Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Review of MANET Security Features

Gagandeep Kaur
Research Scholar,
Shri Khushal Das University, Hanumangarh
gaganromana21@gmail.com

Dr. Kalpana Midha
Assistant Professor,
Shri Khushal Das University, Hanumangarh
kalpnamidha@gmail.com

Article Info
Page Number: 2430 - 2439
Publication Issue:
Vol 71 No. 4 (2022)

Abstract

The mobile Ad-hoc Network is a wireless, infrastructure-free network that self-organizes as needed. It implies that the network can be dynamically changed without centralized control. A Mobile Agent's ability to switch between systems inside the same network is a special characteristic. This skill somewhat aids researchers in dealing with security concerns in MANET. This leads to topological changes, which expose MANETs to various security threats. A network in which mobile nodes can join and leave at any time is a mobile ad hoc network. Due to the self-configuring nature of the network, malicious nodes can sneak in and launch a range of active and passive attacks. Active attacks affect a network's performance in terms of specific traits several protocols have been developed for these networks to find peer-to-peer paths between active nodes. The malevolent nodes can easily target these routing protocols. It is urgently necessary to identify and stop assaults launched by rogue nodes without disrupting network services. The investigation of numerous risks to the security of MANETS and the methods for detecting and preventing them is presented in this paper.

Keywords: MANETS, Active and Passive Attacks

Article History
Article Received*: 25 March 2022*
Revised*: 30 April 2022*
Accepted*: 15 June 2022*
Publication*: 19 August 2022*

I. Introduction

All nodes in MANETs are free to migrate at random because of the decentralized nature of the network infrastructure. Without a centralized infrastructure, MANETs are capable of building self-configuring and self-maintaining networks. Mobile phones, laptops, palmtops, PDAs, sensors, and other nodes that can participate in a MANET include those that have a wireless transmitter and receiver. The node might be found anywhere, including on people, ships, trucks, cars, airplanes, and even extremely small gadgets. Any node in the network has a radio range that defines its neighborhood. A node can connect to its neighbors via a simple broadcast in this area. However, interference reduces the radio range. MANETs are a collection of mobile nodes that communicate with one another via packets going over multi-hops and without the use of a central controller. There are a significant number of mobile hosts in this network who connect via wireless networks. Because this is an infrastructure-free network with no central control, the movement of the nodes is random in any direction. Because of this property, all nodes in this network operate as routers, allowing the host to send packets. The MANET provides ideal solutions in a variety of situations, such as when there is a problem with broken or overburdened wired or wireless infrastructure. The bandwidth restriction is another key design concern in MANETs [2]. As a result, it is necessary to develop a routing system that can solve the problem of restricted bandwidth while also minimizing network overhead. Collision and congestion are two more key issues in wireless sensor networks. In the process of transmitting packets in MANET, the instantaneous movement of nodes inside the network causes data and control packet collisions. It also has to deal with the issue of concealed and exposed terminals [3]. A concealed terminal problem occurs when packets collide at the receiving node's end. This happens because the nodes transmit at the same time to those who are not in the sender's direct transmission range but are within the receiver's transmission range. The routing protocols will assist to reduce routing overhead and bandwidth usage, ensuring that packets are delivered correctly and on time. In MANET, effective and efficient routing is essential, which necessitates the use of several routing protocols throughout the network [4]. The intermediate nodes play a crucial role in mobile ad hoc networks since it is only through them that packets are routed from source to destination. As a result, for the MANET, numerous routing protocols have been created that are known for effective, secure, and dispersed data packet routing. It is grouped into three categories: protocols, reactive protocols, and hybrid protocols. If a link in a MANET fails, a new route from source to destination is established to keep the communication going. The transmission of data is halted if there are disconnections in the route. As a result, multicasting inside mobile ad hoc networks is reduced. Some phases are taken in the route discovery process, such as looking for node disjoint, link disjoint, or non-disjoint routes [5]. When a link fails, the information is transmitted to the source code, which may then take further measures to reduce the data transfer rate and quickly find another way. The source is alerted of the congestion issue via the congestion management techniques, which include transmission control protocol. It is necessary to gather all users efficiently to maintain and allocate network resources. All resources, such as connection bandwidth and queues on routers or switches, are shared in this process. All of the packets that are waiting for their transmission turns are stacked in a queue. When a high number of packets are waiting for the same link to become available, the queue will overflow [6]. The packets were lost as a result of the overflow, which avoided a request overflow inside the network. When packets drop often inside the network, the network is termed crowded. As a result of the network congestion, there is a problem with connection failure. In MANET, there are two sorts of assaults that compromise the network's security. Passive attacks are security assaults that do not affect network performance in terms of certain characteristics. Malicious nodes can simply detect network information in a passive assault. Spoofing attacks and eves dropping assaults are examples of passive attacks that lead to active attacks in the future [7]. The active attack is the second type of security assault that modifies network data in terms of certain characteristics. Malicious nodes are present in the network during an active attack, which can disrupt network operations. Denial of service assaults, modification attacks, and other active attacks are common. The wormhole attack is a sort of active assault that lowers network performance in terms of latency. The malicious node accepts packets and transmits them to another site through the network tunnel produced by the wormhole attack [8]. When the source node sends the control packets, the malicious node takes the path of least resistance to disrupt network operations. The wormhole is an assault on the network layer. Wormholes are created when network traffic is diverted through a tunnel to increase network latency.

