National College of Ireland

Simulation of Detecting and Preventing DDoS in Vehicular Ad-hoc Networks(VANETS)

MSc Internship
Cybersecurity

Chaitanya Rudraraju
Student ID: x18178863

School of Computing
National College of Ireland

Supervisor: Ben Fletcher

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Chaitanya Rudraraju		
Student ID:	X18178863		
Programme:	M.Sc in Cyber Security	**Year:**	2019-2020
Module:	Academic Internship		
Supervisor:	Ben Fletcher		
Submission Due Date:	29th January,2020		
Project Title:	Simulation of Detecting and Preventing DDoS in Vehicular ad-hoc Networks(VANETS)		
Word Count:	4481	**Page Count:**	18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature:

Date:

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Abstract

The Vehicle Ad-Hoc Network (VANET) is a method that has made Intelligent Transportation Systems (ITS) important for the benefit of daily life. Vehicle Ad-Hoc Networks (VANETs) are gaining rapid attention because of the variety of services they can offer. Real-time identification for all forms of attacks has become an important problem for VANET, including Distributed Denial of Service attacks (DDoS). This is due to the intermittent real-time exchange in VANET of security and the delivery of road emergency messages. Therefore, there is a need for efficient storage and intelligent VANET Infrastructure Architecture (VIA), which includes confidence. To address the problem of DDoS attack to protect the end-users as well as precious resources, E-Firecol composed of intrusion detection is proposed. Dealing with VANET attacks is a challenging issue. Most of the current DDoS detection techniques are suffering from poor accuracy and high overhead computation. To address these issues, a new approach to intrusion detection called the E-Firecol Intrusion Detection System (FIDS) and to prevent DDoS attack from entering the network, a Dynamically Growing Self-Organizing Tree (DGSOT) algorithm within RSU is included. The Proposed methodology was successfully implemented and the proposed method gives effective output.

1. Introduction

“In the modern smart transportation world, Vehicle Ad-hoc Networks(VANETS) are becoming a common and promising technology, which was basically derived from Mobile Ad-hoc Networks(MANETS). VANET has a number of applications such as security, convenience, efficient transportation services, entertainment and much more as it develops in today's automotive industry”. As per VANET's security applications, any information that circulates through the network can be vital to life. The reliability of the data is therefore a vital condition. The node mobility and the volatile nature of the network connections have made VANET vulnerable to numerous security threats. But a lot of problems occur in the actual implementation of this technology due to the mobile nature of the VANETs. Compounding VANETs and modern vehicles will enable opponents to access in-vehicle networks and remotely take control of vehicles to use them as a target or foothold. Comprehensive attention has been paid to violations in VANETs and in-vehicle systems in literary works, but there is still a gap in literature to assess security flaws associated with VANET's access methods. The vulnerabilities are not limited to VANET security issues in real-world implementations. In reality, smart vehicles that are considered to be nodes in VANETS own internal vulnerabilities that are referred to as security issues in the vehicle network [1].

Distributed DoS (DDoS) may also endanger the availability of VANET by sending repeated transmissions where malicious messages are sent by more than one person. Although it is difficult to detect DDoS attacks since the packets are flooded from various number of devices with the help of botnets and other malwares, it is necessary to secure not only end users, but also expensive infrastructure assets in the network. “The system's core is a mix of network-level Intrusion Prevention Systems (IPSs).The achievement of identifying and responding to DDoS attacks depends heavily on the data monitored by the traffic monitoring mechanisms employed, the degree of collaboration between different domains, and the response approach used in different domains.” To detect DDoS attacks in the collaborative network, Firecol algorithm is being used. This algorithm can mitigate the risk of the system's initial intrusion and harm by reacting promptly and quickly detecting an attack while targeting the target system. Firecol, a new cooperative program that detects flooding DDoS attacks from the victim's host as far as possible and at the Internet Service Provider (ISP) range as close as possible to the attack source(s).Firecol depends on a distributed architecture consisting of several IPSs which form overlay secure ring networks around subscribed customers[1].

Firecol is designed to make it possible for customers to subscribe to a service. Taking part IPSs along the road to a subscribed customer cooperate on potential attacks by measuring and sharing beliefs ratings. The IPSs form digital rings of protection around the host they serve. When the degree of a potential attack is strong, the digital rings use horizontal interaction. Throughout this way, the risk is calculated against the client's overall traffic capacity relative to the total bandwidth it supports. In addition to detecting flooding DDoS attacks, FireCol also allows to detect other flooding situations, such as flash crowds, and botnet-based DDoS attacks [2]. The paper consists of related works describing the previous works and the differences between the proposed system and the implemented works. The paper's later section explains the implementation of the proposed method and analysis of obtained results.

2. Related Study

The literature survey in this section that shows the different VANET security analysis and research happened in recent years. Vehicle networks are emerging as a promising new field of wireless technology aimed at implementing vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) applications for protection and non-safety. It includes the vehicle's ability to communicate between the surrounding vehicle and road-side unit (RSU). The issues of privacy concerns the protection and disclosure of personal information such as name, location,

plate number, and many more. Recent research that addresses security and privacy concerns in VANETs has discussed and analyzed this related work. The analysis concludes the security research gap in VANETs.

Vehicle Ad-hoc Network (VANET), an unplanned road vehicle network designed to improve road safety and driving conditions. Today, the number of vehicles is increasing and the roads are becoming more dangerous due to the effect of congestion and the risk of collision is increased. Safety messages must be timely and correctly routed to the vehicles. VANET messages are vulnerable to many attacks due to the wireless medium. Network availability must be obtained at all times to be secure, as network availability is highly needed when a node sends any vital information to other nodes. The availability of the network is exposed to many types of attacks in this regard. DDoS attacks are very technically advanced methods of attacking a network system and either making it unusable for legitimate users or downgrading its performance. "A severity of denial of service attacks in the VANET environment and its different levels. They also suggested a model to safeguard the VANET from the DoS assaults in which they suggested an attacker directory by which their model could classify that it is attacking or not, and if so what kind of assault and according to which this model reacts" [3].

"In VANET, PKI (Public Key Infrastructure) is the authentication and cybersecurity system that protects server-client interaction. For successful usage, a public key system requires a number of different elements. A Certificate Authority (CA) is used to authenticate user's virtual identities, which can vary from individuals to databases to computer systems". A public key infrastructure (PKI) approach that has been broadly accepted as a remedy to security issues due to its usefulness in recent research efforts. One part of a method for PKI is the revocation of certificates. It is one way of ending the subscription of a networked vehicle that performed some malevolent operations in a system [4].

"An attack scenario on the basis of synchronization-based DDoS attack by small contention window sizes and transmission periodicity is identified to reveal the deficiency in the EDCA mechanism". Things get worse when, because broadcast messages in VANET do not have acknowledgments, neither the receivers nor the sender of regular broadcasts will be aware of the assault. The possibility of a synchronization-based DDoS attack on vehicle communications is also evaluated and a method is also suggested to prevent such attacks [5].

