Vol. 2, No. 2 | July – December 2018

Secure Routing in Mobile Ad hoc Network - A Review

Irsa Naz* Sabrina Bashir* Sumbal Abbas*

Abstract

MANET is a wireless ad-hoc network which includes mobile nodes. In MANET mobile refers to the movable nodes which can change their location frequently. MANET is a network which has no central infrastructure; it is a self-managing and self-configuring network. In MANET devices can be heterogeneous like laptops, mobiles, PDAs, etc. Due to the mobility of the nodes and no infrastructure mobile ad hoc network can be used in disaster and emergency situations. Mobile ad-hoc network has the features of dynamic topology, multi-hop routing, energy constraint and easy setup. The nodes in the MANET work as a both host and a router, to make routes in the network. Due to all these flexible features of MANET there are many security vulnerabilities arise. In MANET routing is a main concern due to the mobility and the node work as a router. The security of the routing layer is essential because if any attack interrupts the communication security of whole network can be compromised. There are different types of attacks in MANET: internal attacks, external attacks, active attacks and passive attacks. The attacks of network layer are identified in this paper. Some routing protocols are used for the security of MANET like SAODV, SRP, SEAD and Ariadne etc. In this paper, we present a review of routing attacks and their possible solutions for example, how to avoid f these attacks.

Keywords: *Mobile ad-hoc network, Routing, Attacks, Security*

1. Introduction

One of the emerging technologies of wireless networking is Mobile Ad-Hoc Network, which is an infrastructure free network. There is no central management it is a self-organizing and self-configuring network. In Mobile ad-hoc network, nodes are movable. They can freely move in any direction [1]. Due to these features of MANET, this network can be used in military battlefields, emergency, Commercial Sector, Medical Service and disaster recovery situations. Nodes in MANET not only work as a host but they are also functioning as a router. Nodes include the mobile devices, laptops, PDAs and other handheld devices [2]. In Ad-hoc network nodes depend on the batteries or other resources of energy.

Network topology in MANET is dynamic. When the network change, the nodes have to maintain the routing dynamically according to the network. There are many security challenges for MANET due to no central infrastructure and the dynamic topology [2][3]. Different types of attacks can easily occur in the ad-hoc network like internal attacks, external attacks, active, and passive attacks. In this paper, we described routing layer attacks and there solutions how to avoid these attacks. Three types of routing protocols are used in ad hoc network: table driven, on demand and hybrid protocols [4]. Some routing protocols are used for the security of the ad-hoc network like SEAD, SAODV, and SRP etc. Intrusion detection system, watchdog and some other methods are described for securing the routing layer in ad hoc network.

The paper is arranged as follows. Section 2 presents MANET, section 3 Security attributes of MANET, section 4 Types of attacks in MANET, section 5 Routing protocols of MANET, section 6 Secure routing protocols, section 7 Secure mechanisms for routing attacks and section 8 describes conclusion

2. MANET

MANET is a collection of mobile nodes which are used for communication without any infrastructure. MANETs are used in sensor networks, personal area networks, and commercial sectors, military and emergency situations [5]. The characteristics of MANET are described below:

A. CHARACTERISTICS OF MANET

- No centralized infrastructure because of

*Department of Computer Science and IT University of Lahore, Gujrat Campus Gujrat, Pakistan
Corresponding Email: irsawarraich@gmail.com

nodes self-managing and self-configuring capability.

- Flexibility in organization and rapidly setup network
- Nodes have multi-hop routing
- Dynamic network topology
- Nodes have energy constraints that affect the functionality of network.
- Nodes work as both host and a router
- Less bandwidth than the wired or infrastructure network.
- Nodes can be heterogeneous.
- Ad hoc network are exposed to many security threats.

B. VULNERABILITIES OF MANETs

Due to the some features ad-hoc network is more vulnerable as compared to wire or infrastructure network. Some of the vulnerabilities of MANET are listed below [6]:

1. **No Centralized Management**
   There is a no central manager that manages the network; every node is freely moved in the network. It is very difficult to monitor the traffic in the dynamic environment and the attacker can take the advantage of it.
2. **Dynamic Topology**
   Topology changes any time in the network. So there is a no trusting environment in the network. A malicious node can easily violate the network security.
3. **Power and Bandwidth Limitation**
   Due to limited bandwidth or capacity the signal can be affected by noise and interference. Ad-hoc network depends on the battery. So due to the limited power any node may turn to selfish.
4. **No Boundary**
   In wired networks gateways and firewalls are used for the security of the network but in ad hoc network there is no any secure boundary provided for the security of network.
5. **Cooperativeness**
   In MANET nodes are supportive to each other so a malicious node can take the advantage of it. And it can break the security of the network.

