International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Detection and Prevention of DoS Attacks in VANET with RSU's Cooperative Message Temporal Signature

Mahabaleshwar Kabbur, V. Arul Kumar

Abstract: ***Vehicular Ad Hoc Networks (VANETs) is an emerging wireless data communication technology in computer network, which communicates dynamically to exchange and share real time information between vehicles on roads. This network architecture considers vehicles as nodes and information as packets for communication. Vehicles create an autonomous network with assistance of RSU (Road Side Units). This technology supports real time alert systems to broadcast emergency messages to the police, ambulance and drivers of the vehicles in some unexpected situations like traffic emergency, accident, road conditions, vehicle tracking, whether conditions and message monitoring. Since these nodes operate in a physically insecure environment in the range of 100 to 300 meters circumference. Security is a challenging issue for the technology to provide secured prominent approach for routing. Like other networks VANET network is also prone to various attacks. Timing and DoS is done by capturing the messages in VANET and replaying them at later point of time in bulk, such that RSU and vehicle resources are wasted in processing those messages. We need to have a technology by virtue of which network nodes (vehicles) should be smart enough to manage road safety at their own. In this paper RSU assisted DoS attack detection and prevention technique is proposed for VANET. The proposed method is based on RSU message temporal signature with detection and prevention, build over the RSU message attestation technique.***

Keywords: ***VANET, DoS Attack, detection, prevention, message attestation, Temporal Signature***

I. INTRODUCTION

VANET has become a promising technology for vehicular communication. This technology enables variable infrastructure for communication to improve road safety for vehicles. The efficiency and safety level of transportation solution can be improved using it. Each vehicle has onboard wireless transmitter/receiver and the communication is further assisted with a Road Signal Units (RSU) deployed at various locations in roads. Vehicles can communicate with other vehicle directly or through multi hop manner with RSU and other vehicles in path as relay. The autonomous characteristics of VANET expose itself to various security threats [1]. One of the major and challenging attack of emergency messages with respect to authenticity and identifications in VANET is Denial of Service (DoS) attack. In this emergency message attack, attacker attacks the network components by flooding the communication medium with newly generated or already captured packets. The main purpose of attack is to disrupt the network services by wasting the resources of RSU and other vehicles. The DoS attack can be done on vehicles or on the infrastructure nodes like RSU and other resources as shown in figure 1 and figure 2.

The DoS attack can also launched from multiple locations referred as Distributed Denial of Service attack (DDoS). DoS attackers jam the network or channel by flooding the network with packets and causing vehicles and RSU process invalid messages and thereby prevented from processing legitimate messages. Among all the attacks, DoS attack is a severe vulnerability in VANET and timely detection and prevention of attack is necessary for normal operation of the VANET.

In this work RSU assisted detection and prevention of DoS attack is proposed for VANET. The vehicles in the VANET will process the messages only if the message is signed by the RSU. RSU creates a temporal spatial signature for the messages from vehicles after authentication. This authentication is done by RSU only when, message is from valid source and not a DoS attacker. Based on analysis of the temporal signature, RSU detects time based replay attack and DoS attack. Compared to existing solutions, proposed solution is more authenticated and secured for emergency messages. The main contribution of this paper is to secure emergency messages in VANET from DoS Attack.

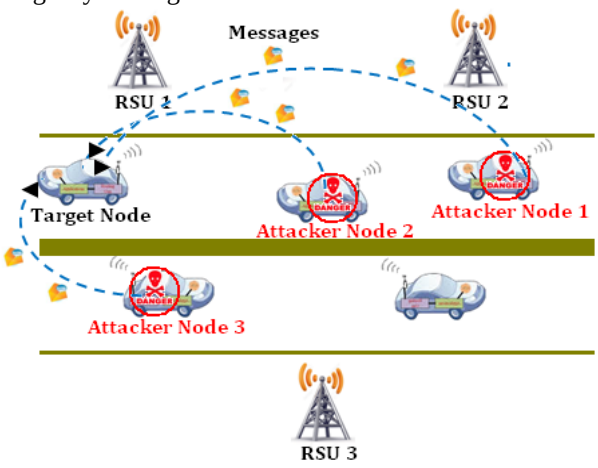

Figure 01 : DoS Attack in Vehicle to Vehicle Scenario

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Mr. Mahabaleshwar Kabbur*, Research Scholar, School of Computer Science & Applications, REVA University, Bengaluru-64
Dr. V. Arul Kumar, Assistant Professor, School of Computer Science & Applications, REVA University, Bengaluru-64,

