Computing, Information Systems & Development Informatics Journal
Vol. 8 No. 4, December, 2017 - www.cisdijournal.org

A Chronology of Routing Protocol on Mobile Ad-Hoc Networks (MANET) and Systemic Vulnerabilities

Nwaocha, V.O. & Osang, F.
Department of Computer Science
National Open University of Nigeria
Abuja, FCT, Nigeria
E-mail: onwaocha@noun.edu.ng ; fosang@noun.edu.ng

ABSTRACT

The adoption and use of ubiquitous computer and network technology to address a myriad of communication challenges and facilitate online interaction has led to the continued focus on developing effective an efficient means to provide end-to-end communication between nodes within Mobile Ad-Hoc networks (MANET). Unfortunately, mobility and the dearth of resource in wireless networks that leverages on the TCP/IP model for communication is faced with the challenge that each layer in the TCP/IP model require redefinition or modifications to function efficiently in MANETs and thus requires routing and rerouting schemes to aid throughput and efficiency. Routing in ad-hoc networks involves finding a path from the source to the destination, and delivering packets to the destination node while nodes in the network are moving freely. Due to node mobility, a path established by a source may not exist after a short interval of time. Therefore, to cope with node mobility, nodes require the maintenance of the routes within the network. This paper presents a number of routing protocols for MANET and demonstrates how nodes establish and maintain paths for efficient and effective routing and elucidates systemic vulnerabilities in these networks.

Keywords: Routing, Protocols, MANET, Vulnerabilities, TCP/IP, Mobility, Resources, Security

CISDI Journal Reference Format
Nwaocha, V.O. & Osang, F. (2017): A Chronology of Routing Protocol on Mobile Ad-Hoc Networks (MANET) and Systemic Vulnerabilities. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 8 No 2. Pp 79-90-. Available online at www.cisdijournal.org

1. INTRODUCTION

People who make use of mobile devices often need to communicate in settings whereby no fixed wired infrastructure is available; this could be due to the fact that it may not be economically feasible or physically possible to provide the necessary infrastructure, or due to the fact that the setting does not permit its installation. Similarly, a group of students in a higher institution may need to share ideas during a lecture, business associates may run into each other in an airport terminal and wish to share files, or a group of emergency rescue workers may need to be rapidly deployed after a flood. In such situations, a collection of any established infrastructure or centralized administration. This sort of wireless network is referred to as a mobile ad hoc network. The mobile ad hoc network (MANET) has been in focus with the wireless research community and is currently a very active field of study. Today, with the rapid proliferation of wireless mobile devices such as laptops, Smartphone's, tablets etc, the significance of nomadic and ubiquitous computing, particularly mobile ad hoc networking have become apparent [1]. Over the last two decades, MANETs of various forms have emerged owing to the ever-increasing application of a wide range of wireless mobile devices. In view of the fact that these devices are getting smaller, cheaper and more powerful, they are becoming increasingly popular. The ad hoc self-organizing feature of MANETs make them quite suitable for virtual conferences, where setting up a traditional network infrastructure could be rather time consuming and could turn out to be a high-costing task [2]

Ordinarily, MANETs do not have an underlying infrastructure; for this reason mobile host in MANETs "join" on the fly and create a network on their own. With the network topology changing dynamically and the lack of a centralized network management functionality, MANETs tend to be highly vulnerable to a number of attacks. In other words, the numerous benefits of the wireless mobile ad hoc network comes at the cost of various security flaws.

The shared and easy to access medium is undoubtedly the major advantage of wireless networks, while at the same time is its Achilles' heel. In other word, it makes it extremely easy for an adversary to launch an attack [3]. Therefore, intruders easily penetrate the network and as a consequence MANETs are extremely susceptible to network attacks due to their open and distributed nature, lack of fixed infrastructure, lack of central management, node mobility and dynamic topology.

While early research effort in MANETs assumed a friendly and cooperative environment and focused on challenges such as wireless channel access and multi-hop routing, yet this is not the case in reality, therefore security has become the main source of concern, in a potentially hostile environment. Recent research on wireless MANETs indicate that this type of network presents greater security challenge than conventional wired and wireless networks [4].

