Research Thesis

Academic Internship
MSc Cyber Security

Uppili Srinivasa Raghavan
Student ID: x18133312

School of Computing
National College of Ireland

Supervisor: Christos Grecos

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Uppili Srinivasa Raghavan
Student ID:	X18133312
Programme:	MSc Cyber Security
Year:	2019
Module:	Academic Internship
Supervisor:	Christos Grecos
Submission Due Date:	12/12/2019
Project Title:	Detection of Denial of Service (DoS) Attacks in VANET using Filters
Word Count:	5532
Page Count:	19

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:	29th January 2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

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

Detection of Denial of Service (DoS) Attacks in VANET using Filters

Uppili Srinivasa Raghavan
x18133312
MSc in Cyber Security

Abstract

Vehicular Ad-Hoc Networks (VANET) are considered as a subset of Mobile Ad-Hoc Networks (MANET). VANET is mainly used for the construction of an intelligent transport system. VANET enables communication between the vehicles (V2V) and vehicles to infrastructure (V2I). VANET can be used to coordinate the traffic, improve safety measures, support the drivers for hassle-free driving. It plays a major role in building smart cities in the near future. VANET is vulnerable to a number of security issues among which the DoS attack is a major part. DoS attack in VANET involves a malicious node flooding a huge amount of traffic using spoofed identities. This, in turn, may disrupt the services of vehicles in the network. The detection of the attack becomes very difficult due to fake identities. The detection scheme uses a cuckoo filter and IP detection technique to detect the attack in the network. Once the attack is detected it generates a broadcast message to all the other vehicles that are present in the network.

1 Introduction

Vehicular ad-hoc networks are usually described as a network on wheels in which the vehicles are considered to be the components of the system. VANET has some specific characteristics such as high mobility, rapid change in topology, no power constraints, localization, a huge number of nodes, etc. VANET is usually a special kind of MANET where the vehicles are used as nodes that helps to communicate among themselves (V2V) and nearby infrastructures(V2I). Every vehicle will have an On-Board-Unit (OBU) which helps the vehicles to communicate among themselves and with the nearby Road Side Units (RSU). VANET is considered to be one of the largest ad-hoc networks around the world. The advancements in the vehicular industries and wireless technology VANET has a promising future in research fields [1].

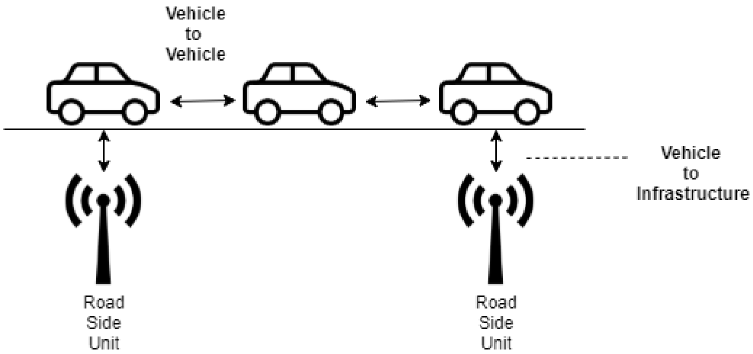


Figure 1: VANET architecture

With the increasing number of vehicles in road hassle-free driving has become one of the major areas of concern. VANET helps in facilitating safe, secure and comfortable driving. The inter-vehicle communication helps to in traffic info sharing, cooperative driving, internet-enabled cars, navigation mechanisms. It plays a pivotal role in building smart cities and intelligent transport systems in order to ensure security. VANET applications are used in two areas either they are safety-related or comfort-related. The safety-related applications are used to ensure security and protect the public. The major aim of the applications is to transfer the messages to the intended receivers when there is a situation of danger and to avoid collisions. On the other hand, comfort applications are used to provide internet access, entertainment apps, and E-toll collections, etc. The benefits of these value-added services in VANETS can generate many business opportunities [2]. But on the other hand, it has a lot of challenges and issues which make it a double-edged sword. Some of the most common challenges in VANETs are:

- Rapid change in topology.
- Highly dense environment.
- Connectivity variations.
- Security and Privacy.
- Quality of service.

Among all the above challenges security is considered to be one of the major ones overcome. The challenges are security is given a thought of over and over again since it is life-critical [3]. The vehicular network is vulnerable to various types of attacks some of them are:

Bogus information Attack is used to send false information to the vehicles which may cause adverse effects. In this case, the attacker can inject false information about a traffic jam which is not existing or accident that has not occurred and diver route.

Sybil Attack is where an attacker uses multiple identities at the same time. These multiple false impersonations will create as if there are more vehicles on the road. These fake identities can be used to play any type of attack in the network.

Black hole Attack is where a vehicle refuses to be a part of the network or it forms a black hole where all the traffic of the network is redirected to that particular vehicle which in turn could cause loss of data.

Alteration Attack is where the attacker alters the data that is being transferred. This can eventually cause a delay in transmission, replaying of existing data, alteration of the original data.

Social Attack is where the attacker sends inappropriate messages in order to confuse the driver. It may involve unethical and abnormal messages which annoy the victim. The main aim of the attacker is to disturb the victim which will indirectly affect the driver and may cause any life-critical problem.

Timing Attack is where the attacker adds a time slice to the message in order to delay its delivery to the receiver. This may be disastrous since the message may involve any life-critical information. The time is considered as one of the crucial factors in vehicular networks.

Jamming Attack is where the attacker uses radio signals to disrupt network communication. Due to this, the signal to noise ratio in the network will increase which may cause service unavailability, hence the security of the entire network in under huge threat.

Among these attacks Denial of Service, the attack is considered to be one of the destructive ones since the amount of damage it could cause to the network.

Denial of Service attack is an interruption in the service of user access which is done with malicious intent. The attack involves one node flooding the victim with a large number of packets. The main objective is to overload the victim's resources. This will make the node unavailable for the purpose of communication and will not allow the node to communicate with other nodes within the network. As safety is the primary concern of the road users Denial of service attack in the vehicular network is life-critical. The attack becomes very difficult to counter since it can be initiated in different patterns.

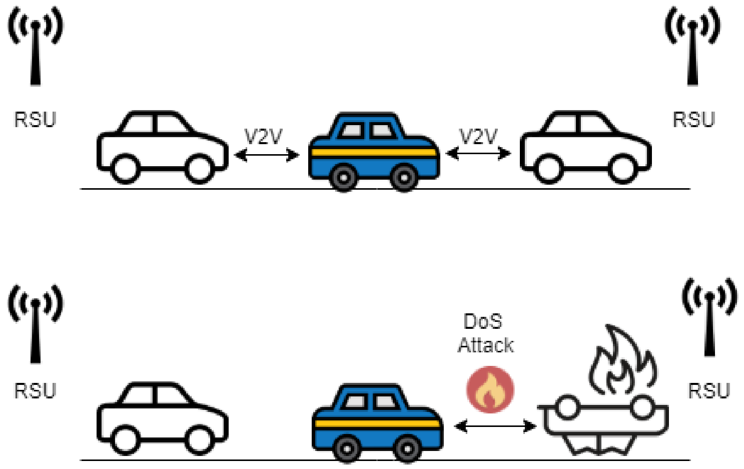


Figure 2: DoS attack in VANET

In order to secure the from the devastating Denial of Service attack, we require an effective detection system in VANET. A Cuckoo filter-based detection is used to detect the attack in the vehicular network. The cuckoo filter is the most efficient probabilistic data structure when compared with other filters. Cuckoo filters an extended version of the design of bloom filter which offers an additional operation deletion, limited counting, and abounded false positive rate, while it still maintains a similar space complexity. They filter uses cuckoo hashing to resolve collisions and for the purpose of storage uses essentially a compact cuckoo hash table. The next section will review some of the previous works that were done for the detection and prevention of Denial of Service attacks in VANET.

