International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 594 - 602

# A Survey on Recent Secure Routing Techniques in Mobile Ad-Hoc Networks

Dr. J. Viji Gripsy[1] K. R. Kanchana[2]

*Assistant Professor, Department of Computer Science,PSGR Krishnammal College forWomen, Coimbatore,India.*
*Research Scholar,Department of Computer Science,PSGR Krishnammal College for Women,Coimbatore, India.*
vijigripsy@gmail.com[1],kanchumsc@gmail.com[2]

***Abstract***

*In the current scenario, wireless technologies have attained massive popularity. This wireless technology is used in many applications. In wireless technology, Mobile Ad-hoc Networks (MANETs) are a part and it doesn't require any pre-established infrastructure. The dynamic character of those networks makes them more functional and it is suitable for many applications. MANET has high mobility and doesn't rely on centralized authority. This nature of MANET is more vulnerable to many security attacks and threats. When comparing to the traditional networks, ad-hoc networks are having higher chances for many routing attacks. Securing MANET is a challenging issue, which need more analysis. In past few years, numerous researchers proposed different solutions for detecting the routing attacks in MANET. In this survey, recent approaches and techniques done for MANET routing attacks is discussed. The review thoroughly presents the problems and merits of those existing approaches.*

***Keywords:*** *Mobile Ad-hoc networks, Secure routing, Security issues, Sequence number attacks, Proactive scheme*

## 1. Introduction

Mobile Ad-hoc Network (MANET) is a kind of wireless mobile devices together which communicates with each other. This type of network is infrastructure less based [1]. So the routing packets can be transmitted to any node without any infrastructure. Mobile Ad-hoc networks are battle field and natural disasters. For remote and rural areas long haul MANETs can also be useful where no communication and infrastructure exists. Nodes forming MANETs follow MANET routing protocols, which can be categorized into Proactive and Reactive. Proactive protocols consider the changes of topology at all times, and in Reactive protocols discover the necessary information only when they need it. Some principles of MANET routing protocols are similar to the traditional wired networks. When comparing to the traditional wired network, wireless networks are energy limited and the resources are challenged. The network topology is dynamic and the routes, links are not static. Mobile nodes are too vulnerable for several types of attacks. Secure routing Protocols are the best resolution to get rid of the routing vulnerability in MANET. Even in the presence of malicious routers, the Secure MANET routing protocols function effectively. This routing protocol provides assurance for security. However, the security protocols are affected by network overhead, Because MANET device are battery operated, and they cannot tolerate excessive overheads. With minimal overhead proactive safety functions are critical for proper functioning of Ad hoc networks. So, the designs of secure routing protocols are more challenging. The main aim of Secure MANET Protocols [2] is to achieve high security with less overhead. The routing protocols perform topology information exchange and the topology information can be used to find the optimal route. These MANET protocols include some features to mitigate attackers in MANET. In this paper, we first review different predictive techniques and recent approaches which address different routing security issues in wireless ad-hoc networks. Based on the analysis and summary, different types of future works can be established.

ISSN: 2233-7857 IJFGCN

## 1.1 Security Attacks in MANET

Due to the dynamic and changing characteristics in topology of MANET, many security violations are still unsolvable. Because MANETs are structure less, high mobility, self configuring and not depend on any fixed server in nature. The vulnerability of MANET is exploited by the malicious nodes to disrupt network transactions. Few common attacks in routing for MANET's were discussed below.

### a. Gray-hole Attack

In the MANET routing process, Gray Hole attack is more popular and it studied by many authors. This type of attack advertises the fake route information as it contains a valid path. The main intention is to perform routing attack to intercepting the packets. After attacked the route, the attacked node will drop the packets passes through on it. This is difficult to identify due to various behavior of different nodes. It drops packets forwarded from a specific node and forwards the packet from unique set of destination nodes. The assault may be detected by means of several parameters which include packet change, packet drop.

### b. Black-hole Attack

The most important motive of black-hole attack is to reinforce the heavy congestion in network routing method. In black hole attack, the malicious node drops all the acquired packets in place of forwarding any packets. The packets will no longer be reached because of this type of attack. Due to retransmit the network congestion spread than typical.

