Kolandaisamy, 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. *Wireless Communications and Mobile Computing*, 1–13.

Available online: https://doi.org/10.1155/2018/2874509

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 2874509, 13 pages
https://doi.org/10.1155/2018/2874509

Research Article

A Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks

Raenu Kolandaisamy,[1,2] Rafidah Md Noor,[1] Ismail Ahmedy,[1] Iftikhar Ahmad,[1,3] Muhammad Reza Z'aba,[1] Muhammad Imran,[4] and Mohammed Alnuem[4]

[1] *Faculty of Computer Science & Information Technology, University of Malaya, Kuala Lumpur, Malaysia*
[2] *Faculty of Business & Information Science, UCSI University, Jalan Menara Gading, Kuala Lumpur, Malaysia*
[3] *Department of CS and IT, Mirpur University of Science and Technology (MUST), Mirpur 10250 (AJK), Pakistan*
[4] *College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia*

Correspondence should be addressed to Raenu Kolandaisamy; raenu@ucsiuniversity.edu.my
and Rafidah Md Noor; fidah@um.edu.my

Received 29 December 2017; Accepted 1 April 2018; Published 20 May 2018

Academic Editor: Yin Zhang

Vehicular Ad Hoc Networks (VANETs) are rapidly gaining attention due to the diversity of services that they can potentially offer. However, VANET communication is vulnerable to numerous security threats such as Distributed Denial of Service (DDoS) attacks. Dealing with these attacks in VANET is a challenging problem. Most of the existing DDoS detection techniques suffer from poor accuracy and high computational overhead. To cope with these problems, we present a novel Multivariant Stream Analysis (MVSA) approach. The proposed MVSA approach maintains the multiple stages for detection DDoS attack in network. The Multivariant Stream Analysis gives unique result based on the Vehicle-to-Vehicle communication through Road Side Unit. The approach observes the traffic in different situations and time frames and maintains different rules for various traffic classes in various time windows. The performance of the MVSA is evaluated using an NS2 simulator. Simulation results demonstrate the effectiveness and efficiency of the MVSA regarding detection accuracy and reducing the impact on VANET communication.

1. Introduction

Vehicular Ad Hoc Network (VANET) [1] is a wireless network that allows vehicles to interconnect and communicate with other nearby vehicles, Road Side Units (RSU), or roadside infrastructure. In VANET, each vehicle is considered as a network node which is equipped with an On-Board Unit (OBU) and an Application Unit (AU). The nodes may connect and communicate with each other directly (i.e., Vehicle to Vehicle (V2V)) or through RSUs (i.e., Vehicle to Infrastructure (V2I)) [2–4]. This is primarily for alleviating an Intelligent Transport System (ITS) that aims to provide a wide range of applications and services including safety, nonsafety, and infotainment. In most of these applications, a large number of nodes acquire various services from the network, and the service providing node had a certain capability to handle a specific number of requests. When such requests exceed the capability, the service cannot be guaranteed. On the other hand, the service providing node can accept only a limited amount of data at any point in time, and when it receives a higher payload data packet, it suffers from overload. This high payload data also affects the performance of the network [5, 6]. A VANET architecture and its components are depicted in Figure 1.

The vehicles and RSU act as both transmitters and receivers. The mobility of vehicles is continuous and very fast, especially on highways. Thus, the communication links between vehicles are established only for a short period of time; that is, vehicles are rapidly connecting and disconnecting in the network. This is due to the quickly changing topology. However, mobility of vehicles is predictable as they move on prebuilt highways and roads. Hence the motion pattern of the vehicles can be predicted based on the road topology and layout. Nonetheless, there could be some uncertainty in the movement of vehicles depending upon the

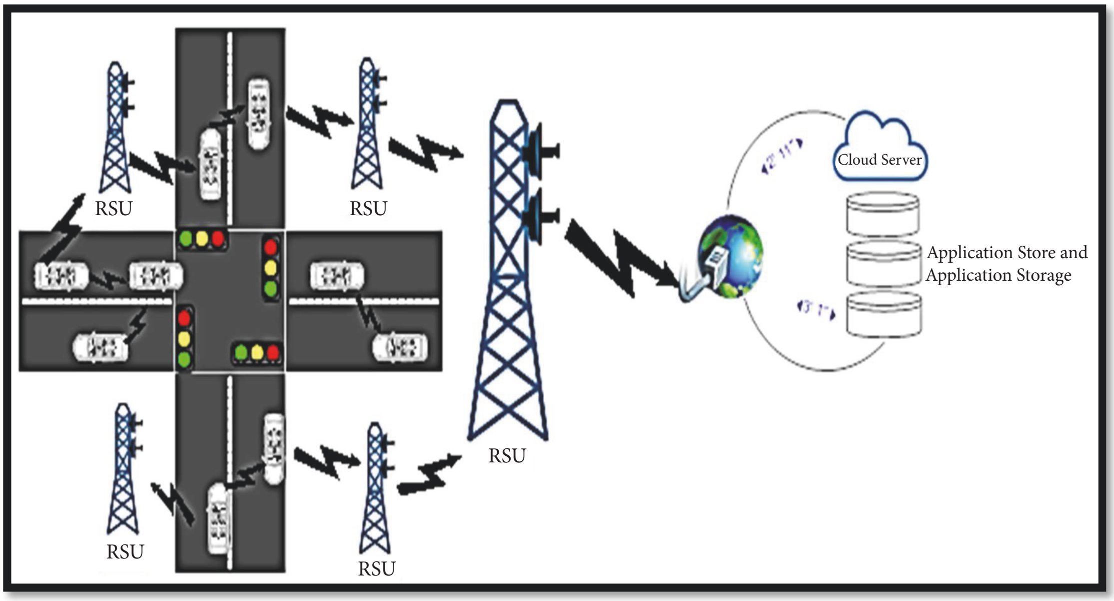


Figure 1: Vehicular Ad Hoc Network architecture.

layout of the road, traffic density, structure of lane, and of course the behavior of the drivers. The nodes in a VANET move at a higher average speed compared to Mobile Ad Hoc Networks (MANETs). The number of nodes in a VANET can be very high on busy highways and very sparse in remote highways. Similarly, at a particular location, traffic is at its busiest during office hours and quiet during midnight hours. Hence any protocol designed should take into consideration these scenarios.

Each vehicular node may acquire a service through various RSU, or the packets might have to travel through several nodes, which makes it vulnerable to Denial of Service (DoS) attacks. In VANET, DoS attacks [6] strive to disrupt the communication channel by flooding it with redundant messages so that legitimate nodes can no longer acquire or use its services. A Distributed Denial of Service (DDoS) attack [6] is more severe as the attack is larger in scale. It involves the participation of multiple nodes across the Internet that the attacker maliciously controls. In a DDoS attack, the attacker may overwhelm the network by using different time slots to send the messages or changing all time slots and messages for different nodes. It is imperative to prevent these types of attacks from crippling the network to allow it to continue its services for safety applications. The objective of this paper is to provide early DDoS detection in VANET environment and make sure the safety of the VANET environment is protected.

