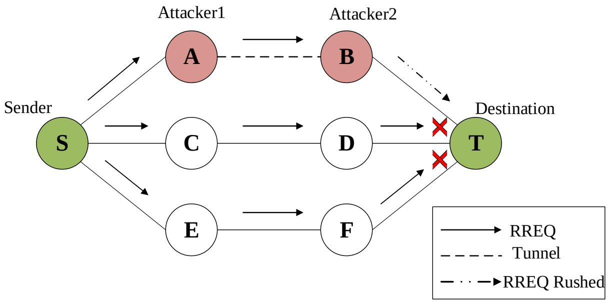


Fig. 3. Demonstration of wormhole attack.

6) HELLO Flood Attack

Attacker nodes flood the networks with superior quality routes with powerful transmitters. Thus, each node attempts to pass on their respective packets to that node expecting that it is the best possible route to the destination node. Some nodes may forward their packets to the destination nodes that are beyond the range of attacker nodes [22].

7) Bogus Registration Attack

It is an active attack where attackers disguise themselves as some other nodes by creating fake beacons or transmitting stolen beacons to register themselves with the nodes as neighbours [22].

8) Man-in-the-Middle Attack

In this attack, the assailant nodes sneak into a genuine route and attempt to sniff the packets that flow through it [21].

9) Rushing Attack

In this attack, route request sequence numbers are multiplied by the attacker (Fig. 4). The reactive protocols maintain the sequence numbers for suppressing replica packets at the nodes [24].

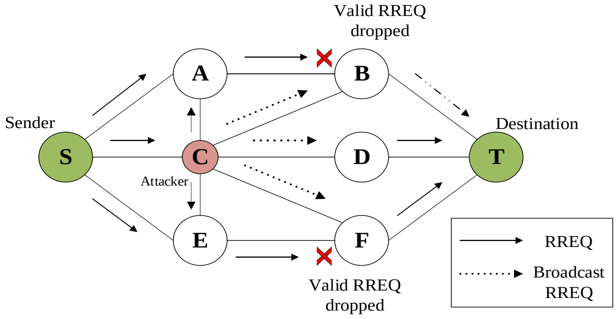


Fig. 4. Demonstration of the rushing attack.

10) Sybil Attack

The attacker, in this case, produces multiple fake identities by feigning to be made up of various nodes in the system [26]. Subsequently, one node may adopt the function of numerous nodes (as depicted in Fig. 5) and might analyze or get in the way of numerous nodes simultaneously.

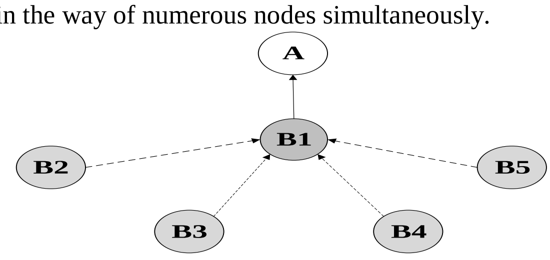


Fig. 5. Demonstration of Sybil attack

11) Byzantine Attack

A set of intermediate nodes collaborate in Byzantine attack to carry out attacks that comprise of generating routing loops, passing on packets to non-optimal routes resulting in an interruption in the routing services of the network [27].

12) Sinkhole

In this attack, the attacker nodes eavesdrop on the entire data that is being transmitted among neighbouring nodes. This attack may be implemented in MANET like AODV protocol utilising computation for reducing hop count and maximizing the sequence network; such a malicious node appears to be the best path available for node communication [27].

13) SYN Flooding

This attack comes under the category of Denial of Service. An opponent frequently sends connection requests until the resources needed for every connection reach a limit or are exhausted. SYN flooding creates resource restrictions for the valid nodes [28].

14) Eavesdropping

The process in which an unauthorized attacker intercepts messages and reads them without changing the message contents is referred to as eavesdropping [29]. Mobile nodes in MANETs share a wireless medium where messages are broadcast and thus can be intercepted quite easily when the specific frequency of the message is tuned.

15) Routing Attack

In this type of attack, malicious nodes attempt to delete or alter the routing tables of the network nodes [30], [31]. Since the information in the routing table is destroyed, processing time, as well as packet overhead increases.

16) Resource Consumption Attack

Malicious nodes, in this attack, employ some means to waste network or node resources [32]. For example, malicious nodes lead packets into a loop comprising of ordinal nodes. Thus, the energy of the node gets used up in the transmission of forged packets. This also leads to network congestion and increased probability of packet loss.

17) Session Hijacking

It is a grave error that provides a chance for malicious nodes to act as a sound system [29]. Through this attack, malicious nodes conduct themselves like real nodes in the communications. The most efficient way to defeat this attack is considered to be cryptography.

18) Denial of Service

In this type of attack, malicious nodes prevent regular nodes from accessing network services or data [29], [33]. A particular service or node shall be unapproachable, and resources (e.g., bandwidth) will be wasted. In addition, packet delay as well as congestion increases.

19) Jamming Attack

This attack is a category of DoS attack [29].

