A Fuzzy Rule Based Forensic Analysis of DDoS Attack in MANET

Ms. Sarah Ahmed
Research Scholar: dept. of Computer Science & Engineering
G. H. Raisoni College of Engineering, Nagpur
Maharashtra, India

Ms. S. M. Nirkhi
Assistance Professor: dept. of Computer Science & Engineering
G. H. Raisoni College of Engineering, Nagpur
Maharashtra, India

***Abstract*—Mobile Ad Hoc Network (MANET) is a mobile distributed wireless networks. In MANET each node are self capable that support routing functionality in an ad hoc scenario, forwarding of data or exchange of topology information using wireless communications. These characteristic specifies a better scalability of network. But this advantage leads to the scope of security compromising. One of the easy ways of security compromise is denial of services (DoS) form of attack, this attack may paralyze a node or the entire network and when coordinated by group of attackers is considered as distributed denial of services (DDoS) attack. A typical, DoS attack is flooding excessive volume of traffic to deplete key resources of the target network. In MANET flooding can be done at routing. Ad Hoc nature of MANET calls for dynamic route management. In flat ad hoc routing categories there falls the reactive protocols sub category, in which one of the most prominent member of this subcategory is dynamic source routing (DSR) which works well for smaller number of nodes and low mobility situations. DSR allows on demand route discovery, for this they broadcast a route request message (RREQ). Intelligently flooding RREQ message there forth causing DoS or DDoS attack, making targeted network paralyzed for a small duration of time is not very difficult to launch and have potential of loss to the network. After an attack on the target system is successful enough to crash or disrupt MANET for some period of time, this event of breach triggers for investigation. Investigation and forensically analyzing attack scenario provides the source of digital proof against attacker. In this paper, the parameters for RREQ flooding are pointed, on basis of these parameters fuzzy logic based rules are deduced and described for both DoS and DDoS. We implemented a fuzzy forensic tool to determine the flooding RREQ attack of the form DoS and DDoS. For this implementation various experiments and results are elaborated in this paper.**

***Keywords*—DoS and DDoS attack; DSR; Fuzzy logic; MANET; Network forensic 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) a kind of wireless networks. It is the distributed systems having wireless mobile nodes that can freely and dynamically self-organise into arbitrary, temporary, and ad hoc network topologies, allowing connections within the network neither having pre-existing communication infrastructure nor centralized administered control management. As any network are having security vulnerabilities, so as MANET. However, the MANET unique characteristics and features are advantageous, on the contrary can add up to security threats. 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, which cannot be made stealth [5]. MANET are particularly susceptible to DDoS attack [1]. So, DoS/DDoS are easy to implement in MANET and to make it unrecognizable it is required to be done keenly. Flooding attack causes excessive volume of traffic to deplete key resources of the target legitimate users, 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. The dynamic nature of MANET allows routing like dynamic source routing (DSR) and attackers can take the advantage of this dynamic source routing (categorized under the reactive routing) in which route is discovered on demand or when needed, for this interested node sends Route request message (RREQ) at discover phase and attacker can flood the network with RREQ causing denial of services.

Mission-critical applications demands technologies and methods for security incident investigation [2]. 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]. Network forensics uncovers the facts of unauthorised or malicious activities. Forensic investigation aims to gain insight into and reach conclusions about critical questions of network security incident. The study of network forensics analysis for attacks in wireless network [2] and in MANET is considered still in progress. Forensic analysis can be done by unsupervised method it may require long iterations. Statistical methods like Cumulative sum (CUSUM), adaptive threshold, statistical moments. 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 deals with reasoning that is approximation and uncertainty assumption rather than exact value. 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]. This technique is efficient in complex analysis and it is rule based so easily modifiable, but requires fine tuning of rules.

This paper is organized as follows. Section II defines problem statement. Section III, IV points out various parameter of register request message in dynamic source routing is considered at general scenario and attack scenario. Section V describes the proposed fuzzy rules for network forensics analysis. Section VI determines the experiment and result for fuzzy forensic analysis tool. Section VII describe conclusion. Section VIII shows snapshots.

II. Problem Statement

Flooding attack is a kind of DoS attack. DoS are active attacks. DoS can be caused by an attacker to compromise one node or group of nodes in a network and DDoS can be caused by group of attacker nodes to compromise one node or group of nodes in the network. In our work, we have considered the DoS caused by an attacker to compromise group of nodes and DDoS caused group of attackers to compromise group of nodes.