1.1. Problem Description. DDoS attack is considered as one of the most severe attacks in VANET. This attack will take down the network to make the service unavailable for the drivers or passengers. This is a vital issue where it may create problem to the drivers on the road and it will particularly be more important if there is life critical information that needs to be transmitted to the drivers. The unavailability of this service or inability to access to it may lead to car accidents [5]. So, this DDoS attack issue cannot be neglected and must be taken seriously. DDoS attack can also occur in any layer of network communication model. The attack will become worse when a DDoS attack which started by more than one perpetrator is executing the attack. This attack is easy to implement and unavoidable for most of the time. In DDoS attack, the attacker controls over the other nodes in network and starts launching attacks from different locations. There are 2 possible scenarios that will happen when a DDoS attack is launched. Figure 2 illustrates DDoS in Vehicle-to-Vehicle communications and Figure 3 illustrates DDoS in Vehicle-to-Infrastructure communications.

(a) Vehicle to Vehicle. Attacker sends messages to victim from different locations or vehicles with the possibility of using different time slot. This attack is to take down the network to make it unavailable for the victim [6].

(b) Vehicle to Infrastructure. Instead of targeting the vehicles, the attacker targets the RSU. The attack will come from different locations and if there are other nodes that wanted to communicate with the RSU, it has already been overloaded. Hence, the service is not available [6].

1.2. Limitations of Existing Approaches. Therefore, there are limited existing solutions for VANETs from DoS and DDoS attacks. The limitations are due to advanced technology and the current threats which are more difficult to prevent. This situation would allow the attackers to detect the ways to intrude into networks. The main limitation of the existing approach is more time is taken to detect the DoS and DDoS

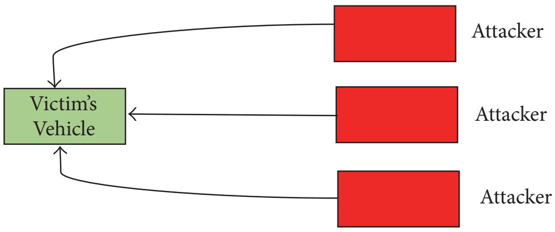


Figure 2: DDoS in Vehicle-to-Vehicle communications.

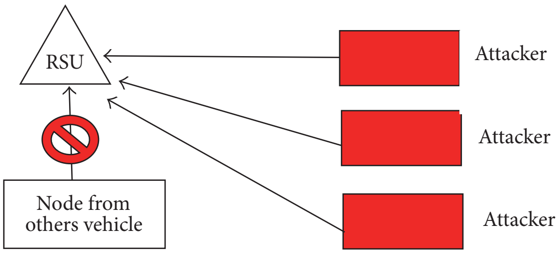


Figure 3: DDoS in Vehicle-to-Infrastructure communications.

attack in VANET environment. Moreover, the existing model has more steps and long algorithm which affects the efficiency and effectiveness [7].

To solve the problems mentioned above, we present a Multivariant Stream Analysis (MVSA) approach to detect and mitigate DoS/DDoS attacks. The proposed approach classifies the traffic into safety and nonsafety applications and RSUs initially maintain structure for V2V communication for generating the traces in the network, to check all node packets. If there is no trace (that means attack), then each packet will be considered as genuine. Uncertainty attack or trace occurs, then it will identify the type of the traffic and compute the multivariant stream factor for each time window. Once identifying the traffic, it will compute the stream weight with the help of traces. Finally, MVSA will classify the effected packet. The performance of the proposed approach is evaluated through simulations. Simulation results demonstrate the efficiency and effectiveness of the proposed approach compared to similar existing approaches regarding various performance metrics such as throughput, detection time, detection accuracy, and ratio.

This paper is organized into six sections: the related works are presented in Section 2. Section 3 describes most common attacks in VANET and discusses safety and nonsafety applications. Section 4 describes the proposed approach. Results and analysis are provided in Section 5. Section 6 presents the conclusion.

2. Related Works

VANET security has been extensively investigated in recent years [1, 7]. However, not much work has been done on identification and mitigation of DoS/DDoS attacks in VANET. Therefore, we specifically focus on this topic in the following.

In [8], the author used Dedicated Short Range Communication (DSRC) and revocation techniques. The detection method is constructed on the offender transfer or sending a message to the target node and then to different locations and may also have a diverse time slot for transferring the message, and the offender will attempt to modify the time slot and the message for different vehicular nodes. However, the main reason for the occurrence is to make the network inaccessible to the victims or vehicle nodes by bringing the entire network down. It has seven channels in DSRC, and the author has created four classes that are sorted based on precedence. Class 1 represents the highest, while class 4 represents the lowest. Nevertheless, some node in the VANET infrastructure will receive a restricted amount of security messages at a specified timestamp, so it is considered as the node that has already been attacked. In this way, it can safeguard itself against any DoS and DDoS attacks.

Another potential method to distinguish DDoS attack is using the Bloom Filter and Traffic Capacity methods [9]. The Bloom Filter is constructed with detection scheme, which is used in providing and protecting against IP spoofing in network addresses. The traffic measurements exposure is based on the detection algorithm, and the algorithm works in three phases. Phase one is in charge of gathering data and the second phase will process the data that has been collected from phase one. If no malicious node is found then the data will be kept in the database. Stage three is the Bloom Filter thru hash function; uncertainly any hateful node was initiated by the second phase, then it generates an alarm and sends the information to the entire nodes in VANET.

The Attacked Packet Detection Algorithm (APDA) [9] and Malicious Node Detection Algorithm (MVND) [10] methods are proposed to detect DoS and DDoS attacks. The APDA method considers time stamp, position, and velocity to detect false or malicious nodes. The method of detecting the malicious node before the verification time will reduce the overhead delay of processing in improving the security in VANET. However, the MVND method is used to detect the malicious node before the verification time by using a hybrid network. MVND method firstly will allocate the cluster keys by assigning a primary misgiving value to regulate a threshold value by using standard nonconformity and collecting the behavioral data to determine whether the vehicle is abnormal or modified. If it is detected, then it will isolate the vehicle from the network.

The Hybrid Intrusion Detection System (H-IDS) is proposed by the author [11] to detect DDoS attacks. To enhance the overall detection accuracy, the authors combine the anomaly based and the signature-based detection methods. These methods apply for 2 different datasets of the projected scheme to test the H-IDS performance, and the summary of this proposed method provided improved result compared to a system based on the nonhybrid detection. However, two previous works [12, 13] have used the anomaly based method to detect DDoS attacks. The proposed method is not very effective in detecting DDoS; it is because H-IDS method uses two approaches to detect the DDoS attack. However, if we have more than two approaches in one method, it will take some time to complete the process and will affect the detection time.