2 Related Work

2.1 Cryptographic countermeasures

In a research was done by Jonathan Petit [4] in which he uses the Elliptic Curve Digital signature algorithm (ECDSA) for the purpose of verifying authentication in VANET. The communication medium is Wireless Access in Vehicular Environment (WAVE) which demands the use of PKI in order to encrypt all the application messages. The ECDSA yields authentication with the help of issuing digital signatures. This technique ensures the integrity of the message is not broken. There is a trade-off between the security of an application to the performance of the application. Since the proposed technique provides strong security it would cause a computation overhead which makes it infeasible when used in real-time.

Studer A, Bai F, Bellur B, Perrig A [5] proposed a unique combination of TESLA++ and ECDSA to protect the VANET messages which are called VAST. This combination helps to provide authentication in a timely fashion and protects the vehicular network from the DoS attack. The technique also provides non-repudiation along with message authentication with some acceptable processing overhead. It uses certificate management together with VAST to secure the network and to effectively manage authentication of a message without exposing the identity of the vehicles present in the network. In a network where there are fewer vehicles more number of signatures will be used which will lead to computational overhead which makes this technique inefficient.

Recent research by Hsiao HC, Studer A, Chen C, Perrig A, Bai F, Bellur B, Iyer A [6] uses Fast authentication (FastAuth) and Selective authentication (SelectiveAuth) which provides both authenticity and non-repudiation in broadcast communication. This method focuses on preventing the flooding of signatures such as multiple signature verification requests which will deplete the resources. FastAuth uses the ECDSA algorithm which is 50 times faster to verify authentication by exploiting the ability to predict future beacon messages. SelectiveAuth helps in preventing the bogus messages to spread to different applications. It finds the malicious node and isolates that node by using less computational power. When a packet is lost it becomes difficult to perform authentication. This is arguably one of the best cryptographic defense techniques that are proposed but the usage of this application in real-time becomes questionable.

In 2015 yu C, Gu D, Zeng Y, Mohapatra P [7] proposed Predication Based Authentication (PBA) as a formidable technique to prevent Dos attacks. Unlike other authentication mechanisms, it is considered to be lightweight since it utilizes symmetric key cryptography. This technique also helps in reducing the packet loss during data transmission between high-speed vehicles. It uses beacons signals with which it predicts the sender's message during emergency situations. One striking feature of this method is it also protects the network from computation based DoS attacks. The computation overhead is comparatively less than other methods since it uses a shorter form of MAC which in turn reduces the overload in terms of storage. Since security and privacy go hand in hand these techniques also have few drawbacks.

2.2 Packet Detection based Countermeasures

RoselinMary S, Maheshwari M, Thamaraiselvan M [8] proposed the Attacked Packet Detection Algorithm (APDA) to secure the vehicular network from being DoS attack. Every vehicle in the network will have an On-Board Unit in which this algorithm will be integrated. When the vehicles communicate with Road Side Units the details about the vehicles are recorded. Most of the algorithms try to defend the attack after the verification time this causes time delay during the detection process. In this technique, the detection is done even before the verification process which will reduce the time delay. All the packets that are transferred between the sender and receiver are recorded. The attacked packets are classified based on the velocity, frequency, and speed. This method fails to detect packets when it receives multiple invalid requests from numerous vehicles which make will affect the security of the vehicular network.

Singh A, Sharma P [9] proposed a novel scheme of an enhanced version of the Attacked Packet Detection Algorithm which is (EAPDA). The flaws in ADPA are addressed in EADPA which focuses on the network performance when the network undergoes an attack. This algorithm is also integrated with Road Side Units which verifies the messages. As the previous research has mentioned the Road Side Units records the details of the vehicles it also keeps track of the amount of data that is transferred. It monitors the behavior of the node if there is any malicious activity from a particular node the respective node will be isolated or removed from the network. The malicious nodes are found during the verification time so that it becomes more efficient than the previous method. It is considered to be one of the formidable techniques in comparison with the previous technique in terms of false-positive rate since no legitimate node will be affected and removed from the network.

Recent research by Quyoom A, Ali R, Gouttam DN, Sharma H [10] which uses the Malicious and Irrelevant Packet Detection algorithm (MIPDA) for the protection of the vehicular network from DoS attacks. As the previous algorithms, it is also associated and integrated with Road Side Units. It finds the position of the node it detects the malicious packets that are transferred, Similar to the APDA it also uses speed, frequency, velocity of the vehicle to find the malicious packets If the value of frequency and velocity are high then the packet is considered to be malicious, if velocity and frequency are normal then it is a legitimate packet and if the velocity and frequency are less then the packets is considered to be irrelevant. The method is considered to be a significant defense technique with less computational overhead and a false positive rate when compared to the earlier techniques.

2.3 Diversion based Countermeasures

Patel KN, Jhaveri RH [11] in 2015 proposed a scheme that uses the Anti-Colony Optimization (ACO) algorithm which is one of the significant methods to defend against the DoS attack. .The routing algorithm helps in the transmission of packets based on the reliability and trustworthiness of the neighbor node. The data exchange is done with the help of agents called (Ants) which helps to find the shorting route from source to destination. The method secures the routing process in order to segregate the malicious node in the same path of the destination. The node that has the least reliable is malicious and is isolated from the vehicular network for safety reasons. The technique is one of the best defense against the DoS attack in terms of average end-to-end delay, energy consumption, optimized routing, packet delivery ratio. On the other hand, the issue is to handle the overhead caused to find and update the trust of every node in the network.

Research by Hasbullah H, Soomro IA [12] use a frequency hopping technique to protect the vehicular network from the DoS attack. Every vehicle present in the network will consist of an On-Board Unit. The On-Board Unit will be connected to various technologies such as Wi-Fi, WiMAX, Zig-Bee in a different frequency. The On-Board Unit will switch from one connection medium to the other once the network is detected with the DoS attack. Hence the attack is prevented and the messages diverted through a different communication medium. The frequency of the medium is changed when the attack is detected with the help of a frequency hopping technique. The main feature of this technique is to switch from channel to others when one channel is jammed. The system is integrated with the On-Board Unit which is in the vehicle and does not involve any other technologies which in turn may affect the performance of the On-Board Unit and can cause performance overhead.

2.4 Recent defense Countermeasures

In 2016 Nyabuga SM, Cheruiyot W, Kimwele M [13] used Particle Swarm Optimization (PSO) algorithm as a technique to defend against the DoS attack. This technique was inspired by the social behavior of insects and animals. The concept is based on solving a particular problem as a group rather than doing it individually. In PSO every member of the population is considered as a particle and the entire population is considered as a swarm. Every particle moves in a random velocity in search of a proper position during which it captures the routing details. The particles are strongly influenced by their peers during the search for a proper position to communicate with their peers. By changing their velocity randomly the particles find a suitable optimal position to communicate with their peers. Their particles undergo three major processes such as evaluating, comparing, imitating during the process of finding a suitable position. When compared with the genetic algorithm PSO is more valuable in protecting the network from various attacks.

Jeffane K, Ibrahimi K [14] is 2016 proposed that the values of the Packet Delivery Ratio (PDR) for the detection of DoS attack in VANET. This technique is majorly utilized in Short Range Communications especially in the physical and MAC layer. The values in the Packet Delivery Ratio are recognized to be critical in terms of the detection of the DoS attack.The method helps to find malicious IPs and create a blacklist to protect the network from these nodes. If the packet delivery ratio is decreasing then the node is considered to be subjected to an attack. If the packet delivery ratio is high then the node is considered to be malicious, If the packet delivery ratio is on an average then the node is considered normal. This method is one of the efficient techniques that can detect DoS attacks within seconds and blacklist the nodes.