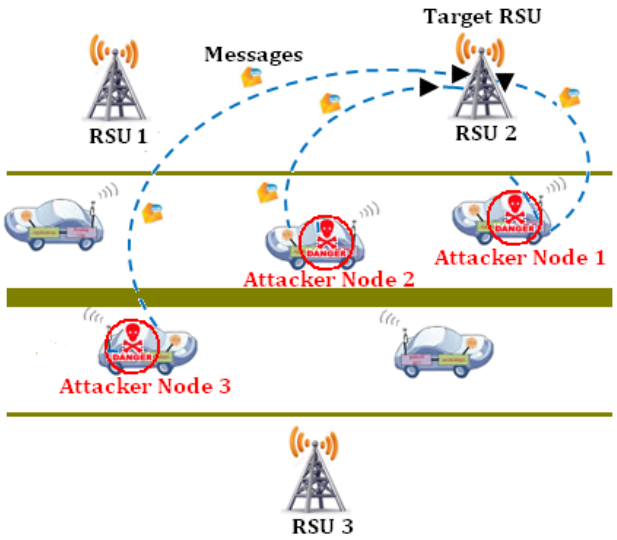

Figure 02 : DoS Attack in Vehicle to Infrastructure Scenario

II. RELATED WORK

In [1] author proposed a DoS detection scheme based on abnormality in communication period between normal and DoS case. Malicious hosts are detected based on the abnormality in number of packets communicated and their IP is broadcasted to prevent the attacks from them. This approach can be easily deceived by frequently changing IP address or launching in DDoS mode. Also there is higher latency in detection of DoS attacks due to which the packet delivery ratio is severely affected.

Authors in [2] proposed a distributed and robust methodology to prevent from DoS attack. Each node learns the IP address using beacon exchanges. Similar IP address and packet outflow from those are used as measure for detecting DoS attack. Prevention of packets from these IP address is done with IP-CHOCK. The latency to detect DoS attack is higher in this approach and it becomes effective only after learning all the IP address in the network.

In [3] author proposed a mitigation scheme against DoS attack on signature-based broadcast authentication. Author designed a pre-authentication technique, which uses two different schemes. In that, one is hash chain and another one is group rekeying. The destination end called receiver must verify the authenticated signature only after processing pre-authentication process for the message. By this resource wastage on processing of DoS messages is avoided. But the process is unsafe if he one way hash gain can be hacked.

Author in [4] proposed a simple algorithm for real-time detection DoS attack launched by beaconing in 802.11p vehicular networks. But the approach has constraints on beaconing order which cannot be implemented in practice.

In [5] to prevent and to detect DoS attack with respective to the emergency message in VANET, a well secured generic based mechanism is implemented. The RSUs uses this algorithm to measure the fitness of vehicle nodes in VANET to justify the survival of the fittest after each timestamp. The worst nodes will be identified as malicious nodes and vehicles will ceased in VANET environment. The malicious nodes are discarded and lose its credentials. A non malicious vehicle node will transmit its generic properties in the form parameters to the RSU. Once the RSU receives parameters from RSU, it computes the fitness of vehicles node based on function of fitness. The authors proposed well structured authentic scheme for message broad casting called Prediction based Authentication to secure an emergency message from DOS attacks. This mechanism is having an advantage of quick authentication by controlling the predictability for one hop applications.

In [6] author proposed a Multivariant Stream Analysis (MVSA) approach for DoS attack detection. 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 weight. By using the computed stream weight, the method classifies the packet into either malicious or genuine.

In [7] author of this paper considered position, time_stamp and velocity as parameters to identify the vehicle node whether it is in the range of radar or not. These parameters are also considered to detect false alarms. In the network, if count of packets and speed of packet is higher than the vehicle node velocity, then node will be considered as attacked node with quick change in position. Similarly, if it is lesser then, it will not change much in the position.

In [8] author used an OBU for the prevention from DoS attack and to extend security for the VANET. The OBU will be fitted in each vehicle to deter a DoS attack. In this methodology processing unit sends an information to OBU. The OBU uses four switching options through switch channel program to detect the received information. These switching options are program switching, path or channel switching, FHSS and radio transceivers.

