International Journal of
Circuit, Computing and Networking

**E-ISSN:** 2707-5931
**P-ISSN:** 2707-5923
IJCCN 2020; 1(2): 40-44
Received: 27-11-2019
Accepted: 29-12-2019

**Amrish Khari**
Assistant Professor, ECE
Panchwati Institute of
Engineering & Technology,
Meerut, Uttar Pradesh, India

**Sonika Singh**
Head of the Department,
Assistant Professor, ECE at
Radha Govind Engineering
College Meerut, Uttar Pradesh,
India

**Corresponding Author:**
**Amrish Khari**
Assistant Professor, ECE
Panchwati Institute of
Engineering & Technology,
Meerut, Uttar Pradesh, India

# Mobile ad hoc networks security: Challenges and solutions

**Amrish Khari and Sonika Singh**

**DOI:** https://doi.org/10.33545/27075923.2020.v1.i1a.10

**Abstract**
Security plays a very important role in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wire line networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. In this article only focus on the fundamental security problem of protecting the multi-hop network connectivity between mobile nodes in a MANET. Ad hoc networks are a wireless networking pattern for mobile Amphitryon. Unlike traditionary mobile wireless networks, ad hoc networks do not depend on any fixed infrastructure. Instead, these networks are self-configurable and self-governing systems which are able to support mobility and consolidated themselves arbitrarily. In this article only focus on the rudimentary security problem of protecting the multi-hop network connectivity among mobile nodes in a MANET. We identify the security issues related to this problem, discuss the challenges to security design, and review the state-of-the-art security proposals that protect the MANET link- and network-layer operations of delivering packets over the multihop wireless channel

**Keywords:** Rudimentary, MANET, dynamic network topology

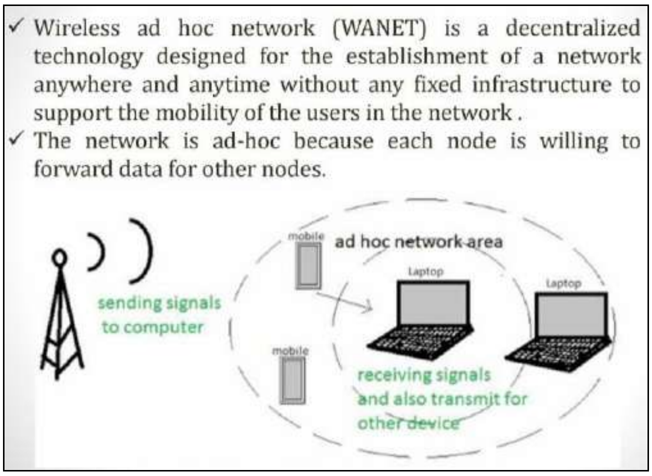
## Introduction

Form Last few years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multi-hop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Although security has long been an active research topic in wire line networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. Table 1 describes the security issues in each layer. In this article, we consider a fundamental security problem in MANET: the protection of its basic functionality to deliver data bits from one node to another. In other words, we seek to protect the network connectivity between mobile nodes over potentially multi-hop wireless channels, which is the basis to support any network security services. Multi-hop connectivity is provided in MANETs through two steps: (1) ensuring one-hop connectivity through link-layer protocols (e.g., wireless medium access control, MAC); and (2) extending connectivity to multiple hops through network-layer routing and data forwarding protocols (e.g., ad hoc routing). Accordingly, we focus on the link- and network-layer security issues, challenges, and solutions in MANETs in this article. One distinguishing characteristic of MANETs from the security, design perspective is the lack of a clear line of defence. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well-defined place where traffic monitoring or access control mechanisms can be deployed. As a result, the boundary that separates the inside network from the outside world becomes blurred.

On the other hand, the existing ad hoc routing protocols, such as Ad Hoc On-Demand Distance Vector (AODV) [1] and Dynamic Source Routing (DSR) [2], and wireless MAC protocols, such as 802.11 [3], typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by intentionally disobeying the protocol specifications. There are basically two approaches to protecting MANETs: proactive and reactive. The proactive approach attempts to prevent an attacker from launching attacks in the first place, typically through various cryptographic techniques

