*I.J. Information Engineering and Electronic Business*, 2013, 3, 49-58
Published Online September 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2013.03.06

# Security Challenges and Attacks in Mobile Ad Hoc Networks

**CH.V. Raghavendran**
Associate Professor, Ideal College of Arts & Sciences, Kakinada, Andhra Pradesh, India
*E-mail: raghuchv@yahoo.com*

**G. Naga Satish**
Associate Professor, Ideal College of Arts & Sciences, Kakinada, Andhra Pradesh, India
*E-mail: gantinagasatish@gmail.com*

**P. Suresh Varma**
Dr. , Professor, Adikavi Nannaya University, Rajahmundry, Andhra Pradesh, India
*E-mail: vermaps@gmail.com*

***Abstract***—Mobile Ad hoc Network (MANET) is an autonomous collection of mobile nodes that form a temporary network without of any existing network infrastructure or central access point. The popularity of these networks created security challenges as an important issue. The traditional routing protocols perform well with dynamically changing topology but are not designed to defense against security challenges. In this paper we discuss about current challenges in an ad hoc environment which includes the different types of potential attacks that are possible in the Mobile Ad hoc Networks that can harm its working and operation. We have done literature study and gathered information relating to various types of attacks. In our study, we have found that there is no general algorithm that suits well against the most commonly known attacks. But the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET. To develop suitable security solutions for such environments, we must first understand how MANETs can be attacked. This paper provides a comprehensive study of attacks against mobile ad hoc networks. We present a detailed classification of the attacks against MANETs.

***Index Terms***— MANETs, Security, Passive Attacks, Active Attacks, Network Layers.

## I. Introduction

Security is an essential service for wired and wireless network communications. The success of MANET strongly depends on whether its security can be trusted. In this paper we focused on the routing security in MANET. Due to mobility and ad hoc nature, security in mobile ad hoc networks is particularly hard to achieve: the wireless links are usually fragile with high link broken ratio; nodes lack of enough physical protection can be easily captured, compromised, and hijacked; the sporadic nature of connectivity and the dynamically changed topology may cause frequent routes update; the absence of a certification authority and the lack of centralized monitoring or management point further deteriorate the situations. However, the characteristics of MANET pose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. There are a wide variety of attacks that target the weakness of MANET.

During the last decade, extensive studies have been conducted on routing in mobile ad hoc networks, and have resulted in several mature routing protocols. However, in order to work properly, these protocols need trusted working environments, which are not always available. In many situations, the environment may be adversarial. For example, some nodes may be selfish, malicious, or compromised by attackers. To address these issues, many schemes have been proposed to secure the routing protocols in ad hoc networks. So, in order to make MANETs secure, all types of attacks are to be identified and solutions to be considered to make MANETs safe. Some of the attacks are considered in our study. However the list is possibly incomplete, and some more attacks on MANETs are likely to be discovered in near future. So Security issues in MANETs will remain a potential research area in near future.

The rest of the paper is organized as follows. In Section 2 we introduced Mobile Ad Hoc Networks. In Section 3, we discussed on security requirements for MANETs. In Section 4, we described the security challenges. In Section 5, we briefly discuss about different type of attacks. In Section 6, security attacks are discussed on layer wise. In Section 7, we concluded our study on security challenges.

## II. Mobile Ad Hoc Networks

Now-a-days, Mobile ad hoc network (MANET) is one of the recent active fields and has received marvelous attention because of their self-configuration and self-maintenance capabilities [1]. MANET is a collection of mobile devices connected through wireless links to serve a specific purpose. MANETs provide users with easier ways to connect and communicate without the need for prior setup or a centralized server. MANETs are particularly used in situation where a fast installation is needed and no infrastructure is available. The only condition the device has to fulfill is the communication interface, as it needs one to build up a connection to other devices. The networks are self-organized and adaptive. As it has no infrastructure the participants are directly connected with one another and not to an access point, to a gateway or something similar. The nodes must, therefore, not just send and receive, but also forward packets. In MANETs the composition of the nodes varies very rapidly: in every moment a new node may connect or an established node may disconnect. MANETs use wireless connections for communication and that the devices are battery powered.