“Firecol was designed to make it easier for consumers to subscribe to a service. Participating IPSs along the road to a subscribed customer work together (vertical communication) by measuring and sharing scores of beliefs about potential attacks. The IPSs form digital rings of protection around the host they are shielding. When the degree of a potential attack is high, the digital rings use horizontal interaction. In this way, relative to the total bandwidth it supports, the risk is calculated based on the overall traffic capacity directed at the customer. Firecol also helps detect other flooding situations, such as flash crowds, and botnet-based DDoS attacks in addition to detecting flooding DDoS attacks”. Firecol is providing an ISP-level cooperative framework for detecting flood-based DDoS attacks as close to the source(s) of the attack. Multiple IPSs form an overlay of defensive rings around subscribing customers and work together on potential attacks by computing and sharing creed ratings. Relative to the total bandwidth that it supports, the attack is calculated based on the overall traffic bandwidth directed to the customer [6] .

Using consistent existing IP address data, the fake identities of malicious vehicles are analyzed. All vehicles regularly exchange beacon packets in order to signal their presence and become aware of the next node. Each module keeps track of their database regularly by sharing information in their environment. If some nodes find similar IP addresses in the database, they will be identified as DoS attacks. Nevertheless, due to more and more mobile applications being built on the well-known exposed nature of the wireless medium, security threats are likely to increase in the future. The availability of the network is exposed to many types of attacks in this regard.” In this paper, a DoS attack on network availability is being developed. A product interaction model for DoS prevention has been developed called "IP-CHOCK," which will lead to DoS attacks being prevented” [7].

Distributed denial-of-service (DDoS) attacks were major network security issues. The prevention of which is especially difficult when it comes to botnet-based attacks that are widely distributed. “An Expanded Firecol (E-FireCol) consisting of Internet service providers (ISPs)-level intrusion prevention schemes. Intrusion prevention systems form digital rings around the hosts to protect against DDoS attacks and cooperate through the sharing of selected traffic information. By detecting more DDOS attacks compared to the FireCol, E-FireCol is effective and supports the various ISP rule structures” [8].

Conventional protection strategies, such as customer authentication, firewall and data encryption as the main security barrier board, are insufficient to spread the entire system security scene when facing difficulties from ever-advancing interference technologies and methods. For example, an intrusion detection system (IDS) is highly suggested as a result of this. Various types of paradigm-related methods are addressed using knowledge-based data discovery (KDD) data sets to detect DDOS and other related attacks in wireless ad hoc networks [9].

In recent years, VANET safety has been extensively investigated. Nevertheless, there was not much work done in VANET to detect and mitigate DoS / DDoS attacks [4]. Presentation of Dedicated Short Range Communication (DSRC) and methods for revocation. The method of detection is based on transferring the offender or sending a message to the target node and then to different locations, and may also have a different time slot for transferring the message, and the offender will try to change the time slot and message for different vehicle nodes. The main reason for the occurrence, however, is to make the network inaccessible by downloading the entire network to the victims or vehicle nodes. Nevertheless, any node in the VANET network can receive a limited amount of security messages at a given timestamp, so it is known to be the node already targeted. This allows it to protect itself from any DoS and DDoS attacks [10].

Some points are explored during the survey, where it suggests the disadvantages of the existing technique. In this paper, the proposed research work effectively implements defense mechanisms in VANET and can improve security by accurately distinguishing legitimate and malicious requests.

3. Research Methodology

Within VANETs there are a number of possible attacks. These attacks are intended to create problems for users to access the network or to phase out some data. In order to cause the channel or some problem to networks or nodes, the attacker attacks the communication medium or network nodes. The vehicle is unable to access the networks, resulting in the nodes and the resources of the network being devastated and overtired. Most of the researchers in VANETs is currently focusing on DoS and DDoS attacks. Therefore, the method is proposed to provide a security from DDoS attack in VANET through the convergence of FireCol with DGSOT

algorithm. The Public Key Infrastructure is implemented using the cloud for authentication of vehicles.

3.1. Proposed Method

The collaborative architecture proposed in this model consists of two implementation levels that are FireCol implementation and DGSOT algorithm implementation.

FireCol Architecture

The FireCol, which consists of Internet service provider-level intrusion prevention systems. It uses the rings around a host of intrusion prevention systems as a single prevention system is not enough to defend flood-based DDoS attacks. Figure 1 depicts the FireCol architecture.

Steps:

1. Observing the detection window to find out the deviation of traffic from normal traffic pattern detects the attacks. The attacks are graded as low or high potential attack based on the percentage of variance.
2. For subscribers, the FireCol system has some rules that match an IP address pattern. The system's packet processor reviews incoming traffic and updates counter and frequencies whenever a rule matches. Entropies and relative entropies(the uniformity of the frequencies) are calculated by the metrics manager.
3. Selection manager checks if the profile was within the traffic distribution.
4. A score is assigned to each selected rule based on values of entropy and frequency, by the score manager
5. Lastly, detection manager confirms flooding attack when the traffic generated is countless than the capability of the customer to recieve.

3.2. Level of protection

3.2.1. Ring Based Protection:

The FireCol detection upholds virtual circles or protective armors around the vehicles of the network.

3.2.2. Subscription Protocol:

FireCol protects the vehicles following the defined rules. A rule of FireCol matches an IP packet pattern. FireCol is a value added service that customers use the protocol to subscribe to.

3.2.3. Multiple customers:

FireCol allows several virtual rings for protection to coexist for numerous vehicles across the same set of IPSs due to inherent complete independence.

3.2.4. Algorithm:

Algorithm 1:

checkRule (IPS_id, I $rate_i$, cap_i)

The algorithm used for the mitigation shield.

Algorithm 2:

Mitigate (r_i,firstring)

When an attack is identified, FireCol circles around the target to form defensive shields. The IPS detecting the attack informs its upper-ring IPSs in order to defend the attack as adjacent as possible to its source(s), which also applies communication process vertically and enforces the security at its ring level. After an attack against some host has been detected and mitigated, FireCol carry on the exposure process in search of some further sources of attack.

