International Journal of Science and Modern Engineering (IJISME)
ISSN: 2319-6386, Volume-1, Issue-7, June 2013

# Fuzzy Forensic Analysis System for DDoS Attack in MANET Response Analysis

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

***Abstract*— Mobile Ad Hoc Networks (MANET) are wireless communication network; in which self capable mobile nodes can dynamically self organize into ad hoc topologies. Seamless interconnection with each other without pre-existing infrastructure makes MANET scalable. In turn scalability also increases the scope of security threats. Dynamic nature of MANET calls for self route management routing algorithm like DSR. Attacks at discovery phase of DSR to discover the route could be launched by attacker/malicious node by flooding (violating broadcasting rules) the route request message (RREQ) and prohibit the normal working of network for duration of time. Flooding is a kind of denial of service (DoS/DDoS) attack. When an attack on the target system is successful enough to hamper the normal working of network, this event triggers investigation. Network forensic analysis is done to analyze the attack scenario and to come up with digital proof against the attacker/attackers. To gather the proof there is the need to empirically analyze the evidential knowledge. Fuzzy logic is good choice for empirical analysis. So, we have implemented a fuzzy forensic analysis system. In this paper, we analyzed the response of fuzzy forensic analysis system that we have implemented.***

***Index Terms*— DDoS attack; Dynamic source routing; Fuzzy logic; MANET; Network forensics analysis.***

## I. INTRODUCTION

Network forensics is still under active investigation by the research community, especially to address the issues in wireless networks [2]. Mobile Ad hoc network (MANET) is susceptible to vulnerabilities like other networks. One of the major types of problems in the network security is Denial of service (DoS) attacks because they are one of the most frequently used attack methods [6]. DoS are active attacks [5]. MANET is particularly susceptible to DDoS attack [1]. MANETs permits reactive routing like dynamic source routing (DSR) in which route is discovered on demand/on require and for this node sends route request message (RREQ) at discover phase. Attacker can do flooding of RREQ packets/message (violating broadcasting rules) that can cause denial of services. Once, the attacker is successful to overload the network and crash the network then there is quest related to this breach. Network forensic provide answer to various questions related to this breach and provide digital proofs. Network forensic is the act of capturing, recording, and analysing network audit trails in order to discover the source of security breaches or other information assurance problems [7]. Mission-critical applications demand technologies and methods for security incident investigation [2]. Forensic analysis can be done by unsupervised methods but require long iterations.

**Manuscript received on June, 2013.**

**S. Ahmed**, Research Scholar, Dept. of Computer Science & Engineering, G.H. Raisoni College of Engineering Nagpur, Maharashtra, India.

**S. M. Nirkhi**, Dept. of Computer Science & Engineering, G.H. Raisoni College of Engineering Nagpur, Maharashtra, India.

Statistical methods like Cumulative sum (CUSUM), adaptive threshold, statistical moments etc. CUSUM or adaptive threshold methods main disadvantage is that require parameters for appropriate threshold value and statistical modelling method main problem is modelling the network traffic [6]. Modelling and estimating accurate threshold parameter for network traffic is a difficult problem. Security expert or forensic investigator analyses the network traffic using the empirical knowledge. Fuzzy logic is good choice for empirical analysis. This technique can be well implemented for analysis. Fuzzy based analysis system perform better for low and high intensity attack [6] and reduce the time and cost of analysis [7]. Fuzzy logic deals with reasoning empirically and rules based approach is easily modifiable.

So, implementing fuzzy logic based rules for forensic analysis is an appropriate choice. As a major source of evidences, the data maintained by network devices include log files, configuration settings, routing tables and etc [1]. Forensic analysis can be done on any source of evidences that can be considered as input for analysis. In the given work, we have simulated the attacks because security incident (attack) details are not open to the public. After simulation the trace files are deduced, which will act as log, which is, input to the system. Analysis is done over inputted based on this the output proof is produced. The system response analysis on the basis experiments is being done and results are evaluated. This paper is organized as follows. Section II defines problem statement. Section III determines the response analysis of fuzzy forensic analysis system with input and output characteristics. Section IV describes the conclusion.