MANETs are currently used in many areas and have various defining characteristics that differentiate them from other wireless networks such as WLAN. Possible applications of MANET include: soldiers relaying information for situational awareness on the battlefield, business associates sharing information during a meeting, attendees using laptop computers to participate in an interactive conference, and emergency disaster relief personnel coordinating efforts after a fire, hurricane or earthquake. Other possible applications include personal area and home networking, location-based services, and sensor networks.

## III. Security Requirements

Ad hoc networks are very open to anyone. Their biggest advantage is also one of their biggest disadvantages. Anyone with the proper hardware and knowledge of the network topology and protocols can connect to the network. This allows potential attackers to infiltrate the network and carry out attacks on its participants with the purpose of stealing or altering information.

Any routing protocol must encapsulate an essential set of security requirements like confidentiality, authentication, availability, integrity, non-repudiation, authorization and accounting [2]. These need to be addressed in order to maintain a reliable and secure ad-hoc network environment. These have to be protected against defects and more importantly against malicious intent.

### 3.1 Confidentiality

Confidentiality is the process of keeping the information sent unreadable to unauthorized readers [2]. Transmission of sensitive information requires confidentiality. Routing and packet forwarding information must also remain confidential. Attacks against confidentiality aims at getting access to private or confidential data, for instance user names and passwords, credit card numbers, secret reports etc. To keep the confidentiality, it is required to ensure to communicate with right partner. Confidentiality can be achieved using any of the available encryption techniques, provided that proper access key systems are used. Protecting privacy involves more than encryption and requires more sophisticated techniques to hide the identity or the location of the user.

### 3.2 Authentication

Authenticity means the verifying and proving the identity of the participants in a network. This is important to ensure genuine access to the network. The nodes wish to communicate with each other need to verity the identity of each other to satisfy that they are communicating with authorized party [2].

### 3.3 Availability

Services or resources should be available to genuine users whenever required. It ensures the survivability of the network despite malicious incidents. This is very important in many applications.

### 3.4 Integrity

The integrity is the ability to guarantee that the received message is the real one that has not been tampered or changed. This is an essential in situations such as banking, military operations and equipment controls. As with confidentiality, integrity can apply to a stream of messages, a single message or selected fields within a message [2]. But, the most useful and straightforward approach is total stream protection. Integrity guarantees that the authorized parties are only allowed to modify the information or messages so that it is never corrupted.

### 3.5 Non-repudiation

The goal of non-repudiation is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it. If a message is sent, the receiver can prove that the message was sent by the alleged sender. In the same way, after sending a message, the sender can prove that the message was received by the alleged receiver. This may be of great importance in some situations but might not be in some others.

### 3.6 Authorization and Accounting

Nodes participating in a network need to have proper permissions to access shared resources on that network. In a MANET, nodes should be able to restrict others from accessing private information on their devices. Moreover, in some cases, the authorization policies are accompanied by accounting mechanisms to track resource utilization to identify bottlenecks, charging users for services or for statistical information about the network. Both authorization and accounting require robust methods to ensure correctness of protocols and proper utilization of resources.

## IV. Security Challenges

Active attacks [3, 4, 5] in MANET range from deleting messages, injecting messages, impersonate a node etc thus violating confidentiality, authentication, availability, integrity, and non-repudiation. Unlike the wired networks achieving security in MANETs is challenging. According [6] Ad hoc networks pose a number of nontrivial challenges to security design, such as the following.

### 4.1 Dynamic Topology

Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network vary timely and are based on the proximity of one node to another node. This dynamism could be better protected with distributed and adaptive security mechanisms [2].

### 4.2 Scalability

Scalability is an important issue concerning security. Security mechanisms should be capable of handling a large network as well as small ones [1].

### 4.3 Autonomous

No centralized administration entity is available to manage the operation of the different mobile nodes.

### 4.4 Poor Transmission Quality

This is an inherent problem of wireless communication caused by several error sources that result in degradation of the received signal.

### 4.5 Bandwidth Optimization

Wireless links have significantly lower bandwidth than the wired links.

### 4.6 Device Discovery

Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection.

### 4.7 Infrastructure less and Self Operated

Self healing feature demands MANET should realign itself to blanket any node moving out of its range.

### 4.8 Limited Resources

Mobile nodes rely on battery power, which is a scarce resource. Also computational power and storage capacity are limited.