The goal of the jammer is to intrude with normal wireless communications. Jammers may acquire their goals by blocking a true traffic source from transmitting a packet, or by inhibiting the delivery of valid packets [22].

20) Malicious Message Injecting

The attacker, in this case, injects forged streams into the actual message and degrades the message integrity [34]. As a result, the attacker disrupts network functionality.

21) Active Interference

It is a kind of DoS attack that disrupts communication or blockades wireless communication channels. The impact of such an attack is based on the routing protocol and their duration. The attacker shall either try to replay previous messages or counterfeit the order of messages. Previous messages can be replayed for reintroducing outdated information [34].

22) Malicious Code Attacks

Such attacks affect the operating system as well as user application and also includes viruses, worm attacks, etc. [2], [35].

23) Multilayer Attacks

The artificial attacks, DoS attacks, man-in-the-middle attack, etc. affect multiple MANET layers [35].

24) Traffic Analysis and Location Disclosure

Attackers, in this type of attack, eavesdrop on the wireless link traffic to determinine the position of the target node by examining the broadcasting features, amount of information broadcast by nodes and the prototype of the message [29]. For example, large traffic streams to and from the control centre in the actual scenario. The study of traffic prototype thus allows intruders to ascertain the MANET commanding nodes. Although the communication information is secured using encryption, the evaluation of traffic can be done to remove some crucial information. The passive attacks do not affect the functionality of the network directly; however, the discovery of important information during the evaluation of traffic or eavesdropping could prove expensive in various MANET application developments like military communication, etc.

25) Sleep Deprivation Attack

It is a category of Distributed Denial of Service attack in which the attackers interact with nodes that seem to be authentic, but the main objective of such an interaction is to bring out the victim nodes from their power-conserving sleep mode [36].

26) Spoofing

In spoofing, malicious nodes pretend to be some other node. This is done to change the visualization of the network topology that is acquired by a legitimate node [22]. The attacker achieves it by falsely indicating some other node's IP as its own [4]. This attack is sometimes also referred to as man-in-the-middle.

27) Replay Attack

In the replay attack, the assailant disrupts the network routing traffic by continuing to retransmit the valid data which have been captured before. Generally, such an attack is directed at the freshness of routes, but it is also beneficial to test the weakly designed security approaches of networks [10].

VI. EFFECTS OF SECURITY ATTACKS IN MANET

When various security attacks in MANETs are discussed, considering the issues caused by different attacks is a must. Several problems arise as a consequence of attacks on different layers [37].

A. Time Delay

Any attack results in network time delay that lead to the rejection of the request by the receiver.

B. Data Loss

Attacks such as grey hole attack, blackhole attack, malicious node attack, etc. attract traffic by providing false routing information and drop control packets and some/all data that pass through it. In such situations, partial or complete loss of data is likely to occur.

C. Full/Partial Network Paralysis

In modification attack, fabrication attack, etc. when the connection is not working or node routing tables are trashed with incorrect information; there is a chance of paralyzing the network [32].

D. Compromise QoS

Attacks such as wormhole attack or tunnelling compromise network security. In such situations, the packets are forwarded to the nodes which are at a multi-hop distance via a tunnel and are redirected to the network [38]. In this way, the other node may acquire the entire information about the network which could affect the Quality of Service.

E. Misuse of Services

When any node acts selfishly, it tends to exploit the services offered by the mobile adhoc network, such as consumption of bandwidth and network flooding.

VII. SECURITY APPROACHES IN MANETS

The security approaches that have been designed for MANETs are divided into two types: *Preventive* and *Reactive Mechanisms*.

A. Preventive Mechanisms

In such mechanisms, the conventional prevention methods like encryption, digital signature, authentication, access control, etc. are employed as the first defence line for authenticating the data source and verifying the integrity of data [2]. The message digest is sufficient for ensuring data integrity while it's being transmitted. Threshold cryptography might be utilised for concealing data by splitting it up into various shares. Digital signatures may be employed for achieving authentication and data integrity.

Nevertheless, these mechanisms fail in securing the network against internal attacks once the attacker possesses a valid decryption

and encryption key and may use them to perform malicious actions. The assailants may also attempt to launch fresh attacks unknown to the secure system.

The preventive mechanisms can be further categorized into two types: Secure Key Management Schemes and Secure Routing Protocols.

1) Secure Key Management Approaches: Prevention from External Attacks

Key management, authentication and encryption are extensively employed for thwarting external attacks. Nevertheless, key management schemes face many issues in ad hoc networks owing to their characteristic features. Key management scheme comprises of two main aspects: *key revocation* and *key distribution*.

A Trusted Third Party (TTP) comprises a trusted entity to communicate the network nodes about the provision of key management services. The TTP can be offline, online or in-line [2]. Owing to a dynamic environment, a centralized certificate authority is not possible to be deployed in MANETs. Thus, several attempts have been made by the researchers to distribute the CA tasks among nodes in the distributed and dynamic MANET environment [39]. The Distributed Certificate Authority (DCA) conducts its work in a distributed manner when the mobile nodes cooperate.