## II. PROBLEM STATEMENT

In MANET when attack is launched at routing (DSR routing), multiple ROUTE REQUEST (RREQ) packet is broadcasted in hop by hop pattern in the network causing DoS/DDoS due to flooding. This attack type does not require special capabilities and the normal working of network is interrupted due to unnecessary traffic. Rules were developed [8], by considering the attack characteristics, like in attack situation broadcast mechanism rule is not followed by attacker (not more than one RREQ message in per unit time can be sent), hop count is forming expanding ring, acknowledgement is over looked etc. RREQ message can be sent either with address spoofing or none address spoofing. In the work, non address spoofed RREQ message is considered since it is easier way from the point of view of attacker. Denial of service attack can be caused by an attacker that targets attack on a node or an attacker targets group of nodes in the network. Distributed denial of service attack is caused by group of attackers that target attack on a node or group of nodes in the network. In the elaborated work, we considered DoS and DDoS targeted on group of nodes. After

attacks that had compromised the security of the entire network for duration of time, investigation of attack is needed to be done, in order to provide proof, for this we implemented fuzzy forensic analysis system.

The Fuzzy forensic analysis system first generates the case and provides the hash value to that particular case.

After case is generated, log as evidence information of attack is inputted in the fuzzy forensic analysis system tool.

Then Fuzzy forensic analysis system applies the fuzzy rules for the analysis purpose and empirically analyze the log to generate the report as proof, which determines whether the flooding attack is of type DoS or DDoS and other output characteristics.

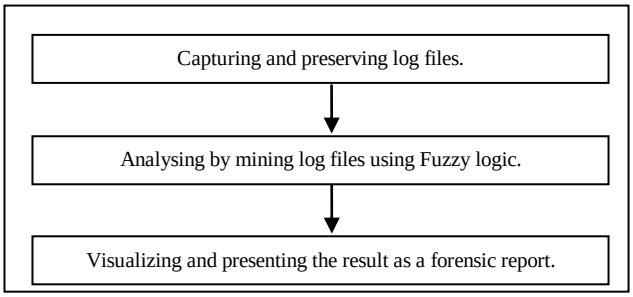



Fig. 1. Flow of work.

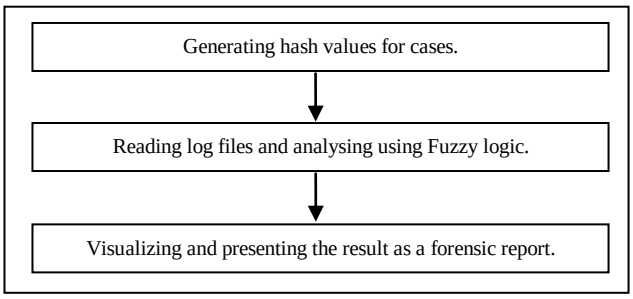



Fig. 2. Flow of working of fuzzy forensic analysis system .

## III. RESPONSE ANALYSIS OF THE SYSTEM

For log generation; we implemented the various attack scenarios, for this, we simulated the various attacks using '.Net' technology and NS2.

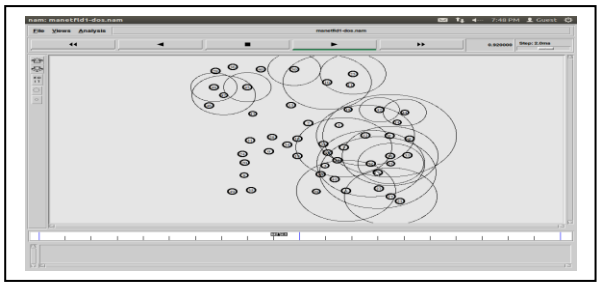
In NS2 simulation the nodes are random with varying mobility but the attackers where fixed. In .net simulation the nodes as well as the attackers are randomly selected. After simulating attack the trace files are generated. These trace files as an evidence log is inputted to the fuzzy forensic analysis system.

## IV. INPUT CHARACTERISTICS

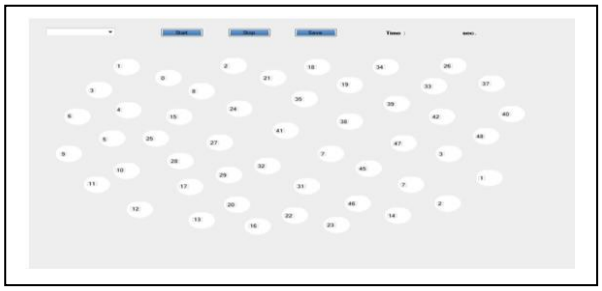
Input to the system is log, that is, the trace generated from simulation. The log contains the information like sender identity or unique id, message size, message type, destination identity, hop count, acknowledgement option, time to live information etc; various routing and movement trace information. We do simulation in NS2 and also we develop simulation environment using .Net technology; did simulation over 50 nodes, then trace files are generated and used as log input.