### 4.9 Limited Physical Security

Mobility implies higher security risks such as peer-to-peer network architecture or a shared wireless medium accessible to both legitimate network users and malicious attackers.

### 4.10 Ad hoc Addressing

Challenges in standard addressing scheme are to be implemented.

### 4.11 Topology Maintenance

Updating information of dynamic links among nodes in MANETs is a major challenge.

Providing secure communication in such changing and dynamic environment, as well as protection against specific threats and attacks, leads to development of various security schemes and architectures.

## V. Security Attacks

MANET provides network connectivity between mobile nodes over potentially multihop 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 assume that all nodes are cooperative. This assumption is unfortunately not true in an unfriendly environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications.

Many characteristics might be used to classify security attacks in the MANETs [7]. They would include looking at the behavior of the attacks (passive vs. active), the source of the attacks (external vs. internal), the processing capability of the attackers (mobile vs. wired), the number of the attackers (single vs. multiple) different protocol layer, stealthy or non-stealthy, and cryptography or non-cryptography related.

### 5.1 Passive vs. Active

The Passive attacks steal valuable information in the targeted networks. Examples of passive attacks are eavesdropping attacks and traffic analysis attacks. Detecting this kind of attack is difficult because neither the system resources nor the critical network functions are physically affected to prove the intrusions [8].

An Active attack attempts to alter system resources or affect their operation [8]. These actively alter the data, with the intent of overloading the network, obstructing the operation or to cut off certain nodes from their neighbors so they can not use the networks services effectively anymore. To execute active attacks, the attacker must be able to inject packets into the network. Table 1 shows the general taxonomy of security attacks against MANET. Examples of active attacks comprise actions such as message modifications, message replays, message fabrications and the denial of service attacks.

Table 1: Security Attacks Classification

| Passive Attacks | Active Attacks |
|---|---|
| Eavesdropping<br>Traffic analysis<br>Monitoring | Jamming<br>Spoofing<br>Replaying<br>Modification and DoS |

### 5.2 External vs. Internal

External attacks are launched by adversaries that are not legally part of the network. These attacks usually aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations. Bogus packets injection, denial of service, and impersonation are some of the attacks that are usually initiated by the external attackers.

Internal attacks are sourced from inside a particular network. A compromised node with access to all other nodes within its range poses a high threat to the functional efficiency of the whole network. Attacks that are caused by the misbehaving internal nodes are difficult to detect because to distinguish between normal network failures and misbehavior activities in the ad hoc networks is not an easy task.

### 5.3 Mobile vs. Wired Attackers

Mobile attackers have the same capabilities as the other nodes in the ad hoc networks. Their capabilities to harm the networks operations are also limited because of limited resources. With the limited transmitting capabilities and battery powers, mobile attackers could only jam the wireless links within its vicinity but not the whole networks operations.

Wired attackers are attackers that are capable of gaining access to the external resources such as the electricity. Since they have more resources, they could launch more severe attacks in the networks, such as jamming the whole networks or breaking expensive cryptography algorithms. Existence of the wired attackers in the ad hoc networks is always possible as long as the wired attackers are able to locate themselves in the communication range and have access to the wired infrastructures.

### 5.4 Single vs. Multiple Attackers

Attackers might choose to launch attacks against the ad hoc networks independently or by colluding with the other attackers. Single attackers usually generate a moderate traffic load as long as they are not capable to reach any wired facilities. Since they also have similar abilities to the other nodes in the networks, their limited resources become the weak points to them [9].

If several attackers are colluding to launch attacks, defending the ad hoc networks against them will be much harder. Colluding attackers could easily shut down any single node in the network and be capable to degrading the effectiveness of network's distributed operations including the security mechanisms.

### 5.5 Attacks on Different Layers of the Internet Model

The attacks can be classified according to the five layers of the Internet model. Table 2 presents a classification of various security attacks on each layer of the Internet model. Some attacks can be launched at multiple layers.