The Ensemble Based Multifilter Feature Selection method is introduced by the authors in [14] to detect DDoS in cloud computing environments. The proposed method combines the output of 4 filter approaches to attain the best choice which will then evaluate the method with an intrusion detection benchmark dataset and a decision tree classifier. The finding shows that the projected technique can successfully decrease the number of features from 41 to 13 and consumes a top finding rate. The classification accuracy and detection rate are reasonably good compared to other classification techniques. This particular method is used in cloud computing network.

Trilateral trust is based on a defense mechanism compared to DDoS attacks in cloud computing environments [15]. The proposed "trilateral trust mechanism" helps in detecting different kinds of attack groups at different points of time. The direct trust based defense mechanism is for segregating legitimate attack groups from the huge number of incoming requestors. It is a hybrid mechanism of trust that tracks the zero-trust approach initially and eventually supports mutually momentary trust and mutual trust. This combinatorial trust mechanism helps in detecting almost all kinds of overload conditions at a cautionary period. Detecting the high rate of an attack at an earlier moment in time could reduce the traffic impact towards data centers. The results demonstrated that the mechanism proposed is deployable at data centers for resource protection.

Another method is the Queue Limiting Algorithm (QLA) [16], for Defensive VANET from DoS attacks. This proposed scheme works on the safety channels of DSRC to protect the lives of drivers on the road. Classifications have been done for types of application (safety and nonsafety) and DSCR channels. According to the classification, the safety message will trigger first because the safety message is set at a high priority level. In this technique, each vehicle has a restricted size of receiving safety messages. The capacity limit is decided by the proposed algorithm.

Most methods have the problem of poor performance in DDoS detection accuracy, and this paper intends to outline an efficient approach to improve the performance of DDoS detection.

3. Potential Attacks in VANET and Safety and Nonsafety Applications

Interest in the use of VANET is gradually increasing as it improves the safety of passengers. As VANET is used in the open wireless medium, it attracts numerous possible attacks. Hence, the probability of possible attacks is high. The overview of our proposed DDoS attack detection using Multivariant Stream Analysis method is given in this section. The entire detection process consists of three major steps: step 1: preprocessing, step 2: MVSA, and step 3: DDoS mitigation. Figure 2 illustrates the VANET scenario. The web server handles the instruction noted in the RSU through the Internet. The adaptable nature of networks conveys problems associated with security and traffic safety. Network accessibility has been pretentious straight in the situation of DDoS and DoS attacks, wherever the DDoS attack will occur, then the entire network will collapse [17]. The objective of the offender was to initiate problems for authorized users, and as a consequence, services are not accessible, leading to a DoS attack or DDoS attack [1].

(a) Types of Attack. A description of DoS attacks is provided below.

ID Disclosure. ID disclosure is the uniqueness of other vehicular nodes in the intricate infrastructure network and to identify the present position of the target vehicular node. Ultimately, the offender observes the target vehicular node and sends a dangerous virus to the nearby target node. Once attacked, then they will identify the target node ID and the existing location of the target node. These techniques are used by car rental companies to track their cars [18].

Sending False Information. Sending false information is bogus information intentionally directed by a vehicular node to different vehicular nodes in the VANET network to produce confusion which might lead to misunderstanding of the actual condition. Once the false information has been disseminated, most users will leave the road. The attacker can then subsequently use the road for their personal purposes [18].

Timing Attack. In safety applications, the user should receive accurate information or messages on time without any delay; if it is delayed then it will result in a major accident. Time is a very important concern in safety applications. In this attack, the offender will include time slots to generate delays in the message, and the user will obtain the message after the necessary time [19].

Node Impersonation. A node impersonation is when an attacker alters his or her uniqueness to escape being noticed or detected. The attacker will get a message from the initiator of the message and make some alterations to contents for his/her benefit [19].

Sybil Attack. A Sybil Attack is when a vehicular node directs various messages to different vehicular nodes and every message consists of dissimilar invented source distinctiveness in such a method that the creator does not recognize. The main reason for the attacker is to complicate other vehicular nodes by directing the erroneous messages and to different vehicular nodes consent the road for the profit of the attacker [19].

Denial of Service Attack. In this type of attack, an attacker strives to make the communication channel unavailable for the legitimate vehicular nodes by techniques such as channel jamming. In this case, the affected nodes are unable to send and receive messages [20].

Distributed Denial of Service Attack. The DDoS attacks are produced by DoS attacks [20]. Many offenders launch DoS attacks commencing from dissimilar positions. The offender used altered time slots intended for transferring the messages and time slot of the messages. However, the information may be different from V2V by the attacker. The main reason for the offender is to bring down the entire VANET network in a DoS attack. The circumstance is that the attacker might attack both infrastructure and nodes.

(b) Safety and Nonsafety Applications. As stated earlier, VANET applications can be categorized into safety and nonsafety. The former is more life critical as they are developed to confirm the protection of vehicles and passengers [21, 22]. The latter aims to provide comfort and infotainment to travelers and they can be further divided into pragmatic- and expediency-oriented applications. Table 1 summarizes the different classes of applications and their usage.

4. Multivariant Stream Analysis

In this section, we describe the proposed Multivariant Stream Analysis (MVSA) approach for detection and mitigation of DDoS attacks.

4.1. Preprocessing Stage. In the preprocessing stage, the classification of the safety and nonsafety application traffic will be used. The network trace is maintained by the node which performs DDoS detection. It is just a log of packets received from different source nodes which contain the information of the features considered in this paper. Each packet received will be processed for classification, because the rule is generated at the boot time using the network trace, but if there is no trace, then each packet will be considered as genuine. At the next boot, the detection node will generate the rule. Algorithm 1 discussed the rules. Conversely, the algorithm will compute the rules to perform DDoS attacks detection.

4.2. Multivariant Stream Weight Stage. Multivariant Stream Weight is the second step after the preprocessing step. It is not necessary for the vehicle to read the trace; a single node may be a vehicle which reads the trace and computes the value. The network trace will specify the traffic type and compute the multivariant stream factor. The multivariant stream factor is computed for each time window. By using computed multivariant stream factor, the method computes the multivariant stream weight. Computed stream weight will be used to perform DoS attack detection. Algorithm 2 discusses stream/traffic weight. Conversely, this algorithm will compute the multiattribute stream weight which is used to perform DoS attack detection.

4.3. DDoS Mitigation Stage. DDoS mitigation is the final step in the MVSA approach. In this stage, the node first reads the network trace from neighbor location and preprocesses the logs. The preprocessing algorithm returns the set of rules. As for the received packet stream, the method will compute the multivariant stream weight, by using the rule set generated and stream weight computed, the method will have classified the affected packet. Algorithm 3 discusses the multiattribute similarity measure and stream weight to classify the packet.