The key management approaches in mobile adhoc networks are divided into three kinds: *Asymmetric Key Management, Symmetric Key Management,* and *Group Key Management.*

i) Asymmetric Key Management

In these schemes, two keys (private and public) are employed for network communication. Every receiver node possesses a secret private key and a public key that is broadcast to every network node.

ii) Symmetric Key Management

In these approaches, a single key is utilised to communicate in both directions, and such mechanisms rely on the already deployed key [2]. For n number of nodes in a network, $n(n-1)/2$ number of pairs of keys are needed for secure network communication.

iii) Group Key Management

Simple and Efficient Group Key Management (or SEGK) and Hybrid or Composite Key Management Schemes constitute the group key management approaches in mobile adhoc networks [2]. These two schemes can be employed parallelly, or further approaches can be utilised along with these schemes such that the pros of one method can mitigate the cons of another.

Nonetheless, the research community concluded that the majority of the key management approaches fail to comply with resource constraints as well as other limitations of MANETs.

2) Secure Routing Protocols for Attack Prevention

The secure key management schemes prove beneficial for authenticating mobile nodes and to thwart the masquerading of outsiders as interior nodes in the adhoc network. But such approaches fail to ward off the attacks that are directed at the adhoc routing process. To safeguard the routing process from these assaults, numerous safe routing protocols have been put forward by researchers for enhancing or replacing the existing ones [39]. Different secure routing protocols that exist for MANETs have been discussed in brief in this section:

SAR [40] includes the degree of node trust into conventional routing metrics by making use of the decryption and encryption process, with the same key.

Timed Efficient Stream Loss-tolerant Authentication (TESLA) [41] is a source authentication method that is light-weight and is based on preliminary weak synchronization of time between the senders and the receivers. This is followed by a deferred issue of authentication keys by the senders.

SAODV [42] is a reliable and safe extension of AODV utilising asymmetric cryptography. It employs a digital signature to sign the routing request packets' non-mutable fields.

SRP [43] is an extended scheme that might be applied to numerous reactive routing protocols prevalent. The simple notion of SRP is the establishment of a Security Association (SA) between the destination and the source node. This SA can be formed by the negotiation of a hybrid key distribution that depends on the public keys of destination and source nodes.

SPAAR [44] necessitates that every network device should possess a GPS locator for determining its position. The packets are acknowledged only from a single hop neighbouring node to thwart "invisible node attack".

OSRP (On-demand Secure Routing Protocol Resilient to Byzantine failures) [45] is a secure routing method that relies on onion encryption to detect faulty links in case of manifestation of colluding nodes that introduce byzantine failures in the routing process.

Secure Message Transmission (SMT) [46] makes use of information distribution, node-to-node Security Association (SA) and feedback mechanisms for safeguarding node-to-node network transmission.

SEAD [47] is a proactive routing protocol that employs DSDV-SQ-protocol based threshold secret sharing algorithm. SEAD depends on a one-way hash chain with no application of asymmetric cryptography for ensuring secure MANET communication.

SLSP [48] is utilised for securing distribution as well as discovery of Link State Update (LSU) packets for topologies with a local and network-wide scope.

S-DSDV [49] is a secure variant of DSDV in which a normal node can effectively sense the malicious routing updates with a forged sequence number (smaller or larger) or forged distance (longer, same, or shorter), only if there are no colluding nodes. S-DSDV involves cryptographic methods for message and entity authentication.

ARAN [50] incorporates secure routing over DSR and AODV that uses public-key cryptography such that every node recognizes the precise subsequent hop on a route towards the destination node.

ARAN necessitates the existence of an online certification authority.

Ariadne [51] is a reliable extension of DSR utilising TESLA protocol. It is based on symmetric cryptography and employs a one-way Message Authentication Code (or MAC) for authenticating routing messages between each node pair as well as among the communing nodes.

Secure –MADOV [52] is a stable multicast on-demand routing protocol with each node acquiring a public/private key pair as well as a CA-signed certificate. This certificate attaches the node's public key to its IP address.

SOLSR [53] is a link-state routing protocol that is table-driven with weak clock synchronization to time-stamp the messages. A key distribution centre is expected to exist in the system to handle the public keys or creation of secret keys for message integrity, authentication, or other operations related to security.

Majority of secure routing protocols cover only some possible attacks that target particular state-of-the-art routing protocols without constituting a comprehensive security approach.

3) Trust Management Based Schemes

In terms of effective node collaboration and security enhancement, a significant aspect of mobile adhoc networks is trust. Trust Management (TM) ascertains that every communicating node is trustworthy while the fundamental operations of MANETs are carried out, thus making the conventional security solutions more reliable and robust [2]. Several routing protocols for MANETs based on trust are briefed below:

CORE (COllaborative REputation) [54] is a collaborative reputation system identical to CONFIDANT (where reputation system and monitoring are considered) to detect selfish nodes in a MANET. CORE differs from CONFIDANT in allowing only positive reports through it, while CONFIDANT permits negative reports as well.