Table 2: Security Attacks on each layer in MANET

| Layer | Attacks |
|---|---|
| Application layer | Repudiation, Data corruption |
| Transport layer | Session hijacking, SYN flooding |
| Network layer | Wormhole, Blackhole, Byzantine, Flooding, Resource consumption, Location disclosure attacks |
| Data link layer | Traffic analysis, Monitoring, Disruption MAC (802.11), WEP weakness |
| Physical layer | Eavesdropping, Jamming, Interceptions |
| Multi-layer attacks | DoS, Impersonation, Replay, Man-in-the-middle |

### 5.6 Stealthy vs. Non-stealthy Attacks

Some security attacks use stealth, where the attackers try to hide their actions from either an individual who is monitoring the system or an intrusion detection system (IDS). But other attacks such as DoS cannot be made stealthy.

### 5.7 Cryptography vs. Non-cryptography Related Attacks

Some attacks are non-cryptography related, and others are cryptographic primitive attacks. Table 3 shows cryptographic primitive attacks and the examples.

Table 3: Cryptographic Primitive Attacks

| Cryptographic Primitive Attacks | Examples |
|---|---|
| Pseudorandom number attack | Nonce, Timestamp, Initialization vector (IV) |
| Digital signature attack | RSA signature, ElGamal signature, Digital signature standard (DSS) |
| Hash collision attack | SHA-0, MD4, MD5, HAVAL-128, RIPEMD |

## VI. Layer-Wise Security Attacks

### 6.1 Physical Layer Attacks

### *6.1.1 Eavesdropping:*

This is intercepting and reading of messages and conversations by unintentional receivers. The nodes share a wireless medium and the wireless communication use the RF spectrum and broadcast by nature which can be easily intercepted with receivers tuned to the proper frequency. Signals broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency. As a result transmitted message can be overheard as well as fake message can be injected into the network.

### *6.1.2 Interference and Jamming:*

Accidentally or intentionally, interference can happen with radio waves of MANETs, because WLAN use unlicensed radio frequencies. Other electromagnetic devices operating in the infrared or 2.4 GHz RF can overlap with WLAN traffic. A powerful transmitter can generate signal that will be strong enough to overwhelm the target signal and can disrupting communications. This condition is called jamming. Jamming attacks can be mounted from a location remote to the target networks. This makes this attack extremely inevitable. Pulse and random noise are the most common type of signal jamming [9].

### 6.2 Data Link Layer Attacks

### *6.2.1 Traffic Analysis:*

Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair. Data on who is communicating with whom, how often, how much, and when is easily available to any eavesdropper within range of the wireless network. Even if the payload is encrypted, standard MANET protocols transmit enough header and routing information in the clear making traffic analysis relatively easy for attackers. Traffic analysis is a threat to secure communication, either by identifying targets for attacks such as denial-of-service or encryption cracking, or by revealing communication relationships. Traffic analysis in ad hoc networks may reveal:

- the existence and location of nodes
- the communications network topology
- the roles played by nodes
- the current sources and destination of communications and
- the current location of specific individuals or functions

### *6.2.2 Disruption MAC (802.11):*

Many attacks can be launched in link layer by disrupting the cooperation of the protocols of this layer. Wireless medium access control (MAC) protocols have to coordinate the transmission of the nodes on the common communication or transmission medium. The IEEE 802.11 MAC is vulnerable to DoS attacks. To launch the DoS attack, the attacker may exploit the binary exponential backoff scheme. For example, the attacker may corrupt frames easily by adding some bits or ignoring the ongoing transmission. Capture effect is an important effect to consider in link layer, which means that nodes that are heavily loaded tend to capture the channel by sending data continuously, thereby resulting lightly loaded neighbors to back off endlessly. Malicious nodes may take the advantage of this capture effect vulnerability. Another vulnerability to DoS attacks is exposed in IEEE 802.11 MAC through Network Allocation Vector (NAV) field carried in the RTS/CTS (Ready to Send/Clear to Send) frames.

### *6.2.3 WEP weakness:*

The WEP was designed by a group of IEEE volunteer members, aiming at giving some layer of security to wireless networks. IEEE 802.11 WEP incorporates Wired Equivalent Privacy (WEP) to provide WLAN systems a modest level of privacy by encrypting radio signals. The WEP protection technique suggested for adhoc network fall short of the objective of data privacy, data integrity and authentication. Various security standards such as IEEE 802.11i, WPA, and IEEE 802.1 X were suggested to enhance the security issues in 802.11.Despite their efficiency, these standards do not provide any robustness to the security approach for monitoring of the authentication in a distributed architecture. Some of the weaknesses 802.11 WEP are listed below [11] [12] [13],

- Key management is not specified in the WEP protocol.
- The initialization vector (IV) used in WEP is sent in clear.
- The WEP has not planed a mechanism to ensure data source authentication.