Figure 4 illustrates the VANET scenario. The web server handles the instruction nodes in the RSU through the Internet. A main central management station maintains the overall RSUs. The RSU notices the accidents occurring with vehicles and messages are passed through vehicles in a Vehicle-to-Infrastructure (V2I) communication. The V2V denotes the Vehicle-to-Vehicle communication taking place between the vehicles.

Applications of VANET vary in their requirements according to the timely data delivery. The reply time is for the follow-up of accident avoidance in the neighborhood or barrier on the road which tolerates minimum delays for the route optimization models. A minimum delay is acceptable in noncritical delay-tolerant activity mechanisms. The Multivariant Stream Analysis Model and its functional components are shown in Figure 5. Due to the unpredictable nature of the VANET system and high mobility, the detection of DDoS attacks is more challenging [23].

The MVSA method classifies the traffic based on the type of application. Nevertheless, the method maintains various stream classes. The stream class classifies them into two classes: first is safety application traffic and the second is nonsafety application traffic. Conversely, for each class there is a different rule. The rules will be generated according to the number of time windows used, ranging from 1 to 24. As an example, if the class splits time (24) into 1 hour then we will get a 24-time window. The rule will verify the incoming traffic and computes the multivariant stream weight for the incoming packets. Based on computed weight, the method classifies the stream as malicious.

In our model, we are using four parameters. The first is “Payload” which refers to the amount of data present in the packet. The second is “Hop Count,” which refers to the number of intermediate nodes a message must have to pass through to reach the destination. The third is “time to live (TTL),” which refers to the lifespan of data in the transmission route or network. However, each data packet has some fixed TTL which is fixed by the MAC layer and the protocol being used. It is also fixed according to the number of hops it has to travel according to the Average Hop

```
Input: Network Trace Nt.
Output: Ruleset Rs.
Step 1. Start
Step 2. Read network trace Nt.
Step 3. Split trace into different time window.
Step 4. Trace set $Ts = \int_{i=1}^{24} \text{Split}(Nt, i)$
Step 5. For each time window Ti from Ts
Step 6. For each stream class Si
Step 7. Compute average payload $Ap = (\sum Ts(Ti, Si).payload)/size(\sum Ts(Ti, Si))$
Step 8. Compute average hop count $Ahc = (\sum Ts(Ti, Si).hop\ count)/size(\sum Ts(Ti, Si))$
Step 9. Compute average ttl value $Attl = (\sum Ts(Ti, Si).TTL)/size(\sum Ts(Ti, Si))$
Step 10. Compute average packet frequency $Apf = (\sum Ts(Ti, Si))/size(\sum Ts(Ti))$
Step 11. End
Step 12. Generate Rule $Gr = [24\ Ahc, Attl, Apf]$
Step 13. Add to rule set $Rs = \sum(Rj \in Rs) \cup Gr$
Step 14. End
Step 15. Stop.
```

Algorithm 1

```
Input: Network Trace Nt.
Output: MVSW.
Step 1. Start
Step 2. Read network trace Nt.
Step 3. For each time window Ti
Step 4. Compute average payload $Ap = (\sum Ts(Ti).payload)/size(\sum Ts(Ti))$
Step 5. Compute average hop count $Ahc = (\sum Ts(Ti).hop\ count)/size(\sum Ts(Ti))$
Step 6. Compute average ttl value $Attl = (\sum Ts(Ti).TTL)/size(\sum Ts(Ti))$
Step 7. Compute average packet frequency $Apf = (\sum Ts(Ti))/size(\sum Ts(Ti))$
Step 8. Compute multi-attribute stream factor masv.
Step 9. $MASV = \frac{Ap}{Apf} \times \frac{Ahc}{Attl}$
Step 10. End
Step 11. $Masw = \frac{\sum MASV}{24}$
Step 12. Stop
```

Algorithm 2

```
Input: Network Trace Nt.
Output: Null.
Step 1. Start
Step 2. Read Network Trace Nt.
Step 3. Rule set Rs = Preprocessing(Nt)
Step 4. Receive incoming packet $P$.
Step 5. Compute multi-attribute stream weight MASW.
Step 6. For each rule Ri from Rule set Rs
Step 7. Compute similarity measure $MASM = Dist(Ri.Pl, P.Pl)/\sum \text{Packets receievd in } Ti \times Dist(Ri.hc, P.hc)/P.ttl$
Step 8. If MASM < MASW && MASM<>Ri.Features
Step 9. Classify True
Step 10. Else
Step 11. Classify malicious
Step 12. End
Step 13. End
Step 14. Stop.
```

Algorithm 3

Table 1: Classes of VANET applications and their usage.

Class	Applications	Example usage
Safety oriented	Real-time traffic	(i) RSU stores real-time road traffic data and made it available to vehicles to deal with the problems of traffic jams and avoiding congestion
	Cooperative message transfer	(i) Stopped or slow vehicles to exchange information with other vehicles (ii) Emergency braking to prevent accidents
	Postcrash notification	(i) Vehicles involved in accidents spread warning messages about its location to inform following vehicles
	Road hazard control notification	(i) Disseminating warning messages to other cars about road curves and sudden downhill sections
	Cooperative collision warning	(i) Warning of a driver's capacity on the crash route
	Traffic vigilance	(i) Input: camera installed at RSU (ii) Tool against driving offenses
Pragmatic oriented	Remote vehicle Personalization/diagnostics	(i) Download and install personalized vehicle settings (ii) Uploading of vehicle diagnostics
	Internet access	(i) Through RSU, vehicles can access Internet
	Digital map downloading	(i) Traveler downloads map of region for travel guidance
	Real-time video relay	(i) Traveler watches real-time video
	Value-added advertisements	(i) Online and offline advertisements to attract customers. For example, petrol pumps, 24-hour convenience stores
Expediency Oriented	Route diversions	(i) During road congestion, routes and trips can be planned
	Electronic toll collection	(i) Toll collection via the application. It will help both toll operators and vehicle drivers
	Parking availability	(i) Search for availability of parking slots
	Active prediction	(i) Expect the upcoming terrain
	Environmental benefits	(i) AERIS study program produces and gains environmentally relevant real-time transportation data
	Time utilization	(i) Browse Internet or productive task during traffic jams
	Fuel saving	(i) Vehicle utilizes TOLL system application to pay toll without stopping, saving of fuel approximately 3%

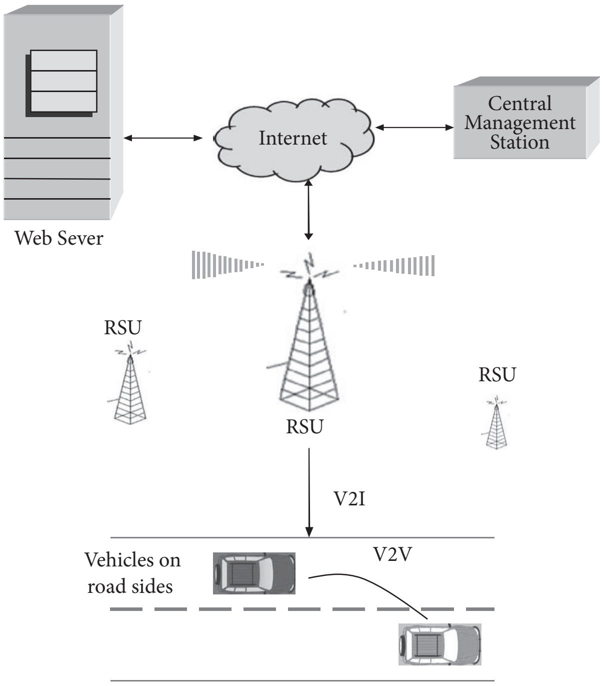


Figure 4: VANET scenario.