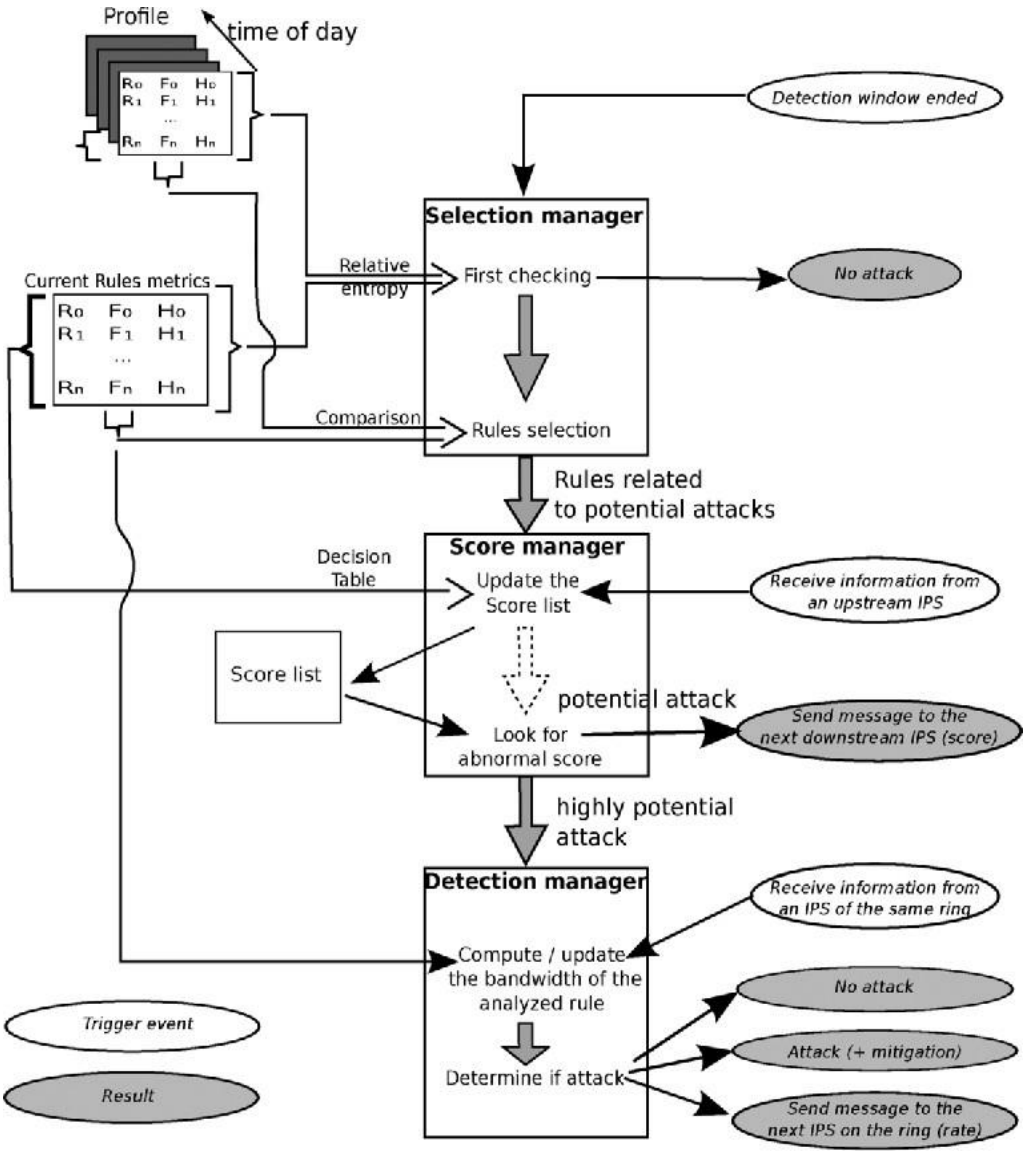

Figure 1. Firecol Architecture

Based on the rules specified, FireCol protects registered subscribers. FireCol rule fits an IP packet pattern and applies to a single IP address or an IP subnetwork. The rule description may include any other information that can be tracked. FireCol is a utility system that customers use the protocol shown to subscribe to. The trusted server contributes an entry along with its time period to live(TTL) and the supported capability to the subscription rule. A private / public key authentication scheme is used to protect all correspondence between subscribers and the server. Customers or the ISP can provide control capabilities. Large companies ' IT providers should be able to provide the required information about their networks. FireCol allows multiple digital security rings to coexist across the same collection of IPSs for multiple customers due to their inherent complete independence.

3.3. DGSOT Algorithm

3.3.1. Procedure

To prevent DDoS attacks from accessing the network, DGSOT is included. The DGSOT algorithm builds a hierarchy by division from topmost to lowermost. The DGSOT enhances the number of clusters at each categorized level, from which the proper hierarchical structure can be found for the underlying data set. It is designed in an underlying data set to discover the correct hierarchical structure. The DGSOT grows in two ways: horizontal and vertical. The DGSOT adds downs in the direction of vertical growth. Only two kids are added to the node in the vertical growth of a node (x). The need is to decide if these two boys, added to node (x), are sufficient to represent the node's proper hierarchical structure. In horizontal growth, we aim to determine the number of these two children's siblings needed to represent the node-related data, x. Thus, during the tree construction process, the DGSOT selects the right number of children (sub clusters) of each node at each hierarchical level. A learning process is invoked during each vertical and horizontal growth in which data is distributed among newly created node children, x. The trust and reputation determine the position of nodes in a hierarchical tree and perceive risks associated with the likelihood of identifying and encountering malicious behavior.

3.3.2. Algorithm

1. Initialization : Start with one root node. Set the root node reference vector in the middle of the packets beings exchanged between RSU's. Compare all packets with the root. Initialize the time parameter t to 1.
2. Vertical Growing : The leaf turns into a node, creating two subnodes or leaves of parent. Initialise the new leaves reference vector with the reference vector of the node Set the new leaves ' horizontal growing flag to true.
3. Learning: Find winner and update winner and neighbourhood comparison vectors.
4. Horizontal Growing: If the horizontal growing stop rule is unsatisfied then the growing horizontal flag is equal to true and add a child leaf tothis node. Delete a child from this node and fake the growing horizontal flag.
5. Repeat steps 1-4 until the energy of all leaf nodes are below the threshold T_R.

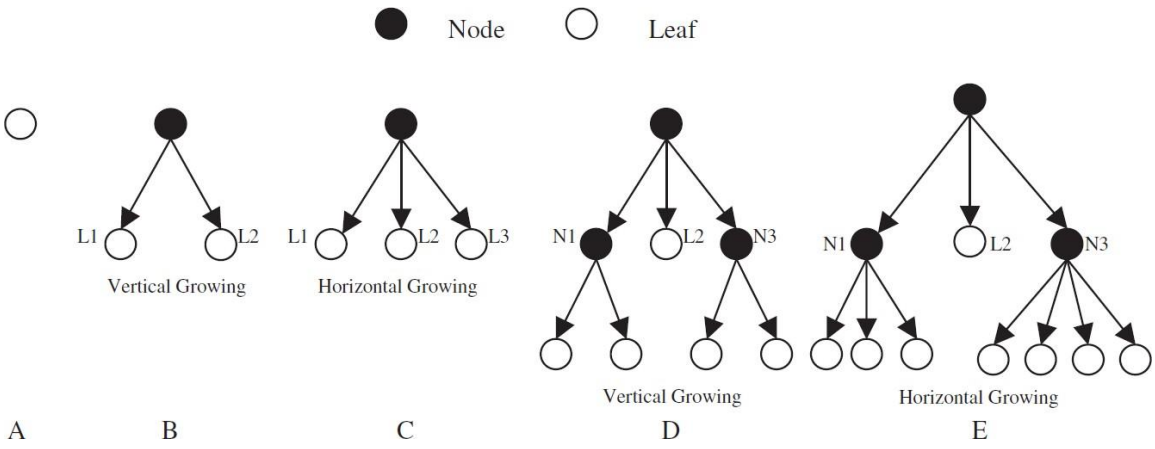

Figure 2. DGSOT Algorithm Illustration

By combining FireCol followed by Dynamically Growing Self Organizing Tree followed architecture, the DDoS attack based intrusion can be detected and prevented on collaborative networks.