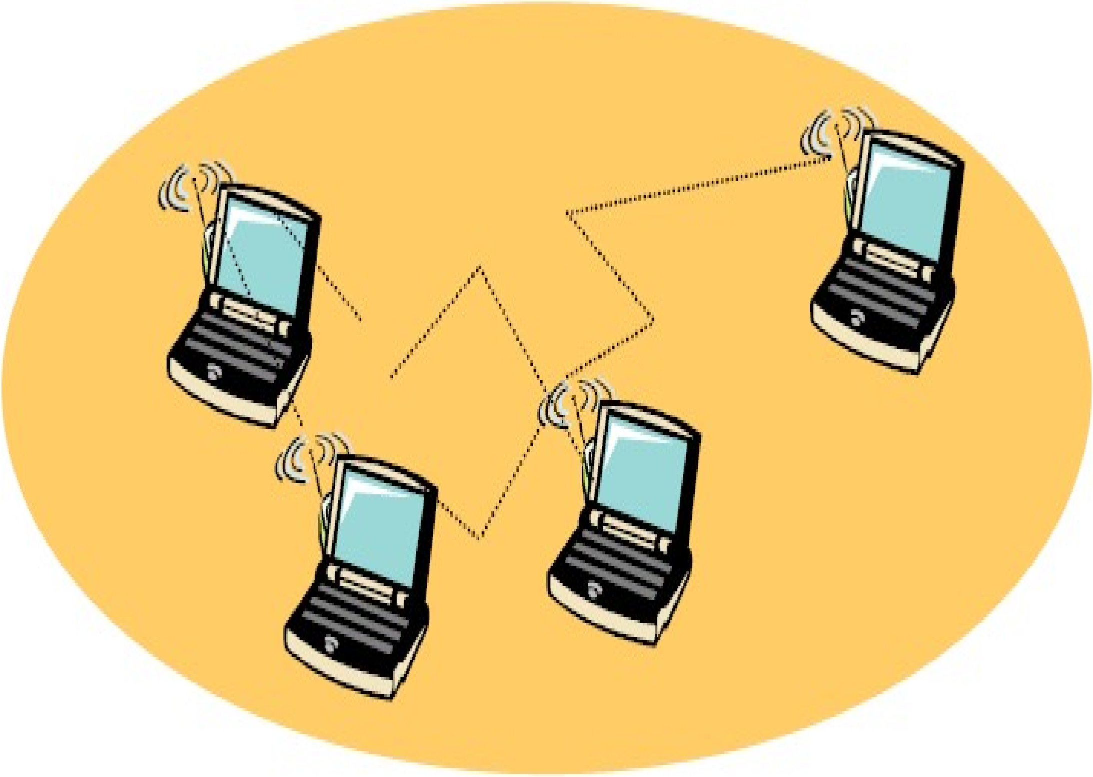


Figure 1: Mobile Ad hoc Network [2]

2. ROUTING IN MANETS

The term routing refers to the process of finding a path between two communicating host in a given network [5] In conventional networks, the routers are preconfigured by the administrator to perform the task of routing, and each packet is forwarded according to its Internet protocol (IP) address, In the case of an ad hoc network, comprising of a number of hand-held devices which communicate with each other over wireless channels without any infrastructure, the network topology changes rapidly and unpredictably and no dedicated nod has to be defined to perform routing in MANETs. As a result, the conventional routing protocols are not suitable for application in MANETs.

Normally routing in ad-hoc networks involves finding a path from the source to the destination, and delivering packets to the destination node while nodes in the network are moving freely. Due to node mobility, a path established by a source may not exist after a short interval of time.

