Journal of Ambient Intelligence and Humanized Computing (2021) 12:6599–6612
https://doi.org/10.1007/s12652-020-02279-2

ORIGINAL RESEARCH

A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET

Raenu Kolandaisamy[1,2] · Rafidah Md Noor[1] · Indraah Kolandaisamy[3] · Ismail Ahmedy[1] · Miss Laiha Mat Kiah[1] · Mohd Emran Mohd Tamil[1] · Tarak Nandy[1]

Received: 13 April 2020 / Accepted: 26 June 2020 / Published online: 3 July 2020

Abstract
The strength of Vehicular Ad hoc Networks (VANETs) and the rapid deployment capability, can be used in many situations where the network should be arranged in a short time and there is a need to collect sensitive information. We consider cluster-based attack detection in data compilation wherever the neighbor nodes give the important information to the cluster head. Moreover, evidence is obtainable in the cluster head may possibly be accumulated by some vehicular nodes and executes numerous responsibilities such as decision making about delivering information. The existence of malicious nodes threatens determination making through transmitting malevolent information, which is not appropriate to the VANET categorized data and might send a substantial number of packets to the vehicles or Road Side Unit (RSU). To overcome this issue, we have proposed a Stream Position Performance Analysis (SPPA) approach. This approach monitors the position of any field station in sending the information to perform a Distributed Denial of Service (DDoS) attack. The method computes various factors like Conflict field, Conflict data and Attack signature sample rate (CCA). Using all these factors, the method identifies the trustworthiness of the packet and includes it in decision making. The proposed approach increases the performance of a Distributed Denial of Service (DDoS) attack detection in a VANET environment.

Keywords VANET · DDoS attack · Cluster · Routing · Detection

1 Introduction

The Vehicular Ad-hoc Networks (VANETs) are evident examples of Mobile Ad Hoc Networks (MANETs), where nodes are vehicles connected with a Road Side Units (RSUs) and On Board Unit. In VANET, vehicles are equipped with an OBU capable of message processing and short-range wireless communication. The OBU implements the communication protocols and algorithms that vehicles use to interconnect through each additional or fixed positions connected along roads, called Road Side Unit (RSU) (Shakshuki et al. 2013). RSU are fixed infrastructure deployed on the roadside with communication equipment capable of receiving information from vehicles, storing, processing and disseminating information to vehicles. Any vehicle can start and join the communication as per requirements to exchange of information is a building block for the Intelligent Transportation System (ITS) (Yaqoob et al. 2017; Ahmad et al. 2017; de Biasi et al. 2018).

Readily available 2 kinds of interaction or communication in VANETs, for example Vehicle-to-Infrastructure (V2I) and

✉ Raenu Kolandaisamy
raenu@ucsiuniversity.edu.my; malakolasm211@yahoo.com

✉ Rafidah Md Noor
fidah@um.edu.my

Indraah Kolandaisamy
indra@uum.edu.my

Ismail Ahmedy
ismailahmedy@um.edu.my

Mohd Emran Mohd Tamil
emran@um.edu.my

Tarak Nandy
tarak@um.edu.my

[1] Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia

[2] Institute of Computer Science and Digital Innovation, UCSI University, Jalan Menara Garding, Kuala Lumpur, Malaysia

[3] School of Business Management, University Utara Malaysia, Sintok Kedah, Malaysia

Vehicle-to-Vehicle (V2V). V2V involves vehicles sending or sharing information among each other through the VANET (Kolandaisamy et al. 2018). It only allows communication among vehicles such as alerting and notifying the drivers but does not involve taking control of the vehicle when there is an emergency. However, V2I communication takes place between vehicles and road side infrastructure, as depicted in Fig. 1. V2I communication is huge, as many base stations and RSU are needed to cover all the roads. In order to get information such as the closest parking station, petrol stations, salons etc., it is important to have V2I communication. This paper only considers V2V communication. The terms 'node' and 'vehicle' are used interchangeably throughout the paper (Kolandaisamy et al. 2019a, b).

VANETs are a subset of MANETs with various distinct characteristics which change the fundamentals. Any malicious entity can use the information and launch various types of attacks such as fake message broadcasting. These messages can create unnecessary traffic situations and security threats. Attackers can obtain the location of drivers, which violates one's privacy, or can modify life-critical information (Ahmad et al. 2017). Therefore, a proper privacy protection and authentication mechanism for the vehicles has to be put in place. The trust value of a vehicle can be checked and if the value passes a certain testing threshold, then the desired information can be exchanged between the vehicle and other verified vehicles.

1.1 VANET challenges

Many research challenges remain despite the ongoing academic and industrial research efforts on VANET. Vehicle and passenger safety are among the principal issues in VANET (Balan et al. 2015; Fragkiadakis et al. 2015). Other applications and private services have been suggested to lower the cost and encourage VANET deployment and adoption. VANET also has the same inherent security weaknesses that are associated with MANET, and hence are subjected to many security threats. Issues of stability, scalability and reliability are also serious concerns in VANET (Nadeem and Howarth 2014).

Several VANET applications require message dissemination. It needs to broadcast messages to cover the maximum distance with less overhead. The broadcasting should be developing with algorithms and it should also handle the well-known problem of broadcast storm. When designing the algorithms, it is important to keep the message size small and simple. To support real time applications of VANETs, reliable communication is required.

Perhaps a simple definition of Distributed Denial of Service (DDoS) would be useful. A DDoS attack involves sending huge number of packets from multiple sources which can overwhelm RSUs with a high volume of traffic. This may cause the network to fail which prevents drivers from sending life-critical information to the RSU. In normal situations, this life-critical information needs to get to other drivers in a timely manner to avoid untoward incidents. Typically, a DDoS attack can be launched in 2 situations, i.e. in V2V and V2I. Figures 2 and 3 illustrate different scenarios for attacks (Balan et al. 2015).

1.1.1 Vehicle to vehicle (V2V)

Assailant transmits fake messages to a target from various places and time slots to overload and bring down the network in order to make it inaccessible for the victim.

1.1.2 Vehicle to infrastructure (V2I)

Instead of targeting a vehicle, the attack is launched at the RSU. Similarly, the attacks originate from different locations