3.4. Protocol

The Ad-hoc On-Demand Distance Vector(AODV) routing protocol is being used in this simulation for the wireless transmission of packets. This is used as it will be suitable for the random nodes in VANETS which generates the best possible route for the demanding situation for wireless communication between nodes, RSU's and host. The NS2 has used C++ language for the execution of this protocol.

The proposed method using Firecol detection and DGSOT prevented is implemented in the aodv.h and aodv.cc files of NS2, which is open source software and has the copyright to modify the files as per the requirement. The functions created using these algorithms are called in the input file composed of OTCL language to be executed for detecting and preventing the DDoS attack.

4. Design

The Simulation is performed in Ubuntu 16.04 Virtual Machine(VM) by installing the Network Simulator 2.34(NS2), a simulator tool developed by Carnegie Mellon University which is open source offering rights to modify the coding according to individual's requirement. The programming languages used in NS2 are C++ and Object Tool Command Line(OTCL).

The duplex links are created between router and cloud, router and host. The Public Key Infrastructure is executed by sharing the keys from cloud to host via a router. The keys are shared with all RSU's from host through the duplex links that are created. The E-Firecol is

installed in all the mobile nodes to detect the DDoS. The RSU's frequently authenticates the nodes within its zone, monitor if there are any DDoS attack and send alerts to the reachable nodes using DGSOT algorithm. The cloud which generates keys required for authentication is connected to host through a router. The host sends the keys to the seven RSU's that are created in this simulation. Figure 3 represents the structure of the network.

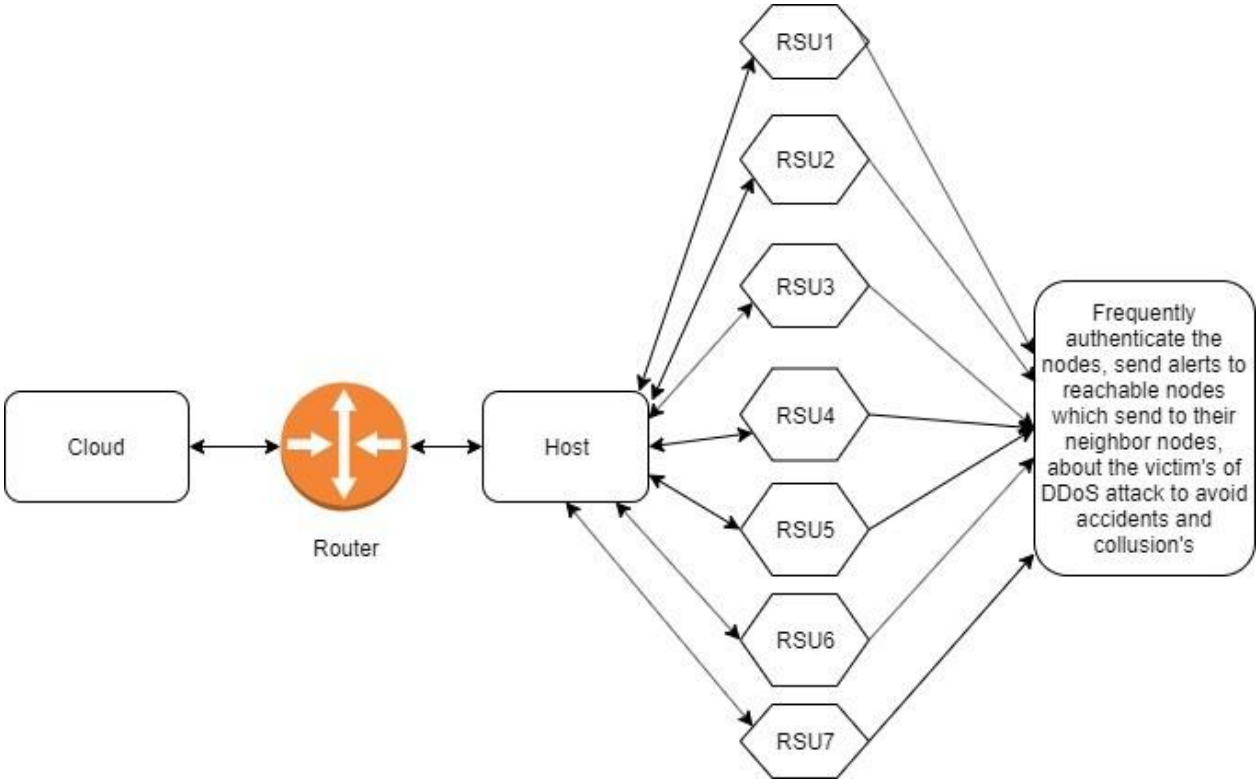

Figure 3. Structure of the Simulation

5. Implementation

The proposed methodologies to detect and prevent DDoS are being implemented in the AODV(An On-Demand Vector) protocol files of NS2 which are located in the aodv folder under NS-2.34 folder where NS2 was installed. The aodv.h and aodv.cc are modified by defining the functions for DDoS attack, to detect DDoS attack by comparing the frequency that is the number of packets sent per second and entropy. The entropy represents the uniformity of the frequency following the E-Firecol algorithm. The DGSOT is implemented on fixed nodes labelled as the Road Side Units(RSU's) which are created using base stations in NS2, when any node that is being attacked detects the DDoS using the E-Firecol which is implemented in all the mobile nodes. RSU monitors the nodes under its zone and transfer's data packets to the nodes that are reachable about the nodes which have attacked by DDoS to avoid collusion's and accidents. The nodes that receive the packets forward it to their nearby nodes and the

process continues until all the nodes receive an alert. Figure 4 represents the requirements and the working process of the simulation.