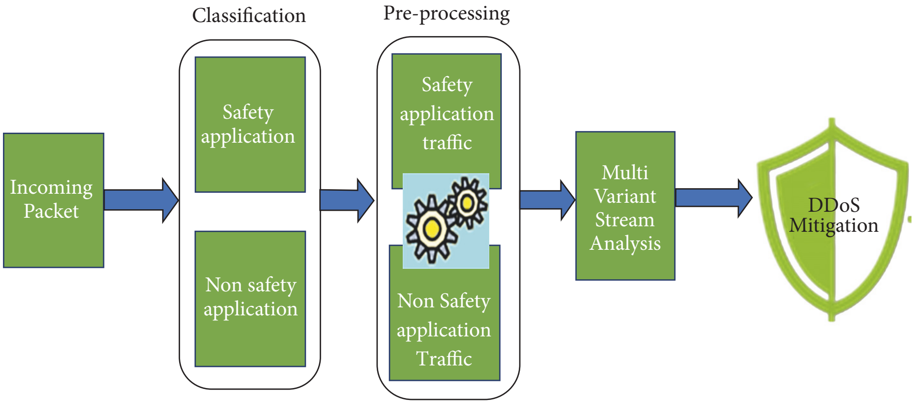


Figure 5: Multivariant Stream Analysis Model.

Table 2: Algorithm rules and its explanation.

Rules	Explanation
Generate rule (Gr) = {Ti, Si, Ap, Ahc, Attl, Apf} Add to rule set (Rs) = $\sum$(Rj ∈ Rs) ∪ Gr	The algorithm will generate the rules according to the Ti, Si, Ap, Ahc, Attl, and Apf. The generated rule will be stored in the set.
$\text{MASV} = \dfrac{\text{Ap}}{\text{Apf}} \times \dfrac{\text{Ahc}}{\text{Attl}}$	The average payload is being used it is because various sources share the bandwidth and the bandwidth utilization is depending on the packet frequency as well. Similarly, the TTL value depends on the hop count.
$\text{Masw} = \dfrac{\sum \text{MASV}}{24}$	The denominator (24) is the entire time value, which is split into the number of the time window. For example, if the class splits time (24) into 1 hour then we will get a 24-time window.
Compute similarity measure MASM $= \text{Dist}(\text{Ri.Pl}, P.\text{Pl}) / \sum \text{Packets receievd in Ti} \times \text{Dist}(\text{Ri.hc}, P.\text{hc}) / P.\text{ttl}$	To compute the similarity, the computed value will be considered. However, computed value for the received packet should fall within the measure of rules that are available for the specific time window. The algorithm must compute the distance between the rules and the features extracted for received packets.
If MASM < MASW && MASM<>Ri.Features	RI. The feature means the feature that is used to detect DDoS attacks. The algorithm has many features in the rule such as time, source, average payload, average TTL, and average hop count. The MASM and MASW are computed according to the mentioned features only. Based on that the decision will be taken.

Count (Ahc). If the packet reaches the destination after the mentioned TTL, then the value is considered as modified or spoofed. So, by counting the TTL value, the chance of being modified can be identified. Nevertheless, if any intermediate node tries to modify or learn the packet features then it will take some time, and it would cross the specified TTL value. Last but not least is the "packet frequency," and the packet frequency is about sending several packets at a particular time. For example, in one minute how many safety application traffic packets have been received and calculate the total number of packets received for safety application.

The incoming packet from V2V and V2I will capture the packet log and send it to the classification stage. In the classification stage, the traffic will identify whether it is safety-oriented or nonsafety-oriented application traffic. Once the traffic is identified, it will go through the preprocessing stage. Once done with the classification process, the preprocessing will generate rules at the boot time using the network trace. If there is no trace, then each packet will be considered genuine. However, the method will read the incoming packet from the classification and split the trace into some classes. One frame is identified for each class, and the method will split the records using traces. The preprocessing will compute the Average Payload (Ap), Average Number of Packets, and Average Hop Count (Ahc). All the three features will compute to generate the rules. The generated rules will be used to perform a DDoS attack. The multivariant stream factor will help to compute each time window. By using computed multivariant stream factors, the method will compute the multivariant stream weight. Computed stream weight will be used to perform DDoS attack detection. Finally, in the DDoS mitigation stage, the rules from preprocessing and stream weight from MVSA will be used to classify the affected packet from the VANET environment. Abbreviations depicts the abbreviation of the algorithm and Table 2 shows the algorithm's rules and its explanations.

5. Results and Discussion

This section describes the simulation setup, performance metrics, baseline approaches, and analysis of results.

Table 3: Simulation configuration.

Parameter	Value
Platform	Ns2
Routing protocol	AODV
Communication range	550 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	Omnidirectional antenna
Traffic type	CBR
Data transmission range	20 Mbps

(a) Simulation Setup. The proposed Multivariant Stream Analysis based DDoS mitigation model has been implemented and evaluated for its efficiency using Network Simulator 2.34. The method has been validated for its efficiency by sometimes maintaining the logs. By using the network trace, the performance of the method for DDoS mitigation was measured. In order to assess the performance, we considered a 4-junction road. In the simulation, the vehicle can initiate a request for its attentive data. However, in the simulation, they were set 5 to 113 vehicles located randomly within the margins. Nevertheless, the vehicle can travel in any direction on the 4-junction road. The time for simulation was executed for 100 Ms. In our simulation, we tested 100 packets and set the simulation time to 100 Ms. Table 3 shows the simulation configuration and parameters for evaluation. However, the mentioned parameters were used in Ns2 to generate simulation to a detected DDoS attack. In this paper we have used AODV routing protocol because our aim is to detect the attack based on routing [1].

There are four junction roads, and they have two lanes in each direction. As shown in Figure 6, there are four crossing junctions through which vehicles may cross each other on the road. In the scenario depicted in the figure, car D is attacked by cars A, C, and E. This is where our proposed model will work to detect the DDoS attack. The result of the simulation is showed in the NAM file, including the trace file routing parameter gained.