Therefore, to cope with node mobility, nodes require the maintenance of the routes within the network. Hence, depending on how nodes establish and maintain paths, routing protocols for mobile ad-hoc networks broadly fall into four categories namely [6]:

i. Proactive routing protocols
ii. Reactive routing protocols
iii. Hybrid routing protocols and
iv. Location-based routing protocols

2.2.1 Proactive Routing Protocols

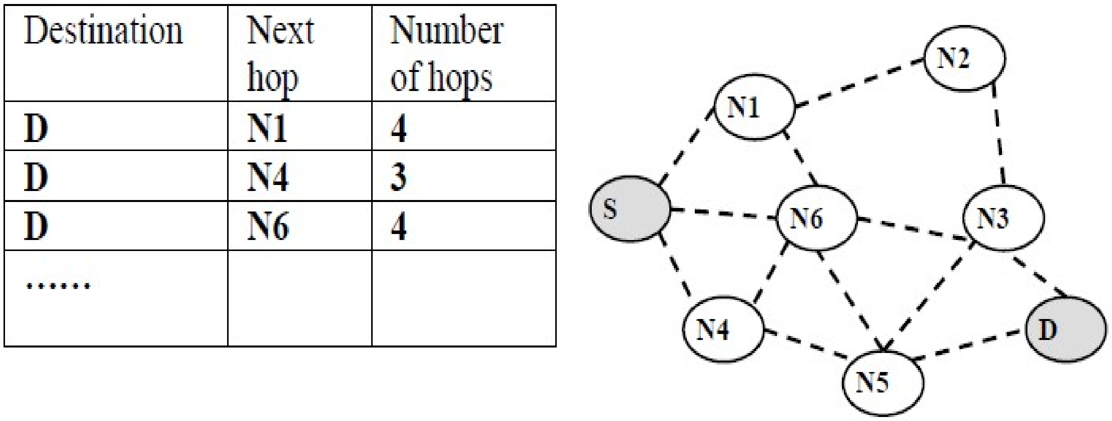
Proactive routing protocols are table-driven protocols that maintain up-to-date routing table using the routing information learnt from the neighbor on a continuous basis. Routing in such node and each intermediate node selects a net hop, by routing table look up, and forwarding the packet to next hop until destination receives the packet. A drawback of proactive protocols is proactive overhead due to route maintenance and frequent route updates to cope with nod mobility.

Classic form of proactive routing protocol include:

i. Destination-Sequenced Distance-Vector Routing protocol (DSDV)[7] and
ii. Optimized Link State Routing Protocol (OLSR) [8]

(i) **Destination-Sequenced Distanced –vector Routing protocol (DSDV)** [7]: The Destination-sequenced Distance-vector Routing protocol (DSDV) is an enhanced version of distributed Bellman-Ford algorithm, for mobile ad-hoc networks, in this protocol, each node maintains a routing table that contains an entry for every node in the network. Each entry in the routing table consists of the destination ID, the next hop ID, a hop count, and a sequence number for that destination. The sequence number helps nodes maintain a fresh route to the destination(s) and avoid routing loops. In order to cope with frequently changing network topology, nodes periodically broadcast routing table updates though-out the network. When a node receives a route-update packet, it changes its routing table entries if the sequence number of the destination in the update packet is higher (fresh) than the one in its routing table. If the sequences numbers are the same, then the node selects a route with smaller metric (hop count). As a means of reducing the network traffic due to huge update packets, DSDV employs two types of update – full dump and incremental. A full dump packet generated by a node contains all entries in its routing table. Whereas an incremental packet contains only the routing table entries that are change by the node since the last full dump. A node triggers an update when either the metric for a destination changes or when the sequence number changes. In the later case, it is called DSDV-SQ.

(ii) **Optimized Link State Routing Protocol (OLSR)** [8] is an optimization of the optimized link state routing protocol (OLSR) is an optimization of node, which where are the direct neighbors. This idea (multi-point relays, MPR) reduce the network traffic but introduces more computation and complexity.



Destination	Next hop	Number of hops
D	N1	4
D	N4	3
D	N6	4
......		

Figure 2: Proactive routing [7]

I. **Reactive Routing Protocols:** Reactive routing protocols are demand-driven protocols that find path on-the-fly as and when necessary. In such protocols establishing a new route involve a route discovery phase consisting of route request (flooding) and a route reply (by the destination node). Nodes maintain only the active routes until a desired period or until destination becomes inaccessible along every path from the source nod. A drawback of protocols is the delay due to route discovery on-the-fly. Typical forms of reactive routing are the ad-hoc On-demand Distance Vector Routing (AODV) and the Dynamic Source Routing (DSR) protocols.

