Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.754705

A STUDY OF MOBILE ADHOC NETWORKS (MANET) ROUTING PROTOCOLS, ATTACKS AND SECURITY MEASURES

[1]Dr. N. Shanmuga Priya, [2]Ms. V. Saranya, [3]Mr. M. Poovarasan.
[1]Associate Professor and Head, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.
[2]PG Student, II MCA, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.
[3]PG Student, II MCA, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.

Abstract: - Mobile ad hoc networks (MANETs) are a set of mobile nodes which are self-configuring and connected by wireless links automatically as per the defined routing protocol. The absence of a central management agency or a fixed infrastructure is a key feature of MANETs. These nodes communicate with each other by interchange of packets, which for those nodes not in wireless range goes hop by hop. Due to lack of a defined central authority, securitizing the routing process becomes a challenging task thereby leaving MANETs vulnerable to attacks, which results in deterioration in the performance characteristics as well as raises a serious question mark about the reliability of such networks. In this paper we have attempted to present an overview of the routing protocols, the known routing attacks and the proposed countermeasures to these attacks in various works.
Keywords: - MANET, Routing Protocols, Attacks, Security Measures, Communicate, Capacity, Malicious, Mobility, Protocols, Packet.

1. INTRODUCTION

Wireless Mobile Ad Hoc Networks (MANETs) have emerged as an advanced networking concept based on collaborative efforts among numerous self-organized wireless devices. MANET is a network where no fixed infrastructure exists. Such networks are expected to play vital role in future civilian and military settings, being useful to provide communication support where no fixed infrastructure exists or the deployment of a fixed infrastructure is not economically profitable and movement of communicating parties is possible. The topology of MANETs is dynamic, because the link among the nodes may vary with time due to device mobility, new device arrivals, and the possibility of having mobile devices [1].

The routing protocol design must take into account the physical limitations and constraints imposed through the ad hoc atmosphere in order that the ensuing routing protocol does now not degrade process performances. Due to the fact that in MANET, there is no constant-infrastructure akin to base stations, cellular gadgets must function as routers with a view to maintain the know-how about the community connectivity, for that reason the traditional routing protocols are not able to be supported effectively by way of ad hoc networks. Several research experiences have been launched to be trained this hassle, these defined with the aid of the IETF MANET group can be classified into two classes: proactive protocols and reactive protocols. MANET's technology offers each new challenges and possibilities for many

functions. The major challenges for ad hoc technology is cozy and efficient routing, due basically to MANET aspects (e.g., open medium, lack of centralized administration, nodes mobility).
The chief characteristics and challenges of the MANETs can be classified as follows [2]:

- **Cooperation: -**

If the source node and destination node are out of range with each other then the communication between them takes place with the cooperation of other nodes such that a valid and optimum chain of mutually connected nodes is formed. This is known as multi hop communication. Hence each node is to act as a host as well as a router simultaneously.

- **Dynamism of Topology: -**

The nodes of MANET are randomly, frequently and unpredictably mobile within the network [3]. These nodes may leave or join the network at any point of time, thereby significantly affecting the status of trust among nodes and the complexity of routing. Such mobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable. So the management of the network environment is a function of the participating nodes.

- **Lack of fixed infrastructure: -**

The absence of a fixed or central infrastructure is a key feature of MANETs. This eliminates the possibility to establish a centralized authority to control the network characteristics. Due to this absence of authority, traditional techniques of network management and security are scarcely applicable to MANETs.

- **Resource constraints: -**

MANETs are a set of mobile devices which are of low or limited power capacity, computational capacity, memory, bandwidth etc. by default. So in order to achieve a secure and reliable communication between nodes, these resource constraints make the task more enduring.