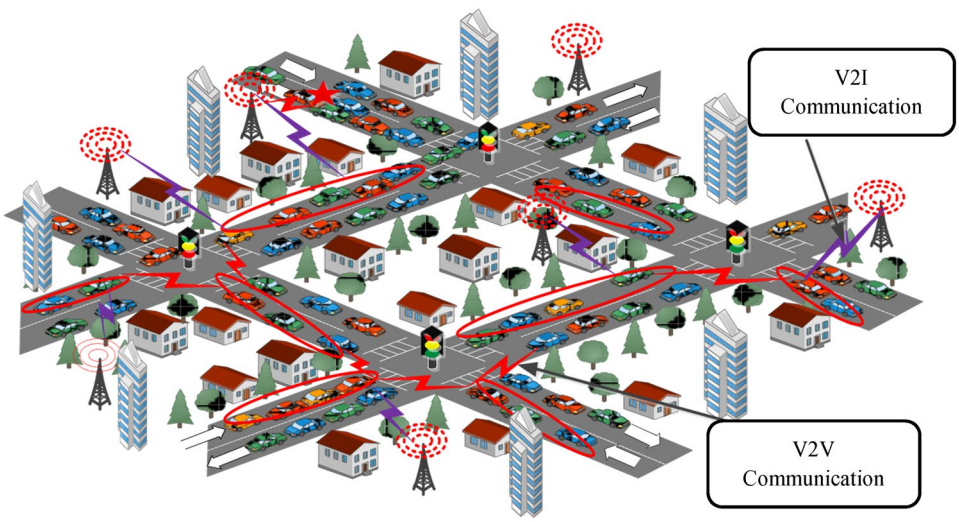


Fig. 1 Vehicular communication in VANETs

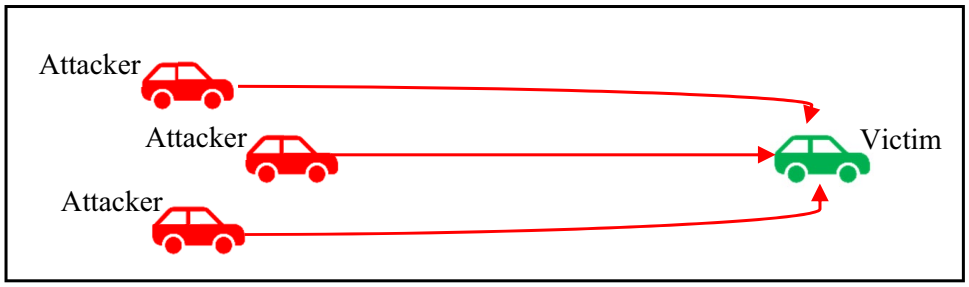


Fig. 2 V2V DDoS attack

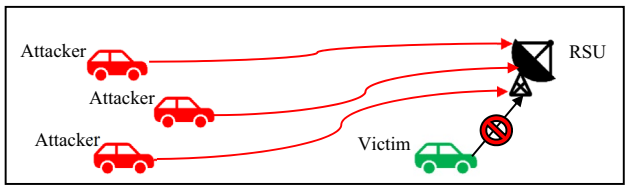


Fig. 3 Vehicle to infrastructure DDoS attack

and time slots to overload the entire RSU network. Hence, if there is a node that wants to transmit along with the RSU, it would not remain respond due to overload.

1.1.3 Limitations of existing approaches

Several possible mitigation measures have been discussed in the background work to prevent and detect DDoS attacks. New standards for VANETs may need to be drafted and manufacturers need to enforce compliance with these specifications for a safer tomorrow. There are still limitations inherent in existing methods, for instance end to end delay, throughput and detection time. Some of the methods take extra time to identify a DDoS attack (Lyamin et al. 2014; Fotohi et al. 2016; Kaur and Mahajan 2015), which may be due to the inefficiency of the algorithm or the requirements of a large number of datasets. Sometimes it is caused by end to end delay and packer delivery ration. As researchers, we need to focus on the important metrics such as Detection Time, Throughput, Packet Loss, Attack Detection Rate, Routing Overhead, and False Classification Ratio. These performance metrics are divided into two categories. The first is DDoS metrics which consist of Attack Detection Time, Attack Detection Ratio and False Classification Ratio (Shah et al. 2018; Saritha et al. 2017). The second category consists of network metrics, such as End to End Delay, Throughput, Routing Overhead and Packet Delivery Ratio.

To resolve the problems revealed above, author offer a Stream Position Performance Analysis (SPPA) method to identify DDoS attacks in the VANET environment. The first stage of the proposed approach involves receiving incoming packets and selecting a Cluster Head (CH). We have more than one CH. The secure cluster heads are formed based on the clustering score. A cluster with the greatest record is designated as the CH. Stage 2 involves stream position analysis, where the CH maintains a trace file by monitoring the behaviour of the leaf node for each cycle of the transmission and computes all 4 features (The Amount of data to be communicated, Payload of the packet, Number of exact messages communicated, and the amount of abnormal messages transmitted).

In Stage 3: Conflict Field, Conflict Data, and Attack Signature Sample Rate (CCA) Computation, the CCA is calculated by computing the Conflict Field, Conflict Data, and Attack Signature Sample Rate by using packet payload, number of the service access and number of exact access. The resulting CCA value is then used in the final stage of the SSPA model, i.e. DDoS attack detection. From the value of the CCA, the legitimate weight of the node is calculated to verify whether the vehicle is an normal or intruder vehicle. The implementation of the projected model is assessed via Ns2 simulations. The simulation outcomes prove the effectiveness and efficiency of the planned method compared to comparable existing method pertain to numerous routine metrics such as detection time, throughput, packet loss, detection ratio, routing overhead, detection probability and false classification ratio.

In this research paper it is divided into 6 more segments. Related works are argued in segment 2. segment 3 designates utmost familiar attacks in VANET and deliberates on safety and non-safety applications. Segment 4 depicts the proposed SPPA model. The analysis and result are delivered in segment 5. segment 6 contains the conclusion.

2 Related works

The intrusion discovery scheme called Enhanced Adaptive Acknowledgement (EAACK) was designed to overcome the security issues in MANET (Shakshuki and Isiuwe 2018). The proposed scheme solves the problem of watchdogs recovering the performance of the system in the event of an intrusion. EAACK is an enhancement of the previous AACK algorithm and it is extended by using a digital signature to prevent attackers from modifying acknowledgement messages. Moreover, the Trilateral trust mechanism (Chikhaoui

et al. 2017) is applied to shield alongside with DDoS attacks in cloud computing. Moreover, the technique improves to identify various types of attack in various time periods. In case of large number of demands, the technique would assist in isolating legitimate attack groupings. Its a combination method of confidence that pursues the zero-trust technique initially and eventually encourages brief confidence and shared trust.

The author (Lyamin et al. 2014) conducted an experiment to test the jamming detection algorithm. A number of vehicles with fixed generation subsequent beacons broadcasted into the channel according to the IEEE 802.11p rules. During the test, two models of attack method are used: random jamming and ON–OFF jamming. There are two phases of attack: installation and normal operation. They then examine the performance of the algorithm. The result shows a detection rate and random jamming probability. The result for each PER is different. But overall PER = 0.01, the detection rates through time in each condition are the most balanced and perform well. However, more overhead algorithm has improved the detection rate which fits the author's conclusion. The author (Fotohi et al 2016) proposed Hybrid Intrusion Detection System (H-IDS) to identify the DDoS Attack in MANET and for this method is used two techniques, anomaly-based detection and signature-based detection. Moreover, H-IDS is improvement procedure on accuracy detection, and they have used two data set. The outcomes shows enhancement of the non-hybrid detection approch (Shah et al. 2018; Saritha et al. 2017).

The VANET is used for managing traffic, to lessen traffic congestion and to alert the drivers on the road. Due to the dynamic behaviour of VANET, attackers may take advantage of it to perform malicious attacks such as DDoS. In Pathre et al. (2013), the authors proposed a defence scheme to identify and prevent malicious nodes from performing a DDoS attack. It is done by requiring the RSUs to observe the communication between vehicles and infrastructure. The schema is used to detect the vehicle that generates false information. However, is will compare the message received from the attacker vehicle. Finally, it will make the genuine vehicle safe and block the attacker's vehicle. The Multi Variant Stream Analysis (MVSA) method categorizes the incoming request stream into a number of sections conferring to the traffic features MVSA technique to maintain the three stages for detection DDoS attack in network. MVSA uses packets clarification and trace get rules compute the multivariant stream factor to detect attacks (Kolandaisamy et al. 2018).