Attack simulation snapshots:

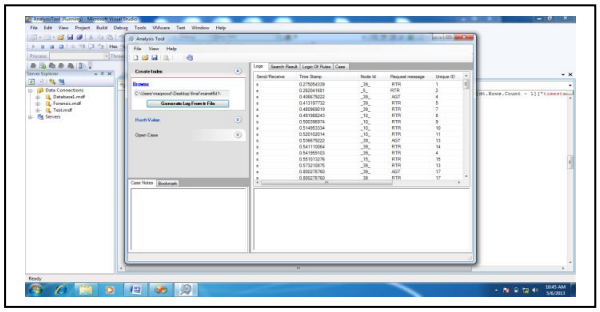
NS2 simulation:



Simulation using .Net technology:



Log reading:



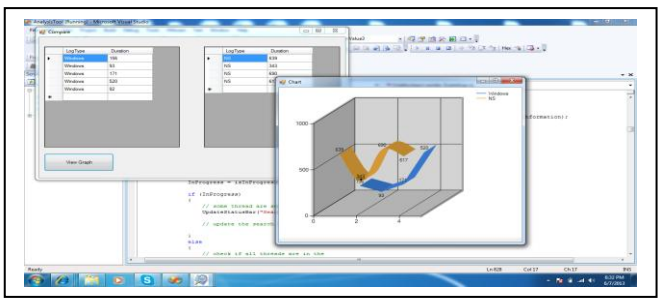
The following table shows the time taken by the system to read input that is log, for some cases:

TABLE I. INPUT LOG READING TIME BY THE SYSTEM.

| Time to read log in micro seconds | |
|---|---|
| **NS2** | **.Net environment simulation** |
| 639 | 156 |
| 343 | 93 |
| 690 | 171 |
| 617 | 520 |

The Fuzzy forensic system takes more time to read NS2 log than .net environment simulation log.

Snapshot of log reading time graph:



## V. OUTPUT CHARACTERISTICS

Fuzzy forensic analysis system do analysis based on fuzzy rules than the proof is generated in form of report which

determines whether the flooding attack is of the type DoS or DDoS, how many attackers with identity were involved in the attack? time duration for which the attack last, rate with which attack was launched etc.

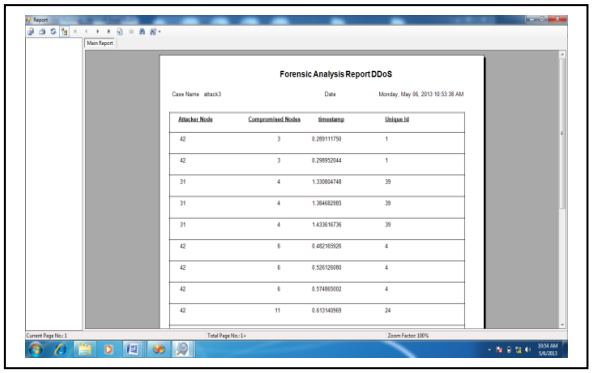
TABLE II. OUTPUT RESPONSE WHEN SYSTEM ANALYSES NS2 LOG .

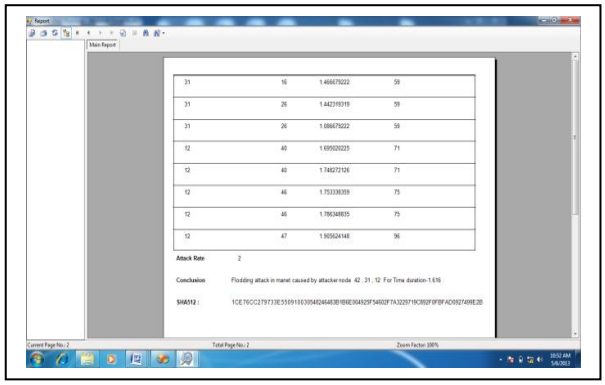
| Simulation time in seconds | Rate of Attack | Time Duration in micro seconds the attack last for number of attempts in an simulation | Number of attacker nodes | Attack found, attack type and detected correctly the output characteristic |
|---|---|---|---|---|
| 60 | 6 | 360,344 | 1 | Y / DoS / Y |
| 150 | 6 | 403,489 | 1 | Y / Dos / Y |
| 200 | 8 | 724 | 1 | Y / DoS / N |
| 225 | 6 | 328 | 1 | N / - / - |
| 300 | 9 | 510,538,807 | 1 | Y/ Dos / Y |
| 60 | 5 | 474,448,510 | 3 | Y / DDoS / Y |
| 150 | 4 | 394,457 | 3 | Y / DDoS / N |
| 200 | 3 | 506,401 | 5 | Y / DDoS / Y |
| 200 | 3 | 200 | 7 | N / - / - |
| 300 | 3 | 427 | 6 | Y / DDoS / N |