3. Security Attributes of MANET

Following are the some attributes for ensuring the security of the mobile ad-hoc network [7].

1. **Availability:** All the time nodes have to be available for the communication.
2. **Confidentiality:** It has to ensure that data is not revealed to illegal users.
3. **Integrity:** It has to be ensured that message is never changed during the transmission.
4. **Authentication:** Before communicating with any node, node has to be checked about the identity of that node.
5. **Non-repudiation:** The sender and the receiver cannot reject the sending and receiving information.

4. Types of Attacks In MANET

Following types of attacks can occur in MANET:

- Internal Attacks
- External Attacks
- Passive Attacks
- Active Attacks

Internal Attacks

Internal attacks are directly hits on a network nodes and connection between these nodes. The node which exists in the network forwards the wrong routing data to the other nodes .It is complex to identify this attack because these attacks arises due to most trustworthy nodes [8].

External Attacks

These attacks are not legally part of that network. Main purpose of attacker in external attacks is to cause congestion in network, broadcast false information of routing and interrupt the operation of entire network [9]. There are two important types of these attacks:

Passive Attacks: MANETs are more susceptible to passive attacks. The passive attack does not change the data spread inside a network. But it comprises unauthorized "listening" to network movement. In Passive attacks the attacker takes valued info in targeted networks. Valued information like node hierarchy as well as network topology is found. The attacker's objective is to attain data that is being transferred [10]. It is difficult to find out passive attacks as the process of network itself doesn't get affected. In order to overcome these attacks, powerful encryption algorithms are used to encrypt the data being transmitted. Monitoring, eavesdropping and traffic analysis are examples of passive attacks.

Active Attacks: These types of attacks are executed by malicious nodes. Active attack includes alteration

of data or may create wrong information. These attacks prevent messages route between different nodes in a network [11]. These attacks can be internal or external. In this attack, attacker attempts to interrupt the route of system or change the system resources. An attacker inserts malicious packets in a network for implementing active attack.

ATTACKS ON DIFFERENT LAYERS

Several attacks in MANET occur and we are classifying these attacks on the basis of protocol stack. But we will mainly focus on attacks at network layer. Attacks are listed in Table 1 [12].

ATTACKS AT NETWORK LAYER

It is very difficult to identify attacks on network layer because in MANET each node is associated with one another via hop-by-hop. Each single node takes decision about path to send packets, due to this way malicious node easily attack on that network. The main reason behind attacks on network layer is to insert malicious node between paths of sender to receiver or grasp traffic of network. Due to this way the attacker may generate routing hoops to form critical congestion in network. Different kinds of attacks are identified as discuss below.

1. **Blackhole Attack:**
   It is a type of attack in which malicious node claims route that is effective and smallest to target node and after that secretly drips data and monitor packets when they transmit via it [13]. Due to this shortest route created by attacker blackhole starts making fake packets by changing total and number of series of transmitting protocol message. The malicious node that is used in sending data packets towards destination instead of sending those is called blackhole node. This malicious node answers to request of each route by falsely declaring that this is a new route towards destination.
2. **Wormhole Attack:**
   In this attack, a malicious node collects data packets from one place to other malicious node through tunnels in similar network above an elevated speed wireless link. The tunnel occurs among two attacker nodes is denoted as a wormhole. Tunnels exist between two malicious nodes. That's why it is called as tunnelling attack [14]. When attacker keeps packet of data at one place, transmits those packets to alternative place, routing is interrupted.
3. **Sinkhole Attack:**
   In sinkhole attack malicious node presents false information of routing to create itself as definite node and obtains entire traffic of network. After getting network traffic, it changes the confidential information. The attacker node attempts to interest in confidential data from close nodes.
4. **Rushing Attack:**
   Rushing attacks are generally against on-demand routing protocols. When compromised node receives a route demand packet from resource node, it overflows the packet in all over the network earlier any other nodes which similarly get the similar route demand packet can respond [15]. In this attack, nodes only retransmit the initially request accepted to find out all route and ignore all others. When initially a route is discovered, the attacker enters in a network through messages request. If attacker's messages reach initially, attacker will be included in route discovery procedure.
5. **Replay Attack:**
   In replay attacks, a malicious node keeps command on messages of further nodes and retransmits them [21]. This is because topology is not static in MANET's; it transform's commonly due to movement of nodes. Due to this reason nodes must keep record of their tables of routing of declared routes.
6. **Link Spoofing Attack:**
   A malicious node transmits or presents the fake information of route to disturb the operation of routing. In this attack, malicious node influences the data or traffic of routing [16].
7. **Sybil Attack**
   In Sybil attack, attacker might create false characters of number of extra nodes. Sybil attack contains a malicious node that is declaring multiple identities. In this attack, a malicious node creates itself as a huge number other than individual node. This attack could be easily disturbed routing, distributed storage algorithms and system of fault tolerant. This is a critical attack because every single node depends on several intermediary nodes for communication.