The author (Kaur and Mahajan 2015) uses a different framework to mitigate DDoS attacks by using packet and location analysis to verify the attacker node and in sort to stop the data produced from the attacker node. Nevertheless, model is called as Novel Security Approach for Data Flow and Data Pattern Analysia to Alleviate DDoS Attack concerning VANETs, the model is by Kaur and Mahajan (2015). The recommended model retains to been created to identify and alleviate the DDoS and DoS attacks in the VANET to prevent several of the misconduct in the arrangement of VANET vehicle collapse, crash or in several ways. In case the anomaly is discovered in the data communicated by the attacker connection, the connection is marked as the DDoS node and all new nodes in the cluster are notified regarding the attacker node and stop accepting data from that node. Moreover, the permanent nodes will connect with each one in the cluster. Assume that permanent nodes A, B and C are situated from East to west separately. Consequently, if a motor vehicle joins the coverage of permanent node A to permanent node B, it is noticeable that the motor vehicle is running in a parallel route. The attacker nodes would be analyzed by the middle node. The experiment is on a small scale and focuses on 3 metrics (PDR, End to End Delay and Throughput). The author did not justify the amount of time taken for attack detection.

The ANN based Scheme (Gupta et al. 2012) aims to predict the number of zombies involved in a DDoS Attack and needs to accept an encoding technique. The existing IP back track technique using different encoding technique. In this method, the researchers select the Advanced Marking Scheme (AMS) (Gupta et al. 2012). When the sufferer starts to rebuild the attack grid, it does not recreate such a lengthy way. The reproduction indicates that as extensive as highly of the contaminated ends surrounded by ten hops are recreated, the sorting method will succeed its target.

According to Xiang et al. (2011) there are many DDoS attack detection methods in MANET, but they did not work well because of their dynamic nature. Besides that, this author (Xiang et al. 2011) introduces a Security-Aware Routing protocol (SAODV) that will sort out available nodes on unrelated or dissimilar security levels. Two types of nodes are used in this paper: the first are Remote Protection Nodes (RPN) and the second are Local Protection Nodes (LPN). Lower level nodes become the LPN and defend high or difficult level nodes to reach their destination securely, whereas the beginning node on the source becomes the RPN to detect hateful or malicious packets and it successfully reduces the packet loss rate.

3 Safety and non-safety applications

VANET applications can be categorized into three classes. Class A is safety-oriented applications, which deal with life-critical situations such as real-time traffic and cooperative collision warning. Class B is designated for pragmatic-oriented applications which support non-critical situations such as digital map downloading and Internet access. Finally, Class C deals with convenience-oriented applications such

as fuel-saving and parking availability (Kolandaisamy et al. 2018; Fung and Zhu 2016). The VANET application classes are further described in Fig. 4. A description of attacks is provided in Fig. 5.

4 Stream position performance analysis model (SPPA)

This section describes the proposed SPPA model to detect DDoS attacks in the vehicular environment. The VANET with its unique environment is deployed in vehicular environments. It helps the vehicular environment to easily set itself up, regardless of the geographical location. Commonly, cluster-based DDoS attack detection has been adopted with more powerful nodes as Cluster Head (CH). The leaf node periodically updates the information of the critical zone to CH. Hence, communication between the leaf node and CH are performed through cluster-based routing, where the leaf node sends any sensitive information about its situation or its necessity to CH. However, intruders try to hack the information and send false information to the CH and CH to the centric controller. The centric controller takes responsibility for the entire node and performs decision based on the necessity of the time of the attack detection.

Vehicular network is formed between vehicles as clusters. As vehicles move at high speed on the roads, the communication between vehicles would disconnect frequently and topology or interconnection between the vehicles would frequently change (Panjeta et al. 2017). The network could be heavy depending on the amount of cars on the highway or road and the comparative speeds at which they travel. Routing of messages between vehicles would need to overcome these topological issues and take into consideration the mobility and communication conditions (Panjeta et al. 2017). The dynamic nature of the topology would require frequent exchange of neighbour information to form the message routes leading to high communication overhead. Since the vehicles have high mobility, maintaining end-to-end connection between them would not always be possible (Pillutla and Arjunan 2019).

Due to malicious activities, the controller neglects to take proper decisions and lets a critical situation happen to the vehicular environment (Cheng et al. 2017). To overcome this issue and to detect such malicious performance, a Stream Position Performance Analysis based attack Detection model has been designed. Figure 6 shows the architecture of the proposed SPPA model which highlights its work flow and its components. Each component has a unique work determination and it has four primary stages, i.e. cluster head selection, stream position, CCA and attack detection. The cluster head selection stage involves choosing the cluster nodes as well as cluster head for data transmission. The stream position stage analyses the neighbour node for better service and data transmission in the network. The CCA is the third stage, the node history is computed based on the calculation for detecting the attacker node in the network. Based on information from CCA, the attack is detected in the final stage. Table 1 shows abbreviations of the algorithm.

Fig. 4 Classes of VANET applications

Fig. 5 Type of attacks

4.1 Selection of cluster head

The CH is the most predominant node, with more energy and the most powerful among the nodes in the cluster. Each CH knows all information about its cluster and its leaf node. Initially, 1-hop clusters are formed by an assumption. Secure cluster heads are formed based on the clustering score. Node list is formed with neighbouring nodes. Clustering score v_i is found for individual nodes in the neighbouring list. Then, nodes are classified into suspect, attacker or normal based on the routing scheme. Suspect nodes are motivated by a reputation mechanism, and attacker nodes are not allowed to participate in the selection process. The process will check the weightage each time. The flow chat shown in the Fig. 7. Finally, the neighbour node with maximum v_i are nominated as cluster head. The data transmission is quickly done if there are high numbers of neighbour nodes available. If any error occurs in the process, then it is easy to choose another neighbour node as CH. It ensures that a node is not allowed a faulty claim in the clustering process.

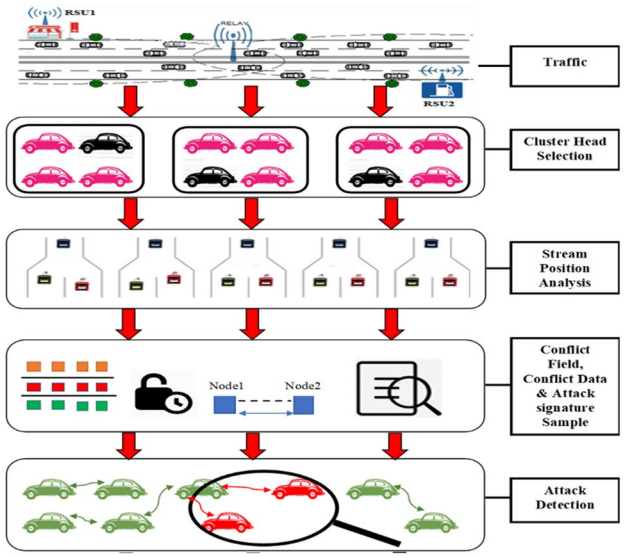


Fig. 6 Proposed SPPA architecture

Table 1 Abbreviations

Abbreviation	Meaning
N_L	Neighbor lists
V_i	Variable score (it's a boundary of 4 sides like north, east, west and south)
CH	Cluster head
N_i	Neighbor initiate
N_f	Neighbor follows
P	Packet
CCA	Conflict field, conflict data, and attack signature sample rate
I	Information
LW	Legitimate Weight
Th	Threshold
N_l	First neighbor
Node i	Initial node

4.2 Stream position analysis

At this stage, the CH maintains a trace file by monitoring the behaviour of the leaf node for each cycle of the transmission. Using its trace file, the stream position analysis will compute:

- The amount of data to be communicated,
- Payload of the packet,
- Amount of exact messages transmitted and
- The number of abnormal messages transmitted.