II. Literature Review

The idea of ad hoc networking is not new. It has been used in the military as a technique for dynamic wireless networks since the 1970s. The development of wireless communications has recently increased commercial interest in these networks. Within the Internet Engineering Task Force (IETF), a new working group for MANET has been established with the objectives of investigating and developing candidate standard Internet routing support for mobile, wireless IP autonomous segments and developing a framework for executing IP-based protocols in ad hoc networks. The recently released IEEE standard 802.11 has raised interest in the field of ad hoc networking, which is now getting increasing attention from government, business, and academia. These networks present several intricate problems, there are numerous unsolved issues and important contributions. A group of autonomous mobile nodes that can communicate with one another using radio waves makes up a mobile ad hoc network. While other mobile nodes require the assistance of intermediary nodes to transport their packets, mobile nodes that are within radio range of one another can interact directly with one another. Each node includes a wireless interface that allows for intercommunication.

Without the assistance of any fixed infrastructure, like access points or base stations, these networks are entirely distributed and can operate anywhere. The discovery and eradication of wormhole attacks throughout the transmission and propagation processes is the primary goal of this work, according to Roshni Verma et al. (2017). This suggested technique improves the security of ad hoc networks. Such assaults are not possible on this network [9]. Through the strengthening of routing protocols in networks, the packet delivery ratio is enhanced and control overhead is reduced. The table entries at the destination node are increased here to detect the wormhole nodes quickly. The unique methodology also aids in the implementation of effective strategies for preventing DoS and hybrid assaults from entering networks, hence improving network security.

Sunil Kumar Jangir et al. (2016) conducted a thorough investigation of the wormhole attack that occurred in MANET. The wormhole presents the fake shortest path, and all network traffic is drawn to it. Due to the prevalence of wormhole assaults, the network's throughput is also decreased, as are network delays. This document [10] also discusses several ways of detecting and blocking wormhole attacks, such as packet leashes, time-based approaches, and many more. This work also examines several protocols, including OLSR, DSR, and AODV, as well as various attacks against them. The quality of all wormhole detecting approaches is compared in this article. As can be observed that much research has been offered to address the issue of wormhole assault. There can't be considered to be an application if there's only one answer for all of the cases. However, by examining the numerous strategies described in this research, a more powerful detection strategy may be discovered. As a result, an appropriate solution to wormhole attacks may be offered.

H.Ghayvat et al. (2016) published a paper on a wormhole attack that may be identified and mitigated using a suggested security approach [11]. With the use of this safe Ad hoc on-demand distance vector (AODV) technology, the wormhole attack within MANETs may be quickly discovered. The use of a digital signature is used to avoid this attack. The determined tunneling duration and threshold value can be used to determine whether a particular node is a real wormhole node. The digital signature as well as the hash chain method are used to mitigate the wormhole node. The lifespan and throughput of the suggested technology are maximized in contrast to the previous approach, and the network latency is decreased. The proposed technique improves the quality of service, but the removal of unnecessary mistakes remains a worry.

According to the results of earlier techniques, Chitra Gupta et al. (2016) found that reactive, anonymous, and stateless features are critical for MANET routing protocols. Here, we'll look at a few different wormhole attack methods. The suggested technique, which is based on the movement or Neighbour based approach, gives improved outcomes in terms of several characteristics such as packet delivery ratio, throughput, and routing overhead decrease [12]. For sudden network improvement, more network parameters are evaluated. With the suggested strategy, several additional sorts of possible network layer assaults are also blocked from entering the network. Furthermore, the suggested technique can be improved in the future to allow for node mobility and dynamic algorithm parameter change.