5. Routing Protocols in MANETs

1. **Table Driven or Proactive Routing Protocols:**
   In Table driven protocols, every node consists of one or more routing table which contains the routing information from every node to all other nodes in the network. Different tables maintain this routing information. So, when the topology changes the nodes circulate the updated information all over the network. So, tables consist of consistent and updated routing information [17]. Table driven protocols use proactive technique. So, when there is a need to forward a packet, it follows the routing information table for route. Proactive protocols include clustered gateway switch routing, wireless routing proto-

Table 1: Attacks on Different Layers

Layers	Attacks
Application Layer	Repudiation, Data Corruption, Viruses and Worms
Network Layer	Wormhole, Black hole, Sinkhole, Rushing attack, Link Spoofing, Sybil, Replay
Transport Layer	Session Hijacking, SYN Flooding
Physical Layer	Jamming, Interception, Eavesdropping, Tempering
Data link Layer	Traffic Analysis, Monitoring, Disruption
Multi- Layer	Denial of service, Impersonation, Replay, Man-In-The-Middle

col, destination sequenced distance vector routing and optimized link state routing.

2. **On Demand or Reactive Routing Protocols:**
   On demand, routing protocols not stored the routing information. These protocols make the route between the source and destination while, it is Necessary. The route is generated on the demand of the source, when it has to communicate to the destination node [18]. Some reactive protocols are Ad-hoc on demand distance Vector routing, dynamic source routing, and temporally ordered routing algorithm, etc.

3. **Hybrid Routing Protocols:**
   Both proactive and reactive protocols have some pros and cons. Hybrid protocols use the both schemes proactive and reactive for the efficient routing. These protocols involve Zone routing protocol. Table 2 shows some strengths and weakness of protocols [19].

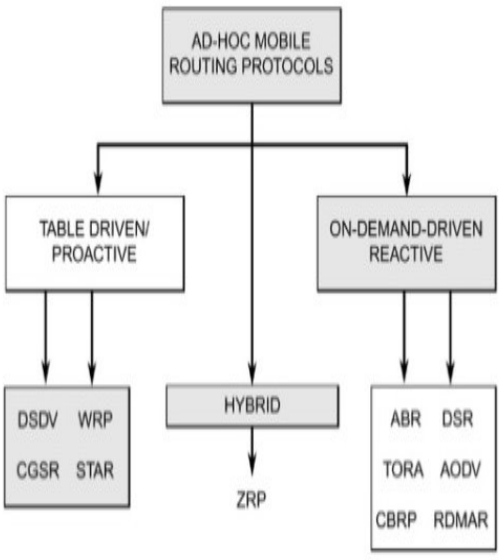

Figure 1: Routing Protocols in MANET

6. Secure Routing Protocols

1. **Ecure Adhoc on Demand Distance Vector Routing (SAODV):**
   SAODV is a reactive protocol that is based on the AODV protocol. It secures the routing messages by using the digital signatures and authenticates the RREQ and RREP messages. This protocol used asymmetric cryptography, hash function are used for getting the integrity. And digital signatures provide the authentication and non-repudiation. This protocol has a robust security mechanism that is very secure and provides a full featured security.