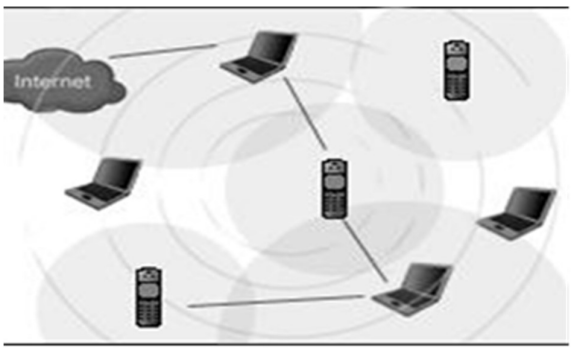

Fig. 1.1: - A typical MNAET

Albeit the security requirements (availability, confidentiality, integrity, authentication, non-repudiation) [4] remain the same whether be it the fixed networks or MANETs, the MANETs are more susceptible to security attacks than fixed networks due their inherent characteristics [5]. Securitizing the routing process is a particular challenge due to open exposure of wireless

channels and nodes to attackers, lack of central agency/infrastructure, dynamic topology etc [6]. The wireless channels are accessible to all, whether meaningful network users or attackers with malicious intent. The lack of central agency inhibits the classical server based solutions to provide security. The dynamic topology entails that at any time any node whether legitimate or malicious can become a member of the network and disrupt the cooperative communication environment by purposely disobeying the routing protocol rules.

1.1. Mobile Ad Hoc Network (MANET)

A MANET is a collection of cell nodes sharing a wireless channel with none centralized control or centered conversation spine. MANET has dynamic topology and each and every mobile node has restricted resources similar to battery, processing vigor and on-board reminiscence. This form of infrastructure-much less community is very priceless in quandary in which normal wired networks isn't possible like battlefields, average disasters and so forth. The nodes that are within the transmission range of each and every different communicate straight or else conversation is finished by means of intermediate nodes which can be inclined to forward packet therefore these networks are also known as as multi-hop networks [7].

Ad-hoc network is clearly includes ad-hoc and network in which the word ‘ad-hoc’ is a Latin word specifies the means ‘for this’ or ‘for this handiest’ and the phrase community specifies a collection of computers and cellular nodes connected through wired or wi-fi link.

Mobile ad hoc network nodes are furnished with wireless transmitters and receivers making use of antennas, which could also be totally directional (factor-to-factor), Omni directional (wide-forged), often steerable, or some mixture. At a given factor in time, depending on positions of nodes, their transmitter and receiver insurance plan patterns, conversation energy levels and co-channel interference levels, a wireless connectivity in the type of a random, multihop graph or Adhoc network exists among the many nodes. This ad hoc topology may regulate with time because the nodes move or adjust their transmission and reception parameters. The characteristics of these networks are summarized as follows [8]:

Conversation by way of wireless Networks

- Nodes can perform the roles of each hosts and routers.
- Bandwidth-restrained, variable ability hyperlinks.
- Limited physical security.

1.2. Major challenges in MANET

Regardless of the attractive applications, the points of MANET introduce a few challenges that need to be studied cautiously earlier than a large industrial deployment will also be anticipated. These include [9]:

- **Dynamic topologies**

Nodes are free to maneuver arbitrarily; hence, the network topology--which is typically multi hop, may change randomly and speedily at unpredictable times, and may include both bidirectional and unidirectional hyperlinks.

- **Routing**

The topology of the community is continuously changing; the limitation of routing packets between any pair of nodes turns into a challenging assignment. Most protocols will have to be based on reactive routing as a substitute of proactive.

- **Device discovery**

Identifying significant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic finest route choice.

- **Bandwidth**

Constrained-variable potential hyperlinks: wi-fi hyperlinks will continue to have greatly scale down capability than their hardwired counterparts.

- **Multicast**

Multicast is fascinating to support multiparty wireless communications. Since the multicast tree is now not static, the multicast routing protocol ought to be in a position to cope with mobility including multicast membership dynamics (depart and join).

The rest of the paper is organized as follows: Section 2 presents routing protocols, Section 3 presents the presently known routing attacks, and Section 4 presents the various proposed countermeasures to these. Finally Section 5 summarizes the survey.