### c. Sink-hole Attack:

In sink-hole attack, the attacker attempts to attack all the nodes in the network. Other nodes will believe this node and transmits their data through the attacker node. This usually uses fake resource information to attract other nodes. After successful attack, the attacker performs packet modification, spoofing and fabrication on the packets received.

### d. Wormhole Attack

The main aim of the wormhole attack is to retransmits the packet on the other side of the network. This attack is executed by a pair of nodes joining to create a wormhole; this will perform the wormhole attack. In this attack, the attacker makes the node to believe that the destination distance is only one hop. But actually the distance is more than one hop. The node believes and transmits the packet to the attacker and that attacker sends the packet to the wormhole. By exploiting this, huge data packets will be dropped by the attacker or illegal network services will be obtained.

### e. Modification Attack

The attacker modifies the routing messages in this kind of attack. And these modifications may cause danger the integrity of the packets in the network. This will change which leads to the network traffic to create DoS attacks. Using this attack different type of misbehaving can be done.

### f. Rushing Attack

The purpose of rushing attack is to encompass the mischievous node at the time of network discovery in the routing path. In the phase of route discovery, the RREQs(Route Request) are sent from malicious nodes to adjacent target nodes. These RREQs reach the adjacent nodes quicker. When the adjacent node receives this quicker RREQ from the invader, the originated request generated from the source node is not forwarded during route discovery. By performing this attack, the attacker adds an incorrect hop count in the routing table and the attacker can alter with the packet.

ISSN: 2233-7857 IJFGCN

### g. Sleep Deprivation

The objective of the attacker in this attack is to retain the target node frequently busy. The particular attack is commenced by flooding the network with routing traffic and doing so the node consumes the complete computing energy source. Sleep deprivation attack urges the target node to consume the entire network resources such as battery power, network bandwidth and resource computation by numerous fake requests for existing or non-existing destination nodes. So it failed to process the authentic requests in the network, actual node will be affected in this type of issue.

### h. Location Disclosure

The location disclosure attack aims to target the confidentiality needs of the mobile network by performing traffic analysis. In this attack, the attacker will screen the nodes within the community and unearths the location of each node. From that it finds the intermediate nodes and gains the structure information in the network. Gaining and utilizing the location information's of the other nodes is the main aim of this attack.

### i. Routing Table Poisoning

The objective of the attacker on this attack is to corrupt the routing table. The routing protocols preserve the routing tables to discover a route to the destination and ahead the packet to the expected node inside the community. In route poisoning attack the attacker change the content of the routing table and manipulates to perform different types of attacks. Here, the malicious nodes creates and transforms the modified traffic into the network. The attacker additionally modifies the valid messages within the network. An alternative manner to execute this assault is via broadcasting a RREQ with higher sequence variety which results the valid packets with decrease series variety are rejected. This assault reasons the routing tables to create wrong entries and shop the corrupt invalid information in the routing tables of the collaborating nodes.

### j. Route Fabrication

The main goal of this attack is to attain the unauthorized access to the packets. This also performs the packet dropping in network while lots of transaction in progress. In this attack, an attacker holds back with the classic routing rules. Altering the routing messages, the Route fabrication attack is accomplished. Sometimes it inserts incorrect routing messages in the packet. While constructing the routing information, the packets are forwarded to non-existing nodes or malicious nodes. It will result in packets delay and bandwidth wastage. Predominantly this type of attacks constructs Denial of Service (DoS) and Flooding attacks: The purpose of this attack is to cripple the even functioning of the network. This attack is fulfilled by sending the packets continuously into the target node. By hitting frequently, target node will be busy in handling fake packets and depriving the authentic RREQs to be dropped. Finally by this attack, infrastructure of the network is collapsed.

### k. Routing Table Overflow

Routing table overflow attack targets to gain the buffering of routing table and it creates much false traffic. In this, the attack is done by transmitting fake and caused traffic into the network with various duplicates. The packets are modified and routed to non-existing nodes. This attack overcomes the routing table buffer by storing false routing data in the routing table. By storing this legitimate routes, the routing table runs out of space.