| **Time duration of simulation in sec** | **Time Duration in micro seconds the attack last for number of attempts in an simulation** | **Rate of Attack** | **Number of attacker nodes** | **Attack found, attack type and detected correctly the output characteristic** |
|---|---|---|---|---|
| 60 | 300,423 | 5 | 1 | Y / DoS / Y |
| 150 | 370,500 | 4 | 3 | Y / DDoS / Y |
| 150 | 298,316 | 3 | 3 | Y / DDoS / N |
| 200 | 310 | 6 | 1 | Y / DDoS / Y |
| 300 | 200 | 3 | 4 | N / - / - |

TABLE III. OUTPUT RESPONSE WHEN SYSTEM ANALYSES LOG GENERATED BY .NET ENVIRONMENT SIMULATION.

Report is generated when attack is found and present the output characteristics in the report when detected correctly. Output Report snap shot:



## VI. CONCLUSION

In this paper, DoS/DDoS attack caused by flooding RREQ packet at discovery phase of DSR in MANET is taken into consideration for implementation work, since this attack is easy to launch and can cause damage by disturbing the working of network for duration of time that to does not require special capabilities and when intelligently manipulated difficult to recognize. If the attack is successful and not recognized then forensic analysis is done to get digital proof against attacker. Fuzzy forensic analysis system analyses attack using fuzzy rule to determine the attack scenario and present the proof report detailing: identity, time, rate and other details of unknown attacker/attackers. For this the fuzzy forensic system is implemented to analyze empirically and deduce the digital proof. The system read log with varying time and NS2 log reading is done slower as compaired simulated attack log in .Net environment. The low rate attack for smaller time duration with less number of attempts is found by the system but the attack information is not detected correctly. The low rate attack for smaller duration in an attempt attack is not found by the system. Else DoS/DDoS attack patterns are detected successfully and the attack information is presented correctly.

## 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] Ying Zhu, "Attack pattern discovery in forensic investigation of network attacks", IEEE journal on selected areas in communications, Vol 29,No. 7, August 2011..

[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] Sarah Ahmed, S. M. Nirkhi, "A Fuzzy Rule Based Forensic Analysis Of DDoS Attack in MAET", IJACSA vol 4, issue 6.

[9] Yi Zhang, Qiang Liu, "A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis", 2010.

[10] R. Nichols and P. Lekkas, *Wireless Security-Models, Threats, and Solutions*, McGraw-Hill, Chapter 7, 2002.

[11] hanant Subhadrabandhu, Saswati Sarkar, Farooq Anjum, "A Framework for Misuse Detection in Ad Hoc Networks", IEEE Journal on selected areas in communications, Vol. 24, No. 2, February 2006.

[12] 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.

[13] Jill Slay, Benjamin Turnbull, "The Need for Technical Approach to Digital Forensic Evidence Collection for Wireless Technologies", Proceedings of the 2006 IEEE workshop on Information Assurance United States Military Academy, NY.

[14] Kevin P. Mc Grath and John Nelson, "A wireless Network Forensic System", ISSC June 2006, Dublin Institute of Technology.

[15] 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.

[16] Y. Oshita, S. Ata, M. Murata, "Detecting Distrubuted Denial of Service Attacks by Analyzing TCP SYN Packets Statistically", pp:2043-2049 Globecom2004.

[17] Jochen H. Schiller, "Mobile communication", Pearson education, chapter 8, 2008.

[18] David B. Johnson, David A. Maltz, Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks".

[19] Rashid Hafeez Khohar, Md Asri Ngadi , Satria Mandala,"A Review of Current Routing Attacks in Mobile Adhoc Networks", International journal of computer science and security, volume 2, No.- 3.

[20] David Irwin and Ray Hunt, "Forensic Information Acquisition in Mobile Networks", IEEE 2009.

[21] Shishir K. Shandilya, Sunita Sahu,"A Trust Based Security Scheme for RREQ Flooding Attack in MANET", International journal of computer applications, Vol. 5- No. 12, August 2010.