2. ROUTING PROTOCOLS IN MANETs

The nodes in MANETs perform the routing functions in addition to the inherent function of being the hosts. The limitation on wireless transmission range requires the routing in multiple hops. So the nodes depend on one another for transmission of packets from source nodes to destination nodes via the routing nodes. The nature of the networks places two fundamental requirements on the routing protocols [10]. First, it has to be distributed. Secondly, since the topology changes are frequent, it should compute multiple, loop-free routes while keeping the communication overheads to a minimum. Based on route discovery time, MANET routing protocols fall into three general categories:

- Proactive routing protocols
- Reactive routing protocols
- Hybrid routing protocols

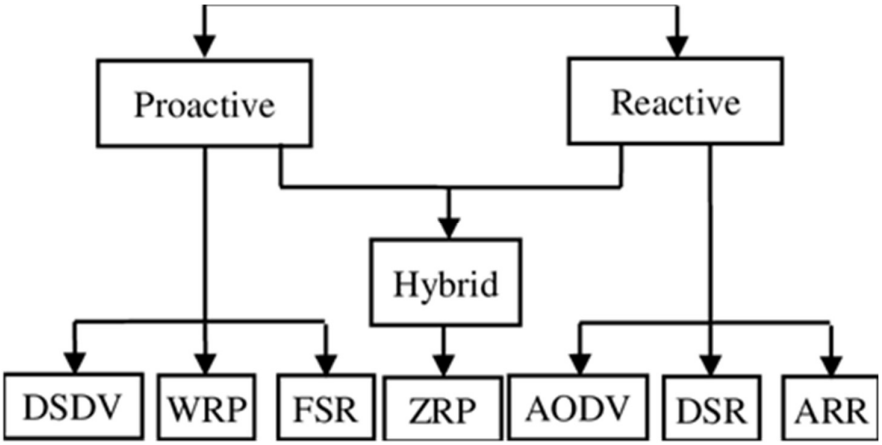

Fig. 2.1: - MANET Routing Protocols

2.1. Proactive Routing Protocols

Proactive MANET protocols are table-driven and will actively determine the layout of the network. The complete picture of the network is maintained at every node, so route selection time is minimal. But the mobility of nodes if high then routing information in the routing table invalidates very quickly, resulting in many short lived routes. This also causes a large amount of traffic overhead generated when evaluating these unnecessary routes. For large size networks and the networks whose member nodes make sparse transmissions, most of the routing information is deemed redundant. Energy conservation being very important in MANETs, the excessive expenditure of energy is not desired.

Thus, proactive MANET protocols work best in networks that have low node mobility or where the nodes transmit data frequently. Examples of proactive MANET protocols include Optimized Link State Routing (OLSR), Topology Broadcast based on Reverse Path Forwarding (TBRPF), Fish-eye State Routing (FSR), Destination-Sequenced Distance Vector (DSDV), Landmark Routing Protocol (LANMAR), Cluster head Gateway Switch Routing Protocol (CGSR).

2.2. Reactive Routing Protocols

Reactive MANET protocols only find a route to the destination node when there is a need to send data. The source node will start by transmitting route requests throughout the network. The sender will then wait for the destination node or an intermediate node (that has a route to the destination) to respond with a list of intermediate nodes between the source and destination. This is known as the global flood search, which in turn brings about a significant delay before the packet can be transmitted. It also requires the transmission of a significant amount of control traffic. Thus, reactive MANET protocols are most suited for networks with high node mobility or where the nodes transmit data infrequently. Examples of reactive MANET protocols include Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporally Ordered Routing Algorithm (TORA), Dynamic MANET On Demand (DYMO).

2.3. Hybrid Routing Protocols

Since proactive and reactive routing protocols each work best in oppositely different scenarios, there is good reason to develop hybrid routing protocols, which use a mix of both proactive and reactive routing protocols. These hybrid protocols can be used to find a balance between the proactive and reactive protocols.

The basic idea behind hybrid routing protocols is to use proactive routing mechanisms in some areas of the network at certain times and reactive routing for the rest of the network. The proactive operations are restricted to a small domain in order to reduce the control overheads and delays. The reactive routing protocols are used for locating nodes outside this domain, as this is more bandwidth-efficient in a constantly changing network. Examples of hybrid routing protocols include Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR), Zone Routing Protocol (ZRP), and Zone Based Hierarchical Link State Routing Protocol (ZHLS).