In this research, Pratik Gite, et al. (2017) suggested the new technology of Mobile Ad-hoc Network, which is widely used in wireless communications. This technology is built on the principles of mobility, wireless communication, and freedom. In a multi-hop Ad-Hoc network, the mobility of the nodes and a lack of power are two reasons that cause network link failure losses. In this study, they introduced a novel routing system in which accessible routes are prioritized based on their path stability [13]. For the illustration, they used the link prediction approach, which is based on signal strength. On the AODV routing protocol, they implemented the recommended routing idea.

The primary issue of connection failure inside the mobile ad hoc network caused by node mobility was presented by Kavitha T, et al. (2017). As a result, they presented an Instant Route Migration technique in this study, which involves constructing an instantaneous path that takes into account path distance and hops count. They built a partly topology-aware technique [14] to quickly find the shortest path. With the aid of this technology, packets to the destination may be readily diverted in the event of a link failure, as cache maintenance is present at every node. In comparison to existing systems, the suggested technique provides maximum throughput, decreased end-to-end latency, and rapid route migration, according to the obtained data.

According to S. B. Geetha et al. (2015), trade-off concerns are still a prominent worry in these techniques. This paper discusses the major challenges with existing techniques. A unique safe routing protocol is also presented [15] to give enough support for complicated cryptographic algorithms so that data transmission security can be improved. A few basic entities are added to the proposed routing mechanism to improve the multicast routing protocols. According to the simulation findings, the new approach outperforms the previously described mechanism in terms of energy efficiency and packet delivery ratio.

Table of Comparison

Authors' Names	Year	Description	Outcome
Roshani Verma	2017	This suggested technique improves the security of ad hoc networks. Such assaults are not possible on this network.	The unique methodology also aids in the implementation of effective strategies for preventing DoS and hybrid assaults from entering networks, hence improving network security.
Sunil Kumar Jangir,	2016	This article discusses a variety of ways of detecting and blocking wormhole attacks, including packet leashes, time-based approaches, and others.	The research of numerous strategies described in this work can be used to identify a more powerful detection strategy. As a result, an appropriate solution to wormhole attacks may be offered.
H.Ghayvat,	2016	With the use of this safe Ad hoc on-demand distance vector (AODV) technology, the wormhole attack within MANETs may be quickly discovered. The use of a digital signature is used to avoid this attack.	The proposed technique improves the quality of service, but the removal of unnecessary mistakes remains a worry.
Chitra Gupta,	2016	The suggested method, which is based on the movement or Neighbour based approach, gives improved outcomes in terms of many characteristics such as packet delivery ratio, throughput, and routing overhead decrease.	With the suggested strategy, several additional sorts of possible network layer assaults are also blocked from entering the network.
Pratik Gite,	2017	In this research, they offer a novel routing system in which accessible routes are prioritized based on their path stability.	This strategy significantly improves the concerns of routing overhead, energy usage, and throughput for various numbers of tests.
Kavitha T,	2017	Various approaches have been presented so far to re-route packets fast, with hop count as a parameter, however, they do not deliver the best end-to-end outcomes in terms of end-to-end latency.	In comparison to existing systems, the suggested technique provides maximum throughput, decreased end-to-end latency, and rapid route migration, according to the obtained data.
S. B. Geetha	2015	They claimed that trade-off concerns remain a prominent concern in these techniques. This paper discusses the major challenges with existing techniques.	According to the simulation findings, the new approach outperforms the previously described mechanism in terms of energy efficiency and packet delivery ratio.

III. MANETS ROUTING PROTOCOLS

MANET uses routing protocols [16] to determine the best route between the source and destination nodes. The ideal path must have the least amount of bandwidth, overhead, and time delay between the two nodes in question. Since the majority of the nodes in these networks are wireless mobile nodes, their topologies are constantly changing. As a result, for effective message routing, nodes must frequently determine the topology of the network. Different routing techniques are required as a result of this shifting topology. A specific protocol can be chosen while taking a few factors into account, such as the density and mobility of the network's wireless nodes.