The combined use of a non-cryptographic integrity algorithm, CRC 32 with the stream chipper is a security risk and may cause message privacy and message integrity attacks.

### 6.3 Network Layer Attacks

### 6.3.1 *Wormhole Attack:*

The wormhole attack [14] is one of the most sophisticated and severe attacks in MANETs. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The Fig 1 shows the Wormhole attack. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Furthermore, the attacker is invisible at higher layers; unlike a malicious node in a routing protocol, which can often easily be named, the presence of the wormhole and the two colluding attackers at either endpoint of the wormhole are not visible in the route.

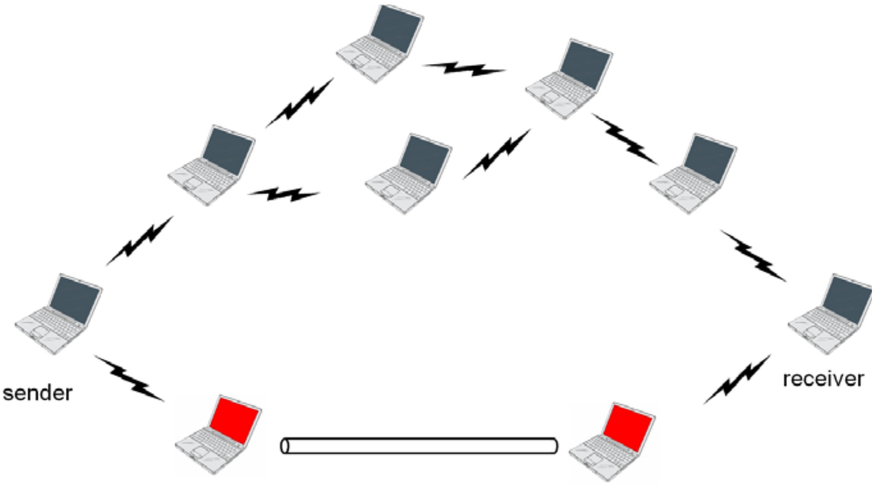

Fig. 1: Wormhole attack

### 6.3.2 *Blackhole Attack:*

In this attack, a malicious nodes trick all their neighboring nodes to attract all the routing packets to them. It exploits the routing protocol to advertise itself as having a good and valid path to a destination node. It tries to become an element of an active route. As in the wormhole attacks, malicious nodes could launch the black hole attacks by advertising themselves to the neighboring nodes as having the most optimal route to the requested destinations. The blackhole attack is illustrated in Fig 2. However, unlike in the wormhole attacks where multiple attackers colluded to attack one neighboring node, in the black hole attacks, only one attacker is involved and it threatens all its neighboring nodes.

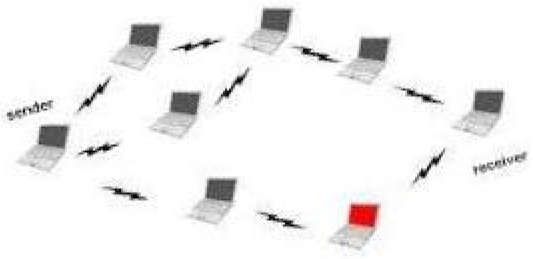

Fig. 2: Blackhole attack

The blackhole attack is performed in two steps. At first step, the malicious node exploits the mobile ad hoc routing protocol such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting the packets. In second step, the attacker consumes the packets and never forwards. In an advanced form, the attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected.

### 6.3.3 *Byzantine attack:*

Byzantine attack can be launched by a single malicious node or a group of nodes that work in cooperation. A compromised intermediate node works alone or set of compromised intermediate nodes works in collusion to form attacks. The compromised nodes may create routing loops, forwarding packets in a long route instead of optimal one, even may drop packets. This attack degrades the routing performance and also disrupts the routing services [15].

### 6.3.4 *Flooding attack:*

In this attack, attacker exhausts the network resources, such as bandwidth and to consume a node’s resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service [16].