3. ROUTING ATTACKS IN MANET

All of the routing protocols in MANETs depend on active cooperation of nodes to provide routing between the nodes and to establish and operate the network. The basic

assumption in such a setup is that all nodes are well behaving and trustworthy. Albeit in an event where one or more of the nodes turn malicious, security attacks can be launched which may disrupt routing operations or create a DOS (Denial of Service) condition in the network [11].

Due to dynamic, distributed infrastructure-less nature of MANETs, and lack of centralized authority, the ad hoc networks are vulnerable to various kinds of attacks. The challenges to be faced by MANETs are over and above to those to be faced by the traditional wireless networks. The accessibility of the wireless channel to both the genuine user and attacker make the MANET susceptible to both passive eavesdroppers as well as active malicious attackers. The limited power backup and limited computational capability of the individual nodes hinders the implementation of complex security algorithms and key exchange mechanisms. There is always a possibility of a genuine trusted node to be compromised by the attackers and subsequently used to launch attacks on the network. Node mobility makes the network topology dynamic forcing frequent networking reconfiguration which creates more chances for attacks [12].

The attacks on MANETs can be categorized as active or passive. In passive attacks the attacker does not send any message, but just listens to the channel. Passive attacks are non disruptive but are information seeking, which may be critical in the operation of a protocol. Active attacks may either be directed to disrupt the normal operation of a specific node or target the operation of the whole network.

A passive attacker listens to the channel and packets containing secret information (e.g., IP addresses, location of nodes, etc.) may be stolen, which violates confidentiality paradigm. In a wireless environment it is normally impossible to detect this attack, as it does not produce any new traffic in the network. The action of an active attacker includes; injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes which violates availability, integrity, authentication, and non-repudiation paradigm. Contrary to the passive attacks, active attacks can be detected and eventually avoided by the legitimate nodes that participate in an ad hoc network [13].

The first approach to develop security solutions is the understanding of potential threats. Supported by this threat analysis and capabilities of potential attackers, the well known routing attacks in MANETs are discussed [14].

Flooding Attack:

- **Routing Table Overflow:**

The attacker node floods the network with bogus route creation packets to fake (non-existing) nodes or simply sends excessive route advertisements to the network. The purpose is to overwhelm the routing-protocol implementations, by creating enough routes to prevent new routes from being created or to overwhelm the protocol implementation. Proactive routing protocols, as they create and maintain routes to all possible destinations are more vulnerable to this attack.

- **Sleep Deprivation:**

In sleep deprivation attack, the resources of the specific node/nodes of the network are consumed by constantly keeping them engaged in routing decisions. The attacker node

continually requests for either existing or non-existing destinations, forcing the neighboring nodes to process and forward these packets and therefore consume batteries and network bandwidth obstructing the normal operation of the network.

- **Impersonation Attack:**

The attacker nodes impersonates a legitimate node and joins the network undetectable, sends false routing information, masked as some other trusted node.

- **Black Hole Attack:**

In this attack, the attacker node injects false route replies to the route requests claiming to have the shortest path to the destination node whose packets it wants to intercept. Once the fictitious route has been established the active route is routed through the attacker node. The attacker node is then in a position to misuse or discard any or all of the network traffic being routed through it.

- **Node Isolation Attack:**

The Node Isolation Attack is a Denial of Service (DOS) attack to isolate the data transmission among the group of mobile nodes. The goal of this attack is to isolate a given node from communicating with other nodes in the network. The idea of this attack is that attacker(s) prevent link information of a specific node or a group of nodes from being spread to the whole network. Thus, other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes.

- **Routing Table Poisoning Attack:**

Different routing protocols maintain tables which hold information regarding routes of the network. In poisoning attacks, the attacker node generates and sends fictitious traffic, or mutates legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. Another possibility is to inject a RREQ packet with a high sequence number. This causes all other legitimate RREQ packets with lower sequence numbers to be deleted. Routing table poisoning attacks can result in selection of non-optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network.

- **Wormhole Attack:**

The wormhole attack involves the cooperation between two attacking nodes. One attacker captures routing traffic at one point of the network and tunnels it to another point in the network that shares a private high speed communication link between the attackers, and then selectively injects tunnel traffic back into the network. The two colluding attacker can potentially distort the topology and establish routes under the control over the wormhole link.

- **Location Disclosure Attack:**

In this attack, the privacy requirements of an ad hoc network are compromised. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, and the structure of the network.

- **Rushing Attacks:**

The attacker (initiator) node initiates a Route Discovery for the target node. If the ROUTE REQUESTs for this Discovery forwarded by the attacker are the first to reach each neighbor of the target, then any route discovered by this Route Discovery will include a hop through the attacker. That is, when a neighbor of the target receives the rushed REQUEST from the attacker, it forwards that REQUEST, and will not forward any further REQUESTs from this Route Discovery. When non-attacking REQUESTs arrive later at these nodes, they will discard those legitimate REQUESTs. As a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes).

- **Blackmail:**

The attack incurs due to lack of authenticity and it grants provision for any node to corrupt other node's legitimate information. Nodes usually keep information of perceived malicious nodes in a blacklist. This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and tell other nodes in the network to add that node to their blacklists and isolate legitimate nodes from the network.

4. SECURITY MEASURES AGAINST ROUTING ATTACKS IN MANETs

In this section, will discuss the countermeasures against the routing attacks and secured routing protocols in MANETS.

Solutions to the Flooding Attack:

Mankotia, V., et al., (2023) provides the Security in a mobile ad-hoc network is an essential requirement that helps in preventing attacks from the malicious node [15]. A flooding attack is a type of denial of service attack that consumes the network bandwidth due to flooding of the fake packets by the flooder node. The different forms of flooding attacks are route request flooding attacks and data flooding attacks. In a route request flooding attack, the flooder node exhausts the network resources with a high number of fake request packets in the network whereas in a data flooding attack; the flooder node sends the fake data packets to the destination. In this paper, we have proposed an Anti-Flooding Attack (AFA) scheme that can detect both types of flooding attacks. NS-2.35 simulator is used to validate the efficiency of the proposed scheme under the effect of different mobility speeds and the number of nodes scenario. The simulation results show that the proposed AFA scheme performs better as compared with an existing scheme on the various performance metrics.

Solutions to the Blackhole Attack:

Kamel, M. B. M., et al., (2017) focus on Mobile ad hoc networks (MANET) is a type of networks that consists of autonomous nodes connecting directly without a top-down network architecture or central controller [16]. Absence of base stations in MANET force the nodes to rely on their adjacent nodes in transmitting messages. The dynamic nature of MANET makes the relationship between nodes untrusted due to mobility of nodes. A malicious node may start denial of service attack at network layer to discard the packets instead of forwarding them to destination which is known as black hole attack. In this paper a secure and trust based approach

based on ad hoc on demand distance vector (STAODV) has been proposed to improve the security of AODV routing protocol. The approach isolates the malicious nodes that try to attack the network depending on their previous information. A trust level is attached to each participating node to detect the level of trust of that node. Each incoming packet will be examined to prevent the black hole attack.

Solution to Node Isolation Attack:

Schweitzer, N., et al., (2023) aims to Mobile ad hoc networks (MANETs) are self-creating, self-configuring, self-healing, decentralized adaptive networks [17]. The Optimized Link State Routing protocol (OLSR) is one of four base routing protocols for use in ad hoc networks. MANETs routing protocols, however, are vulnerable to various attacks. In this paper we introduce PERSUASIVE, a new, sophisticated and devastating node isolation attack variant against the OLSR protocol. This attack allows for an attacker model with enhanced capabilities. It present a novel technique to mitigate PERSUASIVA. The technique guarantees protection for all feasible topologies, incurring only local (centered on the attacker) and relatively-low overhead, independent of the network's topology. Ther new protection mechanism does not disclose its activity to the attacker, and does not impose any network overhead if an attack is not launched. The novelty of the current approach is rooted in the fact that only inherent capabilities of the OLSR protocol are used. This allows for quiet discovery of the adversary, and easy integration with deployed systems.