2. **Authentication Routing for Adhoc Network (ARAN):**
   This protocol uses asymmetric cryptography and provides end to end authentication. A trusted Certification Authority provides the public key, IP address and timestamp to the node before starting the communication. The harmful nodes can't start attacks because it requires the authentication certificate from the trusted certificate authority. Timestamp is defining the time when the certificate is created and when it will expire. Some attacks are possible that are Denial of Service attacks due to the negotiated nodes. The sharing nodes transmitted the route requests that are unnecessary over the network. These unnecessary requests give chance to attacker for attack in the network and it can cause overcrowding there by compromise the functionality of network [20]. Before the packets broadcasting to the next stage and checked for validation, every packet is authenticated in the network by using public keys. Intermediate node cannot reply; only the destination node can reply which is authenticated. ARAN prevents different attacks like spoofing attack, table overflow and black hole, because it has a solid cryptography mechanism and features.

3. **Secure Routing Protocol(SRP):**
   Secure routing protocol is based on hybrid (ZRP) protocol and other reactive routing protocols. This protocol used symmetric cryptography; Security Association is maintained by using the shared keys between the nodes. Packet includes the two identifiers: Query sequence number and

Table 2: Advantages and Disadvantages of Protocols

Type of Protocols	Advantages	Disadvantages
Proactive	1. Each node maintains the routing information before it is needed. 2. Minimizes the end-to-end delay of sending packets by updating the routing information.	1. These protocols are not good for large area networks. It has to maintain the information of each node in the table. 2. More overhead waste the limited bandwidth. 3. Not appropriate for highly mobile networks.
Reactive	1. Routes are only built when they are needed. 2. Scales to medium size networks with moderate mobility. 3. Decreases control overhead and power consumption.	1. Delay occurs due to the Source node has to wait for the route to be built earlier starting the communication.
Hybrid	It provides the advantages of both proactive and reactive, protocols. It decreases the overhead of proactive and decrease the delay of reactive.	In large routing, it gets the disadvantages of proactive protocols, and for small routing get the disadvantage of reactive

random query identifier. The route reply MAC provides integrity protection for the route reply packets. The query identifiers are used by intermediate nodes to check for replay attacks. If a query identifier matches one used in the past, the intermediate node discards the query packet. In network, many queries are received from around for measuring the frequency of these queries using nodes that take part in the process of route discovery and keep the question rate [21]. So the malicious nodes have lower importance for taking part.

4. **Secure Efficient Adhoc Distance Vector (SEAD):**
SEAD was established to provide routing security by symmetric cryptography and it is based on DSDV (Destination Sequence Distance Vector) and also has a function that is One-Way Hash to verify the route updating mechanism. For providing security to table driven protocols is difficult for it but providing security to on demand protocols is much easier for it. No attacker can attack in this network because it is using longer sequence numbers. It gives the verified security to packets for avoiding the wormhole attack using the Hash function, by retransmitting the packets from one place to another [21]. All packets reach their destination safely. Tunnelling, black hole and denial of service attacks are possible.

5. **Ariadne:**
It is an on demand (reactive) routing protocol which is based on DSR protocol. It uses authentication for the routing messages. Shared secrets between the nodes and digital signatures are used for performing the authentication. It also uses hashing for verifying that no intermediate node is missing or removing from the path. Ariadne based on timestamps that record time of any event and it controls some threats like modification and spoofing [22]. By using the source paths, avoided routes loops because packets will not send into loops. Secure protocols can categorize in two categories prevention and detection as Figure 2.

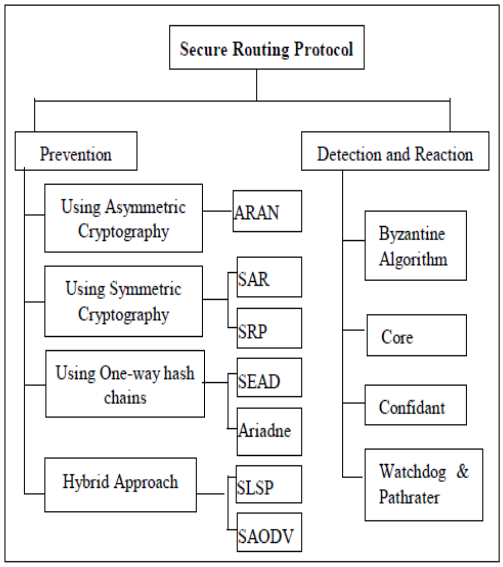

Figure 2: Secure Routing protocols

7. Security Mechanisms For Attacks

1. **Watchdog and Pathrater:**
Watchdog and pathrater are the two techniques which are used to secure the routing between the source and destination. Watchdog is used to check the transmission and misbehaviour of the