**What is Ad-Hoc Network?**

A collection of nodes is known as Ad-hoc network. Ad-hoc network not rely on a predefined infrastructure. The nodes are often mobile in which case the networks are called as mobile ad hoc networks (MANET).These networks are self-configurable and autonomous systems consisting of routers and hosts, which are able to support mobility and organize themselves arbitrarily. The topology of the ad-hoc network changes dynamically and unpredictably. These networks can be formed, merged together or partitioned on the fly with no central administrative server or infrastructure. Thus, it is difficult to distinguish between legal and illegal participants of the network system The Mobile ad hoc network requires a highly flexible technology for establishing communications in situations which demand a fully decentralized network without any base stations, such as battlefields, military applications, and other emergency and disaster situations. Since, all nodes are mobile; the network topology of the MANET is generally dynamic and may vary frequently. Hence, the protocol such as 802.11 to communicate via same frequency require power consumption directly proportional to the distance between hosts and direct single-hop transmissions between two hosts requires significant power that may cause interference. To avoid this problem multi-hop transmissions are used for communication. The router should be able to rank routing information sources from most trustworthy to least trustworthy and accept routing information about any particular destination from the most trustworthy sources first. A router should provide a mechanism to filter out invalid routes and be careful while distributing routing information provided to them by another party.



- ✓ Wireless ad hoc network (WANET) is a decentralized technology designed for the establishment of a network anywhere and anytime without any fixed infrastructure to support the mobility of the users in the network .
- ✓ The network is ad-hoc because each node is willing to forward data for other nodes.

sending signals to computer
mobile
ad hoc network area
Laptop
Laptop
mobile
receiving signals and also transmit for other device

**Fig 1:** Wireless Ad-HOC Networks (WANETs)

**Attacks on MANET**

Provides network connectivity between mobile nodes over potentially multi hop wireless channels mainly through link-layer protocols that ensure one-hop connectivity, and network-layer protocols that extend the connectivity to multiple hops. These distributed protocols typically assume that all nodes are cooperative in the coordination process. This assumption is unfortunately not true in a hostile environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications. The main network-layer operations in MANETs are ad hoc routing and data packet Forwarding, which interact with each other and full fill the functionality of delivering packets from the source to the destination. The ad hoc routing protocols exchange routing messages between nodes and maintain routing states at each node accordingly. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination. Nevertheless, both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. While a comprehensive enumeration of the attacks is out of our scope, such network-layer vulnerabilities generally fall into one of two categories: routing attacks and packet forwarding attacks, based on the target operation of the attacks. The family of routing attacks

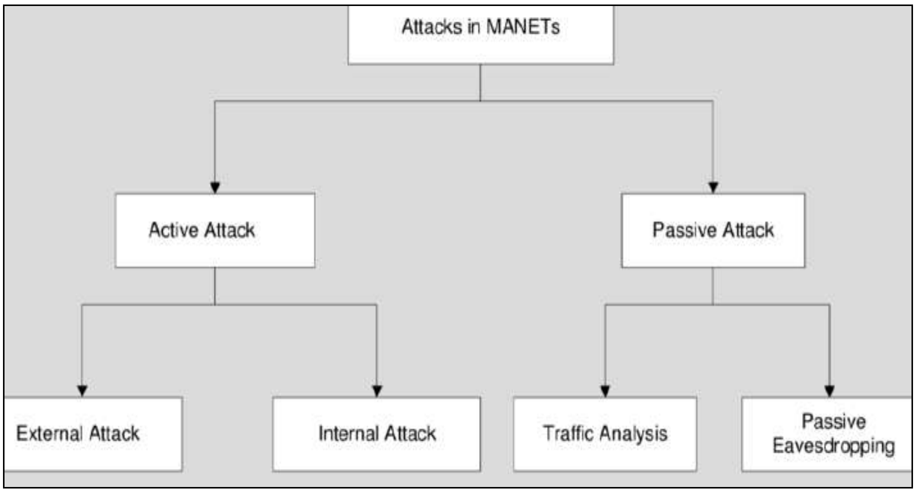


**Fig 2:** Attacks categories in MANETs

refers to any action of advertising routing updates that does not follow the specifications of the routing protocol. The specific attack behaviours are related to the routing protocol used by the MANET. The attacker may modify the source route listed in the RREQ or RREP packets by deleting a node from the list, switching the order of nodes in the list, or appending a new node into the list [5].When distance-vector routing protocols such as AODV [1] are used, the attacker may advertise a route with a smaller distance metric than its actual distance to the destination, or advertise routing updates with a large sequence number and invalidate all the routing updates from other nodes [6]. By attacking the routing protocols, the attackers can attract traffic toward certain destinations in the nodes under their control, and cause the packets to be forwarded along a route that is not optimal or even non-existent. The attackers can create routing loops in the network, and introduce severe network congestion and channel contention in certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, and partition the network in the worst case. In addition to routing attacks, the adversary may launch attacks against packet forwarding operations as well. Such attacks do not disrupt the routing protocol and poison the routing states at each node. Instead, they cause the data packets to be delivered in a way that is intentionally inconsistent with the routing states. For example, the attacker along an established route may drop the packets, modify the content of the packets, or duplicate the packets it has already forwarded. Another type of packet forwarding attack is the denial-of-service (DoS) attack via network-layer packet blasting, in which the attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET.