Network topology-based routing protocols

Mobile nodes with dynamic topology are present in MANETS. The network may at any time have both unidirectional and bidirectional links. The following categories of routing protocols can be made based on the topology employed:

Proactive protocols

Every node in the network keeps a routing table up to date. The data in these tables are used by proactive routing protocols. The other name for this is table-driven routing. In the routing, each node has information about its nearby nodes. Within a set time frame, nodes exchange tables with their neighbors. Small networks with limited node mobility are best suited for proactive routing methods. The dynamic topology of the network may increase the likelihood of failure. There may be a potential for link failure because the routing tables are not updated very frequently. Landmark Routing Protocol (LAMAR), Optimized Link State Routing (OLSR), and other proactive routing protocols are a few examples. The multi-tiered technique used by multi-point relays is used by OLSR (MPR). MPRs make it possible to use scope flooding rather than full node flooding. This may aid in lowering the volume of data transferred. Only nodes with bi-directional links to other nodes are allowed to be service providers due to the way the MPRs are chosen. The MPR technique does not call for a focused entity, and the Optimized Link State Routing protocol likewise operates in a distributed context.

Reactive Routing Protocols

Due to the massive flooding of request and reply packets, certain routing techniques may experience network congestion. Due to various packet exchanges, there may also be a significant time delay when routing the message from source to destination.

Admission Control Enabled on Demand Routing (ACOR), Ad-hoc on-Demand Distance Vector (ADOV), and other reactive routing technologies are examples [17]. A routing protocol of the unicast kind is ADOV. It makes multichip routing easier. The source node just provides the address of the subsequent hop; it does not reveal the address of the entire path. IPsec is one potential solution to the security issues in AODV.

Hybrid Routing Protocols

The proactive and reactive routing strategies are both used in the hybrid approach. The nodes initially employ a proactive algorithm to find a route before switching to reactive techniques for demand routing. Depending on how the network is configured, one of the aforementioned protocols may be used. The hybrid technique is the best option because it combines the advantages of the two previous protocols. Zone-Based Hierarchical Link State (ZHLS), Zone Routing Protocol (ZRP), and others are a few hybrid routing algorithms.

IV. MANETS SECURITY ASPECTS

The MANET network is more vulnerable to assaults than other networks because the nodes, which are movable and are in charge of routing the packets, are mobile. There are a few fundamental security issues with MANET, as follows:

- Due to a shortage of resources, cryptographic techniques that operate in wired networks cannot be implemented in ad-hoc networks. Because of this, innovative solutions in this field are required.

- The interoperability of wireless devices results in a lack of privacy. These make it simple to eavesdrop on messages.
- Because nodes in ad-hoc networks participate in the message relaying process, any malicious node can exploit this to abuse the networks' traffic by altering it.
- Network node location is another security concern. Ad-hoc network nodes may be installed in an unsafe setting. This could lead to a lot of actual physical attacks on the deployed nodes.
- Ad-hoc networks' changeable network topologies give malevolent nodes greater opportunity to attack.

V. MANETS Basic Security Restrictions

When building ad-hoc networks, four main restrictions must be adhered to.

- **Confidentiality:** During the transfer, data shall not be revealed to any unapproved parties. Confidentiality ensures that only those with the proper access should have access to a node's routing information. Nodes should not be allowed to access the routing table without authorization. It is advantageous to limit the vital information to only known nodes using this approach.

  In the case of ad-hoc networks, where transmission of vital information occurs, confidentiality is necessary to ensure that no intrusive party is successful in obtaining any kind of information. Failure to maintain confidentiality results in terrible consequences and becomes a roadblock to achieving security. Data encryption is a key tactic for achieving confidentiality.
- **Integrity:** If a message is changed mid-transmission, integrity has been breached. To stop unauthorized users from changing the content, integrity must be upheld. The correct information to be communicated between the source node and the destination node is maintained through integrity. Every time a sender delivers a message to a recipient, the recipient should have a way to determine if the message has been edited or not. It ought to deliver unaltered data. The message shouldn't be able to be altered or corrupted by an outside node. Inconsistent data result from a lack of integrity.
- **Availability:** Any network is created to facilitate the flow of data and information. This restriction makes sure that the data is accessible throughout the network at all times. Denial-of-Service attacks have the potential to breach this restriction. Whenever a legitimate user requests access to one of the services, availability should be able to provide it. Despite network attacks, messages or data should still be available. Even in the event of a malicious assault, the network should remain operational or active. Attacks like Denial of Service (DoS) or excessive message flooding in the network should be avoided to guarantee good availability.
- **Non-Repudiation :** it is a situation in which the sender of communications that are sent to the recipient cannot thereafter dispute that the messages were not received. No sender can disprove that a message was not sent by him if it is shown to be incorrect. Digital signatures with security measures have been used as proof to avoid this issue because they contain the specific sender's identity.
- **Key Management:** In a mobile ad-hoc network, managing keys [18] for security is a crucial responsibility. The challenge is brought on by its dynamic topology, resource limitations,

various link capacities, and operating under more severe constraints. In MANET, different cryptographic key schemes, including public key, symmetric key, and hybrid key, are used. In public keys, encryption and decryption are accomplished using two distinct keys.