nodes. The node sends the packets to its next node and keeps this information in its buffer. The job of the watchdog is to check that whether the neighbour node forwards the packet or not. If the watched packets are the same with the packets that in the buffer, the node is not malicious. But if the node not forwards the packet and the number of abuses exceeds the threshold value, it considers that node is distrustful. Then watchdog forwards this message to the other nodes about the mischievous node. Then the other nodes check this message and this information is also sent to the pathrater. Pathrater is used to assign the rate to the nodes. Rating is done according to the behaviour of the node. So,when the malicious node is identified ,pathrater assigns the rate to this node by -100.Pathrater informs the protocols for avoiding this node and remove this node . Pathrater remove the unreliable paths and provide the new secure paths for sending the packets.

2. **Location Based Method for Link Spoofing Attack:**
   In this attack, the attacker node distribute wrong links with the other nodes to disturb the functions of routing layer. In ad-hoc network there are MPRs (Multipoint Relay nodes) that are used for spreading the messages among the nodes. If one of the node as a MPRs is selected and this is a malicious node, it can alter the data packets and disturb the network. To remove this attack time stamp and GPS (Global Poisoning system) with cryptography is used. Every node is linked with time stamp and location based GPS. All nodes share its location data among all the nodes through GPS [23]. So, due to the location data, attacks are easily identified by checking the distance among the nodes.

3. **Solution for Wormhole Attack:**
   In this attack, attacker gets the packet at one place and tunnels these packets to another place in the network. Some methods are proposed to avoid this attack like IDS, signal processing techniques and to make changing in the hardware design. A packet leash is a protocol that is used as a solution for wormhole attack. The sender inserted the information in the packet for controlling the distance of transmission, and some information is included to limit the lifetime of packet. At the receiving side the receiver verifies that whether the packet travels the same distance according to the information included by the sender or not [24]. This protocol needs information of location and synchronized clocks. Sector method and directional antennas are also used for avoiding this attack.

4. **Black Hole Attack Solution**
   In black hole attack, the attacker showing an optimal route to the node and gets the packets when the nodes sending request. Then it can change the packets. Many packets are lost in this attack and also cause denial of service (DoS). To prevent this attack different routing protocols are proposed for security such as SAR and SAODV. In Security aware ad-hoc routing protocol (SAR) a route discovery method is used and a trust level is added into the rushing request packets. The other nodes that are intermediary receive a packet with trust level. If the trust level is fulfilled, the node will handle the packet and spread it to neighbours, otherwise dropped. Secure Adhoc on Demand Distance Vector Routing protocol (SAODV) is also used as a solution for this attack. It uses some techniques in routing that are central key controlling, digital signatures for node level authentication and to lessen the modifying node checks a hash chain.

5. **Rushing Attack Solution**
   In rushing attack, the attacker sends many messages in the network for flood of packets. If the node receives message firstly from attacker, Then the node rebroadcasts its request for route discovery. Then it becomes very difficult for the nodes to discover the usable/non-attacking route. Different mechanisms are proposed to prevent this attack Secure Neighbour Detection, Secure Route Delegation, and Randomized ROUTE REQUEST forwarding. These techniques work together to defend this attack. When the sender node sends a Route Request to the neighbour node that is within the range, it allows the neighbour node to forward the request after signs a Route Delegation message. And then the neighbour node signs an Accept Delegation message after determining that the sender node is within the range. With the help of these techniques, the connection of neighbourhood between nodes can be conformed and ensured. Rushing Attack Prevention (RAP) protocol is also used to protect the network from rushing attack. Figure 3 shows the comparison which protocol provides security against these attacks [25].

8. Conclusion

Due to dynamic topology and no infrastructure MANET has many security challenges. This paper describes the different types of attacks of MANET, security attributes of MANET and our main focus on the security of the network layer in MANET. This paper identifies the attacks of network layer like wormhole attack, rush attack, Sybil attack and black hole attack, etc. Different protocols are described in this paper that provide security at the network layer. Some secure mechanisms are reviewed in this paper like watchdog and other solutions against some attacks are described. We present a review of attacks and their solutions in MANET how can avoid these attacks.