### *6.3.5 Resource consumption attack:*

In MANETs energy is a critical parameter because the battery-powered devices try to conserve energy by transmitting only when absolutely necessary [17]. The target of resource consumption attack is to send request of excessive route discovery or unnecessary packets to the victim node in order to consume the battery life. An attacker or compromised node thus can disrupt the normal functionalities of the MANET. This attack is also known as sleep deprivation attack.

### *6.3.6 Location disclosure attacks:*

This attack is a part of the information disclosure attack. The malicious node leaks information regarding the location or the structure of the network and uses the information for further attack. It gathers the node location information such as a route map and knows which nodes are situated on the target route and then plans further attack scenarios. The leakage of such information is devastating in security sensitive scenarios Traffic analysis is one of the unsolved security attacks against MANETs.

## 6.4 Transport Layer Attacks

### *6.4.1 Session hijacking:*

Session hijacking is a critical error and gives a malicious node the opportunity of behaving as a legitimate system. The attacker takes the advantage that, all the communications are authenticated only at the beginning of session setup and performs the session hijacking attack. At first, the attacker spoofs the IP address of target machine and determines the correct sequence number that is expected by the target and performs a DoS attack on the victim. As a result, the target system becomes unavailable for some time. The attacker now continues the session with the other system as a legitimate system.

### *6.4.2 SYN flooding:*

The SYN flooding attack is also Denial of Service (DoS) attack which is performed by creating a large number of half-opened TCP connections with a victim node. For two nodes to communicate using TCP, they must first establish a TCP connection using a three-way handshake. The three messages exchanged during the handshake, illustrated in Figure 3. The sender sends a SYN message to the receiver with a randomly generated ISN (Initial Sequence Number). The receiver also generates another ISN and sends a SYN message including the ISN as an acknowledgement of the received SYN message. The sender sends acknowledgement to the receiver. In this way the connection is established between two communicating parties using TCP three way handshakes.

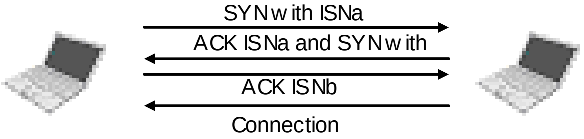

Fig. 3: TCP Three Way Handshake

## 6.5 Application Layer Attacks

### *6.5.1 Repudiation:*

Firewalls are used to keep packets in or keep packets out in the network layer. In the transport layer, entire connections can be encrypted, end-to-end. But these solutions taken to solve authentication or non-repudiation attacks in network layer or in transport layer are not enough to solve the problems. Repudiation refers to a denial of participation in the communication. Example of repudiation attack on a commercial system includes a selfish person could deny conducting an operation on a credit card purchase or deny any on-line transaction [10].

## 6.6 Multilayer Attacks

Some security attacks can be launched from multiple layers instead of a particular layer. Examples of multi-layer attacks are denial of service (DoS), man-in-the middle and impersonation attacks.

### *6.6.1 Denial of Service:*

In Denial of service (DoS) type of attack, the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET. The limitation of the wireless links is utilized in resource depletion attacks. The attackers transfer big, unnecessary volumes of data between them to deplete the bandwidth of the links. The resource depletion attack is shown in the Figure 4. During this transfer A and B might send and receive only with a limited efficiency.

Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow [18] and the sleep deprivation torture [19]. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

