RESEARCH ARTICLE OPEN ACCESS

An Approach for Detection of Attack in VANET

Komal B. Sahare[1], DR. L.G.Malik[*2]
Department of Computer Science and Engineering
G. H. Raisoni College of Engineering,
Nagpur, Maharashtra, India-441110
E-mail: kkomal2428@gmail.com

ABSTRACT
Vehicular Ad Hoc networks are gaining more and more importance now a day, as it is an emerging and promising technology. The life saving factor is the key issue in this network. An attacker is one who can intentionally change the behavior of the other Vehicle or Infrastructure in the network, also try to challenge the network with their malicious attacks. Today research has mostly directed the attention on the security of VANET, while to protect the network from attacks the comprehensive solutions still need to be improved, to achieve safety of life need to reach a satisfactory level for the driver and manufacturer. We discuss the various needs for VANET networks which are strongly dependent on their privacy features and security. The main objective of this paper is to study the various attack detection technique and main goal of this focuses on the detection of hosts participating in a performing a DDoS attack on VANET.

Keywords- *Vehicular Ad Hoc Networks, Attacks, Privacy, Security.DDO attack.*

I. INTRODUCTION

To create a mobile network A Vehicular Ad-Hoc Network, or VANET is a technology that uses moving cars as nodes in a network. In VANET every participating car turns into a wireless router or node, all cars are approximately 100 to 300 meters of each other to connect and create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, so that a mobile Internet is created by connecting vehicles to one another. The first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

Dedicated Short Range Communication (DSRC) is used as communication medium and it operates on 5.9GHz frequency band. DSRC is based on IEEE 802.11a standard and IEEE 1609 working group is being standardized as IEEE802.11p for special vehicular communication [1]. Seven channels are provided for safety and non safety applications with 10 MHz bandwidth. DSRC typically provides 6 to 27 Mbps data rate over 1000m communication range [2]. Safety and non safety messages are forwarded between the Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) on this communication medium. Due to the short range of communication wireless medium, cooperation between the vehicles is essential to communicate with each other. Attacker creates problems in the network using DSRC by launching some attacks. There are many issues in VANET which are summarized as follows:

- Security
- DSRC and collision warning
- Routing
- Information dissemination
- Data access
- Address configuration

DDOS attacks may cause a severe impact on security-critical information systems As such, in order to thwart a DDoS attack, not only the detection of the event must be completed, but the offending hosts need to be identified in order for an incident response control to be effective. In terms of incident response effectiveness, the underlying control must be able to block network traffic belonging to the DDoS attack vector. The main objectives are that is it feasible to detect a DDoS attack within an acceptable timeframe. The scope and main goal of this is focuses on the detection of hosts participating in performing DDoS attack on VANET. The corresponding objectives are as follows, to improve detection times in the case of a DDoS attack, to develop an appropriate incident response plan for proactively protecting the vehicular resources and minimizing the damage, to develop a methodology for forensic analysis of

the identified attack sources, to evaluate and improve open source tool.

II. SECURITY ISSUES OF VEHECULAR AD HOC NETWORKS

VANET suffer from various attacks; these attacks are discussed in the following subsections:

Denial of Service Attack: DoS attacks can be carried out by network insiders and outsiders and renders the network unavailable to authentic users by flooding and jamming with likely catastrophic results. Flooding the control channel with high volumes of artificially generated messages, the network's nodes, onboard units and roadside units cannot sufficiently process the surplus data.

Broadcast Tampering: An inside attacker may inject false safety messages into the network to cause damage, such as causing an accident by suppressing traffic warnings or manipulating the flow of traffic around a chosen route.

Malware: The introduction of malware, such as viruses or worms, into VANETs has the potential to cause serious disruption to its operation. Malware attacks are more likely to be carried out by a rogue insider rather than an outsider and may be introduced into the network when the onboard units and roadside units receive software and firmware updates.

Spamming: The presence of spam messages on VANETs elevates the risk of increased transmission latency. Spamming is made more difficult to control because of the absence of a basic infrastructure and centralized administration.