TAODV [55] employs the fundamental trust management concept for exchanging the trust information among network nodes and safeguarding the routing actions from malicious MANET nodes consequently. In TAODV, opinion represents the value of trust degree among network nodes. This opinion is dynamic and is updated recurrently based on the routing action of nodes.

Trusted-DSR [56] is an extension of DSR, where the route is chosen by the source nodes using the trust values of every intermediate node in the path towards the destination. The node trust value is determined via an approved method from the destination to the source.

Trusted AODV [57] is a modified AODV implementation. Two fresh control packets (viz. Trust Reply packet (TREP) and Trust Request packet (TREQ)) are included in the AODV protocol for securing the routing procedure.

Trusted AOMDV [58] is a trust-based scheme that employs soft encryption in AOMDV protocol.

Secure Routing using Trust (SRT) [59] is an algorithm for safeguarding Node Transition Probability (NTP) protocol utilizing the level of trust.

In *Friendship Based AODV (FrAODV)* [60], two evaluation algorithms are utilised for evaluating the reverse path as well as the forward path between the source and the destination using the neighbours' friendship values (or trust values).

B. Reactive Mechanisms

Intrusion detection methods act as the second defence line in reactive mechanisms. The chief objective of intrusion detection schemes is pinning down the abnormal actions in the exploit before real damage is carried out to the resources [2]. It is a useful method to respond to various attacks after their detection.

1) Intrusion Detection Systems

In MANETs, Intrusion Detection System (or IDS) acts as a second defence line. It is the most effective security solution in the war against security assaults affecting several levels in MANETs. In [61], intrusion detection has been described as "*a process of monitoring the events occurring in a system or network, analyzing them for signs of possible incidents which represent a violation of security policy and standards, and report unauthorized and malicious activities accordingly*". An IDS is a hardware or software entity for automating abnormal activity detection that may compromise the availability, confidentiality or integrity of a system and has the following functionalities [2]:

- Analyse the system behaviour or network traffic.
- Recognize malicious and unauthorized actions in a system/network automatically.
- Activate the alarms after identification of malicious activity.

a) Intrusion Detection Techniques

Intrusion detection techniques can be categorized into four main types based on the employment of the detection mechanism in the system. These are:

i. Signature-based or misuse (knowledge-based) intrusion detection

This mechanism evaluates the activity of the user with the intrusion patterns (known as signatures) that are already recognized [62]. This system comprises of an internal signature database. If any action of the user is found to be identical to the signatures/stored patterns, an alarm shall be triggered.

Pros:

- Efficient and precise method to detect known attacks.
- Safeguard the system/network instantly after installation.
- Easily understandable mechanism.
- High detection speed owing to the short time spent in handling false positives.

Cons:

- Inefficient in detecting various known attacks and unknown attacks.
- Difficulty in updating the signatures regularly.

ii. Anomaly-based (behaviour based) intrusion detection

It assesses the system actions at any time against regular behaviour and produces the alarm when the digression from regular behaviour goes beyond a preset threshold. It includes two steps: detection and training. It has to be trained from regular behaviour prior to its employment in any detection model [63].

Retrieval Number: E6537018520/2020©BEIESP
DOI:10.35940/ijrte.E6537.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

During detection, abnormal behaviour is classified from normal behaviour based on heuristic rules or techniques.

Pros:

- Efficient detection of sudden and new attacks.
- Facilitates in detecting privilege exploitation of resources.
- Very low maintenance needed after installation since it keeps learning from network actions and builds respective profiles.
- Not very reliant on system software.

Cons:

- Misclassification in the detection is possible due to intrusion information in the training phase.
- Weak accuracy of profile because of constant change in the observed events.
- Not scalable to gigabit speeds.
- Acceptance of attack behaviour as 'normal' if the attackers modify their behaviour patterns.
- Hard to generate alerts in real-time.
- Definition of normal behaviour is challenged by the lack of anomalous samples in the training phase.

iii. Specification-based intrusion detection (stateful protocol analysis)

It outlines a set of restraints that portray the accurate functioning of a program or protocol and supervise the protocol at any time with the distinct restraints to identify any deviations [61].

Pros:

- Adds the specification features to the protocol analyser in a quick manner.
- Efficient identification of unexpected action sequences.
- Able to sense unknown attacks with lower rates of false-positive results.

Cons:

- Resource depletion due to of continuous tracing of the protocol's state.
- Failure to sense the assaults that do not breach the protocol behaviour directly.
- The development process of the specification features is tedious.
- Might be incompatible with specific versions of some system software and applications.

iv. Hybrid or compound IDS

Hybrid IDS is a blend of two or more intrusion detection techniques [64].

Pros:

- Efficiently detects the unforeseen and new vulnerabilities.
- Detects unknown assaults with lower rates of false-positive results.

Cons:

- Increased processing overhead.

VIII. FUTURE RESEARCH DIRECTIONS

There are quite a lot of research directions in the implementation and design of security approaches for MANETs.