### l. Impersonation Attack

Data packets are not authenticated in the existing ad-hoc network. So, by camouflaging as another node, the attacker performs spoofing, flooding and a malicious node can launch many attacks in a network. To

ISSN: 2233-7857 IJFGCN

carry out the assault, the intruder needs to thieve the network Id. Spoofing occurs when a malicious node misrepresents their network identity, such as changing their MAC or IP address in outgoing packets.

This kind of attack can be especially done and significantly affect the routing in the advert-hoc network. It shops the direction to every node ensuing in the exhaustion of the route cache. Misbehavior threats may be defined as an unauthorized behavior of an internal node that results in unintended damages to distinct nodes i.e., the goal of the node is not to commence an attack in the network rather it could have other goals like obtaining an iniquitous benefit compared with the other nodes. For instance, the malicious nodes which do not correctly execute the MAC protocol with the motive of having higher bandwidth and they decline to forward packets for others to keep its assets. From the analysis about the network routing attacks, several authors proposed different protection, defending strategies and technique. Many survey prepared and published on this topic, so this survey gives the most recent techniques which proposed to handle network security issues.

## Literature review

The unique features of MANETs like dynamic topology, no fixed server, lack of central administrating authority, and small number of resources in mobile nodes will create more security issues in the network. A node may screen varying forms of misbehaviors at some point of its lifetime in the network .Authors in [4] (2016) Proposed a partially distributed dynamic security model against such misbehaving nodes and secure routing in ad hoc mobile networks. The proposed scheme is partially distributed in the sense that, during the establishment of the route, additional information is implicitly propagated among nodes rather than explicit packets flooding. This also utilizes the dynamic time out based mechanism, this isolates all the misbehaving nodes and its communication based on the attack severity.

The authors proposed a scheme which presents a partially allotted mechanism creating a unique blend of each local and worldwide reputation for handling with misbehaving nodes. It affords a dynamic version that gives differential remedy to numerous misbehaving nodes relying upon the severity of their misbehavior. It considers the forwarding behavior of nodes along with their local and global reputation for the efficient handling of misbehavior. Unlike other schemes it does not aggressively spread specially generated messages to share second-hand information in the network. Rather, the supplementary information is shared among nodes during the route establishment phase.

In the paper [5] (2016) Authors proposed a stable and energy-efficient multi-path stochastic routing protocol for mobile ad hoc networks (MANETs) based on the Markov chain. In conventional routing strategies, an attacker can easily intercept packets or hijack routing (data flow) from source to destination is typically deterministic. Authors used stochastic multi-path routing in this paper to mitigate these issues. The proposed routing protocol measures several paths between origin and destination pairs and stochastically selects an energy-efficient route to forward data packets from those paths. Moreover, this protocol also ensures data flow in the network as the packets are transmitted from the source node to the destination node through random paths. The unpredictable paths at the time of transaction make it thorny to interrupt, intercept, and hijack those transferred data packets as this demands that the attacker snoop to all possible paths from source to destination.

Because of dynamic topology and confined assets, presenting QoS and safety-aware routing is a challenging task on this sort of network, so the primary purpose of secure and trust-based totally multi-route routing is to at ease consider-based routing from source to destination. It takes the parameter into consideration with the intention to satisfy two or greater stop-to-end QoS constraints. In this paper[6 ] (2017), authors suggest the extension of the standard ad hoc on-demand multi-path distance vector protocol to evaluate this model. The authors used a multi-route routing scheme based on a mesh. A cozy adjacent function considers the verification version. Instead, by expanding the standard ad hoc on-demand multi-path distance vector protocol (AOMDV), authors proposed a new secure adjacent trust-enhanced routing protocol in accordance with the trust model, called AOMDV – SAPTV. This will help in seeking

ISSN: 2233-7857 IJFGCN

all possible safe paths. It uses a secure protocol to verify confidence in the adjacent position. This also uses a better process of finding the optimal path connection. For this reason, the Dolphin Echolocation Algorithm was used in MANET of effective communication. The experimental results were conducted to simulate and present the AOMDV SAPTV's performance. The major use of QoS conscious comfy routing is to get a reliable and excellent route.The decided on direction from the source to destination have to fulfill or extra give up to end QoS constrains. The proposed DE set of rules is used to find the most effective and exceptional way for routing. Authors have performed comparative study on the proposed scheme with the existing routing protocols to show the effectiveness. The result suggests that the proposed technique more suitable for the high-quality of routing and had discovered the great direction by the optimization algorithms.