**MANET-Challenges**

There is many challenges in mobile ad hoc networks. Wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defence in MANETs from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. There is no well-defined place/infrastructure where we may deploy a single security solution. Moreover, portable devices, as well as the system security information they store, are vulnerable to compromises or physical capture, especially low-end devices with weak protection. Attackers may sneak into the network through these subverted nodes, which pose the weakest link and incur a domino effect of security breaches in the system. The stringent resource constraints in MANETs constitute another nontrivial challenge to security design. The wireless channel is bandwidth-constrained and shared among multiple networking entities. The computation capability of a mobile node is also constrained. For example, some low-end devices, such as PDAs, can hardly perform computation-intensive tasks like asymmetric cryptographic computation. Because mobile devices are typically powered by batteries, they may have very limited energy resources. The wireless medium and node mobility poses far more dynamics in MANETs compared to the wire-line networks. The network topology is highly dynamic as nodes frequently join or leave the network, and roam in the network on their own will. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay. Despite such dynamics, mobile users may request for anytime, anywhere security services as they move from one place to another. The above characteristics of MANETs clearly make a case for building multi fence security solutions that achieve both broad protection and desirable network performance. First, the security solution should spread across many individual components and rely on their collective protection power to secure the entire network. The security scheme adopted by each device has to work within its own resource limitations in terms of computation capability, memory, communication capacity, and energy supply. Second, the security solution should span different layers of the protocol stack, with each layer contributing to a line of defense. No single-layer solution is possible to thwart all potential attacks. Third, the security solution should thwart threats from both outsiders who launch attacks on the wireless channel and network topology, and insiders who sneak into the system through compromised devices and gain access to certain system knowledge. Fourth, the security solution should encompass all three components of prevention, detection, and reaction that work in concert to guard the system from collapse. Last but not least, the security solution should be practical and affordable in a highly dynamic and resource constrained networking scenario

**Solutions of (MANET)**

We can use encryption technique reduce the possibilities of attacks. Secret key schemes can be used to encrypt messages to ensure the confidentiality, and to some degree the authenticity of routing information and data packets; more elaborate public key schemes can be employed to sign and encrypt messages to ensure the authenticity (of individual nodes), confidentiality, and no repudiation of the communications between mobile nodes. The prevention schemes proposed so far differ in several ways, depending on their assumptions on the intended MANET applications.

**1. Encryption and key Management: Preventing External Attacks**

Encryption, authentication, and key management are widely used to prevent external (outsider) attacks. They however face many challenges in ad-hoc networks. First, we must deal with the dynamic topologies, both in communications and in trust relationship; the assessment of whether to trust a wireless node may change over time. Second, we must deal with the lack of infrastructure support in MANET; any centralized scheme may face difficulties in deployment. Key management consists of various services, of which each is vital for the security of the networking systems. The services must provide solutions to be able to answer the following questions: Trust model: It must be determined how much different elements in the network can trust each other. The environment and area of application of the network greatly affects the required trust model. Consequently, the trust relationships between network elements affect the way the key management system is constructed in network. Cryptosystems: Available for the key management: in some cases only public- or symmetric key mechanisms can be applied, while in other contexts

Elliptic Curve Cryptosystems (ECC) are available. While public-key cryptography offers more convenience (e.g. by well-known digital signature schemes), public-key cryptosystems are significantly slower than their secret-key counterparts when similar level of security is needed. On the contrary, secret key systems offer less functionality and suffer more from problems in e.g. key distribution. ECC cryptosystems are a newer field of cryptography in terms of implementations, but they are already in use widely, for instance in smart card systems. Key creation: it must be determined which parties are allowed to generate keys to themselves or other parties and what kind of keys. Key storage: In ad-hoc networks there may not be a centralized storage for keys. Neither there may be replicated storage available for fault tolerance. In ad-hoc networks any network element may have to store its own key and possibly keys of other elements as well. Moreover, in some proposals such as in, shared secrets are applied to distribute the parts of keys to several nodes. In such systems the compromising of a single node does not yet compromise the secret keys. Key distribution: The key management service must ensure that the generated keys are securely distributed to their owners. Any key that must be kept secret has to be distributed so that confidentiality, authenticity and integrity are not violated. For instance whenever symmetric keys are applied, both or all of the parties involved must receive the key securely. In public-key cryptography the key distribution mechanism must guarantee that private keys are delivered only to authorized parties. The distribution of public keys need not preserve confidentiality, but the integrity and authenticity of the keys must still be ensured.

## 2. Secure Routing Protocols: Preventing Internal Attacks

For a secure route to transport data, a proper routing protocol in Ad-Hoc networks must create a route accurately and maintain it. It means that it doesn't let the hostile nodes prevent accurate building and maintaining of the route. In general, if, in a protocol, the points such as routing signals don't counterfeit, the manipulated signals can't be injected into the network, routing messages don't change during transporting except protocol routines, routing loops don't create during aggressive activities, the shortest routes don't change by hostile nodes and so on are considered, it can be called a secure protocol. To observe these points, we begin to review several protocols as far as possible

## 3. DSR (Dynamic Source Routing)

In this protocol, the source node produces a package called RREQ in which it is determined source and target node. It sends these packages through flooding [34]. By receiving a RREQ package of each node, if it doesn't know about target route, then, it add its name to the package list and broadcast it. So, as the package reach to the target, a package includes data of route nodes and its arrangements will be available for the target node. The target node creates RREP and returns it back via available list in RREQ package header. The middle nodes know the target and do it according to the available list. So, the package traverses the route inversely to reach the source node. Although, it is a good method and certainly applicable but increases the network load and uses high band width which resulted in transporting large headers in the network. Increasing rate of header volumes resulted in increasing distance between links this approach may not work properly. OLSR works in a totally distributed manner, e.g. the MPR approach does not require the use of centralized resources. The OLSR protocol specification does not include any actual suggestions for the preferred security architecture to be applied with the protocol. The protocol is, however, adaptable to protocols such as the Internet MANET Encapsulation Protocol (IMEP), as it has been designed to work totally independently of other protocols. source and target nodes. This volume increase is due to the name of network middle elements name in the package header. Then, data sender can put the target route in the sent data header to inform middle nodes through this route that to whom they send the package. When a node can't deliver data package to the next one, it produces a package called RERR (Route Error) and returns it back to the route. So, RERR receiving nodes acknowledges about these two nodes disconnection and routing operation will be started again.

## 4. AODV (Advanced On-demand Distance Vector)

In contrast to DSR protocol, this protocol doesn't put the route in the package header. But, each node controls it while receiving PREQ according to tables it had before. If the route has the final node it its table, RREP will be sent. Otherwise, it broadcasts RREQ message. Certainly, RREPs can be returned back to RREQ. It is used consecutive number in RREQ messages that a middle node gets inform whether the route is a new one. So, if the number of RREQ consecutive is smaller than route consecutive number, RREP message will be sent by middle node.

## Conclusion

The MANET security research is still in progress. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to prevent such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Ambitious goal for ad hoc network security is to develop a multi fence security solution that is embedded into possibly every component in the network, resulting in in-depth protection that offers multiple lines of defence against many both known and unknown security threats. This new design perspective is call resiliency-oriented security design.

## References

1. Yanping Teng. A Study of Improved Approaches for TCP Congestion Control in Ad Hoc Networks International Workshop on Information and Electronics Engineering (IWIEE), 2012.
2. Schneier B. Secret and Lies, Digital Security in a Networked World, Wiley, 2000.
3. Gupta V, Krishnamurthy S, Faloutsos M. “Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks,” IEEE MILCOM, 2002.
4. Borisov N, Goldberg I, Wagner D. “Intercepting Mobile Communications: The
5. Insecurity of 802.11, ACM MOBICOM, 2001.
6. Zapata M, Asokan N. Securing Ad Hoc Routing Protocols, ACM WiSe, 2002.
7. Basagni S, Herrin K, Bruschi D, Rosti E. Secure pebble nets. In Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and

Computing (MobiHoc 2001), Long Beach, CA, 2001.

8. Balakrishnan K, Deng J, Varshney PK. "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks" Proc. IEEE Wireless Comm. and Networking Conf. (WCNC "05), 2005.
9. Karan Singh, Yadav RS, Ranvijay, International Journal of Computer Science and Security, 1(1): 52.
10. Patroklos g. Argyroudis and donalo"mahony, "Secure Routing for Mobile Ad hoc Networks", IEEE Communications Surveys & Tutorials Third Quarter, 2005.
11. Johnson D, Maltz D, Y Hu. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Internet- Draft, 2011.
12. Prakash S, Saini JP, Gupta SC. "Methodologies and Applications of Wireless Mobile Ad-hoc Networks Routing Protocols", International Journal of Applied Information Systems. 2012; 1(6):5-15.
13. Security in Ad Hoc Networks, Vesa Kärpijoki, Helsinki University of Technology, Telecommunications Software Multimedia Laboratory, Vesa. Karpijoki@hut.fi