Bouali T, Sedjelmaci H, [15] used a Distributed prevention methodology using a Kalman filter to prevent the DoS attack. This technique uses Kalman filters to carefully study the behavior of vehicles carefully and the vehicles are classified on the basis of their behavior respectively. Based on the trust factors of each vehicle they are classified into three different groups such as white, grey and black. The usage of distributed architecture helps in identifying malicious vehicles rapidly. By virtue of that this method helps in achieving a higher Packet Delivery Ratio. The major drawback of this methodology is when the density of the vehicles is high. The accuracy of detecting the malicious vehicle become lesser when the vehicles are in the cluster.

In 2013 Verma K, Hasbullah H [16] proposed a robust technique as a countermeasure to detect DoS attack in VANET using probabilistic data structure Bloom filters. The scheme is integrated with the edge devices present in each and every vehicle in vehicular networks. There are three different stages involved in the process of detection, the first phase where the IP addresses are checked, the second phase the malicious IP address is detected and recorded and the final phase is where the Bloom filter is used for the purpose of filtering the malicious IP's. Once the malicious IP's are found a reference link and an alarm is sent to other vehicles in the VANET. This technique is one of the robust as of now for the prevention of DoS attacks in VANET.

All the existing solutions that are discussed above to prevent the attack in VANET are considered to be optimistic. Some of them are used integrated with road side units and some are integrated with on board units or edge devices that are present in the vehicles. The cryptographic countermeasures that are proposed as discussed have latency issues and computational overhead. The packet filtering and diversion algorithms are very promising but they bring various drawbacks along which causes a delay in the detection. The inspiration to this research is the one based which is Bloom filter-based detection which is possibly the most efficient defense method currently to detect the DoS attack. The security of a vehicular network is considered to be a critical part since the number of vehicles involved is high in proportion with rapidly changing topology, an attack will cause huge devastation to the network. So to protect the network in all forms we need a bulletproof solution that will overcome the shortcoming of the existing solutions.

3 Methodology

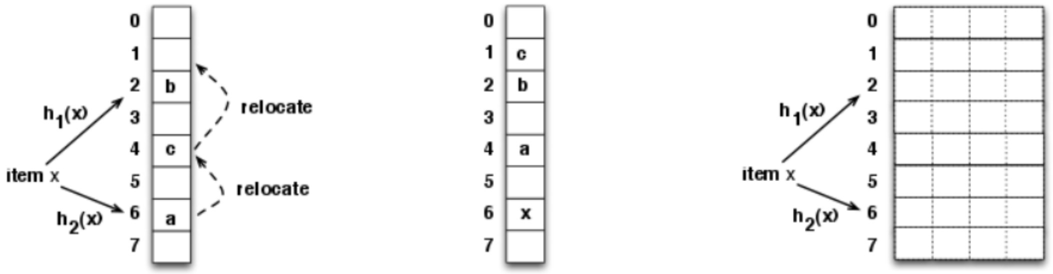
The earlier sections discussed the pros and cons of the existing methods that are used to detect DoS attacks in VANET. This section talks more about the proposed effective defense strategy along with its specification and methodology. The technique involves two techniques which are cuckoo filter and IP detection.

3.1 Cuckoo Filter

The cuckoo filter is an eminent probabilistic data structure that is used to process a large volume of data. The Cuckoo filter is considered to be an extended version of Bloom filters [17]. The cuckoo filter will remedy the deficiencies of the bloom filter. Some of the attractive features of the filter are the offering of deletion operation, less false positive rate, avoid collision using cuckoo hashing. The cuckoo filter uses the cuckoo hash table to store the fingerprints of the items and not the items that are to be inserted. The fingerprints are represented in the bitstream that we get after the item is hashed. When an item is inserted it is mapped to two possible buckets among the array of buckets in the cuckoo hash table which is based on the two hash functions [18]. The buckets are configured to save fingerprints that are variable in number.

3.2 Cuckoo filter algorithm

The Cuckoo filter algorithm is consists of three different operations *insertion*, *deletion* and *look-up* operations.



(a) before inserting item x

(b) after item x inserted

(c) A cuckoo filter, two hash per item and functions and four entries per bucket

Figure 3: Cuckoo Filter

Algorithm 1 Cuckoo Filter Algorithm

```
Insertion
$f$ = fingerprint($x$);
$i1$ = hash($x$);
$i2$ = $i1$  hash($f$);
if f bucket[i1] or bucket[i2] has an empty entry then
    add $f$ to that bucket;
    return Done;
// must relocate existing items;
$i$ = randomly pick $i1$ or $i2$;
for $n$ = 0; $n$ ¡ MaxNumKicks; $n$++ do
    randomly select an entry $e$ from bucket[$i$];
    swap $f$ and the fingerprint stored in entry $e$;
    $i$ = $i$  hash($f$);
    if bucket[$i$] has an empty entry then
        add $f$ to bucket[$i$];
        return Done;
// Hashtable is considered full;
return Failure;

Deletion
$f$ = fingerprint($x$);
$i1$ = hash($x$);
$i2$ = $i1$  hash($f$);
if bucket[$i1$] or bucket[$i2$]has $f$ then
    remove a copy of f from this bucket;
    return True;
return False;

Look-Up
f = fingerprint($x$);
$i1$ = hash($x$);
$i2$= $i1$  hash($f$);
if bucket[$i1$] or bucket[$i2$] has $f$ then
    return True;
return False;
```

3.3 Cuckoo Hashing

Cuckoo hashing is used for handling collision in the probabilistic data structures. The cuckoo hashing uses two hash functions for each key and the values are assigned to one among the two buckets. Once the item is hashed it checks the first bucket if it is empty then the item is inserted. If the first bucket has an item it inserts the item in the second bucket. If the second bucket is occupied by any item it eliminates the previous item to accommodate the new item. The process happens for every item that newly entered. During this process, there is a minimal chance that we may enter into an infinite loop during adding and removing items. In order to prevent the issue we need to log the bucket entries, but the only way to come out of the loop is to rebuild the hash table. It is also called as partial key cuckoo hashing and involves the following steps for item insertion [17, 18].

- Insert a new key K.
- Process the hash for key k where h(k)=k_h using the first hash function .
- Check whether the first bucket is free if so place the hashed value k_h in it.
- If the first bucket occupied then process the key with second hash function on k_h which has the value of first hash function where g(k_h)= k_{h_g}.
- Apply XOR function to both the hash values k_h and k_{h_g} to get the key for the second bucket which is k_g.
- Look-up the second bucket for completing the hashing function.

The reverse of the above steps will provide the bucket and the fingerprint. It is considerably easy to compute and process the location of the other bucket which in turn enables the cuckoo filter to store f-bit fingerprints and save the storage space.

3.4 IP Detection

The dynamic nature of the vehicular network makes it difficult to detect the DoS attack. The IP detection technique helps to store the IP address and monitors malicious traffic. This process takes place while a packet is transferred from source to destination. The detection technique monitors the suspicious traffic pattern of the entire network. There are two important phases in the detection process one is the detection phase and the other is the cuckoo filter phase. The final result of the process purely depends on the first phase where the traffic is monitored and the IP address are collected. All the incoming and outgoing traffic to the network are recorded and monitored. The first phase is where it decided whether the node could possibly affect the network by observing the traffic patterns generated by the node. Based on this the decision is taken at the second stage. The cuckoo filter phase which includes the hash function which is the final stage. From the information collected by the first phase of the detection technique if any malicious IP is found then an alert to all the other vehicles is sent since the filter has a table with all the vehicle's IP address.