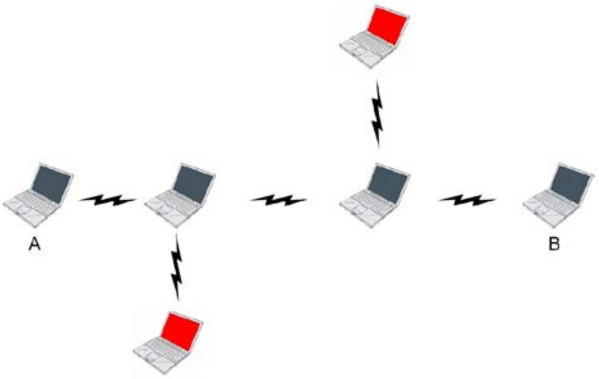

Fig. 4: Resource Depletion Attack

For example, consider the following Figure. 5. Assume a shortest path exists from **S** to **X** and **C** and **X** cannot hear each other, that nodes **B** and **C** cannot hear each other, and that **M** is a malicious node attempting a denial of service attack. Suppose **S** wishes to communicate with **X** and that **S** has an unexpired route to **X** in its route cache. **S** transmits a data packet toward **X** with the source route **S** --> **A** --> **B** --> **M** --> **C** --> **D** --> **X** contained in the packet's header. When **M** receives the packet, it can alter the source route in the packet's header, such as deleting **D** from the source route. Consequently, when **C** receives the altered packet, it attempts to forward the packet to **X**. Since **X** cannot hear **C**, the transmission is unsuccessful.

**S ↔A↔ B↔ M ↔C↔ D↔ X**

Fig. 5: Denial of Service attack

### *6.6.2 Impersonation:*

Impersonation attacks are also called spoofing attacks. Spoofing is a special case of integrity attacks whereby a compromised node impersonates a legitimate one due to the lack of authentication in the ad hoc routing protocols. Depending on the access level of the impersonated node, the intruder may even be able to reconfigure the network so that other attackers can easily join or he could remove security measures to allow subsequent attacks. A compromised node may also have access to encryption keys and authentication information. In many networks, a malicious node could obstruct proper routing by injecting false routing packets into the network or by modifying routing information. As described in [20], an intruder may try to impersonate a node within the path of the data flow of interest. This can be achieved by modifying routing data or implying itself as a trustworthy communication partner to neighboring nodes in parallel.

A spoofing attack allows forming loops in routing packets which may also result in partitioning network. In many cases, lighter solutions like key hashed functions, priori negotiated and certified key and session identifiers are used. However, by using good authentication algorithms, strong data encryption and secure routing protocols, the effects of impersonation can be reduced significantly.

### *6.6.3 Man in the Middle Attack:*

In this attack, the attacker sits between the sender and the receiver and sniffs any information being sent between two ends. In some cases the attacker may impersonate the sender to communicate with the receiver, or impersonate the receiver to reply to the sender.

### 6.7 Other Attacks

According to [16] MANETs may face other security attacks which include Neighbor attack, Jellyfish attack, Packet dropping attacks, Gray hole attack, Device tampering attack, Colluding misrelay attack, Sybil attack, State Pollution attack, Modification, Fabrication, Link spoofing attack etc.

## VII. Conclusion

In this study, we try to inspect the security threats in the MANETs that may vary depend on (1) which environment the attacks are launched, (2) what communication layer the attacks are targeting, and (3) what level of ad hoc network mechanisms are targeted.. It is clear that the security aspects related to MANETs are much higher due to the dynamic and unpredictable nature of most MANETs. On the other hand, ad hoc networks vary from each other greatly from the viewpoint of the area of application. Some ad hoc networks may not need security solutions other than simple encryption and username-password authentication scheme, as in the classroom example, while networks operating in highly dynamic and hostile environment, such as in the battlefield scenario demand extremely efficient and strong mechanisms. As the security requirements and their implications vary, general security architecture for MANET cannot be constructed. Existing papers are typically based on some specific attacks. There are many unanticipated or combined attacks that remain undiscovered. Research is still being performed and will result in the discovery of new security threats as well as the creation of new countermeasures. More research is needed on trust-based protocols, key management system, integrated approaches to routing security, and data security at different layers. The underlying rationale is that, existing security solutions are well-matched with specific attacks, these solutions have proven to be useful to defend against known attacks, but eventually they fail to counteract unanticipated or combined attacks. During the study, we also find some points that can be further explored in the future, such as to find some effective security solutions and protect the MANET from all kinds of security threats.

## References

[1] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhanng, "Security on Mobile Ad Hoc Networks: Challenges and Solutions" 1536-1284/04/IEEE Wireless Communica-tions Feb, '04.

[2] Zhou, L and Haas Z. J., "Securing Ad Hoc Networks" *IEEE Network Magazine*, 13(6), 1999, pp. 24-30.

[3] Nishu Garg and R.P. Mahapatra, "MANET Security Issues". *In IJCSNS International Journal of Computer Science and Network Security,* 9**,** No.8, August 2009.