In [9] author designed DoS attack IP spoofing address detection and prevention methodology using Bloom fitter in network architecture of VANET. In [10] authors designed an algorithm called MADAR which works as DoS attack resistance using mutual privacy preserving methodology. This framework is designed to increase an efficiency based on identity signatures schemes by distinguishing inner region and cross regions.

III. PROPOSED METHODOLOGY

The proposed solution is based on use of RSU in process of attack detection and prevention. Detection relies on cooperation of all the RSU in the network. The prevention is based on vehicles processing only RSU signed messages with signature generated based on spatial and temporal information. With the use of spatio temporal signature, the vehicles takes only limited resources in terms of time and memory to validate the messages. The proposed solutions for attack detection and prevention are detailed below.

A. DoS ATTACK DETECTION

The packet flooded by each vehicle is modeled in terms of a time series at each RSU. For the time series of each vehicle, features are extracted and matched to find the similarity. From the similarity, the probable DDoS attackers are detected in network after categorization of normal and abnormal flows.

The features used for finding the similarity of packet generation time series of vehicles are,

- Power Spectral Density
- Skewness
- Kurtosis

Power spectral Density (PSD): The PSD unit of measure represents strength or quantity of energy of different frequencies within a specific frequency range. Using this we can identify which frequency variations are strong and weak. Measurement unit of PSD is Energy/Frequency.

Periodogram is a tool which is used to identify highest energetic frequency wave in a given frequency range.

The Discrete Fourier Transform (DFT) is the most important mathematical transform which operates on any discrete frequency that varies over time.

In order to find PSD of varies frequencies; Periodogram is the popular estimator [11] uses the coefficients given by Discrete Fourier Transform (DFT) as follows.

$$P\left(\frac{f_k}{N}\right) = \|X(\frac{f_k}{N})\|^2, K = 0,1,2 \ldots \frac{N-1}{2}$$

In an equation X is Fourier coefficient of time series x with N samples.

Skewness: The Skewness of the time series identifies lack of symmetry from the distribution [11]. The value calculated by the skewness function defines the lack of symmetry on time series data. The Skewness for the time series is calculated as,

$$S = \frac{1}{N\sigma^3}\sum_{n=1}^{N}(x_n - \bar{x})^3$$

Where, $\bar{x}$ is the mean and σ is the standard deviation of the sequence.

Kurtosis:

The kurtosis on time series data identifies flat or peaked distribution of frequency compared with normal frequency distribution [11]. The kurtosis for the time series is calculated as,

$$K = \frac{1}{N\sigma^4}\sum_{n=1}^{N}(x_n - \bar{x})^4$$

The features extracted for each vehicle identified in terms of it IP address at each RSU is sent a master RSU for analysis.

<IP address, P, S, K>

K-Means clustering algorithm categorizes the given set of data items into unique group identities, based on certain feature values. In the proposed system the features from all the sources are then clustering using K-Means algorithms into two clusters based on the attributes of <P, S, K>.

After clustering the density of unique IP address in each cluster is calculated. Under the assumption that the attackers will be only very few in the network when compared to normal behavior nodes, the cluster with IP address in the low density cluster is marked as suspicious. The score for each IP address is calculated as,

$$Score(IP) = \begin{cases} 0.5, & IF\ ip\ is\ suspicious \\ -0.5, & IF\ ip\ is\ not\ suspicious \end{cases}$$

The score of IP is updated in every time interval once based on the time series value at that time interval, using exponential moving average model as,

$$Score(IP) = \begin{cases} Score_0(IP), t = 1 \\ \alpha Score_t(IP) + (1-\alpha)Score_{t-1}(IP), t > 1 \end{cases}$$

The Score whose values exceed a Threshold T, IP address is detected as attacker permanently. The IP address of the detected attacker and their feature signatures are sent to each of the RSU for prevention of attacks. The DoS attack detection mechanism is shown in figure 3.