- A great deal of research is anticipated to discover novel security threats and analyse the collective scenario of the current assaults in mobile adhoc networks.
- Majority of the systems proposed in the past cover only some of the potential attacks targetting a particular routing protocol and do not form a complete security solution. Thus, security solutions should have the ability to deal with a wide variety of security challenges together with a comparable cost; and should also adopt the new technological changes.
- It is also essential to design an efficient and practical key management system for enhancing MANET security.
- The effective key agreement and key distribution across an exposed channel in mobile adhoc networks is a hot topic for the research community.
- Over the years, a lot of intrusion detection systems and techniques have been put forth for MANETs. Nevertheless, no globally acknowledged standard/metric for assessing the detection system efficacy exists. Detection latency can be utilised as an essential metric to evaluate the IDS. The CPU processing load, resource consumption, communication overhead, and power consumption might be significant standards and metrics for assessing the IDSs in MANETs. Therefore, defining a set of metrics/ standards for evaluation of the IDS is an open research area.
- Intrusion detection systems should be devised such that they can operate autonomously with no human supervision and offer the requisite protection level to the node as well as the network.
- The efficiency of an IDS sensor node may be hindered by a flooding attack crashing the alert processing functions of IDS sensor nodes due to voluminous false positive alarms. As a result, the IDS should be able to shield itself from security attacks or unauthorized access. The IDS ought to be self-protected and self-monitored.
- Due to highly dynamic network data, detection models representing the normal system behaviour become rigid over time since regular behaviour varies with time. Effective detection systems should be lightweight for updating the standard changes in behavioural model regularly.
- Offline detection schemes expend a reduced amount of energy but need more memory for storing the data for each time window. Consequently, online lightweight detection methods should be given preference for ensuring data integrity and minimizing the detection delay time.
- Majority of the previous research works focus on a few possible attacks only. It is a potential research field for the researchers to deploy cross-layer mechanisms to detect every possible attack targeting data-link, network, transport, and application layers.

Retrieval Number: E6537018520/2020©BEIESP
DOI:10.35940/ijrte.E6537.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

- Designing low-cost security mechanisms supporting source authentication or validity, information correctness and integrity as a combined approach with the prevailing IDSs based on hierarchical architecture is also a challenging research area.
- The prevention techniques prove insufficient in providing adequate network security. Thus, to thwart critical attacks, cooperation enforcement mechanisms and IDSs are needed alongside prevention techniques to monitor the actions violating the MANET security policy. As a result, it is also challenging for the research community to design a hybrid mechanism (prevention as well as detection technique), that ensures data security with no limitations on their individual functions.
- It is a challenging and tough task to state what is "normal" in MANETs due to its applications in on-demand and in emergency conditions.
- Network scalability, i.e., handling a vast number of nodes, is a significant concern in itself while developing security solutions for mobile adhoc networks.
- Lastly, it is worth noting that conventional trade-offs must be made between system complexity, performance, security, etc. The security mechanism must consider the availability of restricted resources in a MANET.

IX. CONCLUSION

MANET communication paradigm has rapidly evolved as the basis of many futuristic application setups in wireless networking. With the ever-increasing proliferation of applications, many underlying threats and security issues are also emerging. The inherent characteristics of MANETs itself make it a target of varied types of attacks, that are non-existent in other networking systems. This paper presented a structured and comprehensive insight into various aspects of security related to MANETs, as reported in the state-of-the-art literature. The emphasis has been to determine the contributing factors leading to threat scenarios, synopsize network security requirements, categorisation of attacks based on the communication protocol stack, and summarise preventive and reactive security schemes. Furthermore, the article sketches out several research directions required for developing promising futuristic security systems in MANETs and allied application paradigms.

ACKNOWLEDGEMENT

This work was supported by the Ministry of Higher Education Malaysia (Kementerian Pendidikan Tinggi) under the Fundamental Research Grant Scheme (FRGS) number FRGS19-137-0746.

