# A Unified Approach for Forensic Analysis of DDOS Attack in Manet

**S. Ahmed, S. M. Nirkhi**

***Abstract*****:** ***Mobile Ad Hoc Network (MANET) facilitates distributed wireless communication without pre-existing centralised infrastructure. The network is mobile and setting of connection is ad-hoc.The design of MANET helps improving network scalability, as well as reducing the time to deploy a new network infrastructure. However, the benefits of MANET come with the cost in reduced security. A typical DDoS attack is the flooding attack in which attackers paralyse the target networks by flooding excessive volume of traffic to deplete key resources of the target. When an attack on the target system is successful enough to crash or disrupt, this event as the breach that triggers investigation. Forensic investigation provide source of network evidence and helpful in design and recovery mechanism for network attacks. This paper review various work done in the field of DDoS attack forensic for MANET.***

***Index Terms: DDoS attack, Fuzzy logic, MANET, Network forensics.***

## I. INTRODUCTION

Network forensics is still under active investigation by the research community, especially to address the issues in wireless networks like WLAN, MANET and WSN. MANET is a distributed system that comprises wireless mobile nodes that can freely and dynamically self-organize into arbitrary, temporary, and *ad hoc* network topologies, allowing seamless interconnections without pre-existing communication infrastructure and central administration. Due to its unique characteristics and features, MANET is more vulnerable to various security threats. Mission-critical applications demands technologies and methods for security incident investigation. Network forensics uncovers the facts of unauthorised or malicious activities. In general practise, the following functions or tasks are carried out in network forensics investigation: network evidence capture, preservation, examination, analysis, visualization and presentation of the results. The analysis process is the core of the whole network forensic investigation. It aims is to gain insight into and reach conclusions about critical questions of network security incident, such as what happened, when, how, who was involved, and for which duration the network was compromised. The study of network forensics for DDoS attacks in MANET is considered still as immature.

Flooding attack causes excessive volume of traffic to deplete key resources of the target legitimate users, as well as, since the system get congested so forth, there is denial of services. Flooding attack is a kind of denial of service attack in which the malicious node tries to inundate the victim by repeatedly sending redundant packets/data. When malicious or attacker nodes collectively do the flooding attack, it is, distributed denial of service attack (DDoS). DoS is active attack, which cannot be made stealth, but it is easy to implement also if keenly implemented then it is difficult to recognize in MANET.

## II. RELATED WORKS

According to [5], in the literature, they proposed the MANET IDS agent conceptual architecture and classified security attacks in MANET at different layers.

Denial of service (DoS) attacks could be launched from several layers. An attacker can employ signal jamming, eavesdropping and intercepting at the physical layer, which disrupts normal communications by tuning to the proper frequency [8] [9]. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. At the link layer, the MANET is an open multipoint peer-to-peer network architecture (one-hop connectivity). Attacks may target the link layer by disrupting the cooperation of the layer’s protocols. Malicious nodes can occupy channels through the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, network layer protocols extend connectivity from neighboring 1-hops nodes to all other nodes in MANET. The connectivity between mobile hosts over a potentially multi-hop wireless link strongly relies on cooperative reactions among all network nodes. By attacks at this layer the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks. According to [1], there are many approaches, working at various layers in the protocol stack, to launch DDoS attacks against MANETs. At the physical layer, the jamming attack can be used to disrupt and suppress normal transmission [10]. At the media access control (MAC) layer, attackers can exploit defects of MAC protocol messages and procedures to cause the DoS attack [11]. Aad et al. [12] identified the JellyFish attacks that drop, reorder or delay TCP packets to disrupt TCP connections at the transport layer. In order to perform above attacks, attackers are required to possess special capabilities. The flooding attack considered at the network layer, it has serious impact on the victim network as well as it is easy to launch.

In DSR routing, attackers behave like normal nodes in all aspects except in routing. They would not comply with broadcast management techniques adopted in current routing protocols such as limiting the maximum number of RREQ packets sent per second,

**Revised Manuscript Received on 30 October 2012**
*****Correspondence Author(s)

**Sarah Ahmed***, Dept. of Computer Science & Engineering (W.C.C), G. H. Raisoni College. of Engineering, Nagpur, Maharashtra, India.
**Prof. S.M. Nirkhi**, Dept. of Computer Science & Engineering, G. H. Raisoni College. of Engineering, Nagpur, Maharashtra, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

and RREQ back-off. Instead, they initiate massive bogus RREQ packets (e.g. their source and/or destination address are randomly generated) that will be re-broadcast by every other nodes in the network. In the end, the aggregated RREQs will form large enough attack traffic to overwhelm the network.