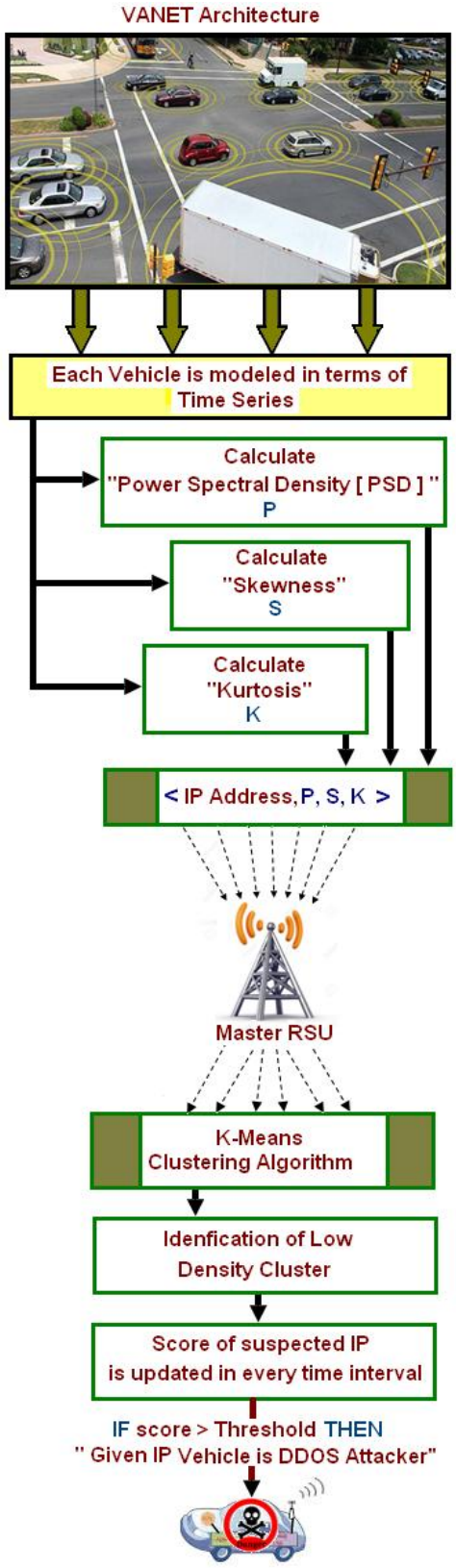

Figure 03: Proposed Model for DoS Attack Detection

Algorithm shown below depicts the actual flow of DoS attack detection mechanism with all necessary attributes and functions.

Algorithm of DoS Attack Detection Method

Algorithm

Step 1 : Start

Step 2 : Extract packets in terms of time series of each vehicle

[Sequence of x with N samples]

Step 3 : Calculate Power Spectral Density (PSD)-**P**

[PSD calculates in terms of Periodogram using DFT]

Step 4 : Calculate Skewness- **S**

[Skewness identifies Symmetry in time series values]

Step 5 : Calculate Kurtosis -**K**

[Kurtosis identifies whether time series data is either peaked or flat]

Step 6 : Features will be extracting for each vehicle and identifing in terms of IP Address at each RSU.

Step 7 : Call **Master_RSU(IP Addresss, P, S, K)**

[Send IP Address, P, S & K Values to Master RSU for Analysis]

Step 8: The features from all the sources are then clustering using K-Means algorithms into two clusters Namely **Normal** & **Abnormal** based on the attributes of <P, S, K>.

Step 9: Calculates density of unique IP Address in each cluster

[Cluster with IP address in the low density cluster is marked as suspicious]

Step 10 : Score of IP is updated in every time interval.

$$Score(IP) = \begin{cases} 0.5, & if\ ip\ is\ suspicious \\ -0.5, & if\ ip\ is\ not\ suspicious \end{cases}$$

Step 11 : IF score > Threshold **Then** "Given IP Vehicle is DoS Attacker Vehicle"

Step 12 : Stop

B. DoS Attack Prevention

The attack prevention is enforced at each RSU. Vehicles can send any messages to other only through RSU. Vehicles must not process any message without RSU signature. From the master RSU, each RSU receives the attacker IP list and the feature signature of the attackers. Each RSU stores it to make the decision about prevention of attacks.

When an unsigned message is received at the RSU, RSU drops the message if the source IP address is in the attacker IP list or if the features gathered over time interval from that IP address is matching to the feature signature of the attackers. Only the messages which are not filtered are signed with RSU signature and broadcasted to vehicles. The RSU signature must be generated in a way satisfying following two conditions.

1. Resilience against timed capture and replay attacks.
2. Low complexity verification.

To satisfy both the above conditions temporal signature scheme is proposed. The messages are signed with a seed created based on RSU's temporal signature. Multiple power levels for transmission are available at RSU and every time RSU selects a random power level for transmission. With all necessary attributes and functions.