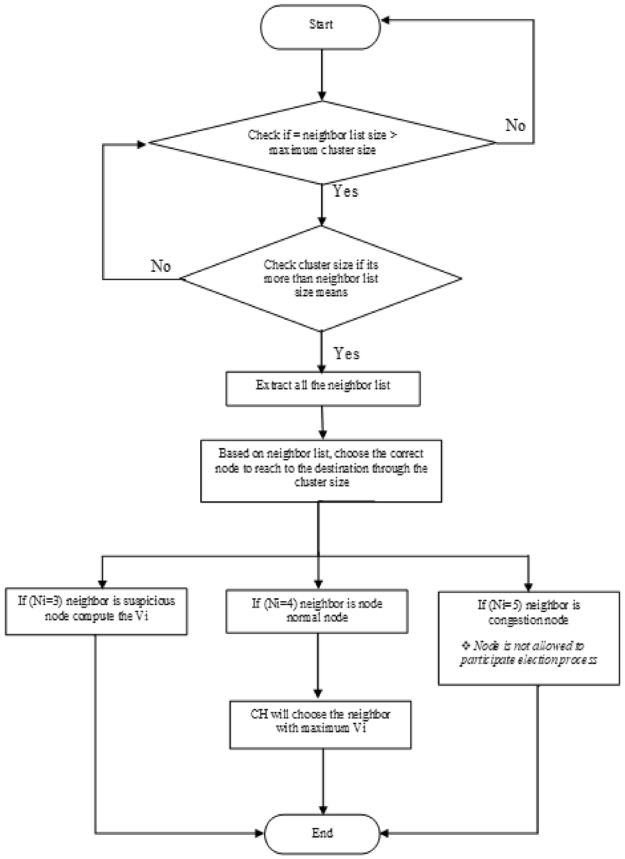


Fig. 7 Flow chart for selection of cluster head stage (SPPA)

The above features are calculated for every node at each cycle of its transmission. The above stage is shown in the flow chart Fig. 8.

4.3 CCA computation

At this stage, the node parameters and node histories are considered for the process. CCA is calculated by computing the Conflict Field, Conflict Data, and Attack Signature Sample Rate (CCA) by using the input factors are:

- The amount of packets or transmission performed,
- The payload,
- The amount of service access and
- The amount of exact access.

Using this above value, the intrusion detection is performed in the VANET environment. The above steps show in the Fig. 9.

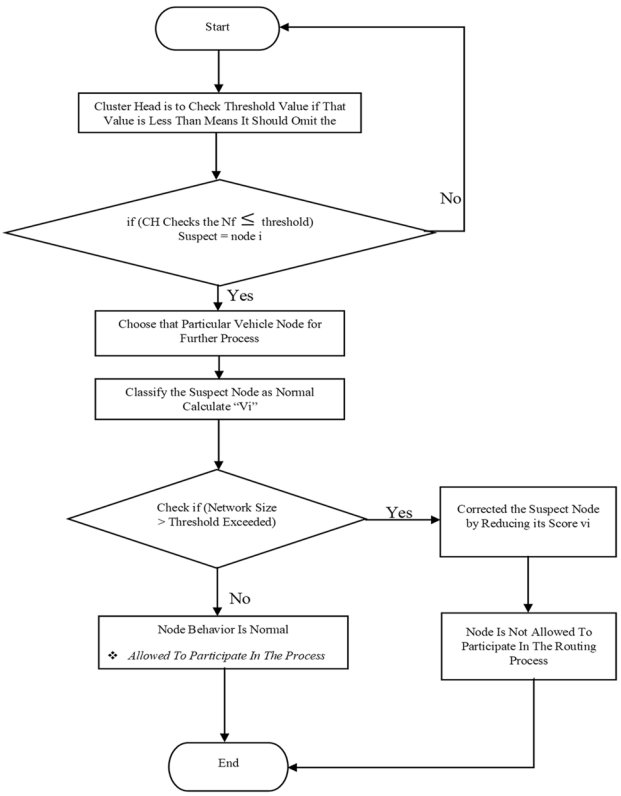


Fig. 8 Flow chart for stream position analysis stage (SPPA)

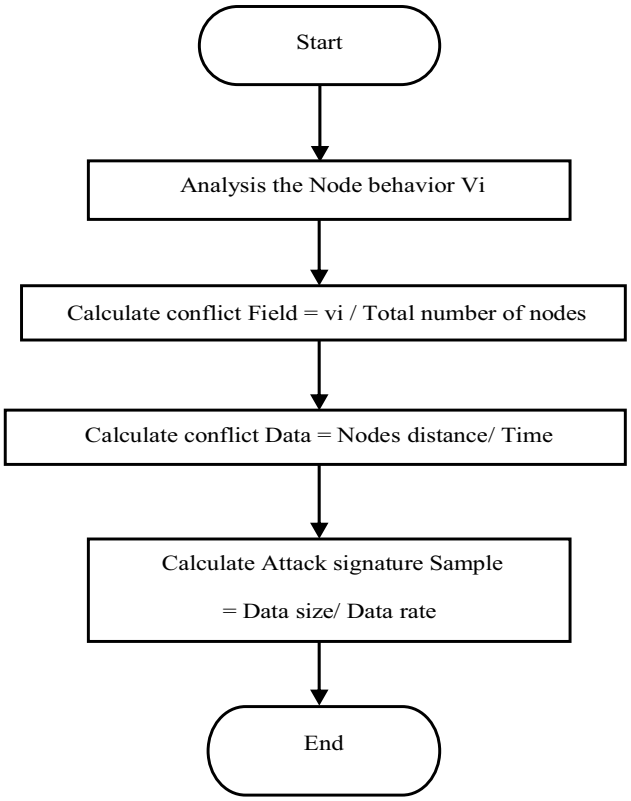


Fig. 9 Flow chart for CCA computation stage (SPPA)

4.4 DDoS attack detection

The discovery is accomplished by applying the above technique. It moniters the traffic of the node with tracking its outgoing and incoming packets and performs CCA design or calculation. Applying the quantity, it determines the genuine weight of the node and comes to a conclusion, whether, it is normal node or intruder node and transmits the existence of the intruder and denies its provision for the continual interaction. The steps for the above stage is shown in Fig. 10.

5 Results and discussion

The cluster attack scenario is illustrated in Fig. 11. In this attack scenario the node is the cluster and node 7 is the attack node. Moreover, the communication not able to continue due to the attack. To detect this kind of attack, our proposed model will be implemented. However, the efficiency of this method is that it can identify the attack in the minimum time, so that the communication can continue smoothly. The outcome of this method is shown in the simulation results.

DDoS attack detection have being realized in simulator version Ns 2.24. The behaviour of the recommended tactics

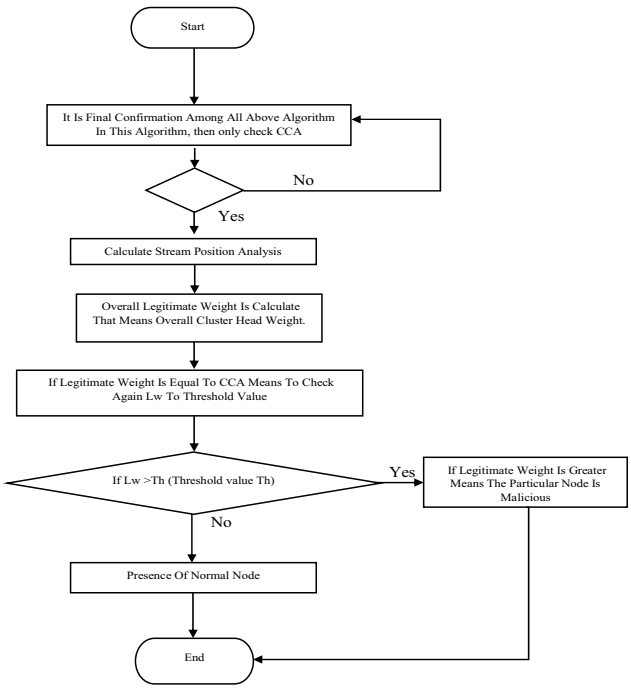
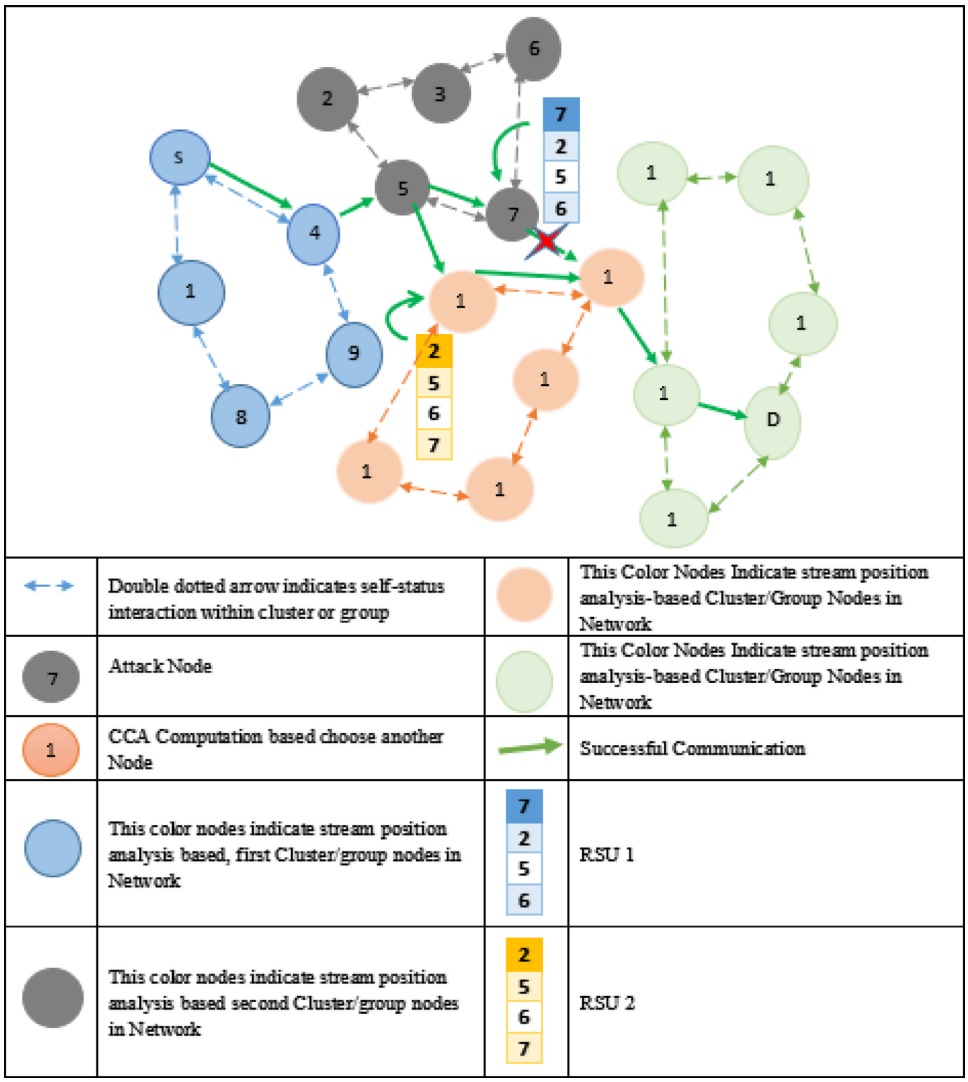


Fig. 10 Flow chart for DDoS attack detection stage (SPPA)

Fig. 11 Cluster attack scenario



is examined with a range of replication factors. Moreover, a vehicle node know how to accurately convey the message to the hubs that exist in its communication scope. Condition a vehicle node needs to speak to a centre that is not nonstop inside its communication run, then it utilizes transitional hubs as switches. In convenience demonstration, the energy of a node since one area to a new area can be allowed using the catchphrase "setdest" in TCL content on the Ns2 (Bhushan and Gupta 2019).

In dominant topology, the neighbours of every node substitute with the specific node for the area. The advancements of convenient nodes are bound to a region of 1000 m × 1000 m with the delay time of 3 s. Information communication is built up among nodes using UDP operator and CBR movement. Our recommended technique is associated with three existing models; they are the Trilateral Trust model, H-IDS model and Multi Filter model. The Table 2, the simulation configuration is shown. Seven performance metrics have been measured for the proposed model: Packet Delivery Ratio (PDR), end to end delay, throughput ratio, attack detection ratio, attack detection time, Routing Overhead (RO), and false classification ratio (Sangulagi et al.

Table 2 Simulation configuration

Parameter	Value
Platform	Ns2.24
Routing protocol	AODV
Communication range	1000 m × 1000 m
Packet size	1000 bytes
Running time	100 ms (minimum time in network)
RSU	2
Visualization tool	NAM
MAC layer	IEEE 802.11p
Antenna model	Omni-directional antenna
Traffic type	CBR
Data transmission range	20 Mbps

2013; Hasrouny et al. 2017; Panjeta et al. 2017). The major purpose of the performance metrics is to evaluate the recital of the SPPA model to detect the DDoS attack in VANET conditions (Wang et al. 2019).

5.1 Analysis of packet delivery ratio (PDR)

The PDR is developed to assess the nature of the procedure, due to an optimized analysis of incoming and outgoing network packets. Hence, it characterizes the proportion among the data received from the vehicle and the packets produced by the source. It can be gained by utilizing awk content, which delivers the follow and the outcome. The following calculation is used to generate the table "PDR = Received packets/Generated packets × 100".

- H-IDS takes an ordinary growth in Packet Delivery Ratio of 4.8% with the current trilateral trust.
- Multi Filter has improved its PDR with an median of 12.0% with H-IDS.
- The third recommended SPPA has amplified its PDR with an median of 11.0% with Multi Filter.

The recommended scheme SPPA betters in relationships of PDR. By altering the system size, the PDR for both existing and the planned algorithms are computed, the proposed scheme offers a high PDR with an average of 30.8% with the existing Trilateral Trust. Advanced the packet delivery ratio, higher the presentation of the system in VANET scenario. Figure 12 illustrate the graph of the PDR.