According to [2], For address-spoofing flooding (ASF) attacks [13], each RREQ packet sent out by each attack node is allocated a random pair of source address and destination address (SA,DA). ASF attack may have certain limitations depending on the protocols; take standard IEEE 802.11 devices adopting TCP/IP for example, even SA can be reconfigured for initiating an ASF attack, MANET can apply address resolution protocol (ARP) to identify the attacking node based on its MAC address, hence to block the attacking node. In addition to data link layer information, it is also possible to analyse signal strength, signal direction (using directional antenna), channel condition, to help identify the attacking node. Because of these properties, it is more difficult for attacking node pretending to be anonymous, and hence it is less preferred way of initiating attack.

But if for a duration of time, the frequency of spoofed address and the rate of bogus RREQ is very much above to some threshold value, then estimating this as ASF attack is easy otherwise if the value is not much above the threshold value this attack is not easily recognizable. Such type of attack is able to breach the network and unnecessarily engage the traffic and denial of services for some duration of time.

According to [1], they modeled ASF attack detection (or determination) as the sequential change point detection problem, and apply the non-parametric CUSUM algorithm as detection feature to perform the ASF attack identification. They propose an analytical model for looking for specific patterns of the ASF attack traffic and there analytical model can help network forensic investigators with (1) determine if there is an anomaly in the traffic and whether the anomaly is the ASF attack (2) Determine time when the ASF attack is launched. They proposed that there traffic analysis model can also be helpful to security enhancement, e.g. IDSs can detect DDoS attacks more effectively by traffic pattern identification proposed in there work.

According to [3], they propose an iterative algorithm for discovering attack patterns via a feedback mechanism, with the degrees of belief for attack instances propagated to the next iteration to further refine the search. They use suspicious scores, which determine the sequence of events as an instance of attack type. The suspicion scores is evaluated from probability distribution of sum of random variables is approximated by Gaussian distribution. In this paper, they proposed an iterative algorithm using graph and iteratively suspicion is evaluated to discover the attack pattern. There unsupervised algorithm, does not require a priori user-defined thresholds.

According to [4], forensic investigation is the examination of the digital evidences collected from the compromised systems to: a) reconstruct the occurred attack scenario; b) identify the location(s) from which the attacker has remotely executed the actions part of the scenario; c) understand what occurred to prevent future similar incidents; and d) argument the results with non refutable proofs. In there work, they proposed the methodologies for digital investigation in wireless ad-hoc networks.

According to [6], In general, Statistical Methods are used to determine the DoS attacks, like Adaptive Threshold Algorithm, Cumulative Sum and Statistical Moments are used for this purpose. While the main disadvantage of the first two methods is to determine required parameters for appropriate threshold value in the last method the main problem is modeling the network traffic. The goal in all of these algorithms is early and true detection of the attacks [15, 16, 17, 18, 19, 20]. In this paper they proposed a fuzzy logic based system for detecting SYN flooding attacks in wired system. According to them there proposed fuzzy system performs better for low and high intensity attacks than other systems.

According to [7], Security expert or forensic investigator analyzes the network traffic using the empirical knowledge. There is no rule to perfectly distinguish attack from network traffic. Fuzzy. logic is a powerful technique for dealing with human reasoning and decision making processes. In this paper they proposed an expert system for detecting DoS attack in wired system. They consider large amount of network traffic, there fuzzy expert system reduce the time and cost of traffic analyzing.

## III. EXISTING METHODOLOGY USED FOR ANALYSIS

Cusum[1]; Cumulative sum control chart is a sequential analsis technique. In this the various samples are summed, when the value exceeds a certain threshold value, a change is been detected then the operation accordingly is implemented. Cusum is built on the principal of maximum likelihood estimation. This technique is good for estimation as well as comparison. Cusum is effective for small shifts and small group size. Cusum give relatively slow response to large shifts, also not so efficient for complex/large special pattern analysis.