The signature is created based on current message (m), current time stamp (t), power level (PL) selected. Signature is generated using MD5 hash function as,

$$S = Subset(MD5(m,t,PL), PL)$$

S is a string and based on the PL, selects a subset from S as signature to be sent in the message. The message broadcasted by RSU has following information.

$$Payload =< message, S >$$

At the receiving end, vehicle measures the PL and adds a degradation values based on RSU's location advertised in the Hello message when the vehicle entered the service area of RSU.

$$PL_{calc} = PL_{measured} + PoweDegration\ (Rl, Vl)$$

Where, *Rl* is RSU location and *Vl* is Vehicle Location.

The latency for reception of message from RSU is found to lie in discrete intervals of lt_{min} *to* lt_{max}

Signature is calculated for all the intervals from lt_{min} *to* lt_{max}

$$S_{calc} = \prod_{l=lt_{min}}^{lt_{max}} Subset(MD5(m, t+l, PL), PL) \ldots$$

Algorithm shown below depicts the actual flow of DoS attack prevention technique with all required attributes and functions.

Algorithm of DoS attack prevention Method

If any of the calculated S_{calc} matches to the S in the message,

Algorithm

Step 1 : Start

Step 2 : Message send by the vehicles.

Step 3 : RSU s receives all emergency message & attacker IP list from Master RSU

Step 4 : IF < Source message from attacker IP list vehicle > **THEN** "RSU drops the message"

ELSE

→Messages signed with RSU Signature & Broadcasted

Call Temporal_signature_process()

$$S = Subset(MD5(m,t,PL), PL)$$

[**S** is a string based on PL]

→The Message broadcasted by RSU with following info to vehicles.

$$Payload =< message, S >$$

Step 5 : At the receiving end , Vehicle measures the PL and Adds the a degradation value based on RSU location.

$$PL_{calc} = PL_{measured} + PoweDegration\ (Rl, Vl)$$

[Where, *Rl* is RSU location and *Vl* is Vehicle Location.]

Step 6: IF *Plcalc* matching with S then Message Accepted & message broadcasted to vehicles

ELSE Message Rejected

Step 7 : Stop

the message is accepted as real message and passed for subsequent processing; else it is dropped as DoS attack message. Proposed mechanism of DoS attack prevention is shown below.