REFERENCES

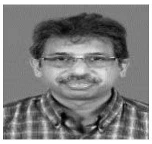
1. S.B. Geetha, and V.C. Patel, "Evaluating the Research Trends and Techniques for Addressing Wormhole Attack in MANET", International Journal of Computer Applications, vol. 110, no. 6, pp. 1-11, 2015.
2. S. Kumar, and K. Dutta, "Securing Mobile Ad Hoc Networks: Challenges and Solutions", International Journal of Handheld Computing Research, vol. 7, no. 1, pp. 26-76, 2016.
3. B. U. I. Khan, R. F. Olanrewaju, F. Anwar and A. Shah, "Manifestation and Mitigation of Node Misbehavior in Adhoc Networks", Wulfenia Journal, vol. 21, no. 3, pp. 462-470, 2014.
4. S. Sarika, A. Pravin, A. Vijayakumar, and K. Selvamani, "Security Issues In Mobile Ad Hoc Networks", in 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), 2016, pp. 329-335.
5. B. U. I. Khan, R. F. Olanrewaju, R. N. Mir, S. H. Yusoff and M. L. Sanni, "Trust and Resource Oriented Communication Scheme in Mobile Ad Hoc Networks", in Proceedings of SAI Intelligent Systems Conference, Springer, Cham, 2016, pp. 414-430.
6. R.F. Olanrewaju, B.U.I. Khan, F. Anwar, A.R. Khan, F.A. Shaikh, and M.S. Mir, "MANET – A Cogitation of its Design and Security Issues", Middle-East Journal of Scientific Research, vol. 24, no. 10, pp. 3094-3107, 2016.
7. L. Fratta, M. Gerla, and K.W. Lim, "Emerging Trends and Applications in Ad Hoc Networks", Annals of Telecommunications, vol. 73, pp. 547–548, 2018.
8. 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, pp. 25-43, 2015.
9. Priyanshu and A.K. Maurya, "Survey: Comparison Estimation of Various Routing Protocols in Mobile Ad-Hoc Network", International Journal of Distributed and Parallel Systems, vol. 5, no. 1/2/3, pp. 87-96, 2014.
10. B. U. I. Khan, R. F. Olanrewaju, A. M. Baba, R. N. Mir, and S. A. Lone, "DTASR: Dual Threshold-Based Authentication for Secure Routing in Mobile Adhoc Network," World Engineering and Applied Sciences Journal, vol. 7, no. 2, pp. 68-73, 2016.
11. K. Udhayakumar, T.P. Venkatesan, and R. Ramkumar, "Security Attacks and Detection Techniques for MANET", Discovery, vol. 15. no. 42, pp. 89-93, 2014.
12. H.N. Saha, D. Bhattacharyya, B. Banerjee, S. Mukherjee, R. Singh, and D. Ghosh, "A Review on Attacks and Secure Routing Protocols in MANET", International Journal of Innovative Research and Review, vol. 1, pp. 12-36, 2013.
13. 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, pp. 286-293, 2013.
14. R. F. Olanrewaju, B. U. I. Khan, R. N. Mir, and A. Shah, "Behaviour Visualization for Malicious-Attacker Node Collusion in MANET based on Probabilistic Approach," American Journal of Computer Science and Engineering, vol. 2, no. 3, pp. 10-19, 2015.
15. B. U. I. Khan, R. F. Olanrewaju, F. Anwar, A. 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, pp. 832-842, 2018.
16. 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, pp. 506-519, 2019.
17. R. F. Olanrewaju, B. U. I. Khan, F. Anwar, R. N. Mir, M. Yaacob, and T. Mehraj, "Bayesian Signaling Game Based Efficient Security Model for MANETs", in Lecture Notes in Networks and Systems series, K. Arai and R. Bhatia, Ed. Switzerland: Springer, Cham, 2019, pp. 1106-1122.
18. B. U. I. Khan, R. F. Olanrewaju, A. M. Baba, N. F. Zulkarnain, and S. A. Lone, "STCM: Secured Trust-Based Communication Method in Vulnerable Mobile Adhoc Network", in Robotic, Vision, Signal Processing and Power Applications, 9th International Conference on, Springer, Singapore, 2017, pp. 149-161.
19. A. Kumar, V.K. Katiyar, and K. Kumar, "Secure Routing Proposals in MANETs: A Review", International Journal in Foundations of Computer Science & Technology (IJFCST), vol. 6, no.1, pp. 21-35, 2016.
20. K.R.K. Reddy, "Consequence of Security Attacks in MANET", International Journal of Scientific Research in Science and Technology, vol. 3, no. 8, pp. 1346-1352, 2017.
21. B. U. I. Khan, R. F. Olanrewaju, M. M. U. I. Mattoo, A. A. Aziz, and S. A. Lone, "Modeling Malicious Multi-Attacker Node Collusion in MANETs via Game Theory", Middle-East Journal of Scientific Research, vol. 25, no. 3, pp. 568-579, 2017.