5.2 Analysis of end to end delay

End to End Delay information traded among the vehicles situated at the various areas in the aspect makes a top of the line delay. Furthermore, the time taken by the source vehicle to deliver the information successfully to the target is termed as end to end delay. The distinction among the time at when packet was created by the source and the time the packages reached the beneficiary, and the outcomes get from the following log file "End to End Delay = Vehicle Packet Received time – vehicle Packet Send Time". Figure 13 demonstrates the final summary of the planned method with the present structures. The different figures give the rate of delivering packets specifically in moments but sometimes a minor alteration will be present. If the target goes nearer to the sender node, then the interruption will reduced. Or else, the packet delay will be enhanced. From Fig. 13, it is clearly realized that the planned SPPA has decreased the end to end delay with delivering packets (Kolandaisamy et al. 2019a, b).

5.3 Throughput ratio

The throughput outcomes describes the amount of information packets established at a target corresponding to the amount of packets produced by the sender node for a required period of time. The result obtains from the following formula "Throughput = received data packet × 8/data packet transmission period". Figure 14 shows the qualified examination of throughput outcomes of the planned structure with the remaining, the details is explain below:

- H-IDS has improved its throughput ratio for an median of 7.5% with the existing Trilateral Trust approach.
- Multi Filter has improved its throughput by 19% with H-IDS.
- The proposed SPPA has improved by an average of 8% with Multi Filter.

From the study, it is clearly demonstrated that the planned SPPA has enhanced its throughput ratio to 34.5, which is contrasted to the present method.

5.4 Analysis of attack detection rate

The Attack Detection Rate is applied to estimate the position of the VANET is implemented thru the routing scheme. Figure 15 depicts the performance of the planned system SPPA with additional systems. The planned method overtakes the existing method in terms of attack detection ratio.

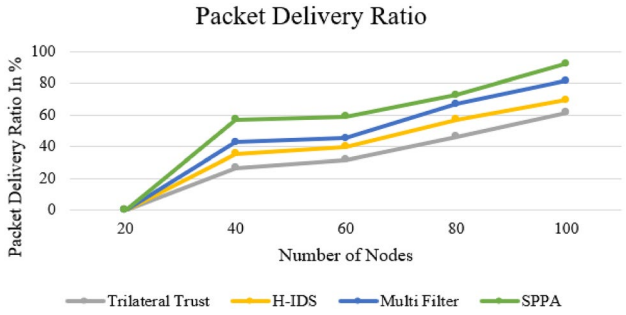


Fig. 12 PDR comparative analysis

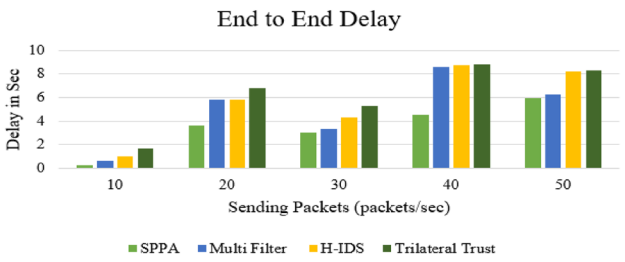


Fig. 13 End to end delay ratio

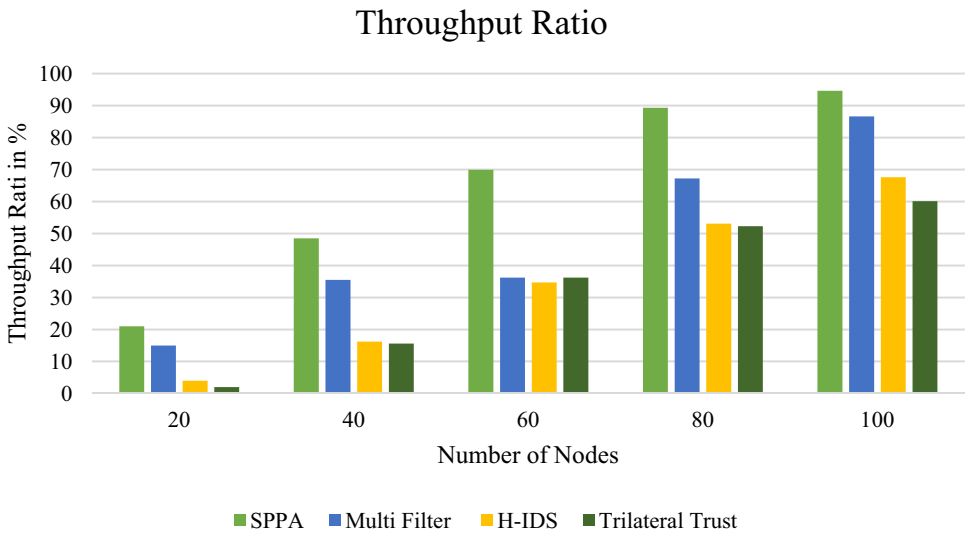


Fig. 14 Throughput analysis

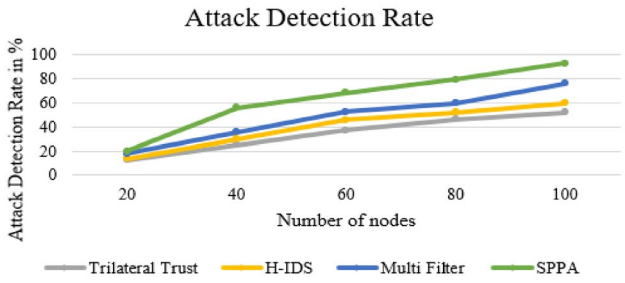


Fig. 15 Attack detection rate

Established on the amount of nodes all the network performance will be varied, this time we get the following results.

The comparative analysis of the existing system depicts the following:

- H-IDS has improved its Detection Rate for an average of 7.58% with the existing Trilateral Trust approach.
- Multi Filter has increased its Detection Rate with an average of 16.23% with H-IDS.
- The third proposed SPPA has slightly increased its Detection Rate with an median of 16.97% with Multi Filter.

The above study clearly shows that the planned proposed model is enhances its detection rate in the entire parts, and its compared with the present model it is recognized that the planned system SPPA has improved its detection rate.

5.5 Analysis of attack detection time

The Fig. 16 reveals the detection time analysis. Before we calculate the attack detection time, we need to identify the malicious nodes first. The identification of malicious nodes is done in our proposed models and it will measure how fast the attack is detected using proposed models. Malevolent node send obstructing messages to drop communications among genuine vehicles. Apart from that, malicious vehicles can distort or capture data from other node when it is an middle node. In the VANET environment, vehicles are able to know about the velocity and location of other vehicles (Fotohi et al. 2016). The result is obtained from the following formula where Detection time is the total time taken to identify the disobedient vehicle in the route from source to destination (Sangulagi et al. 2013). The equation is shown in Eq. (1). DT means Detection Time, meanwhile PL is Path Length which is how far the node travels, and TT is Time Taken for malicious packets to travel from sender to its final destination.