Protocol	Provide protection from Attacks						
	Type	Wormhole	Link spoofing	Replay attack	Black hole	Rushing Attack	Sybil Attack
SAODV	Reactive	No	Yes	Yes	Yes	No	Yes
SEAD	Proactive	Yes	No	No	No	No	No
ARAN	Reactive	No	Yes	No	No	Yes	No
Ariadne	Reactive	Yes	Yes	Yes	Yes	No	Yes
SRP	Hybrid	No	Yes	Yes	Yes	Yes	No

Figure 3: Comparison of Protocols

References

[1] S. Aluvala, K. R. Sekhar, and D. Vodnala, "An Empirical Study of Routing Attacks in Mobile Adhoc Networks," Procedia Computer Science, vol. 92, pp. 554–561, 2016.

[2] S. Sarika, A. Pravin, A. Vijayakumar, and K. Selvamani, "Security Issues in Mobile Ad Hoc Networks," Procedia Computer Science, vol. 92, pp. 329–335, 2016.

[3] P. Joshi, "Security issues in routing protocols in MANETs at network layer," Procedia Computer Science, vol. 3, pp. 954–960, 2011.

[4] A. Dorri and S. R. Kamel, "Security Challenges in Mobile Ad Hoc Networks: A Survey," International Journal of Computer Science & Engineering Survey, vol. 6, no. 1, pp. 15–29, 2015.

[5] R. D. Pietro, S. Guarino, N. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks – A survey," Computer Communications, vol. 51, pp. 1–20, 2014.

[6] R. Khatoun, "ASROP : AD HOC Secure Routing Protocol," International Journal of Wireless & Mobile Networks, vol. 4, no. 5, pp. 1–20, 2012.

[7] A. O. Alkhamisi and S. M. Buhari, "Trusted Secure Adhoc On-demand Multipath Distance Vector Routing in MANET," 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 2016.

[8] S. Chatterjee and S. Das, "Ant colony optimization based enhanced dynamic source routing algorithm for mobile Ad-hoc network," Information Sciences, vol. 295, pp. 67–90, 2015.

[9] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 14, no. 2, pp. 279–298, 2012.

[10] C. Gupta and P. Pathak, "Movement based or neighbor based tehnique for preventing wormhole attack in MANET," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), 2016

[11] S. V. Vasantha and A. Damodaram, "Bulwark AODV against Black hole and Gray hole attacks in MANET," 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2015.

[12] Vij and V. Sharma, "Security issues in mobile adhoc network: A survey paper," 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016.

[13] R. Singh, P. Singh, and M. Duhan, "An effective implementation of security based algorithmic approach in mobile adhoc networks," Human-centric Computing and Information Sciences, vol. 4, no. 1, 2014.

[14] A. Kaur and Dr. A. Singh," A Review on Security Attacks in Mobile Ad-hoc Networks," International Journal of Science and Research (IJSR), 2012.

[15] S. J. Ahmad and P. R. Krishna, "Security on MANETs. using block coding," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015.

[16] M. K. Parmar and H. B. Jethva, "Analyse impact of malicious behaviour of AODV under performance parameters," 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, 2014.

[17] G. Dhananjayan and J. Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET," SpringerPlus, vol. 5, no. 1, Jul. 2016.

[18] J. Rajeshwar and G. Narsimha, "Secure way routing protocol for mobile ad hoc network," Wireless Networks, vol. 23, no. 2, pp. 345–354, 2015.

[19] R. K. Singh and P. Nand, "Literature review of routing attacks in MANET," 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016.

[20] G. M. Borkar and A. R. Mahajan, "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks," Wireless Networks, vol. 23, no. 8, pp. 2455–2472, 2016.

[21] S. Manjula and Suresha, "Energy efficient and secured routing scheme in hybrid network," 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2016.

[22] G. Padmavathi, P. Subashini, and D. D. Aruna, "Hybrid routing protocols to secure network layer for Mobile Ad hoc Networks," 2010 IEEE International Conference on Computational Intelligence and Computing Research, 2010.

[23] P. K. Sharma and V. Sharma, "Survey on security issues in MANET: Wormhole detection and prevention," 2016 International Conferenceon Computing, Communication and Automation (ICCCA), 2016.

[24] K. Madhuri, N. Viswanath, and P. Gayatri, "Performance evaluation of AODV under Black hole attack in MANET using NS2," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), 2016.

[25] K. Sachan and M. Lokhande, "An approach to detect Gray-hole attacks on Mobile ad-hoc Networks," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), 2016