Security protocols were developed to protect routing and application data in order to protect MANETs. But only routes or communication are protected by these protocols. These protocols failed to protect both. The secure routing and effective communication on the security protocols must be implemented. So that the complete protection can be achieved. The wired and WiFi network communication security protocols are not suitable for MANET and it creates big burden due to its limited resource. To address these issues, in the year (2017) authors in [7] proposed a novel secure framework (SUPERMAN). The architecture is designed to enable existing network and routing protocols to carry out their operations, such as node authentication, access control and communication protection mechanisms. This paper presented a new framework named as SUPERMAN, which is a novel security framework. The framework gives high security to all data communicated over a MANET without any restrictions.. SUPERMAN provides security on both routing and communication. so this has been implemented on the network layer.

In [8] (2018) Authors counseled a fuzzy rule-primarily based approach which helps to design and observe Trust-Based Secure Routing Protocol for MANETs (TBSRPM). Due to the in particular dynamic conduct of nodes, the shortest route does not always guarantee a comfortable path. Therefore, path stability is not taken into account as the route in the dynamic MANETs can be easily broken. Thus finding a stable and trusted route is of great importance. The proposed set of rules is the extension of the present day reactive routing protocol (AODV), which allows us to constructed/create a secure route between destination and resources. The protocol behavior depends on trust value and level of trust. The protocol behavior relies upon agree with cost and level of trust. it also makes a decision on what stage of safety motion is required. So based on trust value, the data packet is encrypted. Using this, malicious nodes can be easily removed and the client can also set up a best-as well as a trusted path. So based on trust value, the data packet is encrypted.Using this, malicious nodes can be easily removed and the client can also set up a best-as well as a trusted path. Only particular nodes store topological information around the network in the virtual backbone network. Therefore, the routing of the messages requires only the preferred nodes in the network. In recent years, the researchers have proposed many virtual backbone construction algorithms, but not much work has been done on virtual backbone network security. Authors discussed this issue in this paper [9] (2018) by proposed a protected trivial approach to backbone construction. To secure backbone network, trivial approach is used by authors. By enabling this approach, the existing attacks will be detected to detect many existing attacks without exhausting the node resources.

In another study in [10] (2018), authors concentrated on the secure routing in MANET. A new goal programming model is designed for safe routing in this study using a hybrid optimization algorithm, called M-LionWhale. M-LionWhale is an optimization algorithm integrating lion algorithm (LA) into the whale optimization algorithm (WOA) to optimize the MANET path choice. The multi-objective optimization model achieves numerous quality of service (QoS) parameters like energy minimization, shortest and fast route detection, link lifetime, reducing delay, and increasing trust. With the estimated multi-objective parameters, a fitness function is developed for the best selection of routes.

The overall summary along with the merits and demerits of the existing researches is denoted in table1.

ISSN: 2233-7857 IJFGCN

**Table I. Secure Routing Techniques in MANET Comparison table**

| Paper Id | Description | Techniques | Merits | Demerits |
|---|---|---|---|---|
| 4 | Secure routing against misbehaving nodes | Partially distributed dynamic model which includes, Local Reputation Information, Global Supplementary Information, Dynamic Node Blocking (DNB) Mechanism and Dynamic Chips Allotment (DCA) Mechanism. | Addressed the problem of misbehaving nodes. The proposed scheme employs the dynamic chip allotment mechanism and DNB mechanism to mitigate the adverse effects of misbehaving nodes, which enhances network performance. | The isolation of misbehaving nodes may affect the communication in the network. Increased routing overhead. Routing information's is not secured. So cryptographic mechanisms can be applied. . |
| 5 | Provided security against Route hijack attacks | Stochastic multipath routing which includes Online Value Iteration algorithm. This is based on markov chain. | Energy factors are considered with the security features. Ensures uniform energy consumption among nodes, increases the throughput, and reduces the delay. | Scalability issues affected by the non- uniform energy consumption approach. Approximate result on heterogeneous environment. |
| 6 | Path selection against different routing attacks | A novel secure adjacent trust-enhanced routing protocol combined with the trust model, named as AOMDV–SAPTV and Dolphin Echolocation Algorithm (DE). | Able to find the best and improves the routing quality. better link optimal path selection handles black hole, wormhole, rushing and Sybil attacks. | when there is limited number of mobile nodes, the packet delivery ratio affects. other types of attacks may affect the data transaction using this protocol |
| 7 | Protects routing and application data from various attacks | Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN). And Diffie-Hellman. | The primary focus is to secure access to a virtually closed network (VCN) that allows expedient, reliable communication with confidentiality, integrity and authenticity services. MANET communication is protected completely and efficiently. Provides reliable, confidential and trustworthy communication to all legitimate nodes. | It specifically targets the attributes of MANETs, it is not suitable for use in other types of network at this time. Overhead mitigation is lacking. |

ISSN: 2233-7857 IJFGCN

| | | | | |
|---|---|---|---|---|
| 8 | Finds trusted path against malicious nodes | Trust-Based Secure Routing Protocol for MANETs (TBSRPM) | Utilizes the trust mechanism to select stable and trusted route.<br>Malicious nodes can be easily. | Need more improvement to the secured and fast route selection.<br>Few metrics only considered for efficiency, so the performance improvements are not properly defined. |
| 9 | Reactive protocol against different routing attacks in MANET | Secure backbone construction approach.<br>Control message (ALERT and RE-ALERT) for the identification and isolation of malicious nodes. | The proposed method provides security to a Backbone network of MANETs.<br>The proposed approach is light-weight, so nodes in the backbone may not be overloaded.<br>To detect different attacks, reactive approach is used.<br>Many existing attacks are detected and it uses a distributed approach<br>For communicating and controlling the packets, unicast method is used in the proposed work. | Simultaneously multiple attacks cannot be identified in this approach.<br><br>The nodes are observed as valid or malicious by using binary approach.<br><br>The proposed protocol will not work efficiently if the majority of the nodes are malicious in the backbone network.<br><br>False positive rate is increased. |
| 10 | Provides secure routing with QOS constraints | *M-LionWhale-based goal programming approach for secure routing* | The algorithm discovers the nodes having maximum energy, maximum link lifetime, reduced delay, minimum distance, and maximum trust to form the best path, as they make the fitness maximum.<br>Multi objective, which considers energy, distance and delay. | The proposed approach failed to give route when there is more number of malicious nodes.<br>The proposed uses a hybrid approach in which the results may vary based on the parameters.<br>Time delay<br>Scalability issues. |

## 3. Limitations of the existing Protocols

Most MANET protocols, when originally proposed, simply ignored the possibility of malicious nodes. MANET protocols are still more challenging compared to their wired counterparts even if all nodes behave well, due to higher mobility rates and modest resources. Most secure MANET protocols in the literature are simply extensions of original MANET protocols with the addition of cryptographic authentication of routing data. However, the scope of cryptographic authentication is usually restricted to only detecting inconsistencies. Very little effort has been directed towards extending the scope of the protocols to enable identification of misbehaving nodes. Against such protocols which do not have features to identify misbehaving nodes, attackers can inflict a variety of routing attacks. Some important issues that need to be considered for detecting and identifying attacker nodes are the, the finding the