MANET is mobile wireless network and requires ad-hoc settings, so routing is needed to find the path between source and destination. Dynamic routing eliminates the periodic routing updates and prevents nodes from unnecessary battery loss. In Dynamic source routing (DSR) [16], a node need to discover a route, it broadcasts 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. In MANET when attack is launched at routing (DSR routing), ROUTE REQUEST (RREQ) packet is broadcasted is sent again and again with address spoofing and without address spoofing (in our work we have considered non address spoofed RREQ packet) in a second violating of broadcast management causing DoS/ DDoS in the network. By doing this attacker tries to inundate the legitimate user by redundant RREQ packet. In DoS the rate of attack by a attacker is high as compared to DDoS attack to cause damage of same intensity. DoS attacks can be limited by enforcing the maximum route length that a packet should travel, source authentication, message integrity or using some other active approaches to trace the location of attacker by estimating signal strength, for this, nodes in MANET should have capabilities [1] to implement preventive measure as above which itself has own constrainer.

After attacks that had compromised the security of the entire network for a duration of time investigation. Forensic investigation uncovers the various facts related to attack by forensically analyzing the attack pattern.

In the proposed work, 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 for both DoS and DDoS due to RREQ flooding.

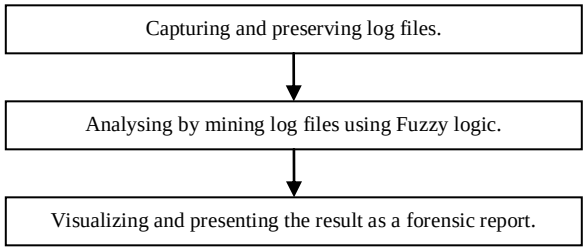


Fig. 1. Flow of work.

III. Parameters Belong to General Scenario for Route Discovery

When a node wants to send a packet to the destination node, it first searches its Route Cache from a suitable route to the destination node. If no route from source node to destination node exists in source route cache, then source node initiates Route Discovery and sends out a ROUTE REQUEST message to find a route. When the message is first sent by a sender node, which is willing to find route of some destination node. The sender that is initiator node set the Initiator ID, the Target Id and the Unique Request Id in the ROUTE REQUEST message and then broadcasts the message. Nodes within the wireless transmission range receive this RREQ. The sender/initiator keeps a copy of the packet in a send buffer. The timestamps of message can be used to determine if it should send packet/message again. When any node receives a ROUTE REQUEST message it examines the Target ID to determine if it is the target/destination of the message. If the node is not the target it searches its own route cache for a route to the target. If a route is found it is returned. If not, the node`s own id is appended to the Address List and the ROUTE REQUEST is broadcasted ahead to its neighbor.

TABLE I. Fields of ROUTE REQUEST(RREQ) message.

Fields	Explanation
Initiator ID	The address of the source node.
Target ID	The address of the target node.
Unique Request ID	A unique ID for identification of message.
Address List	A list of all addresses of intermediate nodes that the passes before its destination.
Hop Limit	The hop limit can be used to limit the number of nodes that the message is allowed to pass (varies from 1 to 255).
Acknowledgement bit	Option is set so that the destination node returns an acknowledgement when a packet is received.

If a node subsequently receives two ROUTE REQUESTs with the same Request id, it is possible to specify that only the first should be handled and the subsequent is discarded .If the node is the destination/target it returns a ROUTE REPLY message to the sender/initiator.

IV. Parameters THAT Belong to Attack Scenario for Route Discovery

Various parameters which can be considered in attack situation for route discovery are:

- Total number of RREQ packet sent by the neighbor per unit time. In attacking scenario, attacker would not comply with broadcast management techniques adopted in current routing protocols such as limiting the maximum number of (continuous flow) RREQ packets sent per second. Therefore in attack scenario there is no limit, on the rate of RREQ message is considered by attackers for continuous flow.
- The hop count (TTL) is limitless in attacking scenario.
- The time duration for which targeted node is compromised, engaged in handling unnecessary routing load.
- In attacking situation the acknowledgement option is not emphasized and acknowledgement is not considered.
- To maintain a continuous flow by an attacker do attack with high rate and group of attackers do attack with low rate.

V. FUZZY RULES

Fuzzy forensic analysis tool uses fuzzy IF-THEN rules. A fuzzy IF-THEN rule is of the form, IF X1 = A1 and X2 = A2 and Xn= An THEN Zn, where Xi is linguistic variable description and A and Z are linguistic terms.

The 'IF' part is the antecedent or premise and the 'THEN' part is the consequence or conclusion.

TABLE II. LINGUISTIC VARIABLES AND DESCRIPTIONS.

Variables	Description
X1	The total number of RREQ continuous flow from a node in a second.
X2	For continuous flow the RREQ message length (Expanding ring searches on hop count).
X3	Time duration count of RREQ a node is targeted.
X4	Count of acknowledgement forwarded to initiator node of continuous flow, which is unattended (Route reply).
X5	The total number of RREQ continuous flow from group of nodes in a second.
X6	Count of Initiator nodes of continuous flow .