4 Design Specification

The design involves two important techniques of the detection of DoS attack in VANET. The first phase is IP detection where the packets are monitored for suspicious activity. The second phase involves the cuckoo filter where the decision is taken. Both these techniques are combined together to detect the attack at a minimal time and alert other vehicles to prevent further damage in the network.

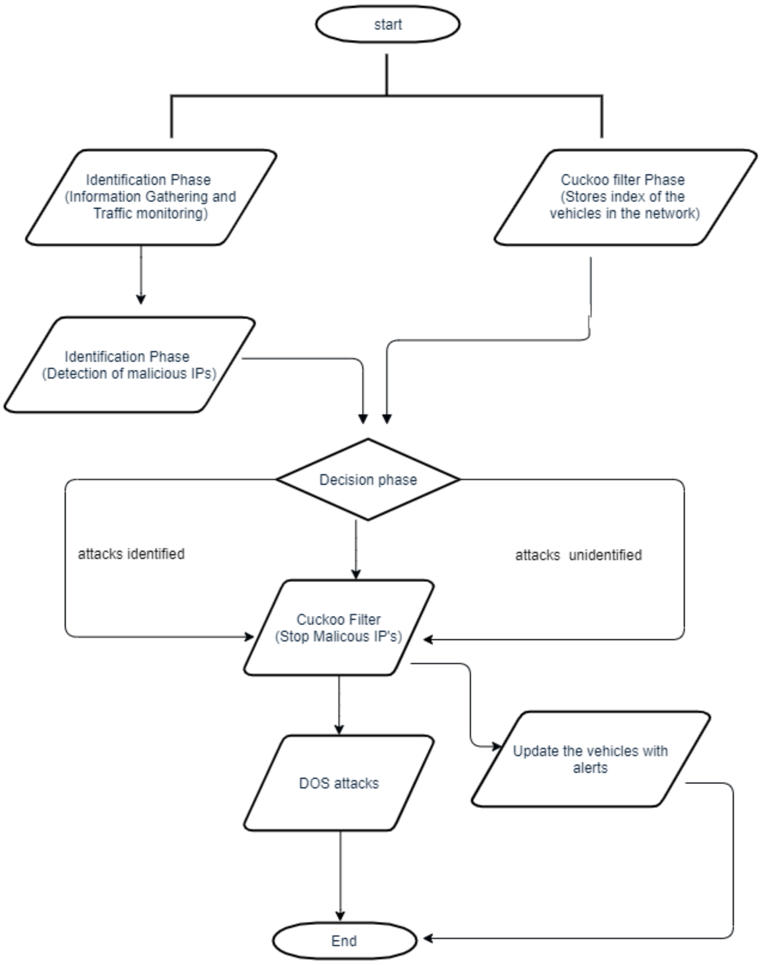

start
Identification Phase (Information Gathering and Traffic monitoring)
Cuckoo filter Phase (Stores index of the vehicles in the network)
Identification Phase (Detection of malicious IPs)
Decision phase
attacks identified
attacks unidentified
Cuckoo Filter (Stop Malicous IP's)
DOS attacks
Update the vehicles with alerts
End

Figure 4: Process of Detection

5 Evaluation

For the purpose of simulation, NS-2.34 was used as a network simulator which is considered to be the most common for MANET/VANET. NS-2.34 is predominantly used to evaluate all the aspects of vehicular networks even though there are other simulation tools available. The simulator provides the ability to write scripts using Object Tool Command Language (OTCL) which is used to design the topology of the network. This scenario file is linked with the predefined libraries which enables to achieve the expected simulation. The simulator enables the TCL scripts to communicate with the objects that are compiled in the C++ files. The NS-2.34 enables the user to be reflect different scenarios through the TCL scripts and the output is generated in the form of trace files [19]. The network simulator is written in C++ which is faster to run but difficult to change which makes implementing a new protocol very difficult whereas the OTCL scripts which are used to create different scenarios takes longer time to execute, but can be changed accordingly. This split helps us in programming critical large scenarios easily which is one of the striking features on NS-2.34 [20].

Another important feature of NS-2.34 is the network animator which is used for visual representation. This animator enables us to see a real-time view of vehicle mobility. It creates a link between nodes so that they can connect with each other. NS-2.34 provides a queue management technique where the packets are been stored for a limited period of time. These queues provide the location of where the packets should be transferred and where it should be dropped [21]. The NS-2.34 is called an event-based simulator which can create a number of real-time large topologies and also supports the IP detection technique we use to monitor the packets and find malicious activities. The simulator helps us to manage different techniques to present the location of the packets in the network. The NS-2.34 version does not support the channel switching functions. It uses the node configuration in order to broadcast the messages over a network. The mobility of each node is done at the application layer and the communication to the other layers is done across gates. It then simulates the packet sending and receiving along with the IP address to the MAC layer which is responsible for acting as a bridge between the routing layer and the physical layer.

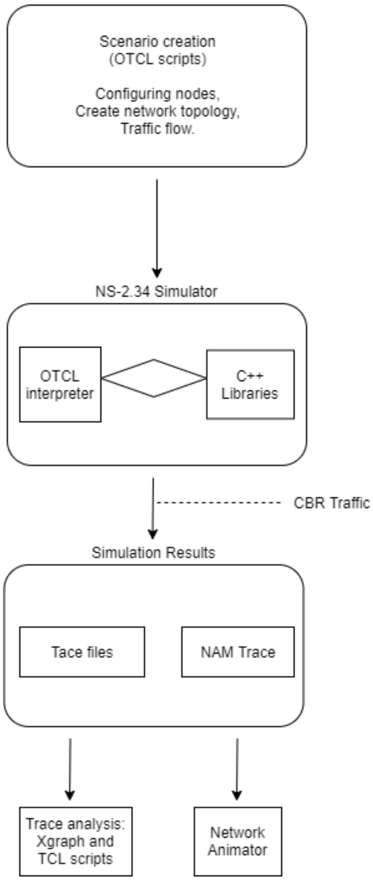


Figure 5: Result analysis process in NS-2.34

In order to verify the effectiveness of the proposed scheme, a possible real-time scenario was created where the vehicles move within a particular area. The simulation involves 50 nodes out of which 46 are mobile nodes and 4 were roadside units. Each simulation is for

100 seconds and is carried out by varying the number of attackers from 5 to 25. A CBR traffic is used to generate the packets at a constant interval. All the above settings are intended to reflect the real-time scenarios which could probably happen. The performance of the proposed method is measured using various metrics such as Detection rate, False probability rate.