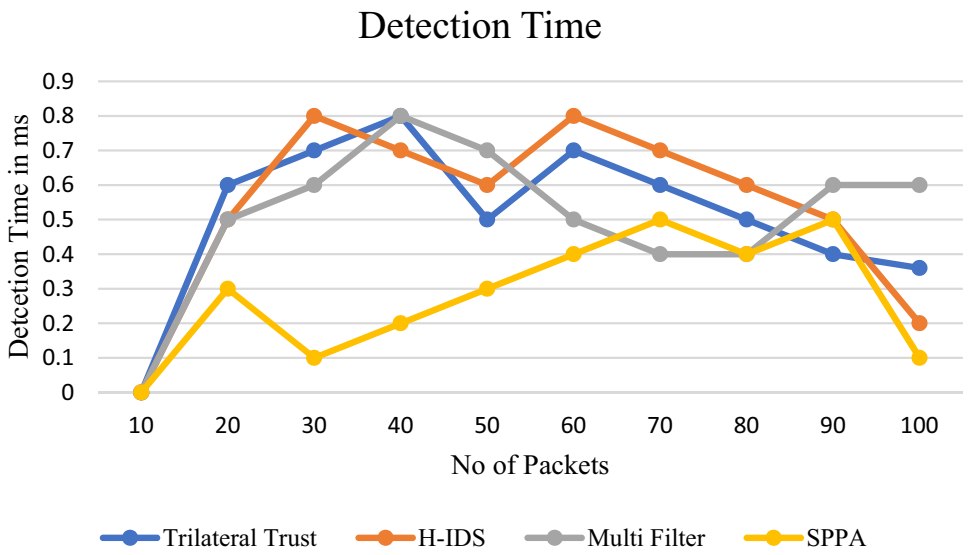
$$DT = (PL/TT) \tag{1}$$

This detection time specifies that SPPA constantly outpaces baseline methods. However, this method used Conflict Field, Conflict Data, and Attack Signature Sample Rate (CCA) to detect DDoS attack and it took a lowest time to identify the attacks contrasted to other methods. Moreover, performance of this method is improved with time. The safety related message needs to be received on time without any delay, and to avoid any delays the SPPA model is implemented to detect the attack within a minimum time frame. According to the analysis graph, the detection time is clearly efficient within the minimum time.

5.6 Routing overhead (RO)

This is the amount of routing packets applied for of frequent link breaks that start to frequent path breakdowns and route breakthroughs. The routing overhead increases with

Fig. 16 Detection time analysis



the number of vehicle nodes, because the control messages turn out to be enormous in VANET networks as they contain the whole neighbour vehicle list. The vehicle routing packet will retain the updated information about the network routes and the algorithm of routing will produce small size vehicle packets named routing packets. For example, to check whether a neighbouring vehicle is active or not by using a "HELLO" packet. Normally, the routing will not carry and application content comparable to the date packet will. Most of the time the network bandwidth needs to be shared by data packets and routing. The overheads in the VANET network are based on routing packets and is called routing overhead. According to research, a good routing protocol would sustain a lower routing overhead. By taking this performance metric, the comparison between the routing mechanism and the current mechanism or method on the same metric can be brought out to test the performance of SPPA model against the existing methods. The performance of Routing Overhead is shown in Fig. 17. The results can be obtained from the following formula:

$$RO = Total\ Number\ of\ the\ Routing\ Packets / Total\ Number\ of\ Data\ Packets\ Received\ from\ Source\ Vehicle \quad (2)$$

Fig. 17 Routing overhead analysis

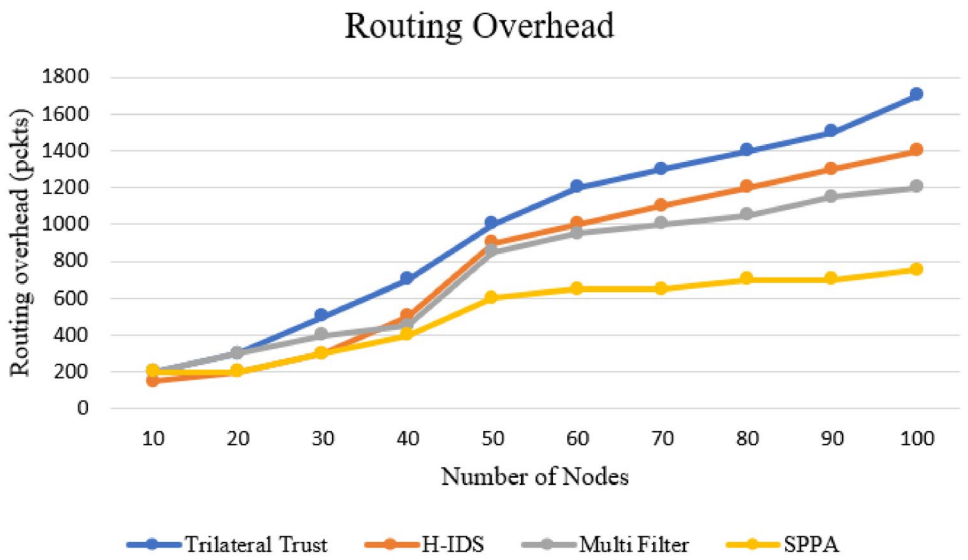
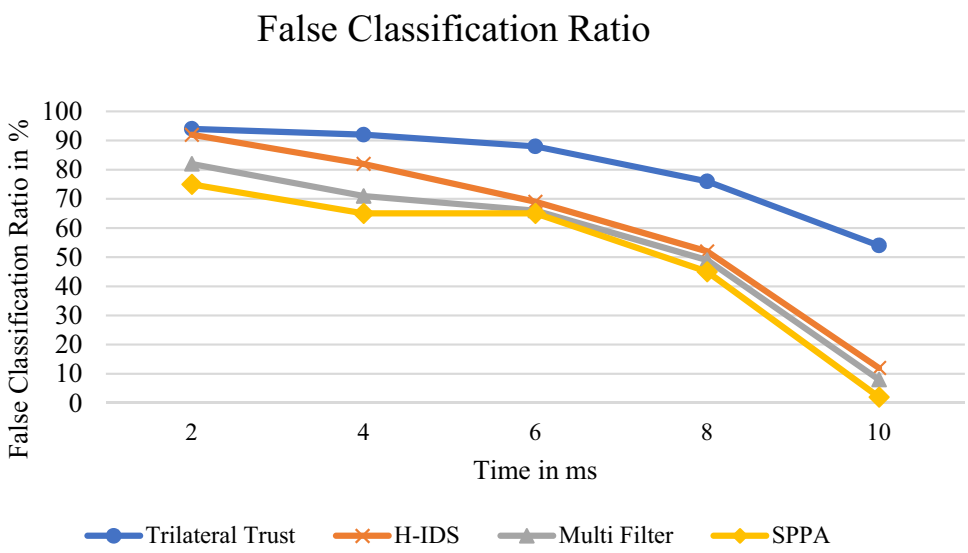


Fig. 18 False classification ratio



5.7 False classification ratio

The false classification has been performed in two ways—either classifying the true vehicle node as the false vehicle node or the false vehicle node as the true vehicle node. So, by computing both, the false classification ratio can be calculated (Kolandaisamy et al. 2019a, b). For calculation we have used terms called TP and FP, where "TP" is True Positive, and "FP" is False Positive. The TP is also called true positive message rate of detection in some field. Besides that, true positive refers to the number of genuine positive messages that are correctly recognized, for example the percentage of the genuine message which is properly recognized as having the issues. Another example is the case where a driver is actually attacked by DDoS (1) and the model classifies the case as DDoS Attack (1). Moreover, False Positive is also referred to as false alarm rate. The false positive itself denotes safety or non-safety messages incorrectly signalling seeing genuine issues such as security breaches or spam. For example, the percentage of genuine messages which are properly recognized as not having issues, such as where a driver NOT attacked by a DDoS and the model flags the case as a DDoS attack. It has been computed as follows:

$$\text{False Classification Ratio} = \frac{TP + FP}{\text{Total number of nodes}}$$

Here TP—true positive and FP—false positive.