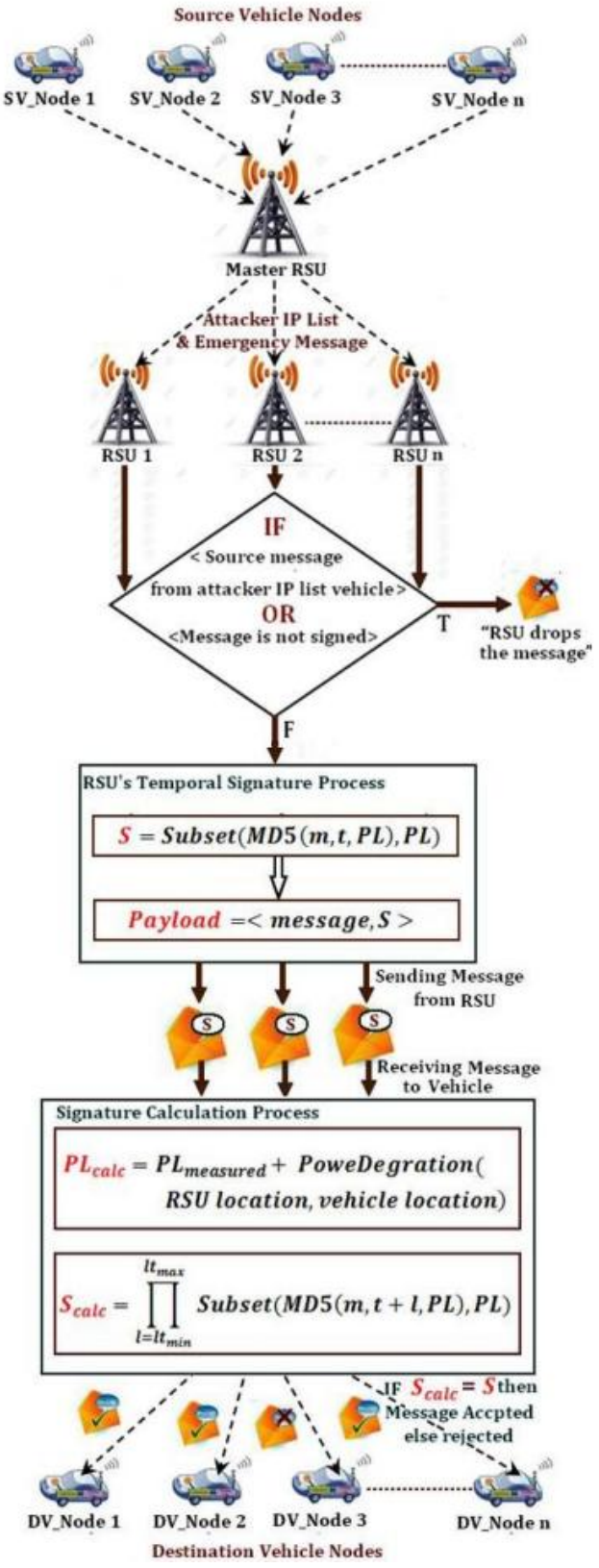

Figure 04: Proposed Model for DoS Attack Prevention

IV. RESULTS

The proposed solution was tested for following VANET topology with RSU at every corner.

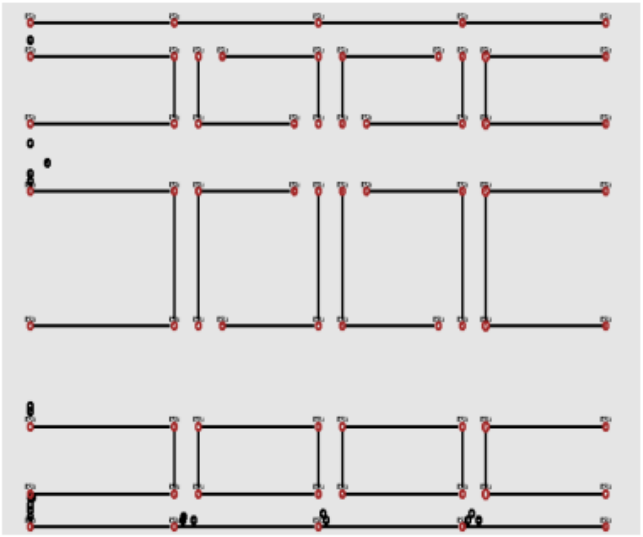

Figure 5: Simulation Topology

The simulation was conducted with following configurations.

Number of Vehicles	100 to 500
Number of Malicious nodes	10 % of Number of Vehicles
Percentage of DoS attackers	10% of the total number of vehicles
Simulation Duration	10 minutes
Vehicle Speed	30 m/ second
DoS Attack rate	10 messages / second

Table 1: Simulation Configuration

The performance of the proposed solution is measured in terms of

1. Attack Detection Ratio : This is the ratio number of DoS attackers detected per minute.

2. DoS Message Rejection Ratio : This is measured as the time to detect all the attackers for different number of vehicle.

3. Attack Detection Accuracy : This is the number of DoS message detected and dropped for every 30 seconds interval.

1. Attack Detection ratio:

The performance of the proposed solution is compared against abnormality based DoS attack detection approach proposed in [1].

Figure 6 shows the attack detection ratio, which is measured by varying the number of vehicles.

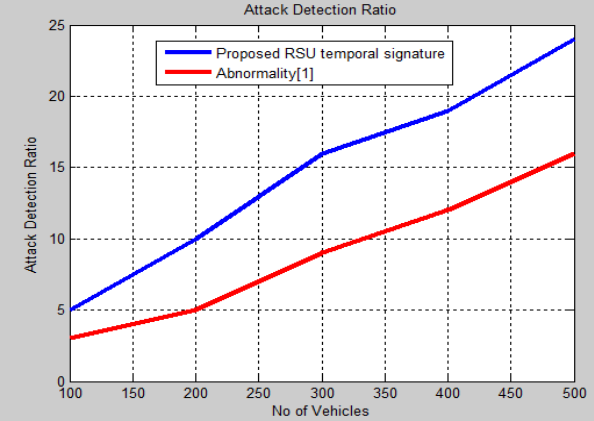

Figure 06: DoS attack detection ratio

Figure 7 shows the attack detection ratio, which is measured for various percentages of attack nodes for the network size of 500 nodes.