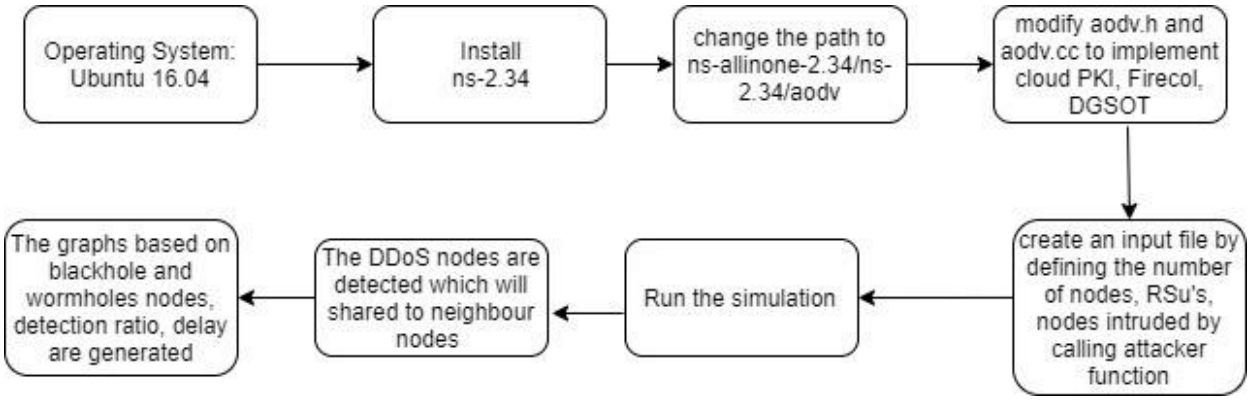

Figure 4. Simulation of the Proposed method

6. Results and Evaluation

Simulation experiments were performed using NS-2.34. The different parameters are used to show system efficiency to analyse flooding DDoS attacks. These delay parameters, average path size, packet delivery ratio, true negative ratio, false detection ratio and overhead routing are considered for the different network parameters.

Table 1. Simulation Parameters

Parameter	Value
Type of Channel	Wireless
Radio Propagation	Two ray ground
Antenna	Omni-directional
Mac	802.11
Area	1000*1000
Mobility	10 m/s
Pause Time	10 sec
Traffic agent	Constant Bit Rate (CBR)
Transport Agent	User Datagram Protocol
CBR	10kbps

VANET's experimental results were predicted using the wireless network that is used as the channel type. The radio wave propagation method is used in a series to estimate the propagation of radio in the VANET network. For the reason of covering the varying degree of coverage in all directions, the Omni-directional antenna is used. The high dynamic node motion has been interpreted by using the random waypoint model, where vehicle movement and position changes over time are illustrated. The simulation parameters illustrated in Table 1. Figure 5 depicts the packet delivery ratio with E-FireCol approach and without E-Firecol. The proposed method shows the outperformance in delivering packets.

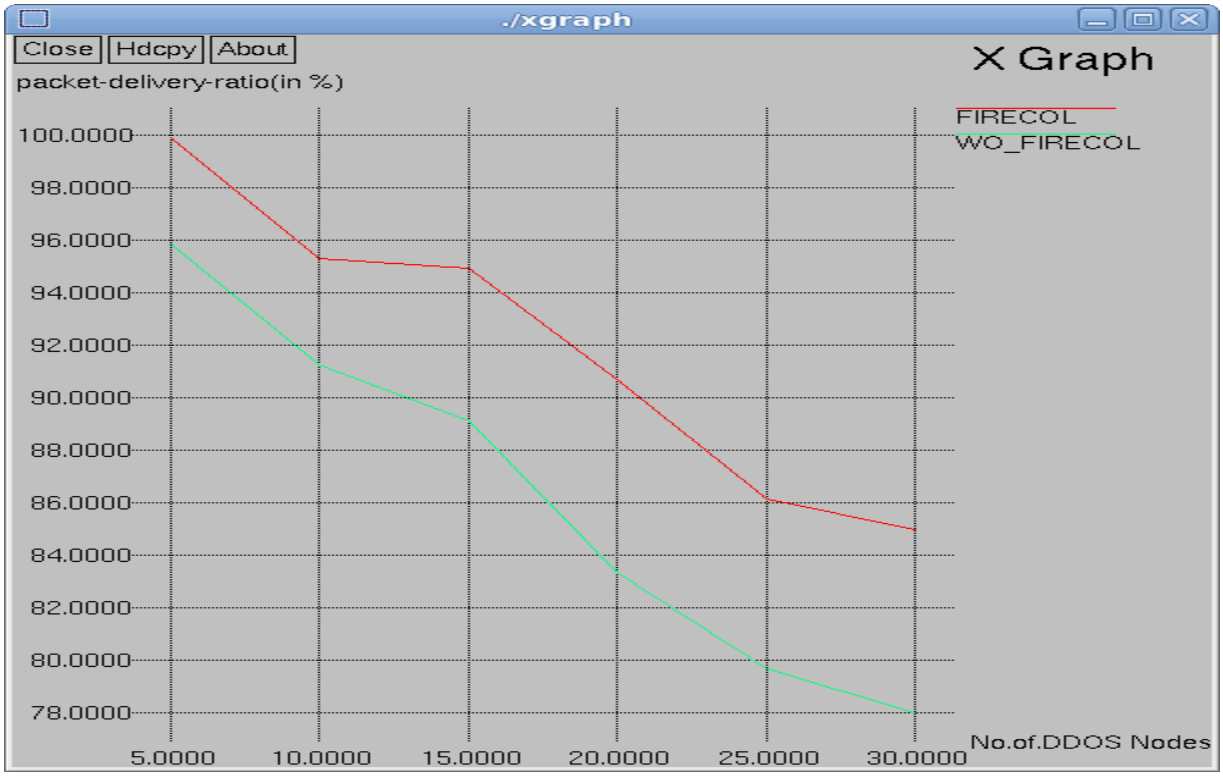

Figure 5. Packet Delivery Ratio Comparison - FireCol Vs WO_FireCol

Overhead routing is the number of routing packets required to access the network. Figure 6 shows the overhead routing performance comparison of FireCol method. The proposed method shows better performance in detection of DDoS nodes with lower overhead in routing.

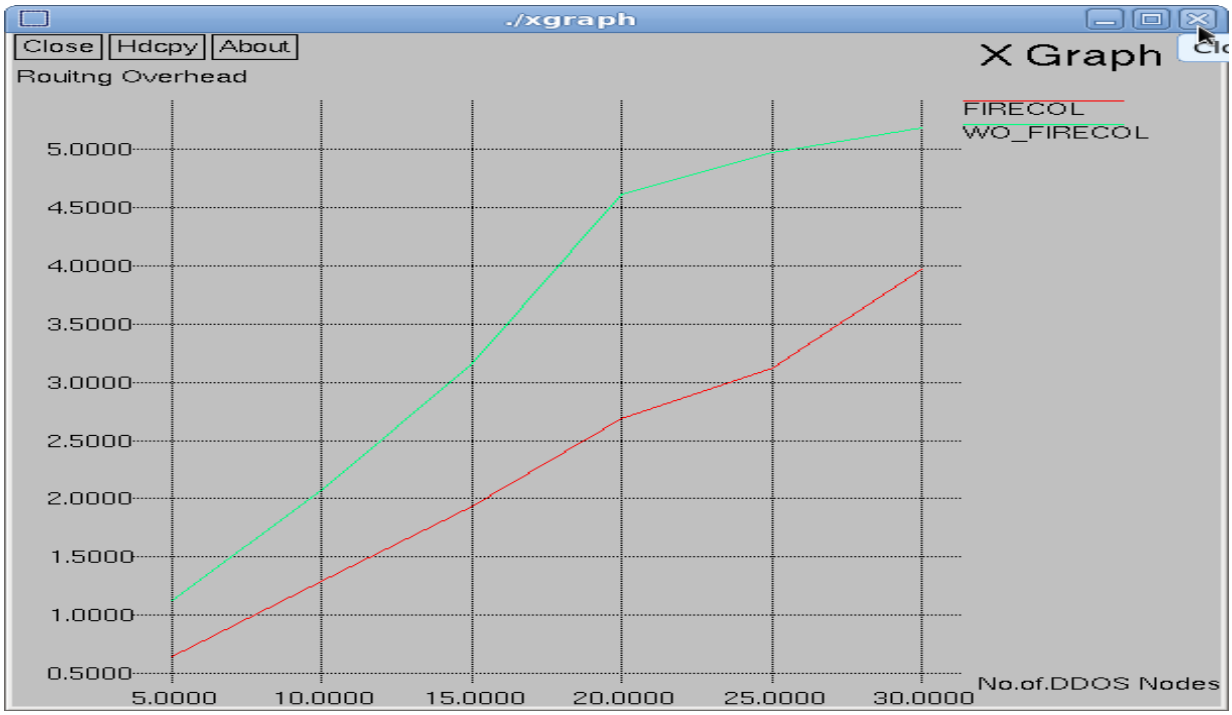

Figure 6. Routing overhead Comparison - FireCol Vs WO_FireCol

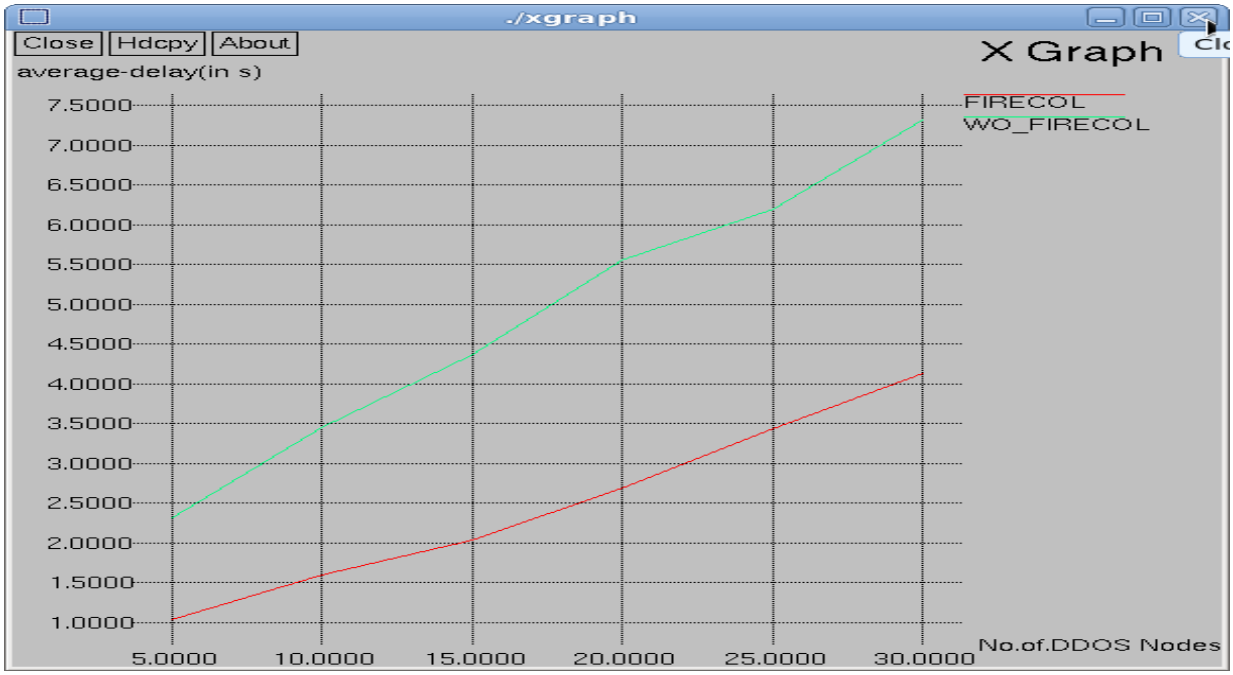

Figure 7. Average Delay Comparison - FireCol Vs WO_FireCol

Average delay refers to the time taken for a packet to be transmitted across a network from source to destination. Figure 7 displays the average delay of existing and proposed approach and shows the outperformance of average delay using proposed FireCol method. The true negative rate is the percentage of persons with a known negative condition for which the result of the test is negative. Figure 8 depicts the true negative ratio and Figure 9 shows the false positive ratio of FireCol based DDoS Detection where False positive ratio (or false alarm

ratio) is the probability that the null hypothesis is wrongly dismissed for a specific test. Detection Rate used to evaluate the detection system's ability for malicious nodes and attackers to be perceived. Figure 10 depicts the detection ratio of FireCol.

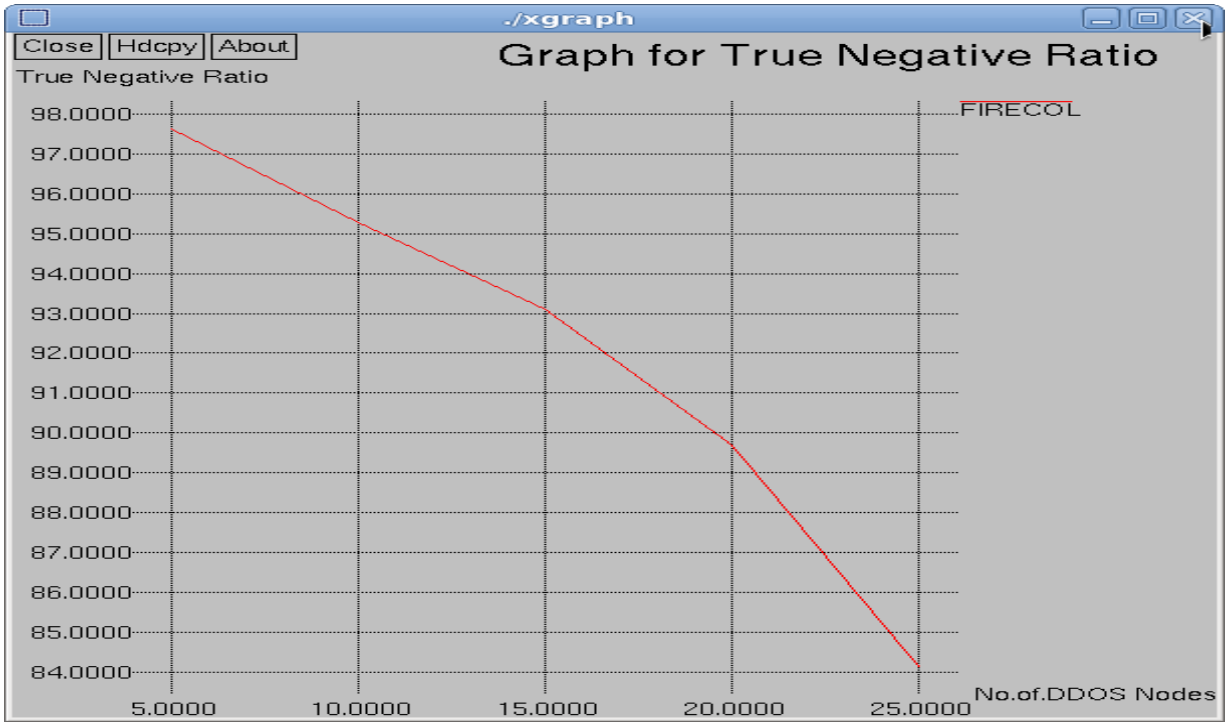

Figure 8. True Negative Ratio - FireCol

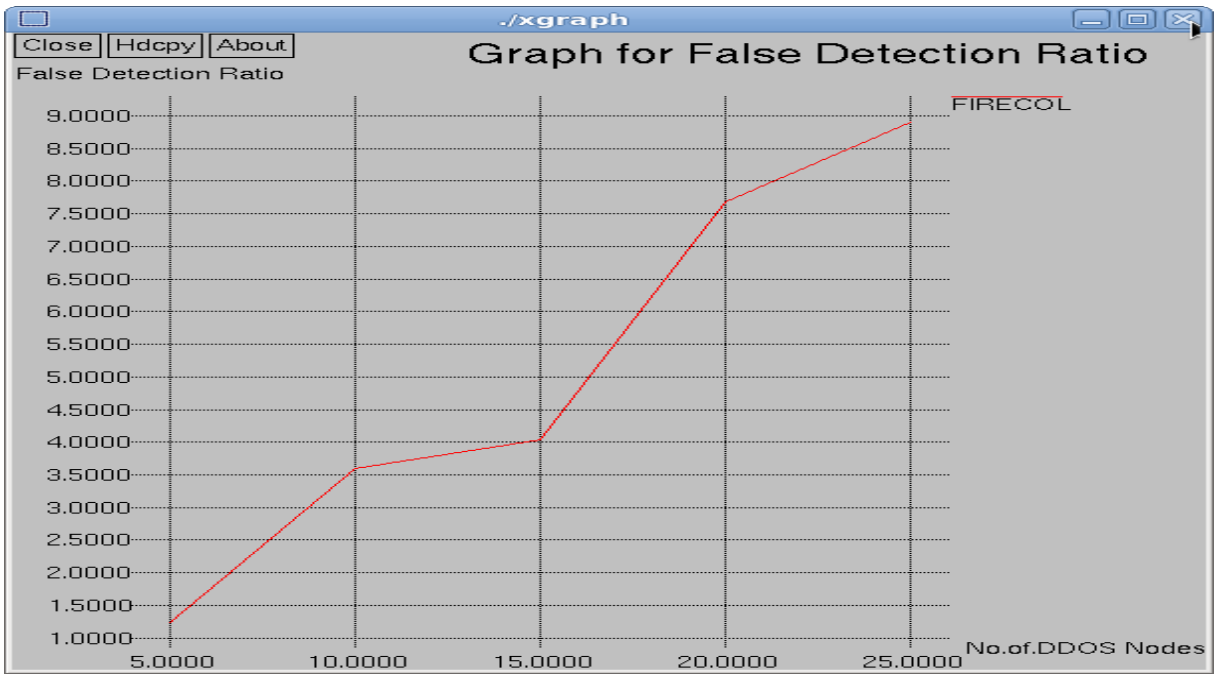

Figure 9. False Detection Ratio - FireCol

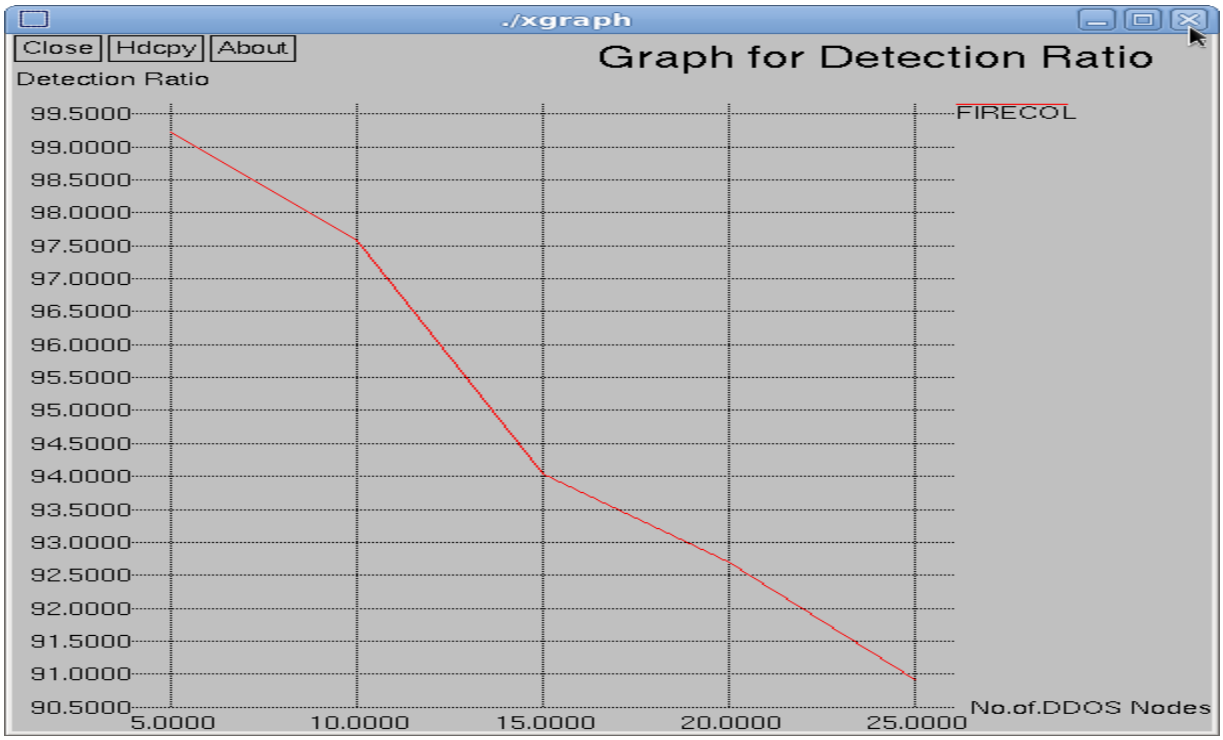

Figure 10. Detection Ratio - FireCol

Figure 11 shows the transfer of packets from source to destination and ongoing packets are sent to the source by the attacker nodes. This FireCol detects attacks that are bound to control the level of the structure. The Figure 5-10 shows the comparison of detecting number of DDoS nodes between FireCol and WO_FireCol. The proposed FireCol-DGSOT detects more DDoS attacks compared to default without Firecol by observing the graphs.

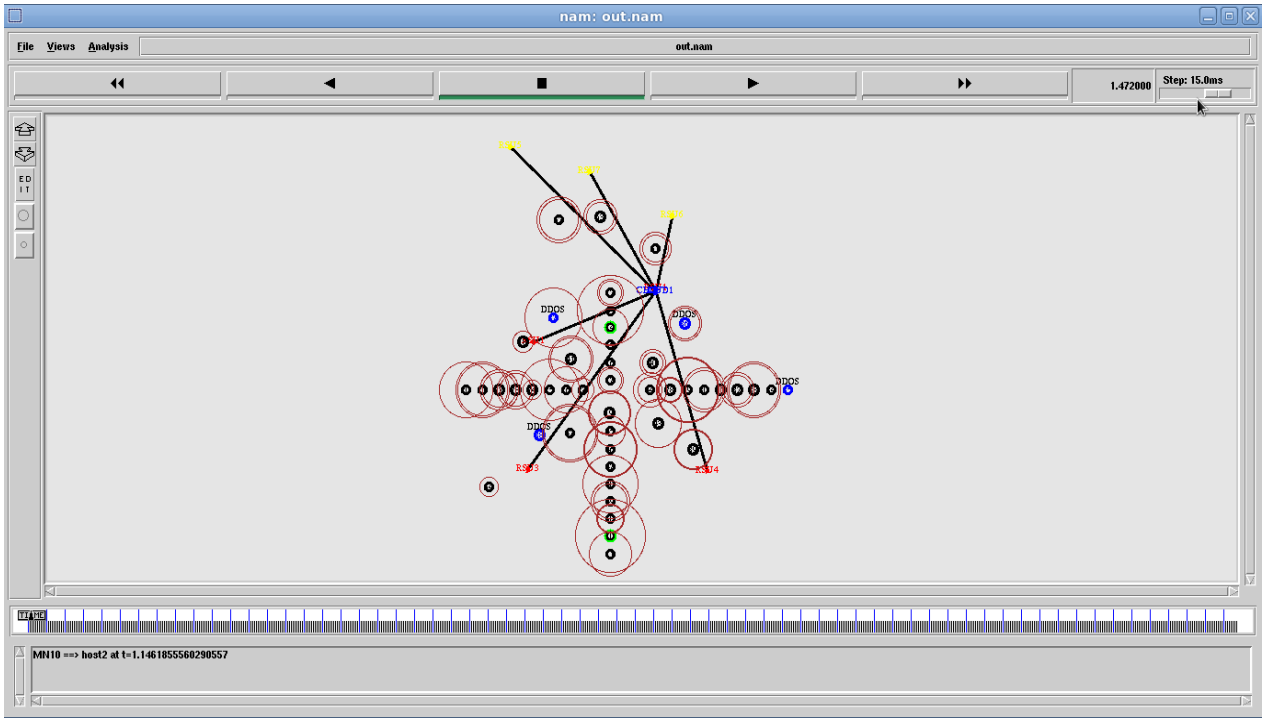

Figure 11. Nam - Proposed Firecol-DGSOT Simulation

7. Conclusion and Future work

DoS attacks in VANET attempt to block the channel of communication by continuously sending unnecessary packets of data so that legitimate nodes can no longer procure or use their services. A Distributed Denial of Service (DDoS) attack is more serious because of the bigger scale of the attack. E-FireCol presents an ISP-level collaborative system to identify flood-based DDoS attacks as close to the source(s) of the attack as possible. A Intrusion Detection and Prevention System is designed in this paper to detect DDoS attacks based on E-Firecol and prevent them by Dynamic Growing Self Organizing Tree (DGSOT) on collaborative networks by using frequency and entropy(uniformity of frequency) as factors. Results of simulation in NS2 show that DGSOT with E-Firecol leads to better detection and prevention of intrusion. From the results obtained using E-Firecol and DGSOT, reliability metrics based on delay parameters, average path size, packet delivery ratio, true negative ratio, false detection ratio, and overhead routing the performance is better than the default system.

Detecting DDoS in a complex situation by considering different factors such as distance between vehicles, road traffic, threshold of requests per vehicle in E-Firecol to detect along with different prevention algorithms in NS3(Network Simulator-3) or GNS3(Graphic Network Simulator-3) and SUMO, the software tools which can be used to create virtual realistic roads with signals and vehicles. Preventing DDoS in a realistic scenario using the NS3 or GNS3 with SUMO is proposed as the future work for research in VANETS.

References

1. Muhammad Sameer Sheikh & Jun Liang 2019, “A Comprehensive Survey on VANET Security Services in Traffic Management System”, Wireless Communications and Mobile Computing, Volume 2019, Article ID 2423915
2. R.Priya, N. Sivakumar & M. Thirumaran 2017, “A Review on Security Attacks in Vehicular Ad hoc Network”, International Journal on Future Revolution in Computer Science & Communication Engineering ISSN: 2454-4248 Volume: 3 Issue: 12.
3. HalabiHasbullah, Irshad Ahmed Soomro & Jamalul-lail Ab Manan 2010, “Denial of Service (DOS) Attack and Its Possible Solutions in VANET”, World Academy of Science, Engineering and Technology ,41p 411-415.
4. Al Falasi, H & Barka, Ezedin 2011, "Revocation in VANETs: A survey," Innovations in Information Technology (IIT), 2011 International Conference on , pp.214,219, 25-27 April.
5. Subir Biswas, JelenaMiˇsi´c & Vojislav Miˇsi´c 2012, “DDoS Attack on WAVE-

enabled VANET Through Synchronization", Communication and Information System Security Symposium -Globecom 2012.

6. François, J, Aib, I & Boutaba, R 2012, "FireCol: A collaborative protection network for the detection of flooding DDoS attacks", IEEE/ACM Trans. Netw. (TON), 20, 1828–1841.
7. Karnan verma, Halabi Hasbullah & Ashok kumar 2013, "Prevention of DoS Attacks in VANET", Journal of wireless personal communications, Volume 73, Issue 1, November
8. Ravi chandra & Madhavi gudavalli 2013, "E-FireCol to Detect Multiple DDOS Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 12, December.
9. Munazza Shabbir & Muazzam A. Khan 2016, "Detection and Prevention of Distributed Denial of Service Attacks in VANETs", 2016 International Conference on Computational Science and Computational Intelligence.
10. S. S. Manvi & S. Tangade 2017, "A survey on authentication schemes in VANETs for secured communication," Vehicular Communications, vol. 9, pp. 19–30.
11. H. Hasrouny, A. E. Samhat, C. Bassil & A. Laouiti 2017, "VANet security challenges and solutions: A survey," Vehicular Communications, vol. 7, pp. 7–20.
12. Pavan Kumar B V S P, S.S.V.N. Sarma & C. Lokanatha Reddy 2019, "Classification of DDOS Attacks in VANETs based on Distributive Collaborative Framework", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-6S3, April.
13. Chaitanya Rudraraju, "Simulation Study of Preventing Distributed Denial of Service(DDoS) in Vehicular ad-hoc Networks(VANETS) Using Intrusion Detection and Prevention Systems(IDPS) by Merging with Cloud".