22. A.K. Khare, R.C. Jain, and J.L. Rana, "A Review: Trust, Attacks and Security Challenges in MANET", Informatics Engineering, an International Journal (IEIJ), vol.3, no.3, pp. 1-10, 2015.
23. J.H. Cho, A. Swami, and I.R. Chen, "A Survey on Trust Management for Mobile Ad-Hoc Networks", IEEE Communications Surveys & Tutorials, vol. 13, no. 4, pp. 562-583, 2011.
24. M.S. Swetha, M. Thungamani, and K. Kumar, "A Survey on Different Types of MANET Attacks in OSI Model", International Journal for Innovative Research in Science & Technology, vol. 4, no. 12, pp. 18-23, 2018.
25. R. Poorvadevi, S. Keerthana, V.S. Ghethalaxmipriya, and K. Venkatasailokesh, "An Enforcement of Guaranteed Client Level Defensive Mechanism in Public Cloud Services", International Journal of Computer Engineering in Research Trends, vol.4, no.2, pp. 20-24, 2017.
26. C.K.Vanamala, P. Singhania, M.S. Kumar, "A Survey of Different Lethal Attacks on MANETs", International Journal of Advancements in Research & Technology, vol. 3, no. 3, pp. 82-90, 2014.
27. A. Saranya, K. Rajasekaran, and C.S. Selin Chandra, "MANET: Types, Tools, Applications, Challenges & Security Attacks", International Journal of Communication and Networking System, vol. 5, no. 1, pp.17-20, 2016.
28. O.H. Younis, S.E. Essa, and A. El-Sayed, "A Survey on Security Attacks/Defenses in Mobile Ad-hoc Networks", Communications on Applied Electronics (CAE), Foundation of Computer Science FCS, vol. 6, no.10, pp. 1-9, 2017.
29. M.G. Meitei, and B. Sen, "A Study on Few Approaches to Counter Security Breaches in MANETs", Advances in Communication, Cloud, and Big Data, Lecture Notes in Networks and Systems 31, Springer, pp. 105-116, 2019.
30. S. Sharma, and A.K. Gupta, "A Comprehensive Review of Security Issues in MANETS", International Journal of Computer Applications, vol. 69, no. 21, pp. 32-36, 2013.
31. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour "A Survey of Routing Attacks in Mobile Ad Hoc Networks", Wireless Communications, IEEE Transactions, vol. 14, no. 5, pp. 85-91, 2007.
32. A. Dorri, S.R. Kamel, and E. Kheyrkhah, "Security Challenges in Mobile Ad Hoc Networks: A Survey", International Journal of Computer Science & Engineering Survey (IJCSES), vol. 6, no. 1, pp. 15-29, 2015.
33. Supriya, and M. Khari, "Mobile Ad Hoc Networks Security Attacks and Secured Routing Protocols: A Survey", Advances in Computer Science and Information Technology, Networks and Communications Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 84, pp. 119-124, 2012.
34. S. Khatri, P. Sharma, P. Chaudhary, and A. Bijalwan, "A Taxonomy of Physical Layer Attacks in MANET", International Journal of Computer Applications, vol. 117, no. 22, pp. 6-11, 2015.
35. I.A. Sumra, P. Sellappan, A. Abdullah, and A. Ali, "Security Issues and Challenges in MANET-VANET-FANET: A Survey", EAI Endorsed Transactions on Energy Web and Information Technology, vol. 5, no. 17, pp. 1-6, 2018.
36. A.K. Trivedi, R. Kapoor, R. Arora, S. Sanyal, and S. Sanyal, "RISM–Reputation Based Intrusion Detection System for Mobile Ad Hoc Networks", in 3rd International Conference on Computers and Devices for Communication (CODEC-06), pp. 234-237, 2013.
37. S. Jadye, "Survey of MANET Attacks, Security Concerns and Measures", International Journal of Computer Science and Information Technologies, vol. 7, no. 2, pp. 1014-1017, 2016.
38. A. Garg, and V. Beniwal, "A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 9, pp. 145-148, 2012.
39. S. Lalar, "Security in MANET: Vulnerabilities, Attacks & Solutions", International Journal of Multidisciplinary and Current Research, vol. 2, no. 2014, pp. 62-68, 2014.
40. S. Yi, P. Naldurg, and R. Kravets, "Security-aware Ad Hoc Routing for Wireless Networks", Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing, ACM, 2001, pp. 299-302.
41. A. Perrig, R. Canetti, D. Song, and J.D. Tygar, "Efficient and Secure Source Authentication for Multicast", Proceedings of the Network and Distributed System Security Symposium NDSS, vol. 1, 2001, pp. 35-46.
42. M.G. Zapata, "Secure Ad Hoc On-Demand Distance Vector Routing", Mobile Computing and Communications Review, vol. 6, no. 3, pp. 106-107, 2002.
43. P. Papadimitratos, and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks", Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, 2002, pp. 193-204.
44. S. Carter, and A. Yasinsac, "Secure Position Aided Ad Hoc Routing", Proceedings of IASTED International Conference on Communications and Computer Networks (CCN02), Cambridge, 2002, pp. 329-334.
45. B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures", Proceedings of the 1st ACM workshop on Wireless security, ACM, 2002, pp. 21-30.
46. P. Papadimitratos, and Z.J. Haas, "Secure Message Transmission in Mobile Ad Hoc Networks", Ad Hoc Networks, vol. 1, no. 1, pp. 193-209, 2003.
47. Y.C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", Ad Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.
48. P. Papadimitratos, and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks", Proceedings of the 2003 Symposium on Applications and the Internet Workshops, IEEE, 2003, pp. 379-383.
49. T. Wan, E. Kranakis, and P.C. Van Oorschot, "Securing the Destination-Sequenced Distance Vector Routing Protocol (S-DSDV)", in Information and Communications Security, Springer Berlin Heidelberg, 2004, pp. 358-374.
50. K. Sanzgiri, D. LaFlamme, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610, 2005.
51. Y.C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks, vol. 11, no. 1-2, pp. 21-38, 2005.
52. S. Roy, V.G. Addada, S. Setia, and S. Jajodia, "Securing MAODV: Attacks and countermeasures", in Proceedings of the IEEE International Conference SECON, 2005, pp. 1-12.
53. C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the OLSR Protocol", Proceedings of Med-Hoc-Net, 2003, pp. 25-27.
54. P. Michiardi, and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks", in Advanced Communications and Multimedia Security, Springer US, 2002, pp. 107-121.
55. X. Li, M.R. Lyu, and J. Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks", Proceedings of the Aerospace Conference '04, vol. 2, IEEE, 2004, pp. 1286-1295.
56. C.D. Jensen, and P.O. Connell, "Trust-based Route Selection in Dynamic Source Routing", in Trust Management, Springer Berlin Heidelberg, 2006, pp. 150-163.
57. A.M. Pushpa, "Trust Based Secure Routing In Aodv Routing Protocol", Proceedings of the International Conference On Internet Multimedia Services Architecture And Applications (IMSAA), 2009, pp. 1-6.
58. J.W. Huang, I. Woungang, H.C. Chao, M.S. Obaidat, T.Y. Chi, and S.K. Dhurandher, "Multi-path Trust-Based Secure AOMDV Routing in Ad Hoc Networks", Proceedings of the Global Telecommunications Conference (GLOBECOM 2011), IEEE, 2011, pp. 1-5.
59. N. Edua Elizabeth, S. Radha, S. Priyadarshini, S. Jayasree, and K. Naga Swathi, "SRT-Secure Routing using Trust Levels in MANETs", European Journal of Scientific Research, vol. 75, no. 3, pp. 409-422, 2012.
60. T. Eissa, S.A. Razak, R.H. Khokhar, and N. Samian, "Trust-Based Routing Mechanism in MANET: Design and Implementation", Mobile Networks and Applications, vol. 18, no. 5, pp. 666-677, 2013.
61. K. Scarfone, and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", NIST Special Publication, 800-94, 2007.
62. S. Kumar, and K. Dutta, "Intrusion Detection in Mobile Ad Hoc Networks: Techniques, Systems, and Future Challenges", Security And Communication Networks, Security Comm. Networks, vol. 9, pp. 2484-2556, 2016.
63. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey", ACM Computing Surveys (CSUR), vol. 41, no. 3, pp. 1-15, 2009.
64. O. Awodele, S. Idowu, O. Anjorin, and V.J. Joshua, "A Multilayered Approach to the Design of Intelligent Intrusion Detection and Prevention System (IIDPS)", Issues in Informing Science & Information Technology, vol.. 6, pp. 20-26, 2009.