Black Hole Attack: A black hole is formed when nodes refuse to participate in the network or when an established node drops out. When the node drops out, all routes it participated in are broken leading to a failure to propagate messages.

Masquerading: Masquerading attacks are easy to perform on VANETs as all that is required for an attacker to join the network is a functioning onboard unit. By posing as legitimate vehicles in the network, outsiders can conduct a variety of attacks such as forming black holes or producing false messages.

Replay Attack: In a replay attack the attacker re-injects previously received packets back into the network, poisoning a node's location table by replaying beacons. VANETs operating in the WAVE framework are protected from replay attacks but to continue protection an accurate source of time must be maintained as this is used to keep a cache of recently received messages, against which new messages can be compared.

Global Positioning System (GPS) Spoofing: The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite.

Position Faking: Authentic and accurate reporting of vehicle position information must be ensured. Vehicles are solely responsible for providing their location information and impersonation must be impossible. Unsecured communication can allow attackers to modify or falsify their own position information to other vehicles, create additional vehicle identifiers (also known as Sybil Attack) or block vehicles from receiving vital safety messages.

Message Tampering: A threat to authenticity can result from an attacker modifying the messages exchanged in vehicle-to-vehicle or vehicle-to-roadside unit communication in order to falsify transaction application requests or to forge responses.

Message Suppression/ Fabrication/ Alteration: In this case an attacker either physically disables inter-vehicle communication or modifies the application to prevent it from sending to, or responding from application beacons.

Key and/or Certificate Replication: Closely related to broadcast tampering is key management and/or certificate replication where an attacker could undermine the system by duplicating a vehicle's identity across several other vehicles. The objective of such an attack would be to confuse authorities and prevent identification of vehicles in hit-and-run events.

Sybil Attack: Since periodic safety messages are single hop broadcasts, the focus has been mostly on securing the application layer. For example, the IEEE 1609.2 standard does not consider the protection of multi-hop routing. However, when the network operation is not secured, an attacker can

potentially partition the network and make delivery of event-driven safety messages impossible.

III. LITERATURE SURVEY

As security of VANET given increasing attention in recent years, different forms of attack detection technique are studied in the literature.Nikita Lyamin *et a.[2]* proposed A method for real-time detection of Denial-of- Service (DoS) attacks in IEEE 802.11p vehicular ad-hoc networks (VANETs). The study is focused on the "jamming" of periodic position messages (beacons) exchanged by vehicles in a platoon. Probabilities of attack detection and false alarm are estimated for two different attacker models i.e., Random jamming, ON-OFF jamming.A. L Toledo and X. Wang *et a.[3]* Real-time detection of DoS attacks in IEEE 802.11 networks have been studied in [3], where the proposed detection system observes the events happening in the wireless channel and computes how "explainable" occurring of each particular collision is. The method in [3] targets the basic mode of IEEE 802.11 with an arbitrary unicast traffic, which is retransmitted according to the binary exponential bakeoff algorithm.

A. Hamieh, J. Ben-othman, and L. Mokdad *et a. [4]* proposed a method to detect the jammers in VANETs with unicast traffic, which is based on linear regression, is proposed in [4]. However, very limited performance evaluation results are reported in [4], e.g. no results on the detection time are given.The authors [5] proposed an Attacked Packet Detection Algorithm (APDA) which is used to detect the DOS (Denial-of- Service) attacks before the verification time. This minimizes the overhead delay for processing and enhances the security in VANET.The authors [6] try to solve the security problem of Dos attack with the use of OBU. The model relies on the use of OBU which fits on each vehicle node, to make a decision as to deter a DOS attack. The processing unit passes information to the OBU, to switch channels technology (or) to use frequency hopping technique. Four options are available to detect the received messages, after the [6] decision will be sent to the next OBU in the network. Switching options are channel switching, technology switching, FHSS, multiple radio transceivers

The authors [7] try to solve the security problems of the Sybil attack detection scheme, which is composed of two complementary techniques. The first one is a localization verification technique, based on receiving signal strength. This technique allows a node to verify the authenticity of another node by locating its future geographical localizations. Compare them to its detected suspect, a second technique [7] is a Sybil detection mechanism, based on the definition of a distinguish ability degree metric. It can be launched individually by every node in the network.