In ad-hoc on-demand Distance Vector Routing (AODV). A node discovers and maintains a route to the destination as and when necessary. Nodes maintain a routing table containing routes towards source(s)-destination(s) that are actively communicating with each other. Each entry in the routing table consist of that destination ID, the next hop III, a hop count, and a sequence number for that destination (the same as one in DSDV). The sequence number helps nodes maintain a fresh route to the destination(s) and avoid routing loops. Thus, each node maintains a sequence number for itself and the respective source(s) and destination(s),

A node increments its sequence number if it initiates a new route request or if it detects a link-break with one of its neighbors. To establish a path to the destination, a source node broadcast a route request RREQ) packet. The RREQ packet contains the source ID, the destination ID, sequence number of the source, and the latest sequence number of the destination node that is known to the source node. When a node receives a RREQ packet, it makes an entry for the route request in the route-request cache and stores the address of the node from which it received the request as the next hop towards the source in its routing table.

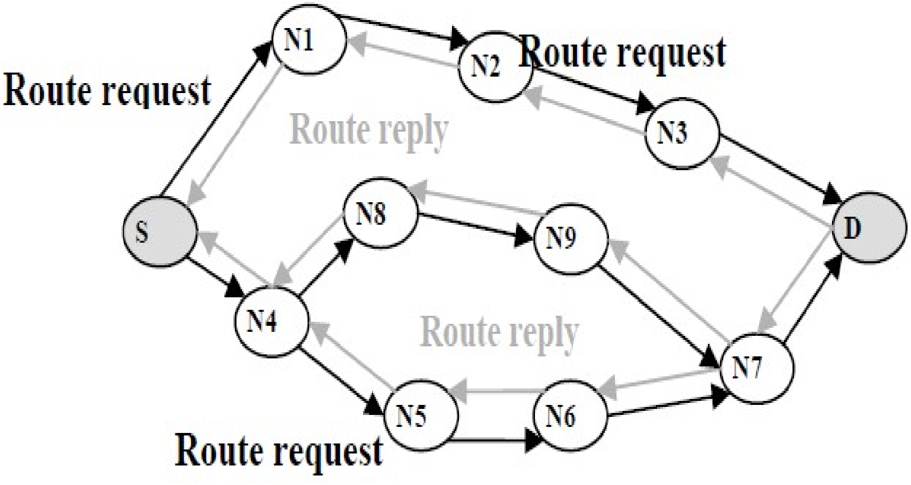


Figure 3: Reactive Routing Protocol [9]

If receiving node is the destination or it has a fresh route to that destination I, then it responds with a route reply (RREP). Otherwise, it rebroadcasts the RREQ to its neighbors. When a need receives a RREP, it stores the address of the node from which it receives RREP as the next hop towards the destination in its routing table and uncast the RREP to the next hop towards the sources nod. Once the source receives the RREP packet, it starts transmitting data packets along the traced by the RREP packet. Due to the node mobility, path(s) established by a source node may break. A node detects a path break if it attempts to forward a data packet and receives a packet-drop notification from the media access control (MAC) layer. When a node detects a path-break, it drops the packet for the destination and generates a route error (RERR) packet for the destination and sends the RERR to the source. Upon receiving a RERR, the source node buffers data packets for the destination and tries to reestablish a path to the destination.

The Dynamic Source Routing (DSR) [9] was one of the first reactive routing protocols for ad-hoc networks. In DSR, nodes use RREQ, RREP and RERR packets to establish and maintain paths to the destination. However, unlike AODV, RREQ packet accumulates a list of node IDs along the path from the source to the destination and the corresponding RRER packet carries this list of IDs back to the source. Once the source node receives RREP packet, it starts transmitting data packets to the destination by embedding the route from the source to the destination in the packet header. The path in the data packet header is referred to as the "source route". Every node in the network stores route to other nodes in the network by maintaining a dynamic route cache. A node determines routes to other nodes when it initiates a RREQ to a particular destination or when the node lies on an active path to that destination. In addition to these, a node may also ascertain a route by overhearing transmissions (in the promiscuous mode along the routes of which it is not a part.