[4] Arun Kumar Bayya, Siddhartha Gupte, Yogesh Kumar Shukla, Anil Garikapati. "Security in Ad-hoc Networks". *Computer Science Department University of Kentucky*.

[5] Sanzgiri K, Dahill B, Levine B.N and Belding-Royer E.M, "A secure routing protocol for Ad-hoc networks," *Proc. Of IEEE ICNP, 2002*.

[6] Er. Tushar Gohil "Overview of Security Threats in Mobile Ad-hoc Network", Journal of High Performance Communication Systems and Networking Volume. 2 (1-2), January-December 2010, pp. 1–10.

[7] A. Burg. "Ad hoc network specific attacks". *In Seminar Ad Hoc networking: Concepts, Applications and Security*. Technische University Munchen, 2003.

[8] S. Bouam and J. B. Othman, "Data Security in Ad hoc Networks using MultiPath Routing," in *Proc. of the 14th IEEE PIMRC*, pp. 1331-1335, Sept. 7-10, 2003.

[9] G. Schäfer, "Research Challenge in Security for Next Generation Mobile Networks," Position Papers PAMPAS '02 - Workshop on Requirements for Mobile Privacy & Security, Sept. 16-17, 2002.

[10] B. Wu, J. Chen, J. Wu, M. Cardei, *"A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,"* Department of Computer Science and Engineering, Florida Atlantic University, http://student.fau.edu/jchen8/web/papers /SurveyBookchapter.pdf

[11] W. Stallings, *Wireless Communication and Networks*, Pearson Education, 2002.

[12] N. Borisov, I. Goldberg and D.Wagner, Interception Mobile Communications: The Insecurity of 802.11. *Conference of Mobile Computing and Networking*, 2001.

[13] T. Karygiannis and L. Owens, Wireless Network Security-802.11, Bluetooth and Handheld Devices. National Institute of Standards and Technology. Technology Administration, U.S Department of Commerce, *Special Publication* 800-848, 2002.

[14] Y.C.Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," *IEEE JSAC*, vol. 24, no. 2, Feb. 2006.

[15] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. *Proceedings of the ACM Workshop on Wireless Security*, pp.21-30, '02.

[16] Pradip M. Jawandhiya et. al. "A Survey of Mobile Ad Hoc Network Attacks" *International Journal of Engineering Science and Technology* Vol. 2(9), 2010, 4063-4071.

[17] H. Deng, W. Li, Agrawal, D.P., "*Routing security in wireless ad hoc networks,*" Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804.

[18] J.-F. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems," *Proc. Wksp. Design Issues in Anonymity and Unobservability*, Berkeley, CA, July '00, pp. 7–26.

[19] K. Sanzgiri *et al.*, "A Secure Routing Protocol for Ad hoc Networks," *Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02)*, 2002, pp. 78–87.

[20] Chris Karlof, David Wagner: Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures http://citeseer.nj.nec.com /576488.html.

## Authors' Profiles

**CH.V. Raghavendran** has received MCA and M.Tech (CSE) degrees from Nagarjuna University in 1994 and 2010 respectively. He received his M.Phil in Computer Science in 2008 from Alagappa University. He is a research scholar in Compute Science Department of Adikavi Nannaya University, Rajahmundry, AP. He has published over 10 papers in various National and International Conferences. He is working as a Director of P.G. Dept. of Computer Sciences, Ideal College of Arts & Sciences, Kakinada, AP. His areas of interest are Mobile Ad hoc Networks, Swarm Intelligence and Data Mining.

**Ganti Naga Satish** is working as Associate Professor in P.G. Department of Computer Sciences, Ideal College of Arts & Sciences, Kakinada, Andhra Pradesh, India. His qualifications are M.Sc, M.Phil, M.Tech. He is pursing Ph.D at Adikavi Nannaya University. He has presented and published papers in National and International Conferences. His areas of interest include Computer Networks.

**Dr. P. Suresh Varma** received the Master’s degree M.Tech in Computer Science & Technology from Andhra University. He received Ph.D. degree in Computer Science & Engineering from Acharya Nagarjuna University. He is currently working as Professor in Department of Computer Science in Adikavi Nannaya University, Rajahmundry, A.P., India. He published several papers in National and International Journals. He is active member of various professional bodies. His current research is focused on Computer Networks, Cloud Computing and Data Mining.