The authors [8] try to solve the problem of the Sybil attack detection based on cryptography in VANET. The proposed schema uses an encryption mechanism to detect attacks and to the four security aspects like authentication, non-repudiation, privacy, and data integrity are introduced. Every vehicle should make sure of message transmitters authority and authenticate it. Non repudiation allows to access personal information of the vehicle, which helps in recognizing the vehicle in case of any claims and crimes. Vehicles identity information's should be attached to the messages, so it can be tracked whenever desired and non repudiation is established in the network. Privacy of personal information [8] about the vehicles and the drivers are restricted not be accessible by other vehicles. The anonymity can be preserved to avoid tracking. Data integrity is that the transmitted message can contain valid information not to be altered by attackers.

The authors [9] try to solve the problem of Wormhole Attack detection. The nodes participating in the VANET communication should register on the network. In order to avoid the formation of wormhole in the route, this paper proposes a method in which after the route reply from the destination, the source has a complete list of the intermediate nodes forming the route. The author [9] proposes a scheme in which they use a special packet called Decision Packet. After the route has been set up between a source node and destination node, the former gets the information about all nodes in the path from RREP packet. Which contains all nodes identity take which has been forming route from source to destination node in recent [9] identified path. Every node computes the hash value of the decision packet which is verified at the next node, so there is no chance of alteration of the hop count by the attacker. If an attacker by somehow changes

[9] the hop count value it will result in a change, in hash value of the packet will be consequently discarded.The authors [10] try to solve the problem of a synchronization based DDoS attacks on vehicular communications Since a WSM packet contains the time of its transmission, and periodic broadcasts allow delivery of frames at a regular interval; an attacker may successfully guess the timing of subsequent broadcast. An RSU can randomize the schedule of its periodic broadcasts following a normal distribution with original transmission time as the mean, and a predetermined delay as the standard deviation. The intention is to

reduce the accuracy of an attacker's jitter estimate, and diminishing its ability to synchronize with the RSU's transmission.In [11] the authors proposed an efficient method called IPCHOCKREFERENCE detection method is used to detect and defend against UDP flooding attacks under different IP spoofing types. The method makes use of a storage-efficient data structure and a Bloom filter based IPCHOCKREFERENCE detection method. This lightweight approach makes it relatively easy to deploy as its resource requirement is reasonably low.

In [12] the authors proposed method to defend denial of sleep attack consists of two parts.

a) Network organization.
Authors propose the following network organization algorithm given Node organization is the first step once the nodes are deployed in the network. Sensor network is built in a tree like structure and organize the nodes. Sink node is at the root of the tree. Each node must know its parent node to which it needs to send packets to reach to sink. Also the parent node must know the child node from which it can receive SYNC packets.

b) Selective Local authentication

There are two different formats for SYNC packet. One is without authentication and other one is with authentication token. During normal operation if the SYNC is under threshold SYNC without authentication is used. If there is a threshold cross over there is a chance of denial of sleep attack and enforces SYNC with authentication token for authentication.In [13] the authors proposed encryption mechanism to detect attack and provides four security aspects Authentication, Non-repudiation, Privacy, and Data Integrity. This paper presents a method base on cryptography to detect Sybil attack in VANET. Result of simulation shown that Execution time of this algorithm is low, because most operations is done in Certification Authority, so the proposed method is a best method for detection of Sybil attacks.

Public Key Cryptography Security issue of Sybil attacks can be solved by using public key cryptography and authentication mechanism as described in [14, 15]. In this security solution, signatures are combined with digital certificates and asymmetric cryptography is used. Certificates are issued by CA and there is a hierarchy of these CAs. For each region, there is one CA. These CAs communicate with each other through secure channel and keep track of issued certificates used by every signed message. This technique can prevent Sybil attacks as only messages with valid certificates are considered and invalid messages are ignored. The only requirement is that each node should be assigned one certificate at a time. For privacy implementation, these certificates are changed from time-to-time. But in VANETs, it is difficult to deploy PKI as there is no guarantee of the presence of infrastructure. It is very complex, consumes large memory, and time consuming as well.Timestamp Series This technique, can be used to detect Sybil attack discussed in [16] in this approach, proposed a timestamp series approach to defend against Sybil attack in a vehicular ad hoc network (VANET) based on roadside unit support. It discovers that it would be rare for arbitrary two vehicles to pass through a few different RSUs (far apart from each other) always at the same time. Therefore, if a traffic message sent out by any vehicle contains several timestamps issued to this vehicle by the previously passed RSUs, Sybil attack can be detected if multiple traffic messages contain very similar series of timestamps. This method has challenges, for example If RSUs are located at intersections, it may make the Sybil attack detection difficult, so this method not suitable approach to detect Sybil attack.

In these authors proposed a DOS attack solution is based on the use of OBU (On Board Unit) that is installed in vehicles. In case of DOS attack the processing unit will suggest to the OBU to switch channel, technology, or to use frequency hopping technique or multiple transceiver [18].

To deal with traffic analysis attack Cencioni et al. [18] proposed VIPER: a vehicle-to infrastructure communication privacy enforcement protocol. It is resilient to traffic analysis attacks. In this vehicle will send their messages directly to RSU but to have vehicle acting as mix nodes.

IV. PROPOSED METHODOLOGY

In our proposed method we are designing analysis tool in order to detect attack in VANET. The Architecture of Proposed method is as follows:

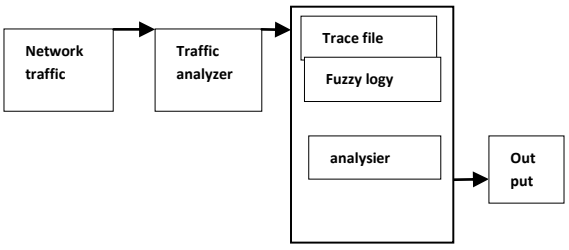

Fig 1: Architecture of attack detection model

The proposed method works as follows

Figure **1** shows the architecture of proposed system. It consists of components: the Traffic Analyzer, the Fuzzification, the Fuzzy Inference Engine, the Knowledge Base, and Forensic Analyzer. The steps of the propose system is summarized below:

- Step **1:** The Traffic Analyzer reads the network traffic from the network trace files which have a similar file format as tcp dump file.
- Step2: then network generated trace file is analyzed to generate log file.
- Step3: once the log file is generated then, an analysis is performed using Fuzzy Algorithm.
- Step4: Finally we get the output

Network analyzer provides a means for identifying, preserving, analyzing, and presenting digital evidence for uncovering facts of unauthorized or malicious activities. In practice, the following functions or tasks are carried out in network analysis investigation: network evidence capture, preservation, examination, analysis, visualization and presentation of the results. The analysis process is the meat of the whole network investigation. It aims to gain insight into and reach conclusions about critical questions of network security incident, such as what happened, where, when, how, who was involved, and why [26].This process involves trend analysis, content clustering, data fusion, correlation, pattern reorganization and detection of traffic abnormality. Generally, there are two broad categories to which digital evidence collected in network analysis investigation belongs [27]: captured network traffic and data maintained by network devices. As a major source of evidences, the data maintained by network devices include log files, configuration settings, routing tables and etc. The capture of live traffic from a network (for example, packet sniffing on an Ethernet segment) is also considered a source of network evidence. An attacker might be able to erase all log files on a compromised host; captured network traffic might therefore be the only evidence available for forensic analysis when dealing with a skilled attacker.

V. EXPERIMENTAL SETUP AND RESULTS

As DDoS attacks cannot be detected effectively by traditional methods in time, a DDoS attack detecting algorithm based on the fuzzy logic parameters is researched according to the analysis of the essential characteristic of DDoS. The scheme can detect DDoS attack traffic in its early stages when the attacking packet's attribute value has no distinct features.

We have implemented a module of our approach on the trace files which consist of well define DDOS attack, thus trace file is taken as input stream.The snapshot of trace file is given in Fig. 2. Experimentation has been performed using visual studio 2010 as frontend, Hardware requirement of proposed approach is general configuration such as Pentium IV or above Processor, 2GB RAM etc.