Statistical Moments and Gaussian distribution [3] are type of distribution, can be characterized by number of features like mean, variance, skewness etc. These features as a parameter define moments and gaussian distribution. Then theses parameters are samples for estimation. In these methods to model network is difficult.

Fuzzy logic [7]deals with reasoning that is approximation rather than exact value. This technique is efficient in complex analysis, accurate, it is rule based so easily modifiable. But requires fine tuning of rules.

## IV. PROPOSED METHOD

Flooding attack is a kind of DoS attack. Collaborative flooding attack by a group of attackers node is DDoS. When attack is launched at routing, a massive bogus RREQ packets is broadcasted in MANET. By doing this attacker tries to inundate the legitimate user by redundant RREQ packet. DoS is active attacks, such as illegal modification of routing messages, can be prevented by mechanisms source authentication and message integrity. DoS attacks on a routing protocol could take many forms. DoS attacks can be limited by preventing the attacker from inserting routing loops, enforcing the maximum route length that a packet should travel, or using some other active approaches to trace the location of attacker by estimating signal strength. But when keenly implemented then it is difficult to recognize in MANET.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

The flooding attack considered at the network layer, it has serious impact on the victim network and it is easy to launch.

Since, MANET is mobile wireless network that to contains ad-hoc settings, routing is needed to find the path between source and destination, each node must be able to forward data for other nodes. Dynamic routing eliminates the periodic routing updates and prevents nodes from unnecessary battery loss. In Dynamic source routing (DSR) [20], a node need to discover a route, it broadcast a route request (RREQ) with a unique identification and the destination address as parameters. Any node that receives a route request, either if the node has already received the request it drops the request packet, or if the node recognizes its own address as destination the request reached target, otherwise the node appends its own address to the list of traversed hops in the packet and broadcasts this update route request. Attackers initiate massive bogus RREQ packets (e.g. their source and/or destination address are randomly generated) that will be re-broadcast by every other nodes in the network causing DDoS due to flooding.

After attacks that had compromised the security of the entire network for a duration of time, investigation of cooperative attacks is needed to be done, in order to provide source of network evidence, where as this investigation is helpful in designing recovery mechanism for network attacks.

Forensic investigation uncovers the various facts related to attack by forensically analyzing the attack pattern. In the proposed work this forensic analysis is done using fuzzy logic. Motivation of using fuzzy logic is that, through fuzzy logic more appropriate pattern analysis rules can be implemented.

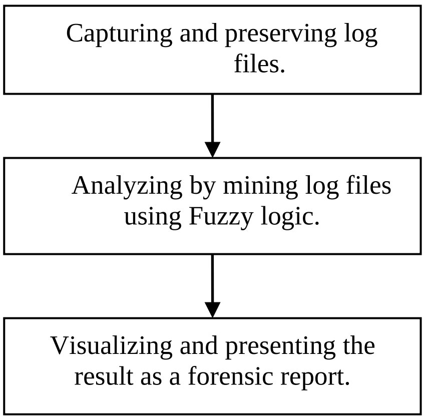
Capturing and preserving log files.
Analyzing by mining log files using Fuzzy logic.
Visualizing and presenting the result as a forensic report.

Fig 1: Flow of proposed work.

## V. CONCLUSION

According to various literature surveyed it is deduced that since MANET features add benefits in many way on contrary expose to variability to security. Network forensic is at the initial stage in MANET. There is research going on to theoretically deducing attack model and various parameter characterizations according to MANET features. DDoS attack is simple to implement and have potential to interrupt the network for certain duration, causing loss to legitimated users of network. After, attack which compromised network for duration of time, leads to the requirement of network forensic. Forensically analyzing the cause of breach and generating forensic report is helpful in two ways: (1) as an evidence (2) study helps in developing recovery system. Analysis can be done by various methods. Fuzzy logic is better choice, since it gives accurate results, even for complex analysis.