ISSN: 2233-7857 IJFGCN

initiator and the attack. Such issues will in turn determine appropriate strategies for reducing the role of misbehaving nodes. An important factor to be considered in determining the attacker and attack time is the type of cryptographic authentication. For purposes of eliminating misbehaving nodes from the network, strategies to obtain non reputable proof of misbehavior are essential. Such an approach can also be a severe deterrent for nodes intending to carry out attacks. Many secure MANET protocols employ non-reputable authentication. However, while non-reputable authentication is necessary, it is not sufficient for providing non reputable proof of misbehavior. The current Securing MANET routing protocols includes offering a few tangible assurances that nodes will abide with the aid of regulations and processes.. Ensuring that any tool is protected is done through improving the agree with in a Trusted Computing Base. Many MANETs protecting strategies use cryptographic routing data authentication to limit the ability of an attacker to disseminate inaccurate routing information. Several trust-based approaches have been suggested. The trust based for facilitating cryptographic authentication includes a set of cryptographic algorithms, which are usually assumed to be unbreakable, and a Trusted Authority, who distributes cryptographic material to all nodes of a MANET network. Secure MANET protocols that leverage this limited trust mechanism. The major disadvantage of the sooner works are that Failed to provide a few essential assurances and typically impose large overhead for resource limited battery operated mobile gadgets. The future extension from this survey is providing assurances to reduce the scope of attacks while preserving the optimizations offered by the routing protocol, and reducing the overhead required for leveraging the trust based approaches. It is assumed that the existing security functions are executed in Trustworthy MANET Modules in every MANET node; only the trust head are trusted the rest of the node all other hardware and software are un-
trusted.

## Conclusion

With these analysis and summary, the limitations of existing security functions in MANET are studied in this survey. This survey aimed at improving the reliability of existing protocols and techniques with lowering their cost, in future a set of simple MANET security functions can be deployed in the ad-hoc protocols. This survey gives the basic knowledge about the security issues in manet and recent techniques proposed to overcome those issues. This shows the maximum number of works used cryptographic hash operations, and that the trust calculation functions to provide routing security in MANET. This has several future directions to ensure that nodes cannot advertise routing information that is inconsistent with information assimilated from other nodes, and to provide several useful assurances, including several assurances that are not provided by current secure MANET protocols.

## References:

[1]. Saudi, NurAmirahMohd, et al. "Mobile Ad-Hoc Network (MANET) Routing Protocols: A Performance Assessment." *Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017)*. Springer, Singapore, 2019.
[2]. Abusalah, Loay, AshfaqKhokhar, and Mohsen Guizani. "A survey of secure mobile ad hoc routing protocols." *IEEE communications surveys & tutorials* 10.4 (2008): 78-93.
[3]. Gagandeep, Aashima, and Pawan Kumar. "Analysis of different security attacks in MANETs on protocol stack A-review." *International Journal of Engineering and Advanced Technology (IJEAT)* 1.5 (2012): 269-75.
[4]. Sarkar, Sajal, and Raja Datta. "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks." *Ad Hoc Networks* 37 (2016): 209-227.
[5]. Anand, Anjali, HimanshuAggarwal, and Rinkle Rani. "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks." *Journal of Communications and Networks* 18.6 (2016): 938-947.

ISSN: 2233-7857 IJFGCN

[6]. Borkar, Gautam M., and A. R. Mahajan. "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks"2017.
[7]. Hurley-Smith, Darren, Jodie Wetherall, and Andrew Adekunle. "SUPERMAN: Security using pre-existing routing for mobile ad hoc networks." *IEEE Transactions on Mobile Computing*16.10 (2017): 2927-2940.*Networks* 23.8 (2017): 2455-2472.
[8]. Garg, Mukesh Kumar, Neeta Singh, and PoonamVerma. "Fuzzy rule-based approach for design and analysis of a Trust-based Secure Routing Protocol for MANETs." *Procedia computer science* 132 (2018): 653-658.
[9]. Gaurav, Akshat, and Awadhesh Kumar Singh. "Light weight approach for secure backbone construction for MANETs." *Journal of King Saud University-Computer and Information Sciences* (2018).
[10]. Chintalapalli, Ram Mohan, and Venugopal Reddy Ananthula. "M-LionWhale: multi-objectiveoptimisation model for secure routing in mobile ad-hoc network." *IET Communications* 12.12 (2018): 1406-1415.\

ISSN: 2233-7857 IJFGCN