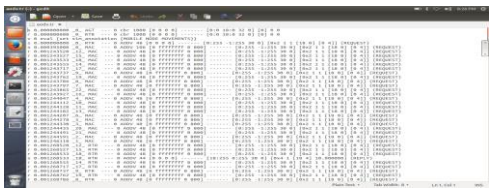

Fig. 2. Snapshot of trace file

The Traffic Analyzer reads the network traffic from the network tcpdump file and generates log files which have a similar file format. The Fuzzification component fuzzifies the values of each input variable to linguistic value using the membership functions defined for each fuzzy set **(as** in Figure 3). The linguistic value is used by the Fuzzy Inference Engine**.** Once all input values have been fuzzifed into their respective values, the Fuzzy Inference Engine accesses the Knowledge Base of the Fuzzy logic Detector (FlD) to derive linguistic values for the intermediate as well as the output linguistic variables. Usually, either the maximum or sum of the degrees of truth of the rules with the same linguistic terms in the THEN parts is computed to determine the degrees of truth of each linguistic term of the output linguistic variable. Show in following fig.

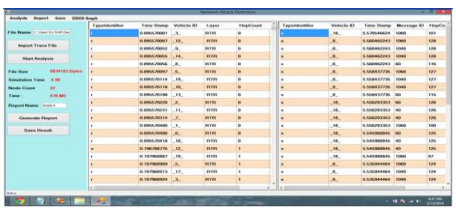

Fig. 3. Snapshot of Analyzer.

The Analyzer decides whether those packets are attack or not, using the output values. In case of determined to an attack. The Analyzer gathers related data and then makes the evidence from categorized network packets. Otherwise,

continues processing to the end of network traffic. System performance is varying along with file size as show in fig 4.

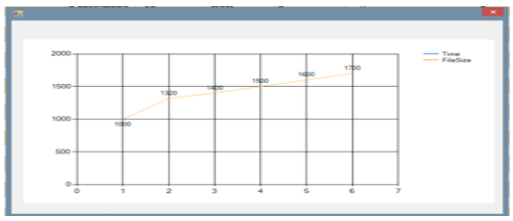

Fig. 4 time vs. file size

VI. CONCLUSION

Thus, these paper contain different techniques that can detect the attack but Security expert or forensic investigator analyzes the VANET network traffic using the empirical knowledge. There is no rule to perfectly distinguish attack from network traffic. Thus, there is need of more efficient attack detection system which will analyse the VANET network traffic and provide a security to the VANET network by detecting various attack's the Fuzzy logic one of the fastest searching engine thus To overcome the problem of DDoS attack a new method was introduced using Fuzzy Logic called Fuzzy logic Detector (FlD) for detection of various attack. Our ongoing work is focused on detection of sibyl attack using same approach.

REFERENCES

[1] Graph-Based Metrics For Insider Attack Detection In VANET Multihop Data Dissemination Protocols Stefan Dietzel, Jonathan Petit, Geert Heijenk, And Frank Kargl IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 4, MAY 2013 1505.

[2] Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks Nikita Lyamin, Alexey Vinel, Magnus Jonsson, and Jonathan Loo IEEE Communications Letters, Accepted For Publication 1 1089-7798/13$31.00 _C 2013 Ieee..

[3] A. L Toledo and X. Wang, "Robust detection of MAC layer denial of- service attacks in CSMA/CA wireless networks," IEEE Trans. Inf. Forensics and Security, vol. 3, no. 3, pp. 347–358, 2008.

[4] A. Hamieh, J. Ben-othman, and L. Mokdad, "Detection of radio interference attacks in VANET," 2009 IEEE Global TelecommunicationsConference, doi:10.1109/GLOCOM.2009.5425381.

[5]S.RoselinMary1,M.Maheshwari2,M.Thamarai selvan3 Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA). *IEEE Trans.*

[6] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET," World Academy of Science, Engineering and Technology 65 2010.

[7] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET," International Journal of Network Security, Vol.9, No.1, PP.22- 33, July 2009.

[8] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET," IJNSA, Vol.3, No.6, November 2011.