Solutions to the Worm Hole Attack:

Zardari, Z. A., et al., (2021) addressed the A mobile ad-hoc network (MANET) is an ordinary and self-orbiting communication network that is capable of managing mobile nodes [18]. Many proposed protocols on MANET address its vulnerability against different threats and attacks. The malicious node exploits these vulnerabilities to lunch attacks, especially when nodes have mobility and network does not have constant topology, like wormhole attack. This work presents a lightweight technique that detects the wormhole attacks in MANET. In the proposed technique, the source node calculates the average sequence number of the reply (RREP) packets. If the sequence number of the corresponding node exceeds the calculated average value of the sequence number, then all traffic is discarded, and the node is marked as malicious. The proposed technique is less complex, power-efficient, and enhances network lifetime as more data packets are delivered to the destination node. This technique is validated through comprehensive simulations results in NS2.

Solutions to the Rushing Attack:

Narayanan, S. S., & Murugaboopathi, G. (2020) focused on Mobile ad hoc networks are a collection of mobile nodes that works without the centralised infrastructure [19]. Every mobile node not only acts as host, it also works as router to forward packets that are received from neighbour nodes. Mobile ad hoc networks are useful in military environments, automated battlefields, emergency, rescue operations, disaster recovery, educational, home and entertainment applications. Here data must be routed via intermediate nodes. Rushing attack is one of the network layer attacks in MANET. In this attack, when the attacker node receives the route request packet, it immediately forwards the route request packet to its neighbours without

processing the packet. Threshold-based approach is used to detect rushing attack in MANET. Proposed method provides better packet delivery ratio and throughput in presence of rushing attacker. Simulation results show that our modified DSR protocol performs better compared to secure DSR algorithm.

5. CONCLUSION

MANETs is an emerging technological field and hence is an active area of research. Because of ease of deployment and defined infrastructure less feature these networks find applications in a variety of scenarios ranging from emergency operations and disaster relief to military service and task forces. Providing security in such scenarios is critical. The primary limitation of the MANETs is the limited resource capability: bandwidth, power back up and computational capacity. Absence of infrastructure, vulnerability of channels and nodes, dynamically changing topology make the security of MANETs particularly difficult. Also no centralized authority is present to monitor the networking operations. Therefore, existing security schemes for wire networks cannot be applied directly to a MANETs, which makes them much more vulnerable to security attacks.

Of these attacks, the passive attacks do not disrupt the operation of a protocol, but is only information seeking in nature whereas active attacks disrupt the normal operation of the MANET as a whole by targeting specific node(s). In this survey, we reviewed the current state of the art routing attacks and countermeasures MANETs. The advantages as well as the drawbacks of the countermeasures have been outlined.

It has been observed that although active research is being carried out in this area, the proposed solutions are not complete in terms of effective and efficient routing security. There are limitations on all solutions. They may be of high computational or communication overhead (in case of cryptography and key management based solutions) which is detrimental in case of resource constrained MANETS, or of the ability to cope with only single malicious node and ineffectiveness in case of multiple colluding attackers. Some solutions may require special hardware such as a GPS or a modification to the existing protocol. Furthermore, most of the proposed solutions can work only with one or two specific attacks and are still vulnerable to unexpected attacks.

A number of challenges like the Invisible Node Attack remain in the area of routing security of MANETs. Although researchers have designed efficient security routing, optimistic approaches like Fellowship-TEAM-SMRITI, CREQ-CREP approach etc., which can provide a better tradeoff between security and performance, a lot more is yet to be done. Future research efforts should be focused not only on improving the effectiveness of the security schemes but also on minimizing the cost to make them suitable for a MANET environment.

6. REFERENCES

[1] Swain, J., Pattanayak, B. K., & Pati, B. (2017, March). Study and analysis of routing issues in MANET. In 2017 international conference on inventive communication and computational technologies (ICICCT) (pp. 506-509). IEEE.