(b) Performance Metrics. We measure the proposed model using six different conditions: throughput ratio, packet delay ratio, packet delivery ratio, packet drop ratio, detection accuracy, and detection time [24–27]. The main aim of the performance metrics is to evaluate the performance of MVSA approach to detect the DDoS attack in VANET environments.

Throughput Ratio. Throughput is the factor that is measured based on the number of bytes being sent from the source node towards the destination and the number of bytes being received at the destination at any fraction of the time. Throughput is measured in Kilobits per second (Kbps). For any protocol to prove the efficiency of the protocol, it should achieve higher throughput.

Packet Delay. The packet delivery ratio is the ratio computed between the number of the packets being sent by source node at any point in time and the number of the packets which was received at the destination at the same time window. The same can be measured based on the number of packets received at the destination at any point in time.

Packet Delivery Ratio. Packet delivery ratio depends on the performance of the routing protocol in the VANET network. There is some important parameter to measure the packet delivery ratio, for example, structure of the network, packet size, transmission range, and number of nodes. The packet delivery ratio can be calculated by dividing the number of the packets sent with the number of packets received by the destination. The higher the packet delivery ratio, the better the performance.

Packet Drop Ratio. The packet drop ratio measured using packet did not or never reached the destination from the source network. Normally it will drop in between transmissions.

Detection Accuracy. A detection accuracy is to monitor a network or systems for malicious activity or policy violations. Any detected activity or violation is typically either reported to an administrator or collected centrally using a security information and event management system.

Detection Time. It is measured based on the time at which the packet has been sent from the origin and the time when it has been delivered to the destination. Detection time = (time received − time sent) in milliseconds.

Figure 7 demonstrates the throughput ratio as a function of time when the baseline approaches are compared with the MVSA. The figure clearly shows that MVSA consistently outperforms baseline approaches. This is due to the simplicity of our MVSA method in detecting DDoS attacks, and we did not merge with any other approach. Moreover, the performance of all the approaches improves with the time. This is because the MVSA approach will generate the rules according to the time windows used, ranging from 1 to 24. As an example, if the class splits time (24) into 30 min then we will get a 48-time window. The rules will verify the incoming traffic and compute the MVSW for the incoming packets. It will execute very fast because of the time windows. The throughput ratio of H-IDS is inferior compared to all other approaches because the method is a combination of two approaches. If we combine two approaches, it will take more time to detect a DDoS attack due to increase in the number of steps.

Figure 8 shows the detection accuracy rate as a function of time when the baseline approaches are compared with the MVSA. This figure indicates that MVSA consistently outperforms baseline approaches. This is because our approach will generate the rules from multivariant stream weight, to classify the effected packet accurately and come out with the high accuracy detection. Moreover, the performance of all

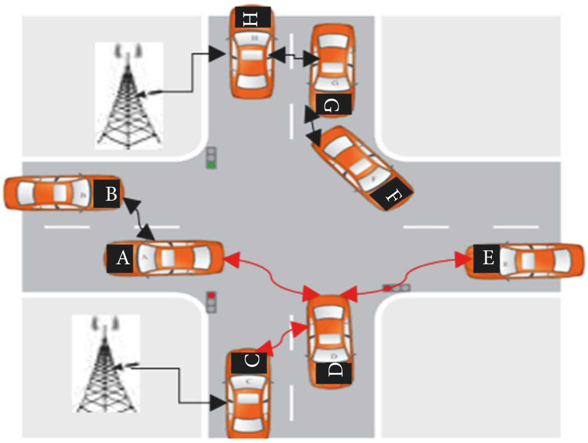


Figure 6: Simulation scenario.

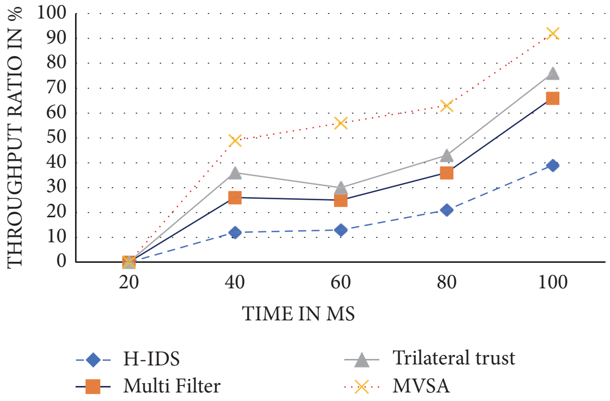


Figure 7: Throughput.

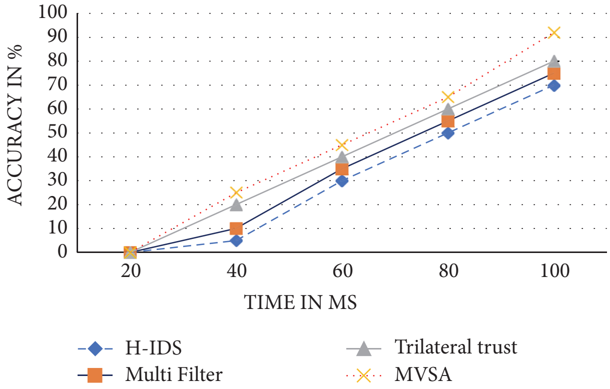


Figure 8: Detection accuracy.

the approaches improves with the time. This is because it takes minimum time to detect in accurate ways. The detection accuracy rate of H-IDS is inferior compared to all other approaches because sometime the vehicle will go far from the neighbor vehicle or RSU.

Figure 9 demonstrates the detection time as a function of time when the baseline approaches are compared with the MVSA. This figure indicates that MVSA consistently outperforms baseline approaches. This is because this approach takes minimum time to detect the DDoS attack compared to another method. Moreover, the performance of all the approaches improves with the time. This is because MVSA approach provides the effective method to detect the attack so that safety application can reach the legitimate user without

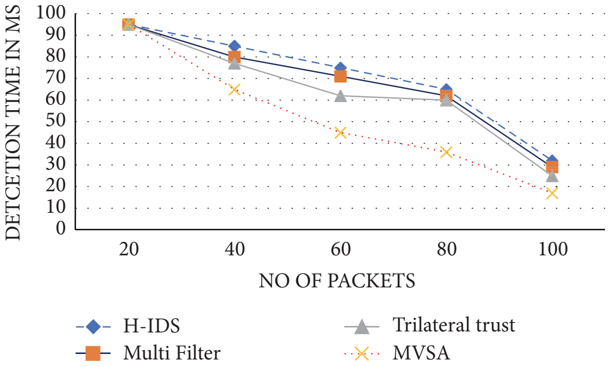


Figure 9: Detection time.