## REFERENCES

1. Yinghua Guo, Matthew Simon, “Network forensics in MANET: traffic analysis of source spoofed DoS attacks”, Nov 2010 IEEE Fourth International Conference on Network and System Security.
2. Yinghua Guo, Matthew Simon, “Forensic analysis of DoS attack traffic in MANET”, Nov 2010 IEEE Fourth International Conference on Network and System Security.
3. ing Zhu, “Attack pattern discovery in forensic investigation of network attacks”, Aug 2011 IEEE journal on selected areas in communications.
4. Slim Rekhis and Noureddine Boudriga, “A Formal Rule-based Scheme for Digital Investigation in Wireless Ad-hoc Networks” 2009 Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering.
5. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks “, Chapter 12, 2006.
6. Taner Tuncer Yetkin Tatar, “Detection SYN Flooding Attacks Using Fuzzy Logic”, 2008 International Conference on Information Security and Assurance.
7. Jung-Sun Kim, Dong-Geun Kim, Bong-Nam Noh, “A Fuzzy Logic Based Expert System as a Network Forensics”, July, 2004 IEEE.
8. 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.
9. R. Nichols and P. Lekkas, *Wireless Security-Models, Threats, and Solutions*, McGraw-Hill, Chapter 7, 2002.
10. A. Perrig, J. Stankovic, D.Wagner and C. Rosenblatt, *Security in wireless sensor networks*, ACM Communication Journal, Vol. 47, No. 6, PP. 53-57, 2004
11. Q. Gu, P. Liu and C.H. Chu, *Tactical bandwidth exhaustion in ad hoc networks*, Proceedings of the Fifth Annual IEEE Information Assurance Workshop, PP. 257-264, 2004.
12. I. Aad, J.P. Hubaux and E.W. Knightly, *Denial of service resilience in ad hoc networks*, Proceedings of the 10th annual international conference on Mobile computing and networking, PP. 202-215, 2004
13. Y. Guo, M. Simon, “Network forensics in MANET: traffic analysis of source spoofed DoS attacks,” *in Proceedings of* 2010 Fourth International Conference on Network and System Security (NSS 2010), 2010.
14. Wang, D. Zang, K.G. Shin, “Detecting SYN Flooding Attacks” Proceedings of IEEE INFOCOM02, 2002.
15. V. A. Siris, Fotini P. “Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attack”, Elseiver, Computer Communications(29), pp:1433-1442, 2006.
16. R.B.Blazek, H. Kim, B.Rozovskii, A. Tartakovsky, “ A Novel Approach to Detection of Denial of Service Attacks via Adaptive Sequential and Batch Sequential Change Point Detection Methods, Proceedings of IEEE Workshop on Systems Man and Cybernetics Information Assurance, 2001.
17. H. Wang, D. Zang, K.G. Shin, “ Change-Point Monitoring for the Detection of DoS Attacks”, IEEE Transaction on Dependable and Secure Computing, vol:1 No:4, pp:193-208, 2004.
18. Y. Oshita, S. Ata, M. Murata, “Detecting Distrubuted Denial of Service Attacks by Analyzing TCP SYN Packets Statistically”, pp:2043-2049 Globecom2004.
19. Leu F.Y., Yang W.J., “Intrusion Detection with CUSUM for TCP based DDoS”, LNCS 3823, pp:1255-1264, 2005.
20. Jochen H. Schiller, “Mobile communication”, Pearson education, chapter 8, 2008.

## AUTHOR PROFILE

**Lect. Ms. Sarah Ahmed** received the B.E. degree in computer science and mathematics from RTMNU (Nagpur University), and perusing the M.E. degree in Wireless Communication and Computing from GHRCE affiliated to RTMNU. She is a Lecturer in the Faculty of Computer Science and Information Technology at GHRIETW. Member of Computer Society of India (CSI). Her main research interests include Wireless networks, Fuzzy logic, Digital Forensics, Pattern analysis.

**Asst. Prof. Ms. S. M. Nirkhi** has completed M.Tech in Computer Science &Engineering & currently Pursuing PHD in computer science. She has received RPS grant of 8 lakhs from AICTE for her Research. She has attended 6 STTPworkshops along with other training programs. She has Published 15 papers in international conferences & 5 papers in international journals. She had presented paper at International Conference at Singapore. She has 12 years of professional experience. Currently working as Assistant professor in Department of Computer Science & Engineering at GHRCE. Her area of interest include Soft computing, Data mining, web mining, pattern recognition, MANET, Digital Forensics.