The same key is used by both parties in symmetric key types. In MANET, a key known as a "Group key" is given to a collection of mobile nodes. The three divisions of the group key protocol are decentralized, distributed [19], and centralized. The group key is managed centrally by a single organization.

VI. ATTACKS IN MANETS

Attacks in MANET can be of two different types: passive assaults, which typically eavesdrop on data and information, and active attacks, which are used to change and alter data and information. The majority of the active attacks are external ones. These result in network congestion, inaccurate traffic information, and delays. To stop these external attacks, several pre-defined mechanisms, including firewalls and encryption techniques, are in place. Internal assaults, on the other hand, are more serious. The rogue nodes involved in this assault are often a part of the network, therefore the security measures do not affect them. These malicious nodes could also collaborate. Since they are insiders, they can employ real security features to keep them safe. Compromise nodes are another name for these nodes.

- **Attack of Sleep Deprivation**

  An instance of a flooding attack is this. Attackers choose a specific node or group of nodes to attack. The goal of this attack is to deplete a node's resources and ability. Because of this, the malicious node delivers bogus requests from the phone nodes to the target node. The targeted node's resources, including its computing capacity and battery life, will be depleted as a result. The targeted node is unable to handle any legitimate requests during the attack timeframe. As a result, the targeted node will lose its absolute status among other network nodes and will be unable to participate in routing.

- **Black Hole Attack**

  The phrase "Black Hole" refers to a node in ad-hoc networks that consumes all data traffic passing through it. The data is not forwarded to the following node. Retransmission rates rise as a result of data packet drops, which congest the network. The request is received by the black hole node, which then delivers the response back to the source because that is where it should be. The source then transmits all the information to the black hole node. Additionally, the malicious black hole node may claim to have the shortest route to any specified destination node.

- **Attack by impersonation**

  Impersonation attacks are conceivable in ad-hoc networks if a malicious node impersonates a real node by forging its physical or logical address. After discovering a trusted node's identity, it may jeopardize the network's authentication standards. The malicious node sends data using the address of the reliable node, then gets data intended for the original node. This allows it to interfere with other nodes' understanding of routing. A network node can be impersonated by guessing its information or subverting the network's authentication process.

- **Rapid-fire Attack (RA)**

  Rushing is employed because a potential attacker will strive to quicken the process of becoming a hop of the path for the target node. The malicious node will do this by transmitting request packets more quickly than any other node in the network. By doing this, there is a higher chance that a malicious node will block the path. Malicious nodes can interfere with the data flowing through them once they have entered the hop path. To slow down the processing speed of neighboring nodes, the attacker can bombard them with erroneous request packets. It will quicken the attacker's forward motion. In another manner, employing a faster transmission rate can also speed up forwarding. Having a greater transmission rate will require fewer hops.

- **Poisoning of Routing Table Attack (PRTA)**
  By taking advantage of their routing tables, the attacker in this attack corrupts the nodes in its vicinity. Numerous errors, such as the fake optimum path problem, bogus routes, circuit formation, and network congestion, can occur by tampering with the routing tables of the nodes. There are a variety of ways that tables might become poisoned. A rogue node has the ability to broadcast bogus traffic and change the entries in the network's other nodes' tables. By creating a fake path with a high sequence number, the malicious node can also delete the real path with a lower sequence number.

VII. Conclusion

The conclusion of this study is that numerous network assaults on MANETS, including Black Hole Attack, Sleep Deprivation Attack, Rushing Attack, Impersonation Attack, and others, were reviewed. In this research, the causes and prevention of the aforementioned attacks have also been examined. It has also been suggested how to secure MANETS from several angles. Each attack that has an impact on the network has unique characteristics. These traits allow for the detection and prevention of these attacks. It is feasible to reduce the risk by removing the rogue node from the network by identifying it in the network. In the future, we will create a secure system for MANET employing these types of detection and prevention techniques. This document contains several errors and shortcomings that need to be fixed to properly integrate the traditional routing protocols for MANET with the study's main issue, security. The in-depth analysis and comparison of various attacks and their prevention will aid future studies in the field. The protocols used to stop assaults can be changed and further examined.