The false classification has been performed either as classifying the true node as false, or the false node as true. So, by computing both, the false classification ratio can be calculated. Figure 18 shows the false classification ratio analysis.

6 Conclusion

In the proposed SPPA model, the detection of a DDoS attack is established on the calculated amount of the CCA. The behaviour of each and every single vehicle is assessed, and the genuine weight of the vehicle or node is calculated. Utilizing this legitimate weight, the attack detection is accomplished by examining whether the vehicle is an intruder or normal node. Finally, the planned method's assessment result reduces the end to end delay and transparency occurred in the complex (Shakshuki et al. 2013; Fotohi et al. 2016) and improves the detection and routine of the network (Shakshuki et al. 2013; Chikhaoui et al. 2017; Fotohi et al. 2016; Jalil et al. 2020). For future work, it will be useful to investigate including an additional layer of classification after the DDoS has been detected in order to identify the impact level of the attack.

Acknowledgements This work was supported in partnership grant between the University of Malaya and Sunway University under Grant RK004-2017 and in part of RU Grants (Under Faculties) GPF004D-2019; and the Pioneer Scientist Incentive Fund (PSIF), UCSI University, through Research Grant no: Proj-2019-In-FOBIS-023.

Compliance with ethical standards

Conflict of interest The authors declare that they have no competing interests.

References

Ahmad I, Ahmad I, Imran M, Sattar K, Shoaib M, Nasir M (2017) Towards intrusion detection to secure VANET-assisted healthcare monitoring system. J Med Imaging Health Inform 7(6):1391–1398

Balan EV, Priyan MK, Gokulnath C, Devi GU (2015) Fuzzy based intrusion detection systems in MANET. Procedia Comput Sci 50:109–114

Bhushan K, Gupta BB (2019) Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. J Ambient Intell Hum Comput 10(5):1985–1997

Cheng J, Tang X, Yin J (2017) A change-point DDoS attack detection method based on half interaction anomaly degree. Int J Auton Adapt Commun Syst 10(1):38–54

Chikhaoui O, Chehida AB, Abassi R, El Fatmi SG (2017) A ticket-based authentication scheme for vanets preserving privacy. In: International conference on ad-hoc networks and wireless. Springer, Cham, pp 77–91

de Biasi G, Vieira LF, Loureiro AA (2018) Sentinel: defense mechanism against DDoS flooding attack in software defined vehicular network. In: 2018 IEEE international conference on communications (ICC). IEEE, pp 1–6

Fotohi R, Ebazadeh Y, Geshlag MS (2016) A new approach for improvement security against DoS attacks in vehicular ad-hoc network. Int J Adv Comput Sci Appl 7(7):10–16

Fragkiadakis AG, Siris VA, Petroulakis NE, Traganitis AP (2015) Anomaly-based intrusion detection of jamming attacks, local versus collaborative detection. Wirel Commun Mob Comput 15(2):276–294

Fung CJ, Zhu Q (2016) FACID: A trust-based collaborative decision framework for intrusion detection networks. Ad Hoc Netw 53:17–31

Gupta BB, Joshi RC, Misra M (2012) Distributed denial of service prevention techniques. arXiv:1208.3557

Hasrouny H, Samhat AE, Bassil C, Laouiti A (2017) VANet security challenges and solutions: a survey. Veh Commun 7:7–20

Jalil AB, Kolandaisamy R, Subaramaniam K, Kolandaisamy I (2020) Designing a mobile application to improve user's productivity on computer-based productivity software. J Adv Res Dyn Control Syst 12(3):226–236

Kaur M, Mahajan M (2015) A novel security approach for data flow and data pattern analysis to mitigate DDoS attacks in VANETs. Int J Hybrid Inf Technol 8(8):113–122

Kolandaisamy R, Md Noor R, Ahmedy I, Ahmad I, Reza Z'aba M, Imran M, Alnuem M (2018) A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks. In: Wireless communications and mobile computing, 2018.

Kolandaisamy R, Noor RM, Z'aba MR, Ahmedy I, Kolandaisamy I (2019a) Adapted stream region for packet marking based on DDoS attack detection in vehicular ad hoc networks. J Supercomput, 1–23

Kolandaisamy R, Noor RM, Zaba MR, Ahmedy I, Kolandaisamy I (2019b) Markov chain based ant colony approach for mitigating DDoS attacks using integrated vehicle mode analysis in VANET. In: 2019 IEEE 1st international conference on energy, systems and information processing (ICESIP). IEEE, pp 1–5

Lyamin N, Vinel A, Jonsson M, Loo J (2014) Real-time detection of denial-of-service attacks in IEEE 802.11 p vehicular networks. IEEE Commun Lett 18(1):110–113

Nadeem A, Howarth MP (2014) An intrusion detection and adaptive response mechanism for MANETs. Ad Hoc Netw 13:368–380

Panjeta S, Aggarwal EK, Student PG (2017) Review paper on different techniques in combination with IDS. Int J Eng Sci

Pathre A, Agrawal C, Jain A (2013) A novel defense scheme against DDOS attack in VANET. In: 2013 Tenth international conference on wireless and optical communications networks (WOCN). IEEE, pp 1–5

Pillutla H, Arjunan A (2019) Fuzzy self organizing maps-based DDoS mitigation mechanism for software defined networking in cloud computing. J Ambient Intell Hum Comput 10(4):1547–1559

Sangulagi P, Sarsamba M, Talwar M, Katgi V (2013) Recognition and elimination of malicious nodes in vehicular ad hoc networks (VANET's). Indian J Comput Sci Eng 4(1).

Saritha V, Krishna PV, Misra S, Obaidat MS (2017) Learning automata based optimized multipath routing using leapfrog algorithm for VANETs. In: 2017 IEEE international conference on communications (ICC). IEEE, pp 1–5

Shah SAA, Ahmed E, Imran M, Zeadally S (2018) 5G for vehicular communications. IEEE Commun Mag 56(1):111–117

Shakshuki EM, Isiuwe S (2018) Resource management approach to an efficient wireless sensor network. Proced Comput Sci 141:190–198

Shakshuki EM, Kang N, Sheltami TR (2013) EAACK—a secure intrusion-detection system for MANETs. IEEE Trans Ind Electron 60(3):1089–1098

Wang X, Guo N, Gao F, Feng J (2019) Distributed denial of service attack defence simulation based on honeynet technology. J Ambient Intell Hum Comput, 1–16

Xiang M, Chen Y, Ku WS, Su Z (2011) Mitigating DDOS attacks using protection nodes in mobile Ad hoc networks. In: 2011 IEEE global telecommunications conference-GLOBECOM 2011. IEEE, pp 1–6

Yaqoob I, Ahmed E, Ur Rehman MH, Ahmed AIA, Al-garadi MA, Imran M, Guizani M (2017) The rise of ransomware and emerging security challenges in the Internet of Things. Comput Netw 129:444–458