2.2.2 Hybrid Routing Protocols

Hybrid protocols combine the advantages of various approaches of routing protocols into a particular protocol. The zone Routing Protocol (ZRP), is one such hybrid protocols that combines both the proactive and reactive routing approaches. ZRP takes advantage of proactive discovery within a node's local neighbourhood, and uses a reactive protocol for communication between these neighbourhoods. The local neighbourhoods are called zones, and each mode may be within multiple overlapping zones. ZRP is motivated by the fact that most communication occur between nodes close to each other. Changes in the topology are most important in the vicinity of a node- the addition or the removal of a node on the other side of the network has only limited impact on the local neighbourhoods".

The performance of ZRP depends on choosing a radius, which decides the transition from pro-active to reactive behavior. With a carefully chosen radius, ZRP can achieve better efficiency and scalability over both pro-active and reactive routing protocols.

2.2.3 Position-base Routing Protocol

Position-based routing protocols utilize position of nodes in the network and make the least use of the topology information. Routing protocols using a scheme eliminate drawbacks due to frequently changing network topology. DEAM, GPSR, and LAR are some of the examples of position-based routing protocols. In position-based routing protocols node maintain local (one or two hop) topology information with the help of a hello protocol. To route a packet to the destination, the source node uses a greedy-forwarding to select a next hop towards the destination. In greedy-forwarding, a node selects a next-hop towards the destination that is geographically closest to the destination among its neighboring nodes. Since there in so pre-established route from a source to the destination, each packet may follow a different path depending on the network topology [10].

There are two parts to the position-based routing:

i. Given the position of the source, the position of the destination, and a local neighbor table of each node, delivering packets from the source to the destination, and
ii. Given that each node can determine its own position, using some positioning system like GPS, obtaining the position of any other node in the system. The former part is the position-based routing, examples include GFG, GPSR.

Position-based routing is classically greedy-forwarding along with a recovery mechanism to circumvent local optima due to greedy-forwarding, a condition where there is no node close to an intermediate node in its neighbourhood than the node itself. The later part is called the location service. Some of the examples of location service protocol are GLS, DLS, and RLS. Interestingly, most location-service protocols including GLS and DLM, rely on the underlying greedy forwarding algorithm to send receive control packets like location updates and location queries. The advantage of these protocols is that nodes need not establish, maintain routes, and these protocols are more scalable compared to reactive and pro-active routing protocols.

3. SYSTEMIC VULNERABILITIES AND FORMS OF ATTACKS IN MANETS

3.2 Vulnerabilities of Mobile Ad hoc Networks

MANETs intrinsically differ from conventional wired networks with the context of their properties and a number of drawbacks which make them more prone to security issues. According to [11], the widespread vulnerabilities of mobile ad hoc networks are as follows:

i. Dynamic topology
ii. Lack of line of defense
iii. Limited resources
iv. Cooperativeness
v. Wireless links

Common vulnerabilities of mobile ad hoc networks are elucidated as follows:

i. **Dynamic topology:** In MANETs, nodes can join and leave the network dynamically and can move independently [12]. Due to such type nature there is no fixed set of topology works in MANETs. The nodes with inaquate physical protection may become malicious node and reduce the network performance.
ii. **Lack of clear line of defense:** There is no clear line defense mechanism available in the MANETs; attacks can come from any directions. Attackers can attack the either internally or externally.

iii. **Limited resources:** The MANETs consists of different set of devices such as laptops, computers, mobile phones etc. Each device has a different storage capacity, processing speed, computational power etc. This often attackers to focus on new attacks.

iv. **Cooperativeness:** In MANETs, all routing protocols assume that nodes provide secure communication. But some nodes may become malicious node and disrupt the network operation by changing routing information [13].

v. **Wireless link:** Nodes in mobile ad hoc networks are inter-connected through wireless interface that make them highly susceptible to link attacks.

Protecting mobile ad-hoc networks from attacks is a very challenging task. Nevertheless, understanding possible forms of attacks is in essence, the first step towards developing high-quality security solutions. There are various attacks that target the weakness of MANETs. Some attacks apply to the broad-spectrum network, a few apply to wireless network and some are specific to MANETs. These attacks can be classified according to different criteria, such as the domain of the attacks, or the techniques used in attacks [14].

Hence, the attacks in MANETs are generally categorized into five categories as follows:

i. Passive vs. active attacks
ii. Internal vs. external attacks
iii. Attacks on different layers of the Internet model.
iv. Stealthy vs. non-Stealthy attacks
v. Cryptography vs. non-cryptography related attacks.

3.1 Categories of Attackers found in MANETs.

Passive vs. Active Attacks

Attacks in mobile ad hoc networks can be classified into two categories, namely passive attacks and active attacks [15]. A passive attack obtains data exchange in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification or fabrication, thereby disrupting the normal functionality of a MANET. Table 2.1 shows the general taxonomy of security attacks against MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DOS), and massage replay.

Table 1: Security Attacks Classification

Type of Attack	Examples
Passive attacks	Eavesdropping, traffic analysis, monitoring
Active attacks	Jamming, spoofing, modification, replaying denial of service (DOS)

Internal vs. External Attacks

Attacks can also be classified into external attacks and internal attacks, according to the domain of the attacks. Some researchers refer to these attacks as insider and outsider attacks.

External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access right.

Attacks on Different Layers

Attacks can equally be classified according to the five layers of the Internet model. Table 2.2 presents a classification of various security attacks on each layer of the internet model.

Table 2: Security Attacks on Each Layer of the Internet Model

Layer	Attacks
Application layer	Repudiation, and corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, black hole, Byzantine, flooding, resource Consumption, Local disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption Mac (802.11). WEP weakness
Physical layer	Jamming, interceptions eavesdropping
Multi-layer attacks	DOS, impersonation replay, man-in-the-middle

Stealthy vs. Non-stealthy Attacks

Some security attacks use stealth [39], where by the attackers try to hide their actions from either an individual who is monitoring the system or an intrusion detection system (IDS). But other attacs such as Dos cannot be made stealthy.

Cryptography vs. Non-Cryptography Related Attacks

Some attacks are non-cryptography related, and others are cryptographic primitive attacks. Table 2.3 shows cryptographic primitive attacks and the examples.

Table 3: Cryptographic Primitive Attacks

Cryptographic Primitive Attacks	**Examples**
Pseudorandom number attack	Timestamp, Initialisation Vector (IV)
Digital signature attack	RSE signature

3.2 Denial of Service and Distributed Denial of Service attacks

Among the different attacks that occur on mobile ad hoc networks, distributed denial of service attacks are fast becoming the most prevalent types of attacks. A Denial of Service (DOS) attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, wed service or computer system [16].

In the same vein, a distributed denial of service (DDOS) attack is an attack whereby multiple systems join together to target a single system causing a denial of service (DOS). The target node is flooded with the data packets that system shutdowns, thereby denying service to legitimate users.

The services under attack are those of the “primary victim”, while the compromised systems used to launch the attacks are often called the “secondary victims” Consequently, the use of secondary victims in a DDOS attack provides the attacker with the ability to wage a much larger and more disruptive attack while remaining anonymous, thereby making it more difficult for network forensics to track down the real attacker.

Individuals or groups responsible for DDOS attacks may be motivated by personal, social or financial benefit. Attackers may do so due to personal revenge, getting publicity or some political motivation. Nevertheless, the financial impact of DDOS attacks on victims can be disastrous. In recent past, criminal groups have launched a number of attacks on stock exchange websites on the entire world. A few DDOS attacks reported in years 2011 and 2012 were on NASDAQ & BATS stock exchanges along with Chicago Board Options Exchange CBOE). New York stock exchange and Hong Kong stock exchange [17].

During the first Q4-2011, one survey found 45% more DDOS attacks compared to the parallel period of 2010, and over double the number of attacks observed during Q3-2011. The average attack bandwidth observed during this period was 5.2G bps, which is 148% higher than the previous quarter. Another survey of DDOS attacks found that more than 40% of respondents experienced attacks that exceeded IGbps in bandwidth in 2013, and 13% were targeted by at least one attack that exceeded 10G bps. From a motivational perspective, recent research found that ideologically motivated DDOS attacks are on the rise. The research also mentioned financial reasons as another common reason for such attacks [18]

3.3 DDOS Attack Taxonomy

There is a broad range of distributed denial of service attacks; however, this research adopts the taxonomy of the main DDOS attack methods propose [18]. Figure 2.4 represent the DDOS attack taxonomy.

There are two main classes of DDOS attacks namely:

i. Bandwidth depletion and
ii. Resource depletion attacks.

I. Bandwidth Depletion

A bandwidth depletion attack is designed to flood the victim network with unwanted traffic from reaching the primary victim.

II Resource Depletion

A resource depletion attack is an attack that is designed to tie up the resources of a victim system making the victim unable to process legitimate requests for service.

4. COMMON FORMS OF DDOS ATTACK

This section presents some common forms of DDOS attacks.

4.1 User Datagram Protocol (UNP) Flood

During a user Datagram protocol (UDP) Flood attack, the victim's network is overwhelmed by a large volume of UDP packets. The attack packets are usually with random port numbers. When the victim receives a packet, if there is no application listening at the corresponding Port., then the victim may generate ICMP packets, leading to significant overall system slowdown.

4.1 SYN Flood

In a SYN flood attack, the adversary takes advantage of the three-way handshake for a TCP connection. Within the normal execution, while a TCP server receives a SYN packet, it opens a session for this new connection and sends back a SYN/ACK packet to the initiator. When it reaches a timeout and there is no ACK packet received from the corresponding initiator, the session will be closed and the corresponding resources for the session are release. During the attack, the adversary continues sending SYN packets without sending back the final ACK packets for the TCP handshakes, the server's resource (e.g. memory) can be speedily depleted by maintaining many half open sessions, thus legitimate connection requests cannot be served. In a SYN flood scenario, the requester sends multiple SYN requests.

But either does not respond to the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgement for each of the requests, binding resources to wait for acknowledgement for each of the requests, binding resources until no new connections can be made, and ultimately resulting in denial of service.

4.3 Ping of Death

A ping of death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassemble the IP fragments into the complete packet. In a ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535 bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets [19].

4.4 Zero-day DDOS for Attacks

"zero-day" DDOS attacks simply refer to unknown or new attacks. Exploiting vulnerabilities for which no patch has yet been released. The term is well-known amongst the members of the backer community, where the practice if trading Zero-day vulnerabilities has become a popular activity [19].

5. SECURITY IN MOBILE AD HOC NETWORKS

Security in mobile ad hoc networks is particularly challenging, because such networks often operate in adverse or even hostile environments. Hence, designing an effective intrusion detection system requires an in-depth understanding of various threat models and adversaries' attack capabilities. Prior to developing a solution to secure a mobile ad hoc network, it is vital to specify the criteria for determining if a mobile ad hoc network, is secure or not. In other words, identify the conditions required in order to attain security in security in a mobile ad hoc network. It is equally pertinent to note that successful implementation of mobile ad hoc network depends on user' confidence in its security. Normally, there are five common attributes required for securing mobile ad hoc networks namely: confidentiality, authenticity, integrity and non-repudiation. These features serve as criteria for assessing if the MANET is secure [40].

5.1 Confidentiality

The term confidentiality refers to the protection of any information from being exposed to unintended entities [20]. In order to attain confidentiality, it is essential that the system stays up and in working states, and provides the right access and functionality to each user. Consequently, confidentially is the target of DOS or DDOS attacks.

5.2 Availability

Availability can be described as the ability of the network to provide service as required.
This security goal makes certain that services that should be available are accessible whenever required. In other words, there should be an assurance of survivability despite the attempt of a denial of service (DOS) attack.

5.3 Authentication

Authentication implies the assurance that an entity of concern or the origin of a communication is what it claims to be or emanates from the claimed source. Through the process of authentication. An entity is issued a credential, which specifies that prevents any form of falsification. Without this security mechanism, an attacker would impersonate a node, gaining unauthorized access to resources, sensitive information and eventually interfere with operation of other nodes.

5.4 Integrity

The security mechanism which guarantees the massage being transmitted is never altered is referred to as, integrity.

5.5 Non-repudiation

This security goal ensures that sending and receiving parties can never deny ever sending or receiving the message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not. On the whole, whenever considering any security issue with respect to a network, it is imperative to ensure these security goals are established for effectiveness.

6. CONCLUDING REMARKS AND FUTURE WORKS

In this paper, we have chronicled several MANET protocols, forms of attacks and security challenges in Mobile Ad-Hoc Networks (MANETs). The adoption and use of ubiquitous computer and network technology to address a myriad of communication challenges and facilitate online interaction has led to the continued focus on developing effective and efficient means to provide end-to-end communication between nodes within Mobile Ad-Hoc networks (MANET) and also developing security schemes that ensures that communication and interaction are seamless and safe on these networks. Our future works will contribute to these discourses by looking at agent, multi-agent technologies and intrusion detection architecture in MANET

REFERENCES

[1] J. P. Macker, V.D. Park, M.S. Corson, "Mobile and Wireless Internet Services: Putting the Pieces Together", to appear on Communication Magazine, June 2001

[2] S. Giordano. ' Mobile Ad-Hoc Networks' ISBN 0-471-XXXXX-X Copyright © 2000 Wiley[Imprint], Inc.

[3] B. Wu et al, ―A Survey of Attacks and Preventionsin Mobile Ad Hoc Networks,‖ Wireless/MobileNetwork Security, Springer, Vol 17, 2006.

[4] S. Murthy and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. J., Special Issue on Routing in Mobile

[5] S. Corson, et al. "An Internet MANET Encapsulation Protocol (IMEP)Specification", IETF internet draft, Aug. 1999.

[6] C.Siva Ram Nurthy and B.S. Manoj. "Ad hoc wireless networks Architectures and Protocols". le Prentice Hall, 2004.

[7] T. Clausen, P. Jacquet, and L. Viennot, "Comparative Study of Routing Protocols for Mobile Ad hoc Networks". Med-Hoc-Net'02, Sardegna, Italy, September 2002.

[8] Xiaoyan Hong; Kaixin Xu; Gerla, M. "Scalable routing protocols for mobile ad hoc networks". IEEE Network , Volume: 16 Issue: 4 , July-Aug. 2002, pp: 11 -21

[9] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks". IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79. Communication Networks, Oct. 1996, pp. 183-97.

[10] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks", IEEE Communication Societies (INFOCOM 2003), IEEE Press, pp. 1976-1986, 2003

[11] Amitabh Mishra, "Security and Quality of Service in Ad hoc Wireless Networks" ISBN- 13 978-0-521-87824-1 Handbook.

[12] T. White and B. Pagurek, "Towards multi-swarm problem solving in networks", Proc. Third International Conference on Multi-Agent Systems (ICMAS '98), pp. 333- 340.(1998)

[13] S. Toner, and D. O'Mahony, "Self-Organising Node Address Management in Ad hoc Networks". Personal Wireless Communications, IFIP-TC6 8th Int'l. Conf. (2003), pp. 476-483.

[14] Gagandeep, Aashima and P. Kumar. “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review”. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, (2012).

[15] P. Papadimitratos and J. Haas. Securing mobile ad hoc networks In
Handbook of Ad Hoc Wireless Networks. CRC Press, pp 31. (2002).

[16] S. M. Specht and R.B, Lee, “Distributed Denial of Service: Taxonomies of Networks, Attacks, Tools, and Countermeasures,” Princeton University Department of Electrical Engineering Technical Report CE-L2003-03, (2003)

[17] J.K. Houle. “Trends in Denial of Service Attack Technology”. CERT Coordination Center, Carnegie Mellon Software Engineering Institute. (2001.)

[18] David Karig and Ruby Lee, “Remote Denial of Service Attacks and Countermeasures,” Princeton University Department of Electrical Engineering Technical Report CEL. (2001).

[19] P. Gupta and M. Kirkire. Intrusion Detection in Manet. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. Vol. 2, Issue 4, April (2013).

[20] W. Lou and Y. Fang, A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions. Ad Hoc Wireless Networks, edited by Academic Publishers, pp. 319-364. (2003).