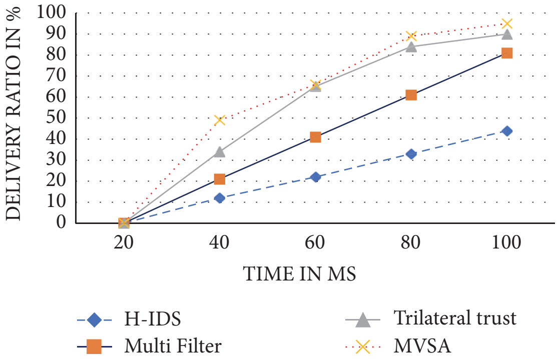


Figure 10: Delivery ratio.

any delay. The detection time of H-IDS is inferior compared to all other approaches because this approach is only focused on throughput and detection accuracy for the network. H-IDS did not focus on detection time, and overall performance is good it will take some time to detect the attack.

Figure 10 demonstrates the packet delivery ratio as a function of time when the baseline approaches are compared with the MVSA. This figure indicates that MVSA consistently outperforms baseline approaches. This is because packet delivery ratio is depending on the performance of the routing protocol in the network. Moreover, the performance of all the approaches improves with the time. This is because if we set more routing protocols then it will take more time to deliver the packet to the destination. Some approach is used for cloud computing network and it will measure the performance of the network. The packet delivery ratio of H-IDS is inferior compared to all other approaches because that approach did not focus on the packet delivery ratio but its more focus on overall throughput, packet delay ration, and detection accuracy.

Figure 11 demonstrates the packet delay ratio as a function of time when the baseline approaches are compared with the MVSA. This figure indicates that MVSA consistently outperforms baseline approaches. This is because of a method that we are using and measurement used based on the stability and performance of the network. Moreover, the performance of all the approaches improves with the time. The packet delay ratio of H-IDS is inferior compared to all other approaches because the approach did not focus on VANET network, its focus on common network. The packet delay is not much different compared with MVSA.

Figure 12 demonstrates the packet drop ratio as a function of time when the baseline approaches are compared with the MVSA. This figure indicates that MVSA consistently outperforms baseline approaches. This is because MVSA approach uses simple method compared with other methods. It is because we spilled rules according to the time windows. Moreover, the performance of all the approaches improves with the time. This is because if we have single process it will reach a destination very fast with less packet drop. If we have more processes it will take more time to process and it will take more time to reach the destination. The packet drop ratios of H-IDS are inferior compared to all other approaches because it focuses on more steps to follow and it also affects the entire packet. Sometimes the vehicle will go far from the neighbor vehicle or the RSU. Its will cause packet drop.

6. Conclusion

In this paper, an efficient Multivariant Stream Analysis (MVSA) approach to detect and mitigate DDoS attacks has been proposed. The vehicle reads the network trace and computes an average measure of payload, time to live, and the frequency for each stream class at different time windows. Four features are measured and computed in the methods to generate the rule set. The rule set is generated, and the features are extracted from the packet received from the user. Nevertheless, the method computes the multivariant stream

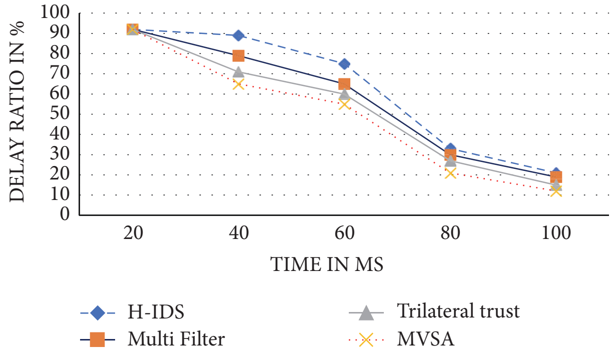


Figure 11: Packet delay.

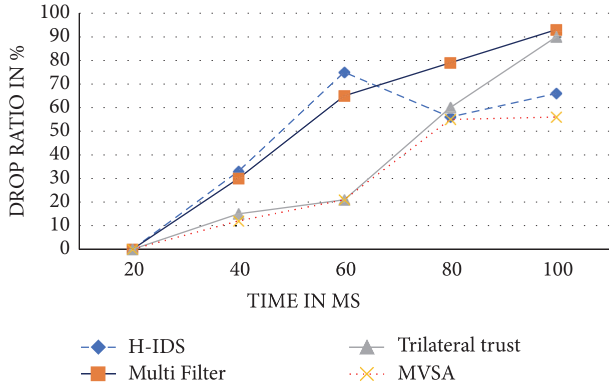


Figure 12: Packet drop ratio.

weight. By using the computed stream weight, the method classifies the packet into either malicious or genuine. The method was shown to be efficient in detecting DDoS attacks in VANET and subsequently reduced the impact on the VANET environment.

Abbreviations

Nt:	Network trace
Gr:	Generate rule
P:	Packet
Rs:	Rule set
Ts:	Trace set
Ap:	Average Payload
Ahc:	Average Hop Count
Apf:	Average Packet Frequency
TTL:	Time to live
Attl:	Average time to live
Ti:	Time window
Si:	Stream class
MVSA:	Multivariant Stream Analysis
MVSW:	Multivariant stream weight
MASV:	Multiattribute stream factor.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the Deanship of Scientific Research, King Saud University, through Research Group no. RG-1435-051.

References

[1] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[2] I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, and N. Guizani, “Overcoming the key challenges to establishing vehicular communication: Is SDN the answer?” *IEEE Communications Magazine*, vol. 55, no. 7, pp. 128–135, 2017.

[3] I. Ahmad, R. M. Noor, I. Ali, M. Imran, and A. Vasilakos, “Characterizing the role of vehicular cloud computing in road traffic management,” *International Journal of Distributed Sensor Networks*, vol. 13, no. 5, 2017.

[4] I. Ahmad, U. Ashraf, and A. Ghafoor, “A comparative QoS survey of mobile ad hoc network routing protocols,” *Journal of the Chinese Institute of Engineers*, vol. 39, no. 5, pp. 585–592, 2016.

[5] L. Li and G. Lee, “DDoS attack detection and wavelets,” *Telecommunication Systems*, vol. 28, no. 3-4, pp. 435–451, 2005.

[6] C. Buragohain, M. Jyoti, S. Singh, and D. K., “Anomaly based DDoS Attack Detection,” *International Journal of Computer Applications*, vol. 123, no. 17, pp. 35–40, 2015.

[7] S. S. Manvi and S. Tangade, “A survey on authentication schemes in VANETs for secured communication,” *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[8] A. Sinha and S. K. Mishra, “Preventing VANET From DOS & DDoS Attack,” *International Journal of Engineering Trends and Technology (IJETT)*, vol. 4, no. 10, 2013.

[9] K. Verma and H. Hasbullah, “Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET,” *Security and Communication Networks*, vol. 8, no. 5, pp. 864–878, 2015.

[10] S. A. Ghorsad, P. P. Karde, V. M. Thakare, and R. V. Dharaskar, “DoS attack detection in vehicular ad-hoc network using malicious node detection algorithm,” *International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE)*, vol. 3, p. 36, 2014.