[9] Harbir Kaur, Sanjay Batish & Arvind Kakaria, "An Approach to Detect the Wormhole Attack in Vehicular Ad-hoc Networks," IJSSAN, 2248-9738 Volume-1, Issue-4, 2012.

[10]Subir Biswas, Jelena Mi˘si´c,Vojislav Mi˘si´c DDoS Attack on WAVE-enabled VANET Through Synchronization.2012 IEEE Communication and Information System Security Symposium

[11]Karan Verma, Halabi Hasbullah, Ashok Kumar 'An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacksin VANET' 2012 IEEE Deptt. Of Computer & Information Sciences University Technology PETRONAS, Malaysia.

[12]Senthil Lekha.S. L. Dr.Sasi Kumar M. 'Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks' Kerala University Proceedings of2013 IEEE Conference on Information and Communication Technologies (ICT 2013)

[13] Efficient Detection Of Sybil Attack Based On Cryptography In VANET International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011 Mina Rahbari1 and Mohammad Ali Jabreil Jamali2.

[14] M. Raya and J.-P. Hubaux, (2007)" Securing vehicular ad hoc networks". Journal of Computer Security, 15(1), 39–68.

[15] A. Khalili, J. Katz, and W. Arbaugh, (2003) "Toward secure key

distribution in truly ad-hoc networks".IEEEWorkshop 2003 International Symposium on Applications and the Internet, Orlando, FL, January

[16] Park, S., Aslam, B., Turgut, D., Zou, C.C., (2009)" Defense against Sybil attack in vehicular ad hoc network based on roadside unit support". In: MILCOM, pp. 1–7.

[17] Sam Ang Chhoeun1, Kannikar Siriwong Na Ayutaya, Chalermpol Charnsripinyo, Kosin Chamnongthai1, Pinit Kumhom1' A Novel Message Fabrication Detection for Beaconless Routing in VANETs 'Thailand 2009 International Conference on Communication Software and Networks2009 IEEE DOI 10.1109/ICCSN.2009.29

[18]Ajay Rawat, Santosh Sharma, Rama Sushil Vanet: Security Attacks And Its Possible Solutions Journal Of Information And Operations Management Issn: 0976–7754 & E-Issn: 0976–7762 , Volume 3, Issue 1, 2012, Pp-301-304.

[19]Jonathan Petit, Michael Feiri, Frank Kargl 'Spoofed Data Detection in Vanets Using Dynamic Thresholds'. Distributed And Embedded Security Group University Of Twente, The Netherlands 2011 IEEE Vehicular Networking Conference (VNC).

[20] D.Jiang, V.Taliwal, A. Meier, W.Holfelder and R.Herrtwich,"Design of 5.9GHz DSRC based vehicular safety communication",IEEEWirelessCommunication Magazine, Vol.13, No.05, Nov 2006, pp: 36-43.

[21] SU. Rahman, H.Falaki,"Security & Privacy for DSRC-based automotive Collision Reporting"www.cs.ucla.edu/falaki/courses/security project.pdf.

[22] Jung-Sun Kim Dong-Geun Kim Bong-Nam Noh ''A Fuzzy Logic Based Expert System as a Network Forensics''*25-29 July, 2004 - Budapest, Hungary*

[23] G. Guette, B.Ducourthial,"On the Sybil attack detection in VANET", Laboratoire Heudiasyc UMR CNRS 6599, France.

[24]Khaleel Mershad and Hassan Artail ''A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks'' IEEE Transactions on Vehicular Technology, Vol. 62, No. 2, February 2013.

[25] Yinghua Guo, Ivan Lee ''Forensic analysis of DoS attack traffic in MANET'' 2010 Fourth International Conference on Network and System Security. 2010 IEEE DOI 10.1109/NSS.2010.48

[26] E. Casey, "Network traffic as a source of evidence: tool strengths, weaknesses, and future needs," *Digital Investigation*, vol. 1, no. 1, pp. 28–43, 2004.

[27] B. Nikkel, "Generalizing sources of live network evidence," *Digital Investigation*, vol. 2, no. 3, pp. 193–200, 2005.