TABLE III. INPUT LINGUISTIC TERMS AND DESCRIPTIONS.

Name	Description
A1	greater than 1.
A2	greater than 255 hops.(for our work we considered 50)
A3	Difference in time stamp of continuous flow is greater than 1.
A4	greater than 0.
A5	greater than 1.
A6	greater than 1.

TABLE IV. OUTPUT LINGUISTIC TERM AND DESCRIPTION.

Name	Description
Z1	Flooding RREQ attack by a node.
Z2	Flooding RREQ attack by group of nodes.

TABLE V. RULES REPRESENTATION

Rule Name	Rule Representation
R1=DoS Attack	If(X1=A1,X2=A2,X3=A3,X4=A4) then Z1
R2=DDoS Attack	If(X2=A2,X3=A3,X4=A4,X5=A5,X6=A6) then Z2

Motivation of using fuzzy logic is that, through fuzzy logic more appropriate attack pattern analysis rules can be implemented [8].

For implementation of complete linguistic description of rule require compound rule structures which is implemented by disjunctive antecedents. One of the compound structures in our implementation is like X1, can be no attack (general normal scenario), lower rate attack and higher rate attack that is evaluated on:

$$\mu X1 = \begin{cases} 0 & \text{if } A1<2, \\ ((A1-2)\ \%\ 9) & \text{if } 2 \le A1 \le 11, \\ 1 & \text{if } A1>11 \end{cases}$$

The membership is considered as 0 when no attack is launched, membership is considered as ((X1-2) % 9) when lower rate attack of RREQ flooding is launched, and 1 when higher rate attack of RREQ flooding is launched.

Same way, other compound structures X2, X3, X4, X5, and XC6 are implemented for A2, A3, A4, A5, A6 respectively.

The Mamdani Min type of fuzzy modeling is used to for composition of rules R1 and R2, using max-min rule of composition.

VI. EXPEREMENT AND RESULTS

In the experiment, for evaluation we implemented the various attack scenario and the trace files we considered as a log, is input to the forensic analysis tool which uses fuzzy logic for analysis to generate the forensic digital proof for each case having a unique hash value.

- Experiment 1st:

To implement the attack scenario we simulated the various attacks in NS-2 simulator. About 20 attack scenarios causing flooding of route request message on random 50 nodes with mobility speed 20ms, with varying simulation time between 60sec to 300sec, and varying number of attackers (one for DoS attack and three to seven for DDoS attack), at different rates per second (six to ten attack rate for DoS and three to five for DDoS attack) had been launched. In NS2 the connectivity is static.

After launching the attacks, the trace file (as log) is inputted to the fuzzy forensic analysis tool. The tool generates the case and attaches the hash value to the particular case. Then the proof report with particular hash value is deduced with details like attacker nodes, compromised nodes time duration of attack and rate of attack. The results are:

TABLE VI. RESULTS FOR DOS ATTACKS

Simulation time in seconds	Rate of Attack	Number of attacks with same rate	Time Duration in micro seconds	Detected Correctly
60/150	6	2	344/403	y/y
80/250	7	2	419/427	y/y
60/200	8	2	423/724	y/n
70/300	9	2	516/807	y/y
60/170	10	2	472/790	y/y

Number of attacker node: one
Number of Attack launched: Ten

TABLE VII. RESULTS FOR DDOS ATTACKS

Simulation time in seconds	Number of attacker nodes	Rate of Attack	Time Duration in micro seconds	Detected Correctly
60	3	5	448	y
150	3	4	394	y
80	4	5	406	y
250	4	4	412	y
60	5	4	386	y
200	5	3	401	y
70	6	4	256	y
300	6	3	427	n
60	7	4	229	y
170	7	3	236	y

Number of Attack launched: Ten

Fuzzy Forensic analysis tool is capable to find eighteen attack scenarios out of twenty attacks.

- Experiment 2nd:

To implement the attack scenario we simulated the various attacks using .Net technology for 50 nodes. In this the nodes as well as the attackers are randomly selected. The results are:

TABLE VIII. RESULTS FOR RANDOM ATTACKS

Random attacking scenario case	Randomly selected Attacker/ attackers	Detected Correctly
1	39	y
2	12,48,26	y
3	31,16	y
4	42	y
5	23,27,39,8	n

Fuzzy Forensic analysis tool is capable to find four attack scenarios out of five attacks.