[2] Ramphull, D., Mungur, A., Armoogum, S., & Pudaruth, S. (2021, May). A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. In 2021 5th international conference on intelligent computing and control systems (ICICCS) (pp. 204-211). IEEE.

[3] Kalime, S., & Sagar, K. (2021). A review: secure routing protocols for mobile adhoc networks (MANETs). Journal of Critical Reviews, 7, 8385-8393.
[4] Karlsson, J., Dooley, L. S., & Pulkkis, G. (2012). Routing security in mobile ad-hoc networks. Issues in Informing Science and Information Technology, 9, 369-383.
[5] Karthigha, M., Latha, L., & Sripriyan, K. (2020, February). A comprehensive survey of routing attacks in wireless mobile ad hoc networks. In 2020 international conference on inventive computation technologies (ICICT) (pp. 396-402). IEEE.
[6] Kumar, S., Goyal, M., Goyal, D., & Poonia, R. C. (2017, December). Routing protocols and security issues in MANET. In 2017 international conference on infocom technologies and unmanned systems (trends and future directions)(ICTUS) (pp. 818-824). IEEE.
[7] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. IEEE Communications magazine, 40(10), 70-75.
[8] Kariyannavar, S. S., Thakur, S., & Maheshwari, A. (2021, January). Security in mobile ADHOC networks: survey. In 2021 6th International Conference on Inventive Computation Technologies (ICICT) (pp. 135-143). IEEE.
[9] Rajeshwar, J., & Narsimha, G. (2017). Secure way routing protocol for mobile ad hoc network. Wireless Networks, 23(2), 345-354.
[10] Tripathy, B. K., Jena, S. K., Bera, P., & Das, S. (2020). An adaptive secure and efficient routing protocol for mobile ad hoc networks. Wireless Personal Communications, 114(2), 1339-1370.
[11] Kumar, S., & Kumar, C. D. S. (2015). Study of manet: characteristics, challenges, application, routing protocol and security attacks. INTERNATIONAL, JOURNAL, 2(5).
[12] Saini, A., & Kumar, V. (2013). Mobile ad-hoc network routing protocols: Comparative study. International Journal of Enhanced Research in Science Technology and Engineering, 3(12), 57-62.
[13] AlRubaiei, M., sh Jassim, H., Sharef, B. T., Safdar, S., Sharef, Z. T., & Malallah, F. L. (2020). Current vulnerabilities, challenges and attacks on routing protocols for mobile ad hoc network: a review. Swarm Intelligence for Resource Management in Internet of Things, 109-129.
[14] Narayanan, S. S., & Murugaboopathi, G. (2020). Prevention of rushing attack in MANET using threshold-based approach. International Journal of Internet Technology and Secured Transactions, 10(5), 576-584.
[15] Mankotia, V., Sunkaria, R. K., & Gurung, S. (2023). AFA: Anti-flooding attack scheme against flooding attack in MANET. Wireless Personal Communications, 130(2), 1161-1190.
[16] Kamel, M. B. M., Alameri, I., & Onaizah, A. N. (2017, March). STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET. In 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 1278-1282). IEEE.
[17] Schweitzer, N., Cohen, L., Dvir, A., & Stulman, A. (2023). Persuasive: A node isolation attack variant for OLSR-based MANETs and its mitigation. Ad Hoc Networks, 148, 103192.
[18] Zardari, Z. A., Memon, K. A., Shah, R. A., Dehraj, S., & Ahmed, I. (2021). A lightweight technique for detection and prevention of wormhole attack in MANET. EAI Endorsed Transactions on Scalable Information Systems, 8(29), e2-e2.

[19] Saudi, N. A. M., Arshad, M. A., Buja, A. G., Fadzil, A. F. A., & Saidi, R. M. (2019). Mobile ad-hoc network (MANET) routing protocols: A performance assessment. In Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017) Transcending Boundaries, Embracing Multidisciplinary Diversities (pp. 53-59). Springer Singapore.