References

[1] R C Poonia, D. Bhargava, and B.Suresh Kumar. "CDRA:Cluster-based dynamic routing approach as a development of the AODV in vehicular ad-hoc networks." In Signal Processing and Communication Engineering Systems (SPACES), International Conferenceon, vol. 6, issue 3, pp.397-401, IEEE, 2015.

[2] S.Umang, BVR Reddy, MN Hoda, "Enhanced intrusion Detection System for Malicious Node detection in ADHoc Routing Protocols using Minimal energy Consumption", IET Communications volume 4, issue 17, pp-2084-2094. 2010.

[3] B Wu, J Chen, J Wu, M Cardei, "A survey of attacks and counter measures in mobile adhoc networks", Wireless network security, volume 15, issue 7, pp-103-135, 2007.

[4] A. Shastri, R. Dadhich, and R.C. Poonia, "Performance analysis of on-demand Routing protocols for vehicular ad-hoc Networks", International Journal of Wireless & Mobile

Networks (IJWMN) Vol 3, issue 6, pp-103-111, 2011.

[5] R A R Mahmood, A L Khan, "A Survey on Detecting Black Hole Attack in AODV-based Mobile AdHoc networks" In High Capacity Optical Networks and Enabling Technologies, 2007. HONET, International Symposium, volume 5, issue 4, pp.1-6. IEEE, 2007.

[6] MS Alkatheiri J Liu, A R Sangi, "AODV Routing Protocol under several Routing Attacks in MANETs" In Communication Technology (ICCT), 2011 IEEE 13th International Conferenceon, volume 6, issue 19, pp.614-618, IEEE, 2011.

[7] S Corson and J Macker, "Mobile adhoc networking (MANET): Routing protocol performance issues and evaluation considerations," IETFRFC 2501, volume 18, isse 14, pp- 624-633, 1999.

[8] S. Hazra, and S.K. Setua. "Black Hole Attack Defending Trusted On-Demand Routing in Ad-Hoc Network." In Advanced Computing, Networking and Informatics-Volume 2, issue 9, pp.59-66, Springer International Publishing, 2014.

[9] Roshani Verma, PROF. Roopesh Sharma, Upendra Singh, "New Approach through Detection and Prevention of Wormhole Attack in MANET", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017.

[10] Sunil Kumar Jangir, Naveen Hemrajani, "A Comprehensive Review On Detection Of Wormhole Attack In MANET", 2016, IEEE.

[11] H.Ghayvat, S.Pandya, S.Shah, S.C.Mukhopadhyay, M.H.Yap, K.H.Wandra, "Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET", 2016 Tenth International Conference on Sensing Technology.

[12] Chitra Gupta, Priya Pathak, "Movement Based or Neighbor Based Tehnique For Preventing Wormhole Attack in MANET", 2016 Symposium on Colossal Data Analysis and Networking (CDAN).

[13] Pratik Gite, "Link Stability Prediction for Mobile Ad-hoc Network Route Stability", International Conference on Inventive Systems and Control, 2017.

[14] Kavitha T, Muthaiah R, " INSTANT ROUTE MIGRATION DURING LINK FAILURE IN MANETS", International Journal of Mechanical Engineering and Technology (IJMET) Volume 8, Issue 8, August 2017.

[15] S. B. Geetha, Dr. Venkanangouda C. Patil, "Elimination of Energy and Communication Tradeoff to Resist Wormhole Attack in MANET", International Conference on Emerging Research in Electronics, Computer Science and Technology – 2015.

[16] S. Corson and J. Macker, "mobile Ad-hoc Networking: Routing Protocol Performance Issues and Evaluation Considerations." The Internet Society, 1999.

[17] C.E. Perkins and E.M Royer, "Ad-hoc on Demand Distance Vector Routing.", Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, 1999.

[18] Bing Wu, Jie Wu and Yuhong Dong, "An efficient Group Key Management Scheme for Mobile Ad-hoc Networks." International Journal and Networks, 2008.

[19] Aldar C-F. Chan, "Distributed Symmetric Key Management for Mobile Ad-hoc Networks", IEEE, 2004.