Table 1: Simulation Parameters

Simulation Time	100 sec
Number of Vehicles	50,5
Traffic type	CBR (UDP traffic)
Visualisation Tool	NAM
Medium	Wirless
Data size	19.5 KB
MAC layer	IEEE 802.11

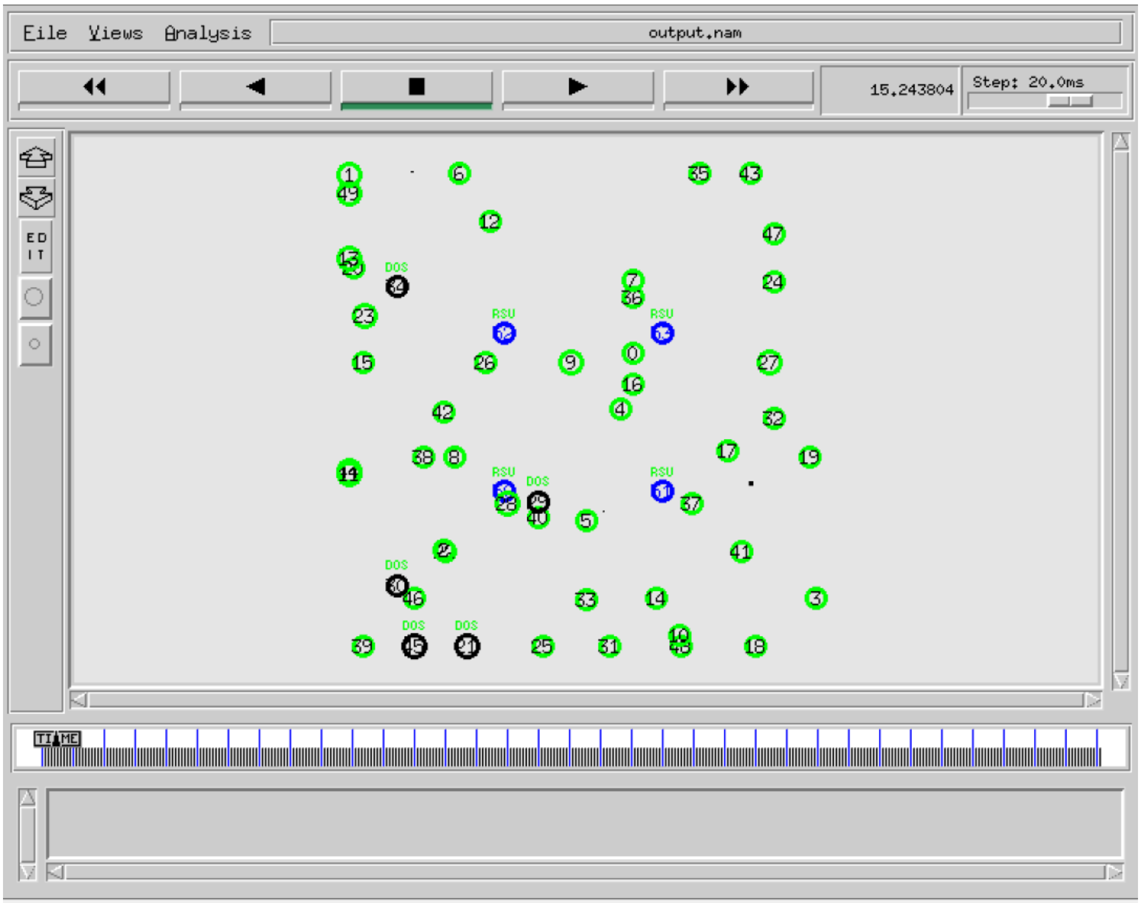


Figure 6: NAM Simulation

5.1 Detection Ratio

Detection ratio represents the number of detected malicious vehicles to that of the total number of vehicles in the network. The detection ratio of the system is directly influenced by the density of the vehicles in the network. The more the vehicles the more will be the number of packets exchanged. The results obtained are obtained by varying the number of attackers in the network. The below graphical representation states that the proposed technique which uses the cuckoo filter has a better detection ratio when compared to a bloom filter.

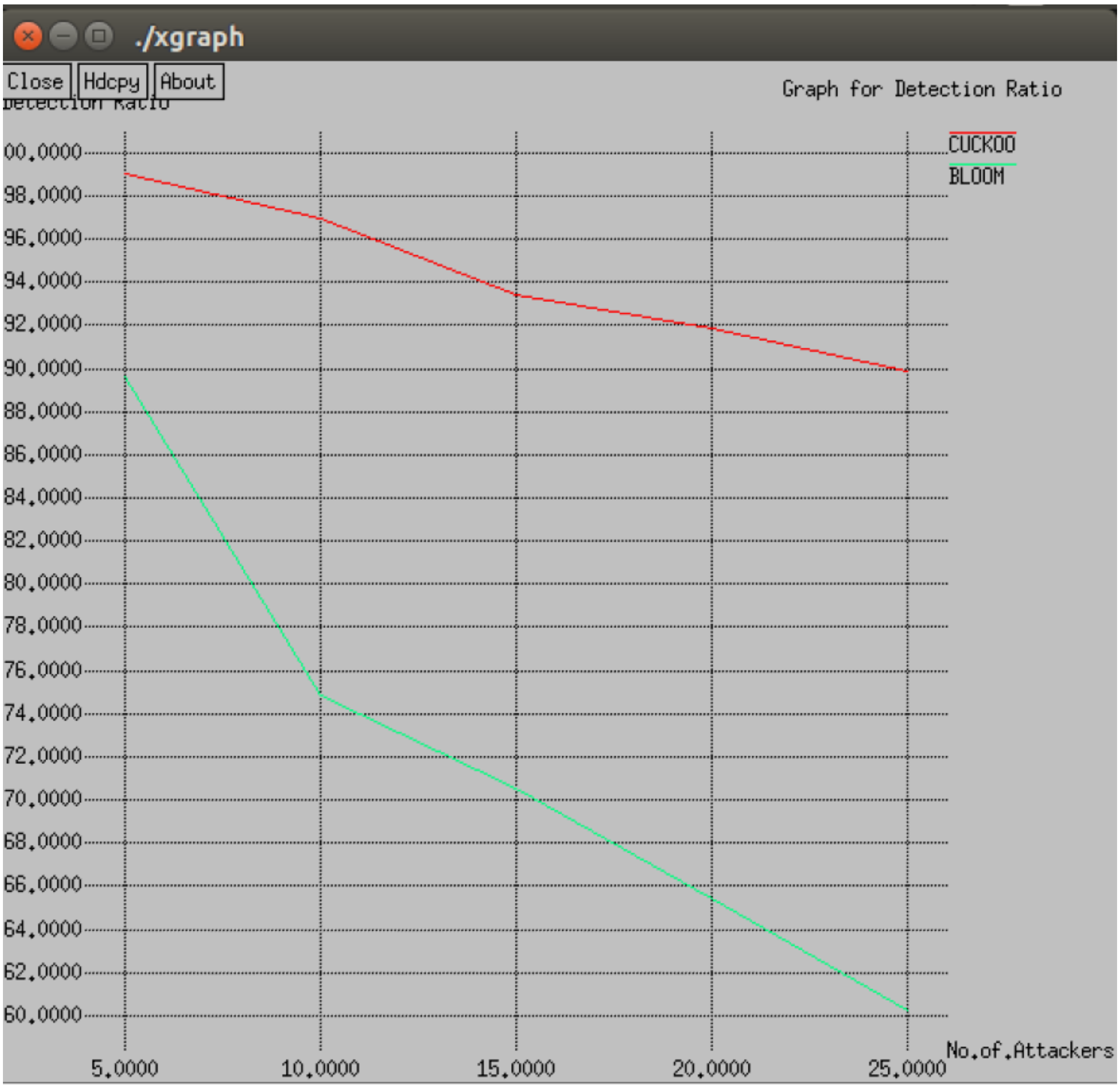


Figure 7: Detection Ratio

The simulation results and graph obtained suggest that the detection ratio of then malicious vehicles is as high when the number of malicious vehicles is low in the count. As the number of malicious increases, we see the detection capability decreases but not as such to that of the bloom filter. Both the filters at some point in time will stabilize the detection ratio even when the number of nodes is high. This is because communication can happen between nodes that are only within a specific range.

5.2 False Positive Ratio

False positives are considered to be an important metric for evaluating the performance of any system. In general the false positive rate is the ratio between negative events grouped as positive to that of the total number of negative events.False Positive Ratio represents the number of authorized vehicles detected to that of the total number of authorized vehicles in the entire network. This parameter is considered to be one of the most important because a legitimate vehicle can be detected as a malicious one. The proposed system has a better false positive rate when compared to the bloom filter.