AUTHORS PROFILE

Burhan Ul Islam Khan is a Ph.D. Scholar and Teaching Assistant at the Department of Electrical & Computer Engineering, International Islamic University Malaysia. He received B.Tech. in CSE from IUST, Kashmir, and MS in CIE from IIUM, Kuala Lumpur during 2011 and 2014 respectively. Before commencing his Ph.D., he has been involved in varying roles as that of Software Engineer, Research Analyst and Assistant Professor. His current research interests include Formulation of Bio-Inspired optimization models in IoT, Designing One Time Password Schemes, Employing Mechanism Design and Game theory to protect ad-hoc networks.

Rashidah Funke Olanrewaju is a Nigerian citizen, born in Kaduna, Nigeria. She received the BSc. Hons degree in Software Engineering from the University of Putra Malaysia, in 2002, and the MSc and PhD degrees in Computer & Information Engineering from the International Islamic University Malaysia (IIUM) Kuala Lumpur, in 2007 and 2011, respectively. She is currently an Associate Professor at the Department of Electrical and Computer Engineering, International Islamic University Malaysia where she is leading the Software Engineering Research Group (SERG). She is an executive committee member of technical associations like IEEE Women in Engineering, Arab Research Institute of Science and Engineers, etc. She represents her university, IIUM, at Malaysian Society for Cryptology Research. Her current in hand projects revolve around: MapReduce Optimization Techniques, Compromising Secure Authentication and Authorization Mechanisms, Secure Routing for ad-hoc networks, Formulating Bio-Inspired Optimization Techniques.



Dr. Farhat Anwar received a PhD degree in Electronic and Electrical Engineering from the University of Strathclyde UK in 1996. His research interest includes QoS in IP networks, routing in ah-hoc and sensor networks, computer and network security, network simulation and performance analysis, IoT, and biometrics. He has published extensively in international journals and conferences. He has been with IIUM since 1999 and currently working as a Professor in the Department of Electrical and Computer Engineering.

Bisma Rasool Pampori completed her M. Tech in Information Technology and B. Tech in Computer Science & Engineering from IUST, Kashmir and CUK, Kashmir respectively.

Roohie Naaz Mir is a Professor & HoD in the Department of Computer Science & Engineering at NIT Srinagar, India. She received B.E. (Hons) in Electrical Engineering from University of Kashmir (India) in 1985, M.E. in Computer Science & Engineering from IISc Bangalore (India) in 1990 and PhD from University of Kashmir, (India) in 2005. She is a Fellow of IEI and IETE India, senior member of IEEE and a member of IACSIT and IAENG. She is the author of many scientific publications in international journals and conferences. Her current research interests include reconfigurable computing and architecture, mobile and pervasive computing, blockchain technology, security and routing in wireless ad-hoc and sensor networks.