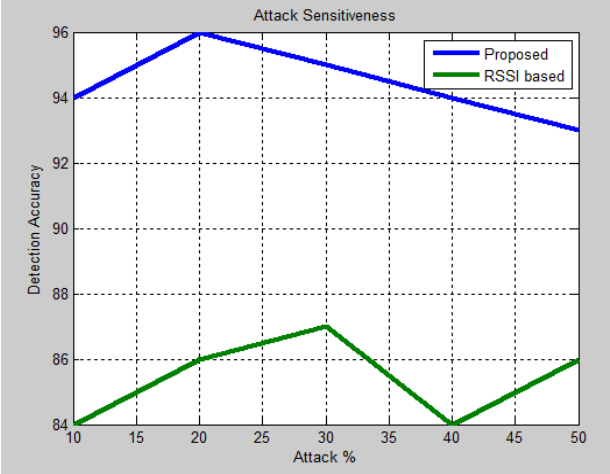

Figure 07 : DoS attack detection ratio

Figure 8 shows the Attack Detection ratio, which is measured for various speed of nodes for a network size of 500 nodes.

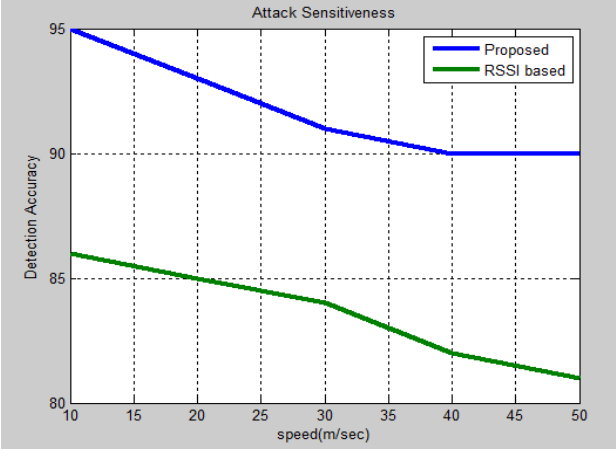

Figure 08 : DoS attack detection ratio

As per the result shown in figure 6, 7 and 8, result is confirming that, the attack detection ratio is higher in the proposed solution compared to Abnormality based detection method proposed in [1]. The higher the attack detection ratio, all the attackers would be detected in less period of time and the effect of DoS messages could be avoided sooner.

2. Attack Detection Time:

The attack detection time is measured for different number of vehicles and comparison result is plotted below.

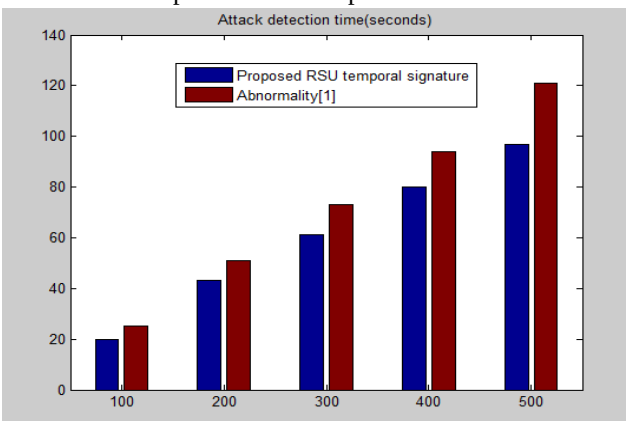

Figure 09: DoS attack detection Time

As per the result shown above (Figure 9), it can be seen that, the time required to detect the attack is comparatively less in the proposed RSU temporal signature method compared to Abnormality based detection method [1].

3. DoS message rejection rate:

The graph of DoS message rejection rate for every 30 second interval with 500 nodes and 50 nodes is plotted below.

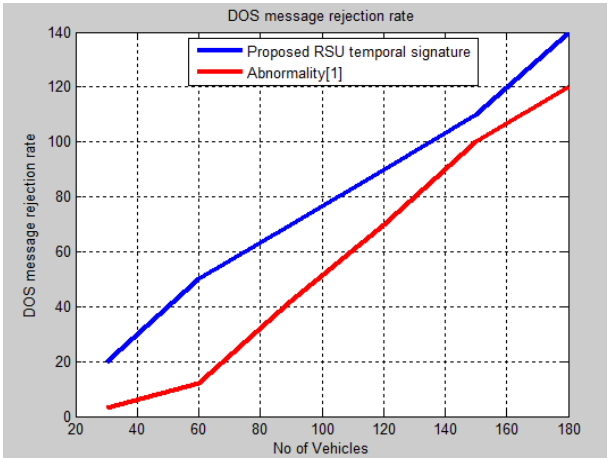

Figure 10: DoS message rejection rate

From the results plotted in Figure 10, it can be seen that, the DoS message rejection ratio is higher in the proposed solution compared to Abnormality based detection method [1].