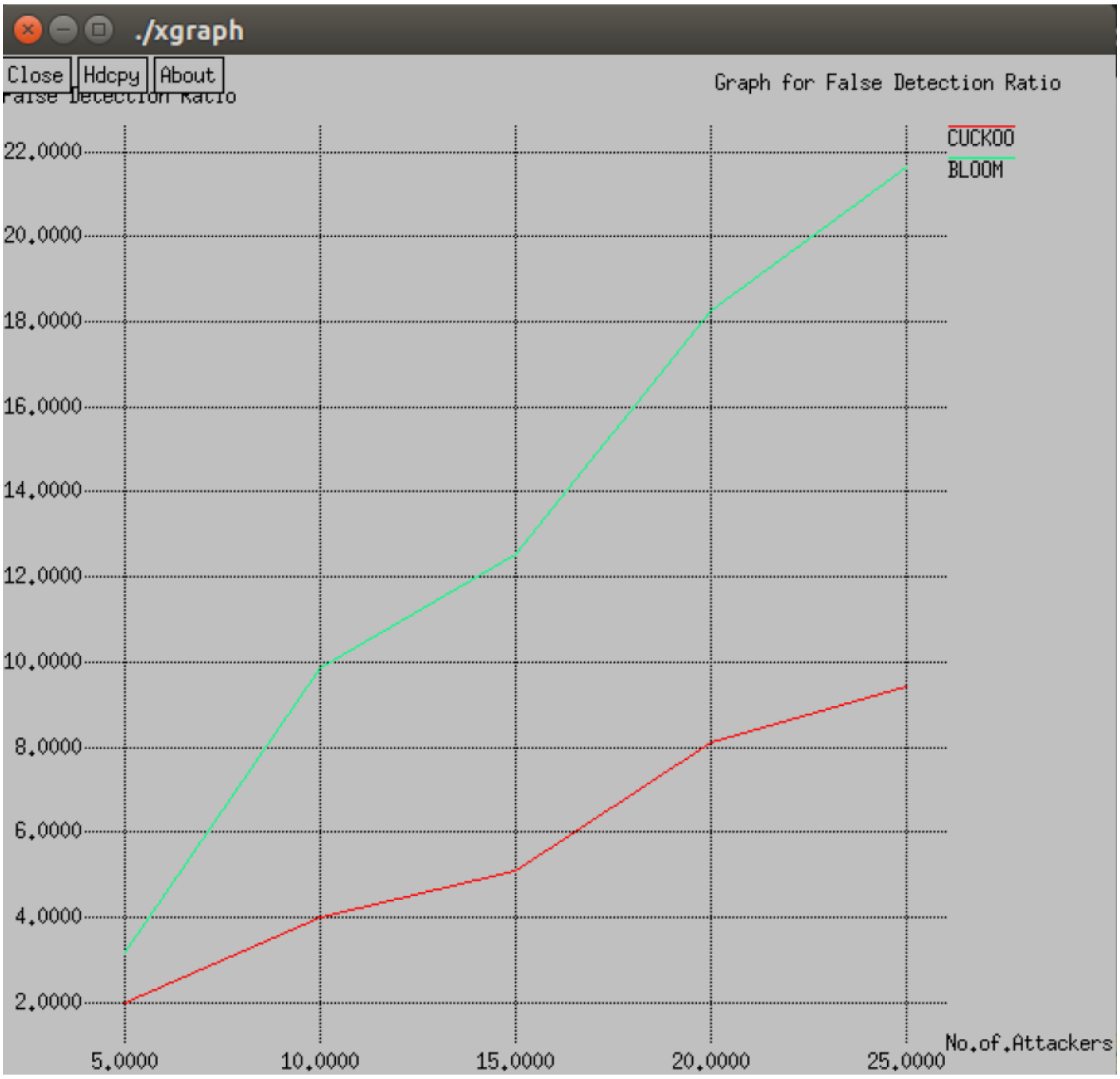


Figure 8: False Positive Ratio

The results of the simulation suggest that the false-positive ratio is as low as the number of malicious vehicles is less. Similar to the detection ratio the false-positive ratio also increases with the number of malicious vehicles. This trend will also stable at some point due to the communication range. But the results of the cuckoo filter is better than that of the bloom filter.

5.3 End-to-End Delay

The end delay is often referred to as time utilized by the packet to be transferred over a network from the source to destination. It can also be termed as the traveling time of the packet across the network. The end delay is considered to be important since it is influenced by the number of malicious vehicles that are present in the network. The delay will be more if the number of malicious vehicles is high.

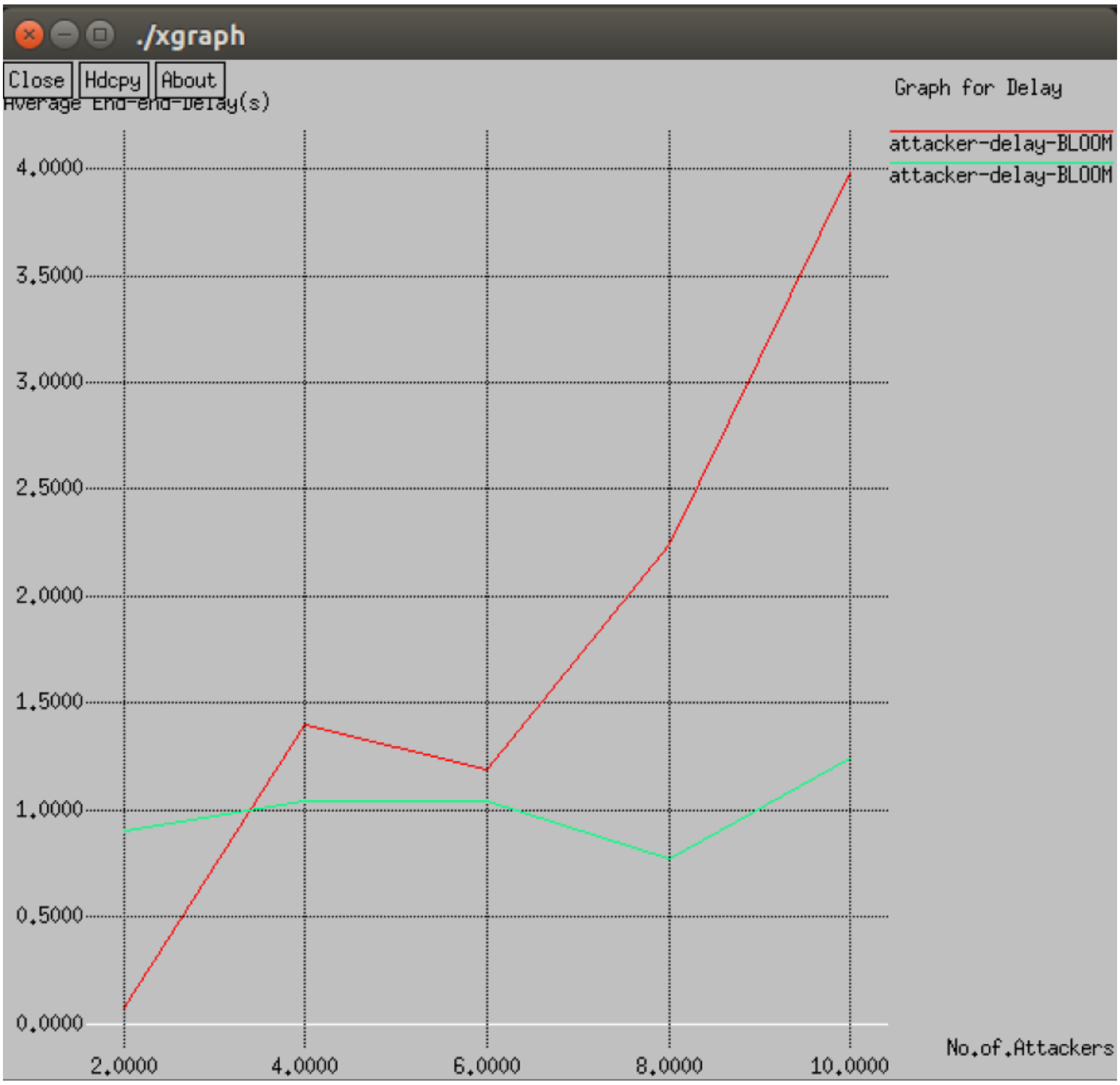


Figure 9: End-to-end delay

The results of the simulation represent the delay caused by varying the number of attackers. The delay caused by the attackers was initially low and there is a sudden drop in the delay when the number of attackers is high. Further increasing the number of malicious vehicles we see a rapid increase in the delay of the cuckoo filter. But the delay in the bloom filter is steadily increasing as the number of malicious vehicles is increased.

In addition to the above evaluation which is based on Detection ratio, False positive ratio, End-to-end delay some of the other key experiments were performed they are:

5.4 Packet Delivery Ratio

The packet delivery ratio is also considered to be one of the important metrics for any network system. The ratio between the total number of packets sent and the total number of packets received gives the packet delivery ratio. In general, the wireless network will have high packet losses due to congestion, obstacles that are present between the transmission. Additionally, we have attackers in the network due to which the packet delivery is affected.

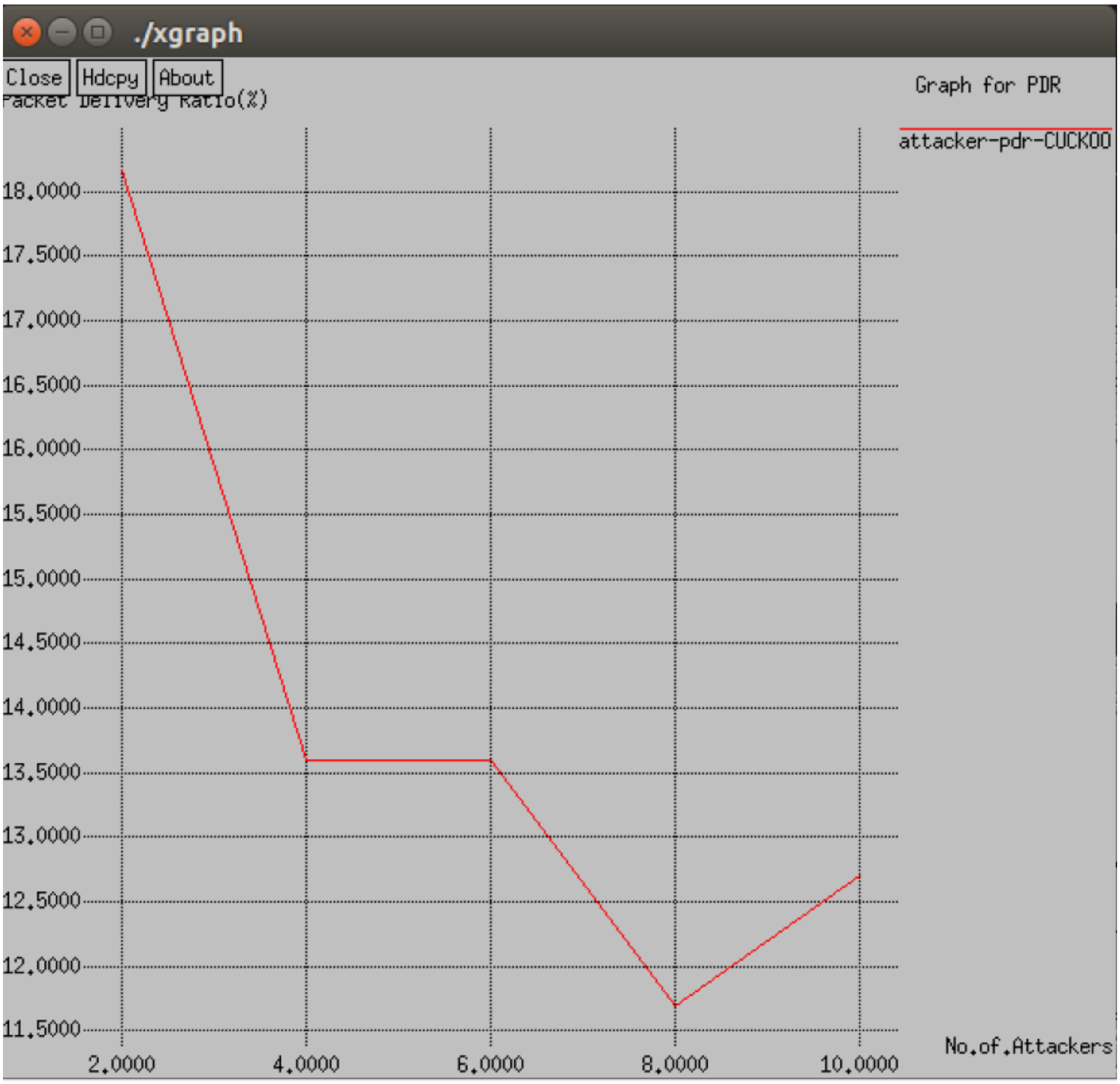


Figure 10: Packet-delivery ratio

The results of the simulation suggest that the packet delivery ratio is quite low as the number of malicious nodes increases.

5.5 Packet-loss Ratio

The packet-loss ratio, in general, is the ratio of a number of packets that are received to that of the total number of packets sent gives the packet loss ratio. As mention in the PDR section since the communication is in wireless medium and the presence of attackers causes huge packet losses in the network.

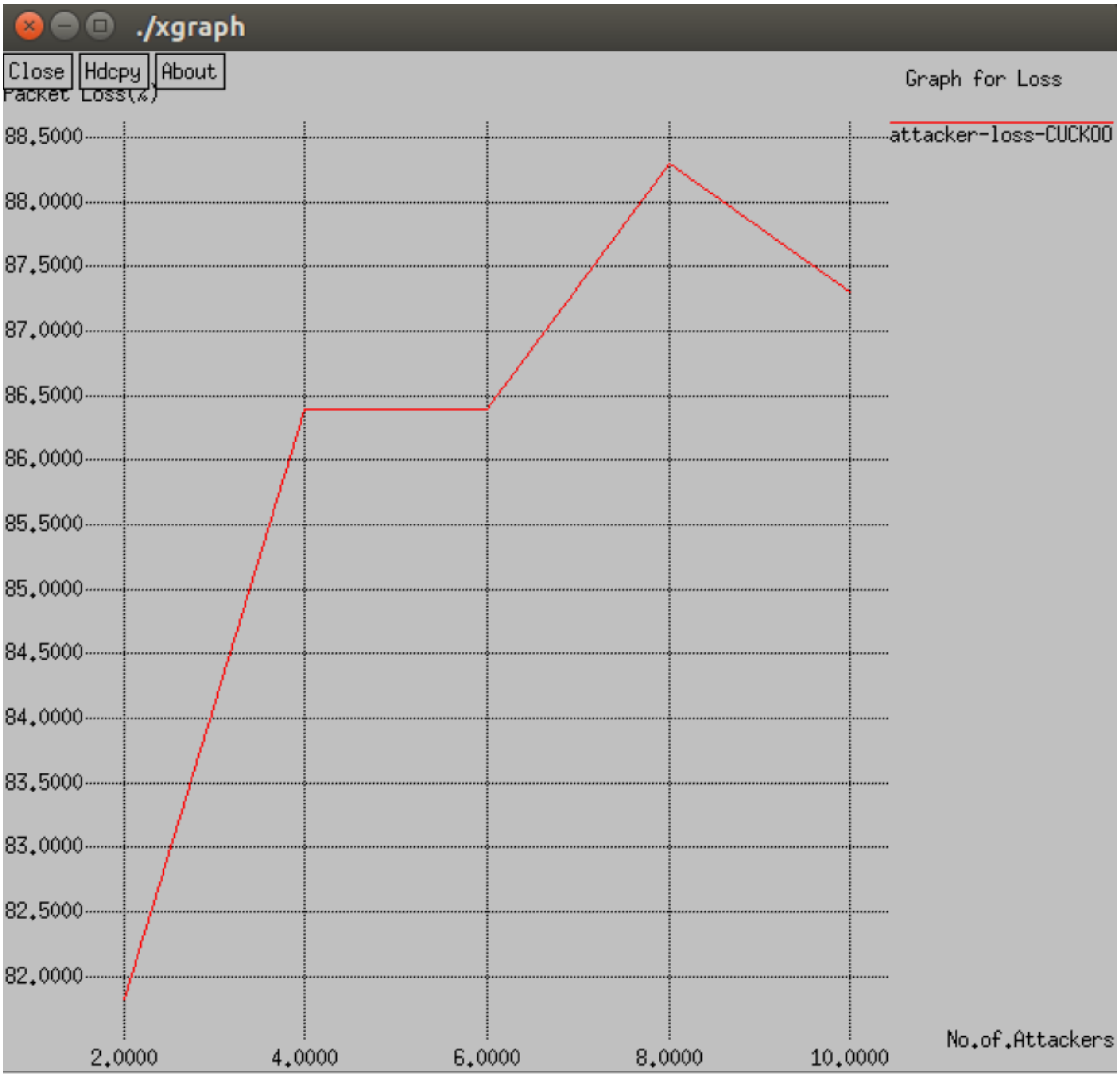


Figure 11: Packet-loss ratio

The results of the simulation state that the usage of the wireless medium and the presence of the attackers play a major role in PDR and PLR. As we can see that the packet loss is very high as the number of malicious nodes is increased.

6 Conclusion and Future Work

DoS attacks have always been a major threat to any kind of network. This is because of the damage that it can cause which in turn cannot be recovered. The rapid detection of the malicious nodes in the vehicular network is imperative when a DoS attack occurs. The proposed scheme is a filter based IP detection scheme which is a concrete way to detect DoS attack in VANET. The technique not only helps to detect the attack but it also helps to broadcast about the detected attack to other nodes within the network. The system will have a better performance in terms of Detection ratio, False positive rate, End-to-end delay than the existing system.

The current work talks only about the detection of the attack and broadcasting it to the other vehicles in the network. In the future we can try to remove the malicious node from the network by disconnecting it which will reduce the damage that it could cause to the network. Another aspect is to classify it into random spoofing, subnet spoofing or fixed spoofing types by analyzing a hash table for the source IP characteristics. Simulation experiments show that the proposed method yields very accurate detection and classification results yet with low computational cost.

References

[1] M. N. Mejri, J. Ben-Othman, and M. Hamdi, “Survey on vanet security challenges and possible cryptographic solutions,” *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[2] R. S. Raw, M. Kumar, and N. Singh, “Security challenges, issues and their solutions for vanet,” *International journal of network security & its applications*, vol. 5, no. 5, p. 95, 2013.

[3] A. Rawat, S. Sharma, and R. Sushil, “Vanet: Security attacks and its possible solutions,” *Journal of Information and Operations Management*, vol. 3, no. 1, p. 301, 2012.

[4] J. Petit, “Analysis of ecdsa authentication processing in vanets,” in *2009 3rd International Conference on New Technologies, Mobility and Security.* IEEE, 2009, pp. 1–5.

[5] A. Studer, F. Bai, B. Bellur, and A. Perrig, “Flexible, extensible, and efficient vanet authentication,” *Journal of Communications and Networks*, vol. 11, no. 6, pp. 574–588, 2009.

[6] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, “Flooding-resilient broadcast authentication for vanets,” in *Proceedings of the 17th annual international conference on Mobile computing and networking.* ACM, 2011, pp. 193–204.

[7] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, “Pba: Prediction-based authentication for vehicle-to-vehicle communications,” *IEEE transactions on dependable and secure computing*, vol. 13, no. 1, pp. 71–83, 2015.

[8] S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, “Early detection of dos attacks in vanet using attacked packet detection algorithm (apda),” in *2013 international conference on information communication and embedded systems (ICICES).* IEEE, 2013, pp. 237–240.

[9] A. Singh and P. Sharma, “A novel mechanism for detecting dos attack in vanet using enhanced attacked packet detection algorithm (eapda),” in *2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS).* IEEE, 2015, pp. 1–5.

[10] A. Quyoom, R. Ali, D. N. Gouttam, and H. Sharma, “A novel mechanism of detection of denial of service attack (dos) in vanet using malicious and irrelevant packet detection algorithm (mipda),” in *International Conference on Computing, Communication & Automation.* IEEE, 2015, pp. 414–419.

[11] K. N. Patel and R. H. Jhaveri, "Isolating packet dropping misbehavior in vanet using ant colony optimization," *International Journal of Computer Applications*, vol. 120, no. 24, 2015.

[12] H. Hasbullah, I. Ahmed Soomro, and J.-l. Ab Manan, "Denial of service (dos) attack and its possible solutions in vanet," *World Academy of Science, Engineering and Technology (WASET)*, vol. 65, pp. 411–415, 2010.

[13] S. M. Nyabuga, W. Cheruiyot, and M. Kimwele, "Using particle swarm optimization (pso) algorithm to protect vehicular ad hoc networks (vanets) from denial of service (dos) attack," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 5, no. 3, 2016.

[14] K. Jeffane and K. Ibrahimi, "Detection and identification of attacks in vehicular ad-hoc network," in *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, 2016, pp. 58–62.

[15] T. Bouali, H. Sedjelmaci, and S.-M. Senouci, "A distributed prevention scheme from malicious nodes in vanets' routing protocols," in *2016 IEEE Wireless Communications and Networking Conference*. IEEE, 2016, pp. 1–6.

[16] K. Verma and H. Hasbullah, "Ip-chock (filter)-based detection scheme for denial of service (dos) attacks in vanet," in *2014 International Conference on Computer and Information Sciences (ICCOINS)*. IEEE, 2014, pp. 1–6.

[17] B. Fan, D. G. Andersen, M. Kaminsky, and M. D. Mitzenmacher, "Cuckoo filter: Practically better than bloom," in *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*. ACM, 2014, pp. 75–88.

[18] V. V. Mahale, N. P. Pareek, and V. U. Uttarwar, "Alleviation of ddos attack using advance technique," in *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. IEEE, 2017, pp. 172–176.

[19] M. Fiore, J. Harri, F. Filali, and C. Bonnet, "Vehicular mobility simulation for vanets," in *40th Annual Simulation Symposium (ANSS'07)*. IEEE, 2007, pp. 301–309.

[20] E. Spaho, L. Barolli, G. Mino, F. Xhafa, and V. Kolici, "Vanet simulators: A survey on mobility and routing protocols," in *2011 International Conference on Broadband and Wireless Computing, Communication and Applications*. IEEE, 2011, pp. 1–10.

[21] K. Verma, H. Hasbullah, and A. Kumar, "An efficient defense method against udp spoofed flooding traffic of denial of service (dos) attacks in vanet," in *2013 3rd IEEE International Advance Computing Conference (IACC)*. IEEE, 2013, pp. 550–555.