# A Novel Intrusion Detection Mechanism for Denial-of-Service Attacks in Mobile Ad Hoc Networks (MANETs) for Secure Healthcare IoT and Emergency Telemedicine Systems

**Dr. Lucas Meyer[1]***
**Prof. Daniel Okafor[2]**
[1] University of Zurich, Institute of Biomedical Cybersecurity and Medical Network Systems, Zurich, Switzerland
[2] University of Lagos, Department of Health Informatics and Network Security, Lagos, Nigeria

## ABSTRACT

A mobile adhoc network (MANET) is a type of network, which contains number of mobile devices with wireless network interconnections. In MANET, each node can act as transmitter, router and data sink. MANET has dynamic topology which allows nodes to join and leave the adhoc network at any point of time. MANETs are more vulnerable than wired networks due to its characteristics like dynamic topology, distributed cooperation and open medium. Security issues in mobile adhoc networks are veiled by various techniques that were introduced in past decade. Due to decentralized nature of MANET, the security issues cultivate resulting in welcoming various lethal vulnerabilities. Out of various Denial of Service (DoS) attacks in MANET, Flooding attackis considered most challenging adversarial modules that tremendously affect the communication system in MANET. In this paper, various previously used techniques are discussed for mitigating Flooding attacks in MANET. The uniqueness of this article is that it presents a comparative study of existing techniques for detecting Flooding attacks in MANET. Finally, we proposed a new technique based on threshold value for detecting Flooding attacker nodes in MANET.

***Keywords:*** *MANET, Security issues, vulnerabilities, Flooding attack, Intrusion Detection Systems*.

## I. INTRODUCTION

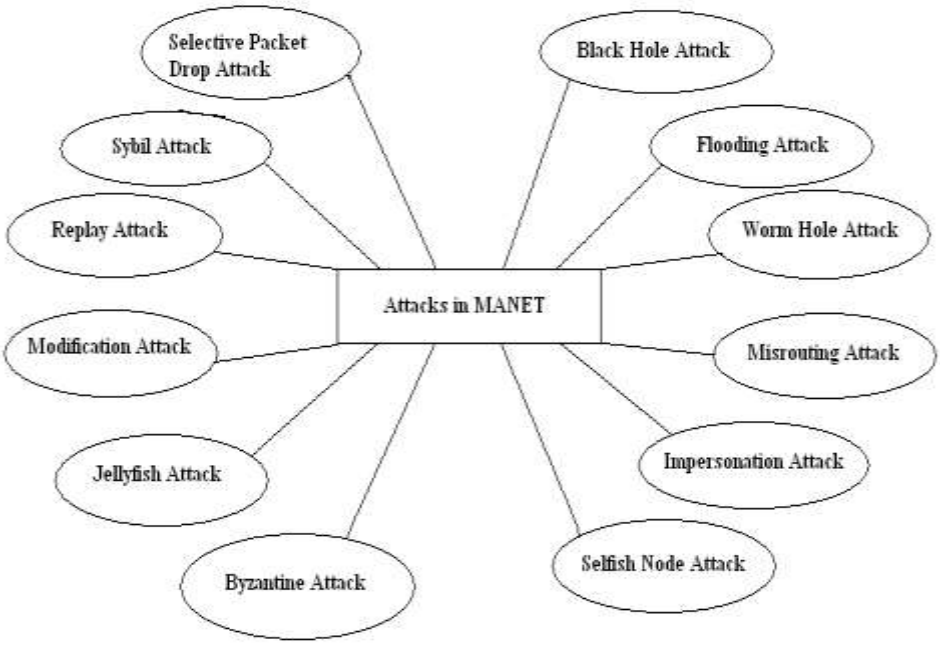
A MANET is a wireless network, which consists of various mobile nodes without any fixed infrastructure. In this network, every node acts as a transmitter, data sink, and router. A MANET works in a dynamic environment in which nodes can leave or join the network at any time. Due to dynamic topology and open medium, these networks are more prone to numerous attacks. On these networks, nodes are self-organized in arbitrary fashion. In MANETs, two nodes can directly transfer the data with each other if they are within range. If two nodes are not in the range, then multi-hop routing is used for communication. Due to the dynamic environment in Adhoc networks, wireless link between nodes are highly vulnerable. In these types of networks, bandwidth constrained wireless links are used for communication.

Due to the dynamic topology of MANETs, mobile nodes can move into and out of the range at any time. This movement results in changing routing information of the network. In MANETS, all of the network activities are executed with the nodes themselves. These activities also include the routing activities. Due to Lack of centralized node, dynamic topology, and bandwidth constraint, these networks are highly vulnerable than fixed networks. MANET has following vulnerabilities [1, 2]:

- Dynamic topology
- Limited power supply
- Scalability
- Lack of centralized node
- Adversary inside the Network
- Bandwidth constraint
- No predefined Boundary
- Limited Resources

*Figure 1: Mobile Ad hoc network*

MANET often suffer from security attacks because of its features like open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats [3,4]. Various attacks on different layers of MANET are shown in the following figure 2.




Because of vulnerabilities, these networks suffer from a number of security attacks. Out of these numerous attacks, Flooding Attack is very dangerous attack which is responsible for reducing the performance of network to a large extent.

**1.1 Flooding Attack**

The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such I.P addresses that do not exist in the network [5,6]. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an immense amount of useless data packets into the network which is directed to all the other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time. The aim of the flooding attack is to exhaust the network resources: bandwidth and to consume a node's resources, such as battery power and computational or to disrupt the routing operation to cause severe degradation in network [7,8].

## II. BRIEF LITERATURE SURVEY

A variety of literature is available related to intrusion detection in MANET for flooding attacks. A few of the related work along with their advantages and drawbacks are discussed below.

***Table 1. Comparative study of various DoS Attack detection techniques in MANET.***

| Sr. No. | Author | Techniques | Advantages | Disadvantages |
|---|---|---|---|---|
| 1. | Shishir, Shandilya and Sunita Sahu | A Trust Based Security Scheme for RREQ Flooding Attack in MANET [9]. | ➢ Detect and respond (i.e., filter) tothe attack traffic at the source and before itwaste lots of resources. | ➢ Sources are distributed among differentdomains; hence, it is difficult for each ofthe sources to detect and filter attack flowsaccurately.<br>➢ Difficult to differentiate legitimate andDoS attack traffic at the sources, sincethe volume of the traffic is not big enough.<br>➢ Low motivation for deployment; since,it is unclear who would pay the expensesassociated with these services. |
| 3. | Jin Tang, Yu Cheng and Yong Hao | Detection and Prevention of SIP Flooding Attacks in Voice over IP Networks [10]. | ➢ Easier and cheaper than other mechanisms in detecting DoS attacks because of their access to the aggregate traffic near the destination hosts. | ➢ They cannot accurately detect and respond to the attack before it reaches the victims and wastes resources on the paths to the victim.<br>➢ Difficult to differentiate legitimate and DoS attack traffic at the sources, since the volume of the traffic is not big enough.<br>➢ |
| 3. | D. Srinivasa Rao and Dr. P.V. Nageswara Rao | An Efficient RREQ Flooding Attack Avoidance Technique for Adaptive Wireless Network [11]. | ➢ More robust against DoS attacks.<br>➢ Easier method for preventing DoS Attacks. | ➢ Attack detection is difficult because of the lack of availability of sufficient aggregated traffic destined for the victims.<br>➢ Lack of incentives for the service providers to cooperate/collaborate. |
| 4. | Jaehak Yu, Hyo-Chan Bang, H. Kang, D. Park | An in-depth analysis on traffic flooding attacks detection and system using data mining techniques [12]. | ➢ Less storage and processing overhead at the routers.<br>➢ More robust against DoS attacks. | ➢ Complexity and overhead because of the cooperation and communication among distributed components scattered all over the Internet.<br>➢ Sources are distributed among different domains; hence, it is difficult for each of the sources to detect and filter attack flows accurately. |

| | | | | |
|---|---|---|---|---|
| 5. | Ms. Neetu Singh Chouhan and Ms. Shweta Yadav | Distributive approachin their paper entitled "Flooding Attacks Prevention in MANET [13]. | ➢ Response time and detection rate are also improved by using this approach.<br>➢ Distributive approach is used to reduce the impact of flooding attack on the performance of MANET. | ➢ Sources are distributed among different domains; hence, it is difficult for each of the sources to detect and filter attack flows accurately.<br>➢ Low motivation for deployment; since, it is unclear who would pay the expenses associated with these services. |
| 6. | Jin Tang, Yu Cheng, Yong Hao, and Wei Song | SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design [14]. | ➢ More robust against DoS attacks.<br>➢ More resources at various levels (e.g., destination, source, and network) are available to tackle DoS attacks. | ➢ Complexity and overhead because of the cooperation and communication among distributed components scattered all over the Internet.<br>➢ Lack of incentives for the service providers to cooperate/collaborate.<br>➢ Need trusted communication among various distributed components in order to cooperate/collaborate. |
| 7. | Saman Taghavi Zargar, James Joshi and David Tipper | Defense Mechanism Against Distributed Denial of Service (DDoS) Flooding Attacks [15]. | ➢ Aims to detect and respond to (i.e., filter) the attack traffic at the intermediate networks and as close to source as possible. | ➢ High storage and processing overhead at the routers.<br>➢ Attack detection is difficult because of the lack of availability of sufficient aggregated traffic destined for the victims. |
| 8. | Jian-Hua Song, , Fan Hong and Yu Zhang | Effective filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks [16]. | ➢ In this technique each node in the network monitors the RREQ and maintain a count table for RREQ received.<br>➢ The node which has high attack rate can be delayed. | ➢ Increased Complexity and Overhead for maintaining Count table.<br>➢ Lack of incentives for the service providers to cooperate/collaborate. |

## III. RESEARCH GAPS

➢ Most of the research work in the past for detecting DoSattacks is carried out indistributed environment but little work is done on threshold based mechanisms. So, work need to be done for fulfilling this research gap.

- There is a lot of research gap for developing an efficient method for tackling with flooding attack under AODV protocol based on statistical methods.
- Most of the work has been carried out for tackling with flooding attack is based on hashing mechanism and cumulative acknowledgement encryption mechanismbut design of an efficient mechanism still remains a challenge.

The exact design consideration for efficient technique for monitoring, detecting and responding to flooding attack in MANET has not been accounted so for according to authors' knowledge.

## IV. THRESHOLD BASED TECHNIQUE

There are number of drawbacks of existing techniques for detecting DoS (flooding) attack in mobile adhoc network which are listed above, so to design an efficient technique for detecting flooding attack in MANET is still remain a challenge. We have proposed a threshold based technique for detecting and preventing flooding attack in MANET. In the MANET if route request sequence no. is detected more than predefined threshold value, then that node is detected as malicious node otherwise source node is true sender. After locating the malicious node, data is updated in the list of black list nodes and alarm is sent to all of the neighbor nodes. In this way we can protect mobile adhoc networks from malicious node creating flooding attack. This threshold based algorithm can be represented with the help of following flowchart:

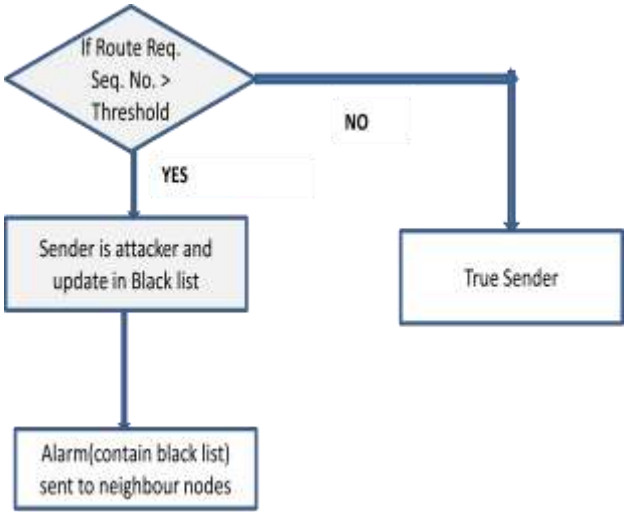



***Figure 3: Threshold based mechanism for detecting DoS Attack***

## V. CONCLUSION AND FUTURE WORK

In this paper, we have presented a comprehensive classification of various DoS attack detection techniques for MANET along with their advantages and disadvantages based on where and when they detect and respond to DoS attacks. An ideal comprehensive DoS defense mechanism must have specific features to combat DoS flooding attacks both in real-time and as close as possible to the attack sources. So, we have also proposed a new mechanism based on threshold values for detecting DoS attacks in MANET. This algorithm removes the several drawbacks of existing techniques. We strongly believe that threshold based mechanism could be the most effective and efficient way for addressing Do Sattacks in MANET. More development and deployment of distributed defense mechanisms from researchers and service providers respectively is what we expect to see in the near future

## REFERENCES

1. *Jatinder Singh, Lakhwinder Kaur, and Savita Gupta, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks", "International Arab Journal of Information Technology", Vol. 9, No. 3, May 2012and ISSN: 1683-3198.*

2. *Ming-Yang Su., "A study of deploying intrusion detection systems in mobile ad hoc networks", "Journal of Computers and Electrical Engineering", Vol. 40, Issue 2, February 2014 and ISSN: 0045-7906.*
3. *Sachin Lalar, "Security in MANET: Vulnerabilities, Attacks & Solutions", "International Journal of Multidisciplinary and Current Research", Vol. 2, Jan-Feb, 2014, ISSN: 2321-3124.*
4. *Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), , Vol. 1, Issue-5, June 2012 and ISSN: 2249 – 8958.*
5. *Satria Mandala, Md. Asri Ngadi, A.Hanan Abdullah, "A Survey on MANET Intrusion Detection", "International Journal of Computer Science and Security", Vol. 2, Issue 1, 2013 and ISSN:1985-1553.*
6. *Sandip Nemade, Manish Kumar Gurjar, Zareena Jamaluddin, Nishanth ,"Early Detection of Syn Flooding Attack by Adaptive Thresholding (EDSAT): A Novel method for detecting Syn Flooding based DOS Attack in Mobile Ad Hoc Network", "International Journal of Advanced Research in Engineering and Technology (IJARET)", Vol. 5, Issue 2, February 2014, ISSN 0976 – 6480(Print), ISSN 0976 – 6499(Online).*
7. *Munish Sharma and Anuradha, "Network Intrusion Detection System for Denial of Service Attack based on Misuse Detection", "IJCEM International Journal of Computational Engineering & Management", Vol. 12, April 2011, ISSN (Online): 2230-7893.*
8. *Jerome François, Issam Aiband Raouf Boutaba, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks", "IEEE/ACM Transactions on Networking", Vol. 20, No. 6, December 2012.*
9. *Shishir K. Shandilya and Sunita Sahu, "A Trust Based Security Scheme for RREQ Flooding Attack in MANET", International Journal of Computer Applications (0975 – 8887) Vol. 5– No.12, August 2010.*
10. *Jin Tang, Yu Cheng and Yong Hao,"Detection and Prevention of SIP Flooding Attacks in Voice over IP Networks", "IEEE INFOCOM,2012" , ISSN-978-1-4673-0775.*
11. *D. Srinivasa Rao, Dr. P.V. Nageswara Rao, "An Efficient RREQ Flooding Attack Avoidance Technique for Adaptive Wireless Network", "International Journal of Applied Engineering Research", Vol. 11, 2016, ISSN 0973-4562.*
12. *Jaehak Yu, Hyo-Chan Bang, H. Kang, D. Park, "An in-depth analysis on traffic flooding attacks detection and system using data mining techniques", "Journal of Systems Architecture: the EUROMICRO Journal", Vol. 59, Issue 10, November, 2013.*
13. *Ms. Neetu Singh Chouhan and Ms. Shweta Yadav, "Flooding Attacks Prevention in MANET", "International Journal of Computer Technology and Electronics Engineering (IJCTEE)", Vol. 1, Issue 3, ISSN 2249-6343.*
14. *Jin Tang, Yu Cheng, Yong Hao, and Wei Song, "SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design", "IEEE Transactions on Dependable and Secure Computing", Vol. 11, No. 6, November/December 2014.*
15. *Saman Taghavi Zargar, James Joshi and David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", "IEEE Communications Surveys & Tutorials", VOL. 15, NO. 4, 2013.*
16. *Jian-Hua Song, Fan Hong, and Yu Zhang, "Effective filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", IEEE Computer Society, 2006.*