V. CONCLUSION

RSU message temporal signature based attack detection and prevention is proposed in this work. RSU cooperate with each other to learn the features from the packet rate time series of each vehicle. Through clustering, those feature data learns the normal and abnormal signatures. The existing attackers detected from their abnormal signatures are blocked and new attackers are detected by matching the features extracted from their packet rate to known attack feature signatures. RSU signs the non DoS attack message with temporal signatures and broadcasts.

Other vehicles are able to validate the RSU signed messages without getting affected by timing message attacks. The proposed methodology is compared against [1] to identify Attack Detection ratio, Attack Detection Time and Message rejection rate. The comparison result shows that proposed methodology is more effective than [1].

REFERENCES

1. M.Shabbir, M A Khan, U S Khan and N A Saqib, "Detection and Prevention of Distributed Denial of Service Attacks in VANETs," 2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, 2016, pp. 970-974.
2. Karan Verma, Halabi Hasbullah, Ashok Kumar, Prevention of DoS Attacks in VANET, New York , Wireless Pers Commun, Springer Science+ Business Media, 2013.
3. He L & Zhu WT, "Mitigating DoS attacks against signature based authentication in VANETs". IEEE Inernational Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China. 2012.
4. Nikita Lyamin, Agnus Jonsson, and Jonathan Loo, "Real Time Detection of DoS Attacks in IEEE 802.11p Vehicular Networks", IEEE Communications Letters , Accepted for Publication 1 1089 – 7798 / 13 2013.
5. Avleen Kaur Malhi1 & Shalini Batra, "Genetic-based framework for prevention of masquerade and Distributed Deniel of Service attacks in VANET", Security Comm, . Networks 2016.
6. Raenu Kolandaisamy, Rafidah Md Noor, Ismail Ahmedy, "A Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in VANET" , Wireless Communications and Mobile Computing 2018.
7. Gandhi UD, Keerthana RVSM. Request response detection algorithm for detecting DoS attack in VANET. 2014 Internatinal Confernce on Reliability, Optimization and Information Technology : ICROIT 2014- MRIU- 2014 Feb- India- p. 6–8.
8. Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan, "DoS Attack and its possible solutions in VANET," World Academy of Science, Engineering and Technology- 65-2010.
9. Karan Verma, Halabi Hasbullah, "Bloom-filter based IP - CHOCK detection scheme for DoS Attacks in VANET", Security and Communication Network - 2014.
10. Cong Sun, Jiao Liu , Xinpeng Xu and Jianfeng Ma, "A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETs", IEEE Access 2169-3536, 2017.
11. Ramin Fadaei Fouladi , Cemil Eren Kayatas & Emin Anarim Ramin Fadaei Fouladi, "Statistical Measures: Promising Features for Time Series Based DDoS Attack Detection" in MDPI Proceedings, 2018.
12. Mahabaleshwar Kabbur & Dr. V. ARUL KUMAR,, "Cooperative RSU Based Detection and Prevention of Sybil Attacks for Emergency Messages in Routing Process of VANET" Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 2, XX-YY-2019

AUTHORS PROFILE

[1]Mr. Mahabaleshwar Kabbur, research scholar of Reva University**.** He has obtained his Master's degree in Computer Applications (MCA) and research degree in Master of Philosophy in computer science (M.Phil). He has 11 years of experience in teaching and 02 years of experience in research. He is pursuing his doctoral research on "Security on Wireless networking with respect to VANET". He is published 05 research articles in UGC approved international journals and presented 12 articles in various National and International conferences. His specializations and research interests include Network Security, Content-Based Image Retrieval Techniques & IoT.

[2]Dr. V. ARUL KUMAR, Assistant Professor in School of Computer Science & Applications holds doctoral degree in Computer Science from Bharathidasan University-Tamil Nadu. He has completed B. Sc (Applied Sciences – Computer Technology), M.Sc (Applied Sciences – Information Technology) from K.S.R College of Technology and M.Phil in Computer Science from Bharathidasan University, Tamil Nadu. He has 5 Years of experience in teaching and 7 years of experience in research. He has qualified in State Eligibility Test (SET) conducted by Mother Teresa Women's University. He has published 18 research articles in the various International / National Journals and conferences. His Research area includes data Mining, cloud security and cryptography.