Snap shots

VII. CONCLUSION

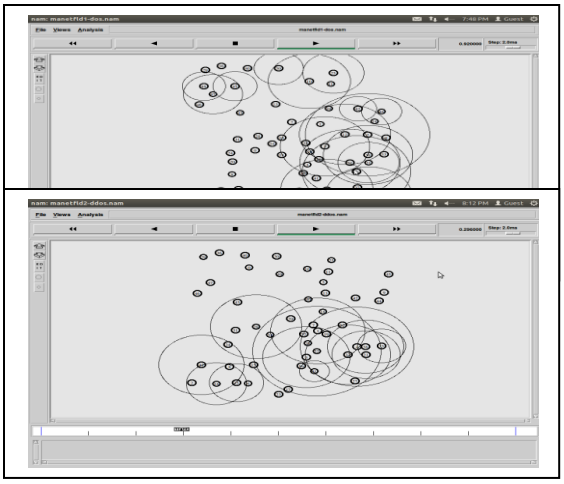
In this paper, we emphasized over the DoS/ DDoS carried due to flooding of RREQ routing packet while dynamic source routing in MANET. Flooding RREQ message per unit time without following broadcasting rule can easily implemented by attacker and for some duration attacker engage the network in unnecessary routing management leading to denial of services for some duration. There is requirement for gathering proof against attacker for this forensic analysis of attack trace evidence is needed to be done. Fuzzy forensic do this analysis using fuzzy logic.

For analysis we considered the various parameters of register request in dynamic source routing protocol at general scenario and in attacking scenario. According to these parameters the fuzzy analysis rules are generated and determined. Attack scenarios having varying simulation time and number of attackers is launched in NS2.

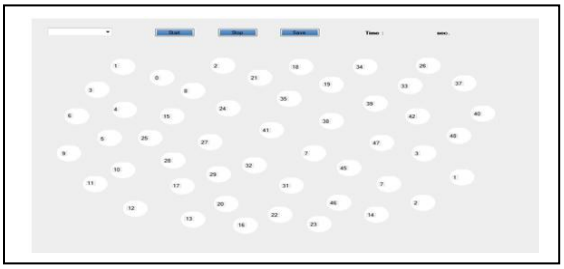
As well as in simulation for attack scenario using .Net having random attackers, random number of attackers is also implemented. Fuzzy forensic analysis tool provide protected reports with hash value with details like attacker nodes, compromised nodes time duration of attack and rate of attack. Our tool gives approximately 90% of correct detection for both DoS and DDoS RREQ flooding.

VIII. SNAPSHOTS

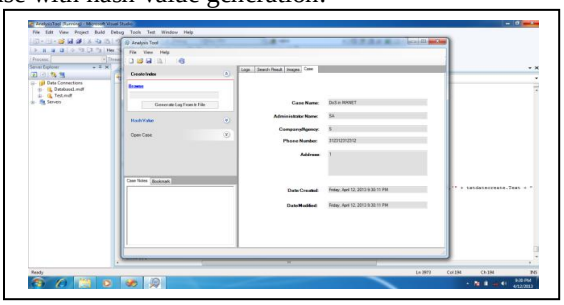
Attack simulation in NS2:



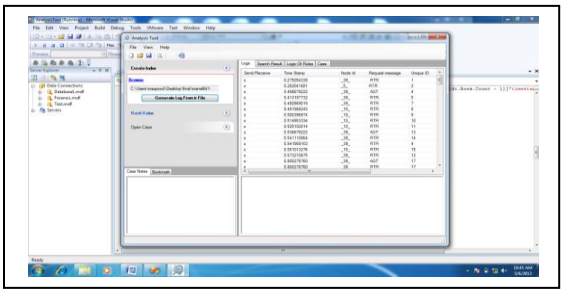
Attack simulation using .net environment:



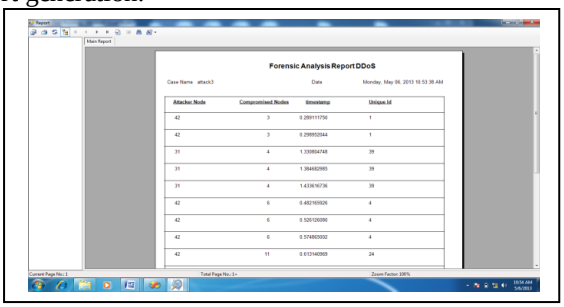
Case with hash value generation:

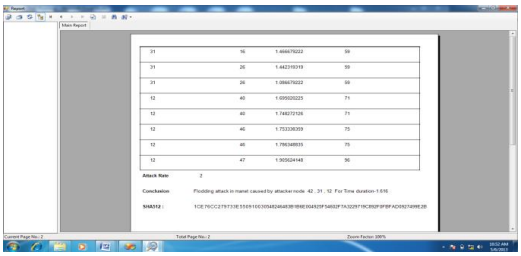


Log evaluation:



Report generation:





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 Approach for Forensic Analysis of DDoS Attack in MANET", Mar 2013, ICCSIT India.

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

[10] Dhanant 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.

[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] 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.

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

[14] 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.

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

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

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

[18] 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.

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

[20] 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.