[11] Ö. Cepheli, S. Büyükçorak, and G. Karabulut Kurt, “Hybrid Intrusion Detection System for DDoS Attacks,” *Journal of Electrical and Computer Engineering*, vol. 2016, Article ID 1075648, 8 pages, 2016.

[12] R. Karimazad and A. Faraahi, “An anomaly-based method for DDoS attacks detection using RBF neural networks,” in *Proceedings of the International Conference on Network and Electronics Engineering*, 2011.

[13] F. Gong, “Deciphering detection techniques: Part ii anomaly-based intrusion detection,” *White Paper, McAfee Security*, vol. 2, p. 1, 2003.

[14] O. Osanaiye, H. Cai, K.-K. R. Choo, A. Dehghantanha, Z. Xu, and M. Dlodlo, “Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, article no. 130, 2016.

[15] N. C. S. N. Iyengar and G. Ganapathy, “Trilateral trust based defense mechanism against DDoS attacks in cloud computing environment,” *Cybernetics and Information Technologies*, vol. 15, no. 2, pp. 119–140, 2015.

[16] A. Sinha and S. K. Mishra, “Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack,” *International Journal of Computer Applications*, vol. 86, no. 8, pp. 14–17, 2014.

[17] E. AnkitaThakur and N. Kapoor, *Novel Technique for DDos Attack Isolation in Vanet*, 2017.

[18] K. Verma, “IP-CHOCK reference detection and prevention of denial of service (DoS) attacks in vehicular Ad-Hoc network: Detection and prevention of denial of service (DoS) attacks in vehicular Ad-Hoc network,” in *Handbook of Research on Advanced Trends in Microwave and Communication Engineering*, pp. 398–420, IGI Global, 2017.

[19] S. Panjeta, E. K. Aggarwal, and P. Student, “Review paper on different techniques in combination with IDS,” *International Journal of Engineering Science*, vol. 11623, 2017.

[20] J. Cheng, X. Tang, and J. Yin, “A change-point DDoS attack detection method based on half interaction anomaly degree,” *International Journal of Autonomous and Adaptive Communications Systems*, vol. 10, no. 1, pp. 38–54, 2017.

[21] A. Rasheed, S. Gillani, S. Ajmal, and A. Qayyum, “Vehicular ad hoc network (VANET): A survey, challenges, and applications,” *Advances in Intelligent Systems and Computing*, vol. 548, pp. 39–51, 2017.

[22] A. Vaibhav, D. Shukla, S. Das, S. Sahana, and P. Johri, “Security Challenges, Authentication, Application and Trust Models for Vehicular Ad Hoc Network- A Survey,” *International Journal of Wireless and Microwave Technologies*, vol. 7, no. 3, pp. 36–48, 2017.

[23] I. Ahmad, I. Ahmad, F. Amin et al., “Towards Intrusion Detection to Secure VANET-Assisted Healthcare Monitoring System,” *Journal of Medical Imaging and Health Informatics*, vol. 7, no. 6, pp. 1391–1398, 2017.

[24] P. Patel and R. Jhaveri, “A Honeypot Scheme to Detect Selfish Vehicles in Vehicular Ad-hoc Network,” in *Computing and Network Sustainability*, vol. 12 of *Lecture Notes in Networks and Systems*, pp. 389–401, Springer, 2017.

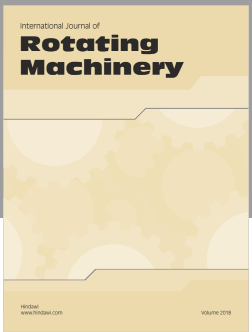
[25] V. Saritha, P. V. Krishna, S. Misra, and M. S. Obaidat, “Learning automata based optimized multipath routingusing leapfrog algorithm for VANETs,” in *Proceedings of the 2017 IEEE International Conference on Communications, ICC 2017*, IEEE, Paris, France, May 2017.

[26] S. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, “5G for Vehicular Communications,” *IEEE Communications Magazine*, vol. 56, no. 1, pp. 111–117, 2018.

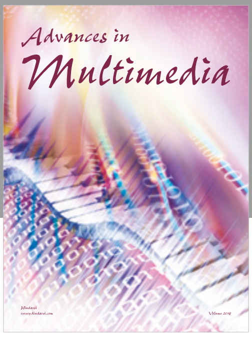
[27] I. Yaqoob, E. Ahmed, M. H. U. Rehman et al., “The rise of ransomware and emerging security challenges in the Internet of Things,” *Computer Networks*, vol. 129, pp. 444–458, 2017.

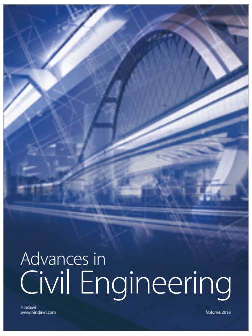
Journal of
Engineering

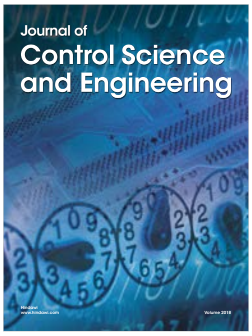
The Scientific
World Journal


International Journal of
Rotating
Machinery

Journal of
Sensors

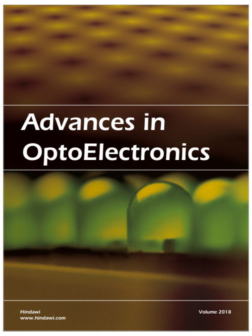

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

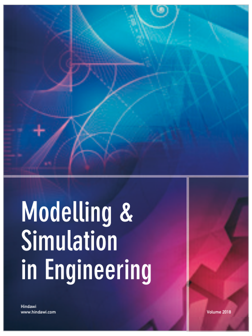
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

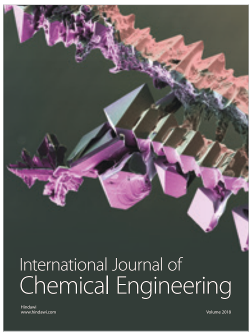

Advances in
OptoElectronics

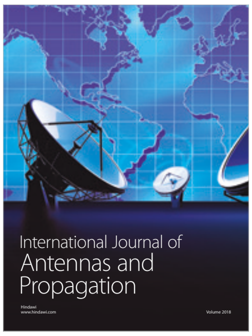
VLSI Design

International Journal of
Navigation and
Observation

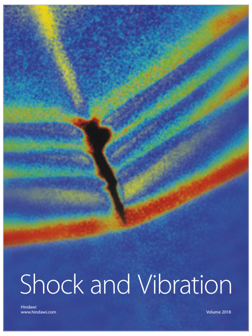

Modelling &
Simulation
in Engineering

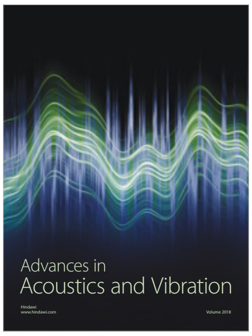
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration