MAR_Spoof: Securing VANET against Spoofing and Tunneling attack with cooperative assistance from RSU

Mr. Mahabaleshwar Kabbur[1], Dr. Arul Kumar V[2]
[1]Research Scholar
School of Computer Science & Applications
REVA University, Bengaluru-64
Email id: mskabbur.reva@gmail.com
[2]Assistant Professor
School of Computer Science & Applications
REVA University, Bengaluru-64
Email id: arulkumar.v@reva.edu.in

Abstract.VANET is also a Mobile ad-hoc network, which consists of moving vehicles as nodes to create an autonomous network with fixed RSU (Road Side Units) and RTA (Regional trusted Authority acts as a certificate authority). All vehicle nodes create a network in the range of 100m to 300m for information interchange [1]. The primary goal of this network is to provide security measures and to increase data transportation efficiency in message communication. It provides useful information to the vehicles about directions, location mapping, premises, etc. In VANET architecture, vehicle nodes will adjust and react to the data received from other nodes or RSU, inflicting a topology change in the network. Once the vehicle gets into the network it aids in providing an alert and warning message to the neighbouring regarding any incidents occurs on the road such as accidents, roadblock due to fog etc.,.[2] In these cases vehicle node must send emergency and local warning messages to the other nodes to avoid secondary accidents in the same place. If the message communication path is not secured and guaranteed, several attacks may affect, thereby emergency messages may not reach to the destination on time. The spoofing & tunnelling attack are major attacks which may occur on emergency messages in VANET infrastructure.In VANET, localization of vehicles is very important for various services like routing, congestion control, navigation etc. GPS (Global Positioning System) is currently the most adopted means for localization with every vehicle fitted with the GPS receiver, which calculates the position with pseudo-random signals from the satellites. But attackers can launch GPS Spoofing attack by sending GPS false signals using GPS simulators and make the localization operation erroneous. Once localization is incorrect, it also affects services built on it like routing, navigation etc. Another important vulnerability in VANET is tunnelling attack. This attack can be launched with GPS Spoofing to continuously deceive the vehicle with incorrect location information without getting detected. This work proposes RSU cooperation-based approach to detect and defend against GPS Spoofing attack which is easy to implement in vehicles without much complexity.

Keywords: VANET, RSU, Spoofing, Emergency message, attack, GPS,Security.

ICASISET 2020, May 16-17, Chennai, India

DOI 10.4108/eai.16-5-2020.2303971

I. Introduction

VANET is the next-generation technology for vehicular communication for entertainment, vehicular safety and emergency services. In VANET all vehicle nodes will communicate with other vehicles or RSU[1]. Due to a wide range of safety and non-safety applications, VANET has become a major area for research. Many of these applications require the location of the vehicles to configure the node in VANET architecture. Figure 01 shows basic architecture with participating components of VANET environment.

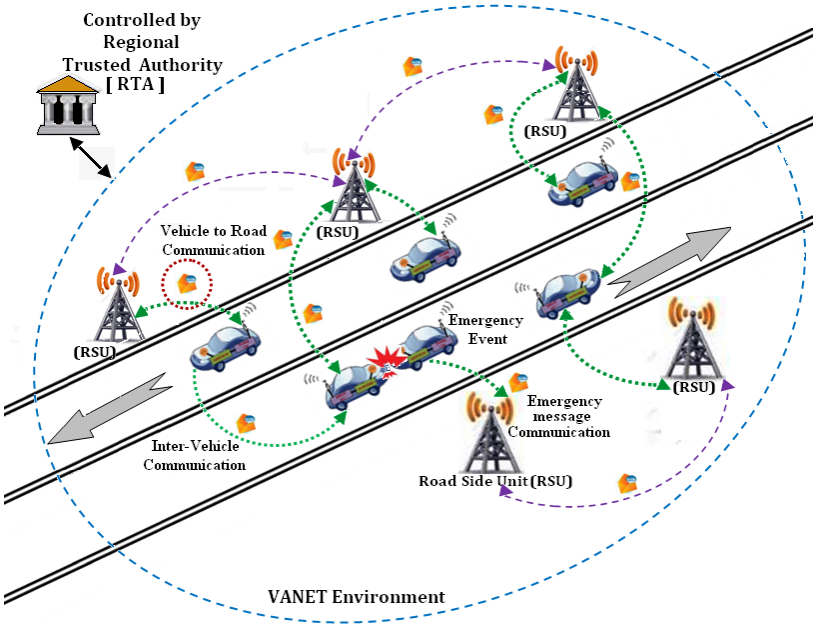

Figure 01: VANET architecture

GPS is currently the most adopted vehicle localization technology. GPS receiver fitted in vehicles which calculate the location of the vehicle using trilateration technique with pseudo-random signals from satellites. Shown in figure 2.

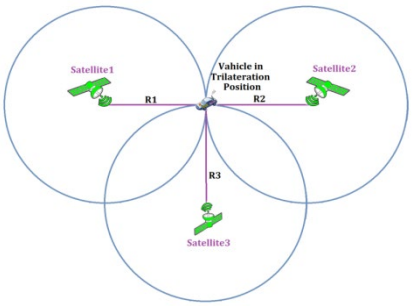

Figure 02: Trilateration technique

The trilateration method can be easily made erroneous by deceiving the GPS receiver with false pseudo-random signals generated from a GPS simulator. This type of attack is called a GPS Spoofing attack is shown in figure 3.

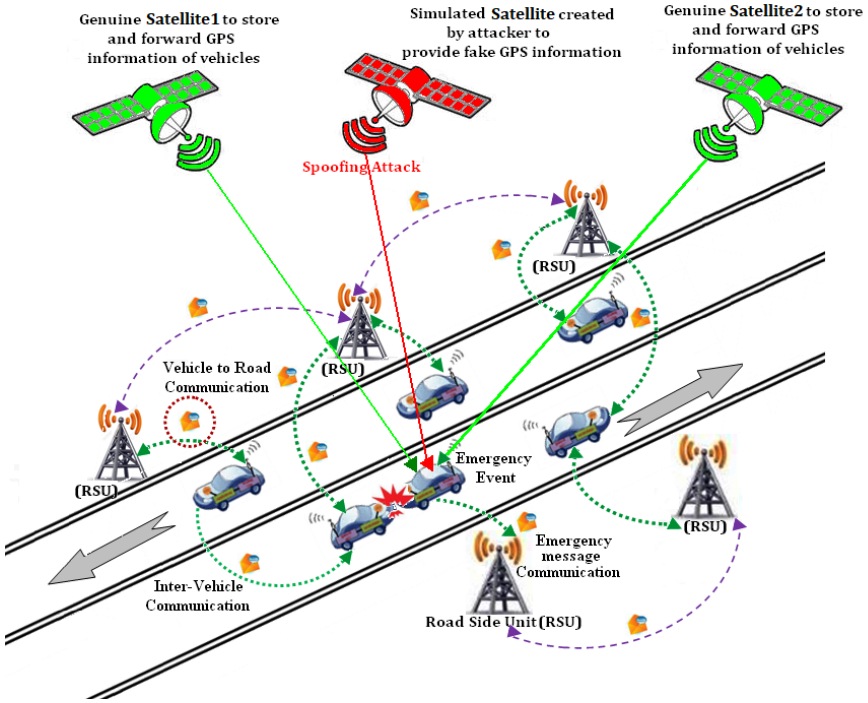

Figure 03: Spoofing attack on vehicle node

Tunnelling attack is another important vulnerability launched along with GPS Spoofing to deter from the detection of spoofing. The attacker creates a virtual channel called tunnel to capture and echo messages from distant network parts and use it to deceive the vehicle from detecting the GPS Spoofing attack. The spoofing attack is more disastrous as it affects many services like navigation, tracking, routing etc. With the availability of more sophisticated low-cost spoofers, there are more incidents of GPS spoofing. Figure 3 shows an architecture of spoofing and tunnelling attack in VANET.

II. Related work

Zhenghao Zhang et.al. [1] proposed a quick spoofing detection method to defend against GPS spoofing. This method uses a second antenna that has a significantly different radiation pattern from that of the original receiver. When there is no significant power difference between the two antennas, on the received GPS signal, it will be detected asan attack. But this method is not secure against cooperative multi-agent spoofing attacks that transmit GPS signals for different power levels. *Parth Pradhan et.al. [2]* proposed a ratio-based hypothesis testing for detecting GPS Spoofing. This method is based on the observation of timing synchronization error in the phasor readings recorded by the Phasor Measurement Unit (PMU). It requires

costly phasor measurement units and not suitable for vehicles. *Mohsen Riahi et.al.[3]* implemented a neural network-based methodology to identify pre-stored GPS spoofing messages stored and sent back to a GPS receiver. The supervised machine learning methodology through ANN is implemented to detect GPS Spoofing. Pseudo range, Doppler shift, and signal-to-noise ratio (SNR) features are extracted from GPS signals and this is used to train an ANN to classify the GPS signal to fake or genuine. This method can be used in fast-moving aerial vehicles where a significant difference in Doppler shift can be noticed between fake sources and real satellites. *Kai Jansen et.al. [4]* represented a methodology called crowdsourcing, based GPS Spoofing detection technique. This technique collects periodically transmitted; GPS derived position information for traffic control purposes. It also analyzes their contents and time of arrival to detect GPS Spoofing. *Nathaniel Carson et.al.[5]* proposed Cooperative Adaptive Cruise Control (CACC), which uses the concept of inter-vehicle ranging and data sharing to detect spoofing. This scheme requires a minimum of two GPS receiver to detect spoofing. *Moon, G.B et.al.[6]* designed an algorithm called GPS Anti-Spoofing and Recovering for a GPS spoofing attack. This scheme based on multiple tracking loops and a feedback structure of an adaptive filter. Estimation from one tracking loop is compared with other loops to measure the difference between the authentic and spoofed signal. *Yinrong Qiao et.al. [7]* proposed a novel spoofing detection system based on vision. The system is designed for small unmanned aerial vehicles. Aircraft position and velocity will be identified using a monocular camera, IMU and UAV's own sensors. They are compared to detect spoofing. *Gaoyang Liuet.al.[8]* designed a GPS spoofing detection algorithm called GPS-Probe, which uses air traffic control messages. A machine learning-enabled framework is trained to estimate the real position of the target aerial vehicle. Based on this position it will detect GPS spoofing attacks. *Qian Wang [9]* proposed a spoofing attack detection using edge computing. The location of the vehicle is constructed using the information of inter-vehicle communication information, vehicle speed and the steering angle. The constructed location is compared with location calculated using GPS to detect Spoofing. Even though this method has low-cost advantages because it assumes inter-vehicle trust. But in the presence of tunnelling attacks, this inter-vehicle trust does not hold good and this method can be deceiving. *Brady W et.al. [10]* proposed a spoofing detection statistic to detect whether GPS receiver is spoofed or not. The code and carrier phase relationship between a spoofed GPS signal and authentic signals is used. It does correlation analysis to confirm whether spoofing is done or not. *Md Tanvir et.al [11]* developed a spoofing detection system using hardware oscillators. In this method for GPS signals frequency, drift and free-running crystal oscillator are used. In this method with respect to GPS signals, frequency drift and offset of a free-running crystal oscillator will be measured. This oscillator will show strengthen and strong correlation with authentic GPS signals. As per these correlation results, any fake GPS signals can be identified. *Jung-Hoon et.al. [12]* designed an accelerometer-based spoofing detection system. This method compares the acceleration calculated using GPS locations from the receiver with the acceleration calculated using an accelerometer to detect the attack. This method is not safe against an intelligent spoofer. It can carefully manipulate the position in the way to fall in line with accelerometer results. *Gabriele Oligeri et.al [13]* developed a spoofing detection approach using the mobile cellular infrastructure. The Broadcast signals transmitted by cellular infrastructure and are used to calculate the distance to a base station. Later it will be validated against distance calculated using GPS coordinates given by GPS receiver. Spoofing is detected when there is a bigger difference. *Fahad et.al. [14]* proposed decentralized a mechanism to detect spoofing attack in VANET. This mechanism is based on vehicular communication GPS code and its pseudo ranges with neighbouring vehicles. Linear operation

is done on exchanged data to result in some statistics variables. A cumulative sum procedure is implemented on these statistics variables to identify spoofed GPS signals time of arrival. The vehicle node in the VANET uses these statistical data to implement cumulative sum procedure. As the result of this technique, it will detect high correlations in the time of arrival of GPS signals. The Min-max-change detection procedure is implemented on these correlations to detect spoofed signals.

III. Proposed RSU cooperation based approach

This research work proposes RSU cooperation-based detection of GPS Spoofing attack launched along with tunnelling attack. The detection method is based on RSU verification of GPS signals against its known location. Besides, the proposed mechanism also learns the spatial and temporal characteristics of the attack and launch a proactive defending mechanism to protect the vehicles. Following are the three contributions in this work

1. Detection of GPS spoofing through RSU based signal verification
2. Digital signature-based message verification to protect from tunneling attack.
3. Proactive defense against GPS spoofing attack by learning the spatial and temporal characteristics of the attack.

The approach based on the assumption of RSU preconfigured with their locations during deployment. Each RSU is equipped with a GPS receiver to calculate the position using trilateration. When the calculated location is different from the preconfigured location, it is detected as a spoofing attack. On the detected spoofed signal, the following four features are extracted.

a. Pseudo range

It is the pseudo distance between a satellite and a global navigation satellite system (GNSS) receiver.Pseudo range is calculated as,

$$\mathbf{PR} = \Delta \mathbf{T}.\mathbf{c} = (\mathbf{T} - \mathbf{T_s}).\mathbf{c}$$

T is the reception time at the receiver, $T_s$is the transmission time at the satellite and c is the speed of light.

b. Carrier Phase Shift

It is a process of sending information by changing the phase of a constant frequency reference signal.Carrier phase shift over time T for a transmitted signal T^S is calculated as

$$\boldsymbol{\varphi^S(T) = f_0 T + \emptyset_0 - f_0 T^S - \emptyset_0^S - P^S}$$

Where T is given as,

$$\mathbf{T} = \frac{\emptyset(\mathbf{t}) - \emptyset_\mathbf{0}}{\mathbf{f_0}}$$

c. Doppler Shift

It is a change in frequency noise with respective to observer point of view.

$$\mathbf{f_d} = \frac{\mathbf{d}\emptyset_\mathbf{d}(\mathbf{t})}{\mathbf{dt}}$$

$\emptyset_d$ is the phase difference between the GPS signal and a reference signal. It is calculated as,

$$\emptyset_{\mathbf{d}}(\mathbf{t}) = \emptyset_{\mathbf{0}}(\mathbf{t}) - \emptyset_{\mathbf{g}}(\mathbf{t}) - \mathbf{P}$$

Where P is the phase ambiguity. At the receiver, GPS carrier signal g(t) is multiplied by reference signal f(t)

$$\mathbf{g(t)} \times \mathbf{f(t)} = \mathbf{A_g}\ \mathbf{sin}(2\pi\emptyset_{\mathbf{g}}(\mathbf{t}))\ \times \mathbf{A_0}\ \mathbf{sin}\ (2\emptyset_{\mathbf{0}}(\mathbf{t}))$$
$$= \frac{\mathbf{A_{0A_g}}}{\mathbf{2}}[\mathbf{cos2\pi}\left(\emptyset_{\mathbf{0}}(\mathbf{t}) - \emptyset_{\mathbf{g}}(\mathbf{t})\right) - \mathbf{cos2\pi}\left(\emptyset_{\mathbf{0}}(\mathbf{t}) + \emptyset_{\mathbf{g}}(\mathbf{t})\right)]\boldsymbol{\pi}$$

The amplitude and phase of received GPS signal is given as, A_g , $\emptyset_g(t)$

The amplitude and phase of received GPS signal is given as, A_0 , $\emptyset_0(t)$

d. Signal to noise ratio (SNR)

SNR is the ratio of power of a signal (S) to the background power of noise (N). It is measured in decibels (dB).

$$\mathbf{SNR} = \frac{\mathbf{Psignal}}{\mathbf{Pnoise}} = \frac{\mathbf{S}}{\mathbf{N}}\ \mathbf{dB}$$

1. Detection of GPS spoofing through RSU based signal verification

In this mechanism, all four features shown above are grouped as a feature vector and encrypted along with RSU coordinates. The encrypted content is broadcasted over the RSU area as a control message. Also, the control message is digitally signed with RSU credentials. In the proposed solution, a private-public key pair is generated and the private key is distributed to all the RSU and a public key is distributed to all the vehicles. The vehicle doesn't process any message without a digital signature and rejects them as fake messages. The vehicle which receives the control message from the RSU verifies the signature before processing it. Once the message is verified, the feature vector is decrypted. The decrypted feature vector is saved locally in the vehicle. Every time GPS signal is received at a vehicle, The pseudo-range, signal to noise ratio, carrier phase shift and Doppler shift features are extracted and compared to the feature vectors stored locally for the closest match. If the matching is lower than a threshold, then the GPS signal is decided as spoofed.

The vehicles remember the signature of the spoofed signal in terms of its feature vector by saving it locally. Generally, any spoofing tool varies its attack pattern only within a limited set. RSU finds all the attack patterns and advertises it to the vehicles, so that any vehicle can use it to detect and to confirm GPS spoofing attack. Thus, in the proposed solution vehicles can detect GPS spoofing with RSU cooperation.The below shown flowchart (figure 4) represents overall detection mechanism of GPS spoofing attack in VANET.

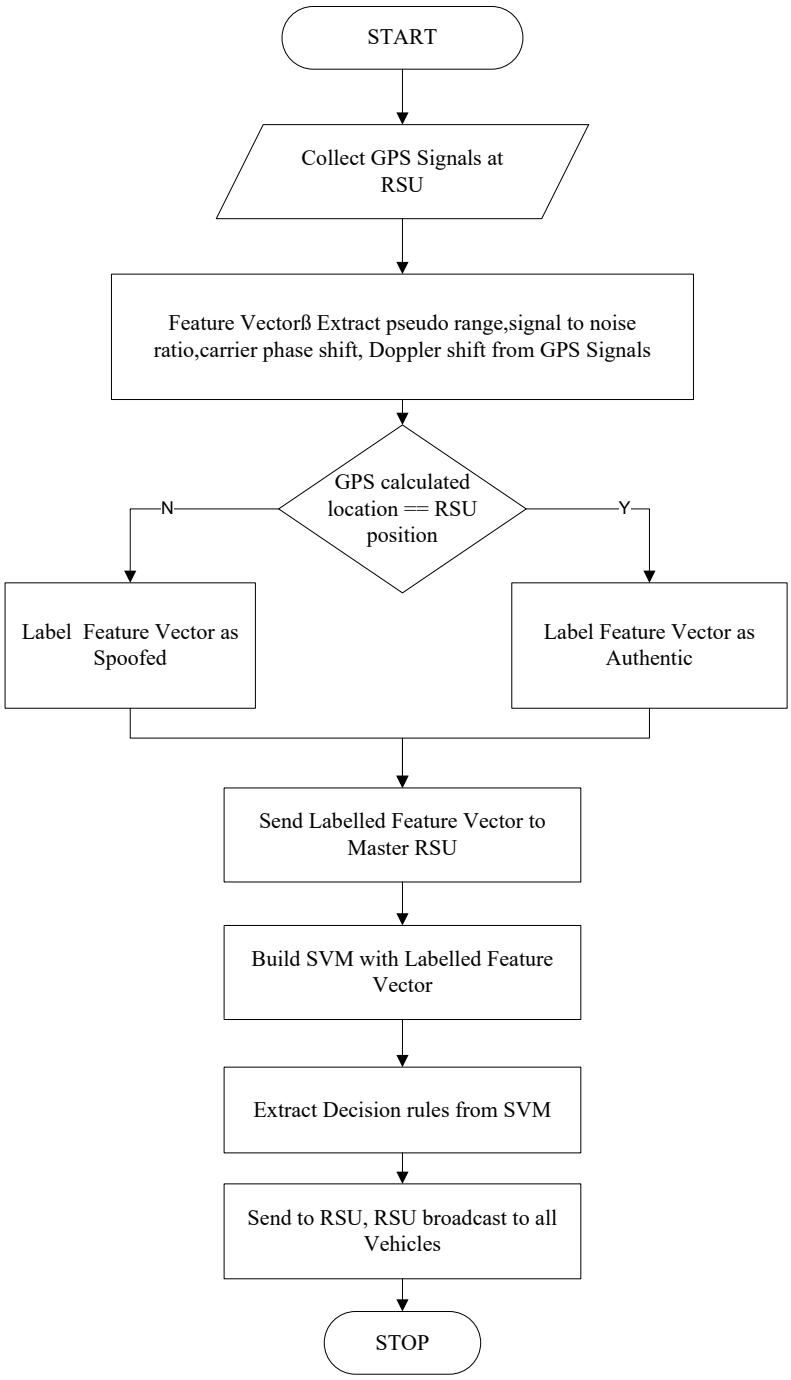

Figure 04: Spoofing attack detection flowchart

2. Digital signature-based message verification to protect from tunnelling attack

The control message which carries the feature vector about attack signature has the following payload.

```
InfoBroadcast
        {
        RSU ID
        RSU latitude
        RSU longitude
        Pseudo range
        Signal to noise ratio
        Carrier Phase shift
        Doppler shift
        }
```

The payload is encrypted with the private key of RSU and HAMC (Hash based Message Authentication Code) hashing is done on the encrypted content. HMAC takes two parameters of encrypted content and a hashing key. The hashing key is generated using μTESLA one-way key chain given below in fugure 5. The HMAC result is inserted as a digital signature and sent in the control packet.

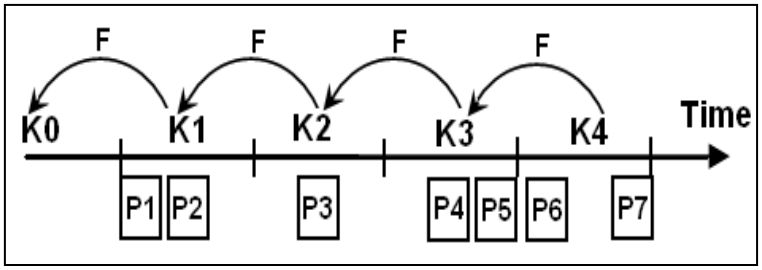

Figure 05: μTESLA keychain mechanism

The RSU first generates a sequence of secret keys (a one-way key chain). To generate a one-way key chain of length n, the sender chooses the last key K_n based on a preconfigured secret known between vehicles and the RSU's. RSU and vehicles generate the remaining values by successively applying a one-way function F (e.g., a cryptographic hash function such as MD5)

$$K_j = F(K_{j+1})$$

Because F is a one-way function, attackers cannot compute forward, e.g., compute $K_0, K_1, .. K_j$ given K_{j+1}. On the other hand, nobody can compute backwards, e.g., compute K_{j+1} given only $K_0, K_1, .. K_j$ because the generator function is one-way.

Once the vehicle receives the control message, it decrypts the InfoBroadcast payload. Before accepting it as valid, it generates the signature using HMAC as detailed above and verifies it against the signature in the control message. It accepts the control message only if the signature matches, otherwise it drops it's capture and plays message caused due to tunnelling attack. The InfoBroadcast payload also has RSU latitude and longitude, so when a vehicle can use this latitude and longitude for its services, in event of an attack.

3. Proactive defence against GPS spoofing attack:

Another important feature in the proposed solution is a proactive defence against spoofing attack by learning the spatial and temporal characteristics of the attack. One of the RSU is designated as master RSU in VANET environment [15]. Each RSU split the feature vector of GPS signals into two categories as authentic and spoofed. Each RSU will send the features vectors and their category to the master RSU. At master RSU, an SVM (Support Vector Machine) classifier is trained and decision rules for classification between authentic and spoofed signal are learnt from the SVM using the approach mentioned in [16]. The learnt decision rules are sent to each of the RSU and then forwarded to each of the vehicles once in a time period. The flowchart for building the spoofing detection is given in figure 4. In the network, all vehicle nodes use these decision rules to decide whether the received GPS signal is spoofed or not. By this way of proactively learning the attack behaviour and sending decision rules to each vehicle, vehicles will have the necessary intelligence to detect the attack when it gets exposed to it.

IV. Experimental Dataset and Results

The proposed solution simulation was conducted using NS2 simulator with the following configurations.

Table 01: Simulation configuration

Number of Vehicles	100
Simulation Duration	10 minutes
Vehicle Speed	30 m /second
GPS Spoofing rate	5 times / second with 5-20 different attack patterns

This methodology was tested on below given VANET topology by constructing RSUs at every corner and by considering vehicles as nodes shown in figure 6.

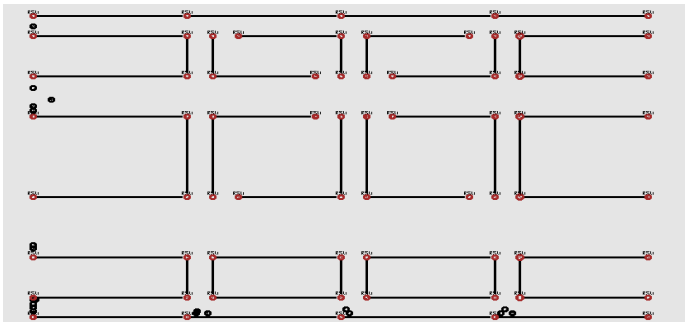

Figure 06: Simulation topology

The performance of the proposed solution is compared against Decentralized detection of spoofing attack proposed in [14]. The performance evaluation is compared in terms of following five ability-enhancing characteristics.

1. Time for attack detection

It's a total time required to detect an attack. The time for detection of attack is measured for a different number of attack patterns and result shown in figure 7. The following table 2 data is considered to depict the comparative result of the proposed system and [14].

Table 02: Data table of time for attack detection

No of attack patterns	Proposed RSU Cooperation	Existing [14]
05	10	30
10	14	50
15	19	90
20	23	130

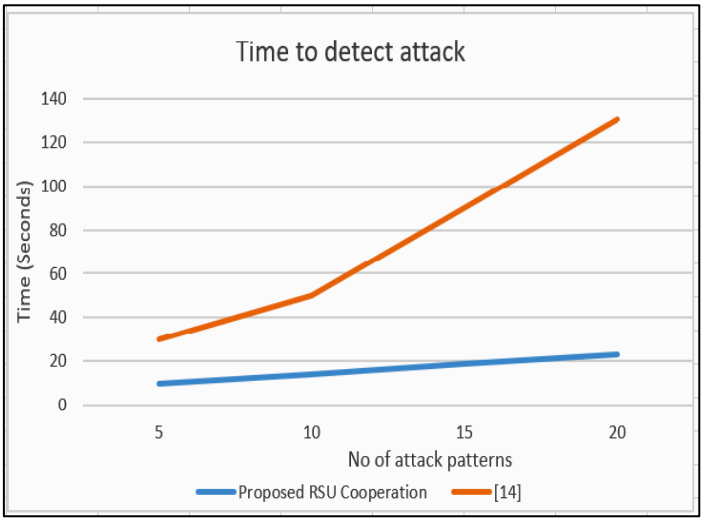

Figure 07: Time for attack detection

As per the result analysis shown in the graph, it can be seen that the time for detection of attack is very low in the proposed scheme compared to existing system [14]. In the proposed system, RSU based detection and communication to vehicles technique used, wherein existing scheme [14], inter-vehicle communication based methodology is used to detect an attack.

2. Network overhead

The network overhead is measured in terms of a number of additional information exchanged in the network to detect spoofing attack.

$$\textbf{Overhead} = (\textbf{IP} - \textbf{AI})\textbf{bytes}$$

Where, IP is information exchanged in bytes and AI is actual information to be exchanged in bytes. The data given in table 3 is used to compare the proposed system with existing system [14] and the result is depicted in figure 8.

Table 03: Data table for network overhead

No of attack patterns	Proposed RSU Cooperation	Existing [14]
05	140	200
10	150	210
15	160	220
20	165	230

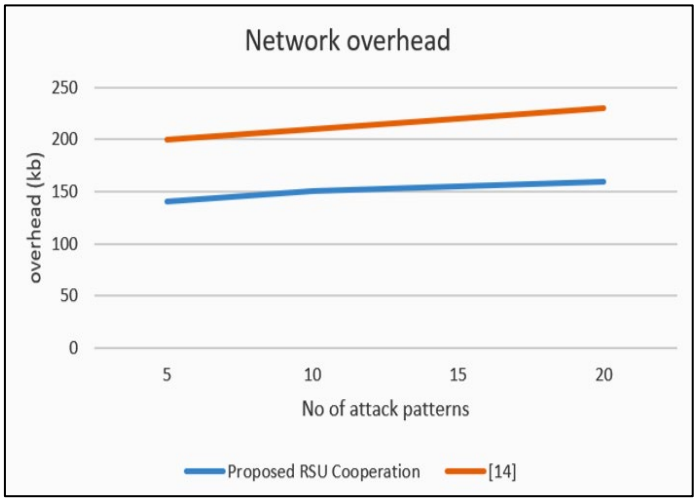

Figure 08: Network overhead

As per the graphical analysis of result, the network overhead is low in proposed RSU based cooperation technique compared to existing system [14]. As the result in proposed system , the control message broadcasting is limited within RSU area.

3. Attack Detection accuracy

It's an accuracy value to detect new attack with a reduced count of errors in attack detection.

$$\textbf{Accuracy} = \frac{\textbf{TP} + \textbf{TN}}{\textbf{TP} + \textbf{TN} + \textbf{FP} + \textbf{FN}}$$

Where, TP is True positive, FP is False positive, TN is True negative and FN is False-negative. The detection accuracy is measured for a different number of attack patterns as shown in table 4 and the graphical outcome is shown in figure 9.

Table 04: Data table for detection accuracy

No of attack patterns	Proposed RSU Cooperation	Existing [14]
05	97	90
10	96	89
15	95	85
20	94	82

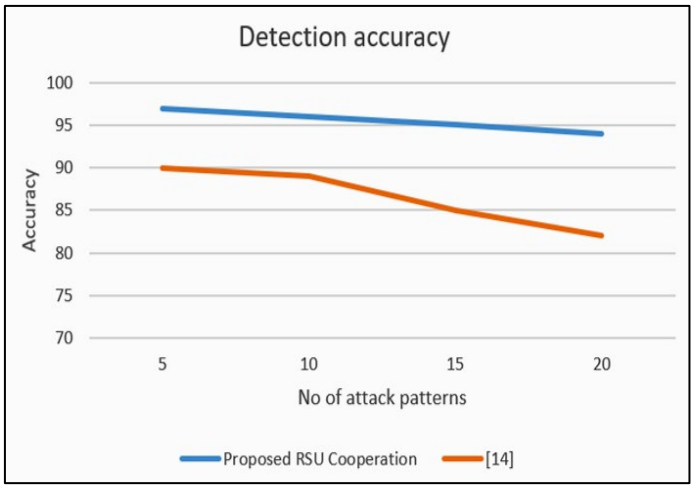

Figure 09: Attack detection accuracy

The accuracy of detection is higher in the proposed RSU based cooperation approach compared to an existing system [14]. This is because SVM based decision rules is used in the proposed system.

4. Sensitivity

It's a test, which determines the ability rate of attack detection for a given set of patterns.

$$\textbf{Sensitivity} = \frac{\textbf{TP}}{\textbf{TP} + \textbf{FN}}$$

Where, ***TP*** is True Positive and ***FN*** is False Negative. The sensitivity or the true positive rate is measured for a different number of attack patterns with the following data, shown in table 5 and the experimental result is given in figure 10.

Table 05: Data table for **s**ensitivity

No of attack patterns	Proposed RSU Cooperation	Existing [14]
05	98	89
10	97	87
15	97	83
20	96	81

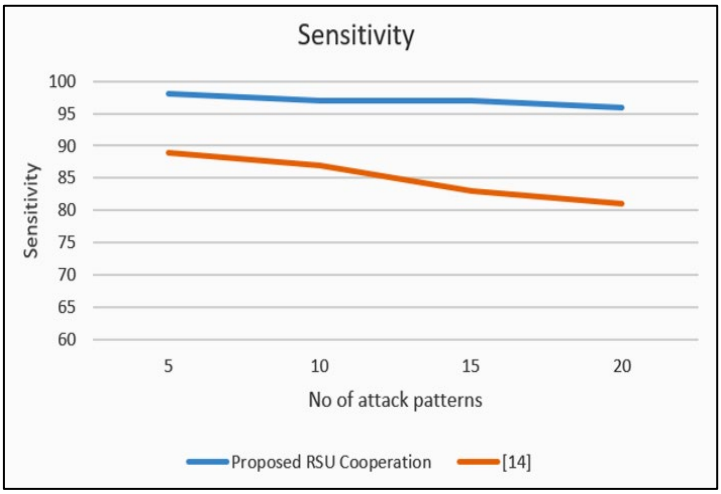

Figure 10: Sensitivity

As shown in the graph, the sensitivity is higher in RSU based cooperation approach as compared to existing system [14].

5. Specificity

It's a test, represents the rate of the ability which will not detect an attack for a given set of patterns.

$$\textbf{Specificity} = \frac{\boldsymbol{TN}}{\boldsymbol{TN + FP}}$$

Where, ***TN*** is True negative and ***FP*** is False Positive. The specificity or the true negative rate is measured for a different number of attack patterns as per data given in table 6 and the result given in figure 11.

Table 06: Data table for specificity

No of attack patterns	Proposed RSU Cooperation	Existing [14]
05	95	85
10	94	83
15	93	82
20	92	80

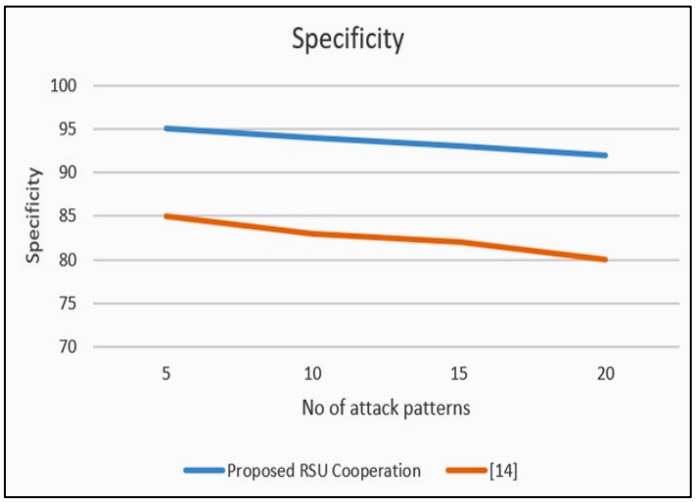

Figure 11: Specificity

The results shown in the graph indicates that, proposed RSU based cooperation technique demonstrating the higher specificity capability compared to existing system [14] and also it identifies true negatives.

V. Conclusion

The proposed methodology represents GPS Spoofing attack detection using RSU cooperation-based technique. This technique will prevent emergency messages sent to vehicles from spoofing attack. The proposed mechanism also includes proactive learning of attack characteristics in terms of SVM based decision rules. It will classify the attacks with higher accuracy. The μTESLA based key generation mechanism with digital signature is used efficiently in proposed solution to secure emergency messages from tunnelling attack. In the future work, detection accuracy can be improved further by analyzing the spoofed signals using wavelets.

VI. References

[1] **Conference proceedings paper:** Z. Zhang, L. Qian and , M. Trinkle , "Quickest detection of GPS spoofing attack,"MIL-COM 2012 IEEE conference on Military Communications", Orlando, FL, 2012, pp. 1.

[2] **Conference proceedings paper:** P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore and R. S. Blum, "GPS spoofing attack characterization and detection in smart grids," IEEE International symposium on Communications and Network Security", Philadelphia, PA, 2016, pp. 391-395.

[3] **Conference proceedings paper:** M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni and N. Kaabouch, "Detection of GPS Spoofing Attacks on Unmanned Aerial Systems," *16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2019, pp. 1-6.

[4] **Conference proceedings paper:** Jansen, Kai, Matthias Schäfer, Daniel Moser, Vincent Lenders, Christina & Jens, "Leveraging Crowd sourcing to Detect & Localize GPS Spoofing Attacks" IEEE international conference on network security and privacy, 2018, pp. 1-14.

[5] **Conference proceedings paper:** N. Carson, S. M. Martin, J. Starling and D. M. Bevly, "GPS spoofing detection and mitigation using Cooperative Adaptive Cruise Control system", *IEEE Intelligent Vehicles Symposium (IV)*, Gothenburg, 2016, pp. 1091-1096.

[6] **Journal article:** Moon, G.B., Im, S-H., Jee, G-I., "A Civil GPS Anti-Spoofing and Recovering Method Using Multiple Tracking Loops and an Adaptive Filter Technique," Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, September 2013, pp. 2916-2920.

[7] **Journal article:** Y.Qiao, Y.Zhang & X.Du, "A Vision Based GPS Spoofing Detection Method for Small UAVs", 13th International Conference on Computational Intelligence and Security, Hong Kong, 2017, pp. 312-316.

[8] **Conference proceedings paper:** G. Liu, R. Zhang, C. Wang and L. Liu, "Synchronization-Free GPS Spoofing Detection with Crowdsourced Air Traffic Control Data," *2019 20th IEEE International Conference on Mobile Data Management (MDM)*, Hong Kong, Hong Kong, 2019, pp. 260-268.

[9] **Conference proceedings paper:** Q. Wang, Z. Lu, M. Gao and G. Qu, "Edge Computing based GPS Spoofing Detection Methods," *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*, Shanghai, China, 2018, pp. 1-5.

[10] **Journal article:** Brady W O'Hanlon, Mark L Psiaki, Jahshan A Bhatti, Daniel P

Shepard, Todd E Humphreys, "Real-time gps spoofing detection via correlation of encrypted signals", *Navigation 2013*, vol. 60, no. 4, pp. 267-278.

[11] **Conference proceedings paper:** Md Tanvir Arafin, Dhananjay Anand, Gang Qu, "A low cost GPS spoofing detector design for IoT applications", International Great Lakes Symposium on VLSI- 2017, pp. 161-166.

[12] **Journal article:** Jung-Hoon Lee, Keum-Cheol Kwon, Dae-Sung An, Duk-Sun Shim, "Gps spoofing detection using accelerometers and performance analysis with probability of detection", *International Journal of Control Automation and Systems*, 2015, vol. 13, no. 4, pp. 951-959.

[13] **Conference proceedings paper:** Gabriele, Savio, Omar & Adel,"GPS spoofing detection via cellular network", 12th national Conference on Security & Privacy in Wireless & Mobile Networks, May-2019.

[14] **Journal article:** Milaat & H Liu, "Decentralized Detection of GPS Spoofing in VANET ", IEEE Communications 2018, Letters 22 , 6, 1256 to 1259.

[15] **Journal article:** Ke Liu,Wenqi Wu,Zhijia Wu,"Spoofing Detection Algorithm Based on Pseudorange Differences",Sensors (Basel). 2018 Oct; 18(10): 3197.

[16] **Journal article:** Yang Zhang, Zhanhuai Li, Yan Tang, Kebin Cui, "DRC-BK: Mining Classification Rules with Help of SVM", PAKDD 2004: 191-195

[17] **Journal article:** Mr. Mahabaleshwar Kabbur & Dr. V. Arul KumarS, "MAR_Sybil: Cooperative RSU Based Detection and Prevention of Sybil Attacks in Routing Process of VANET" in Dec 2019, IOP Publishing, ISSN: 1742-6596.

[18] **Journal article:** Mr. Mahabaleshwar Kabbur & Dr. V. Arul Kumar, "Detection and Prevention of DOS Attacks in VANET with RSU's Co-operative Message Temporal Signature" in July 2019 IJRTE ISSN: 2277-3878.

[19] **Journal article:** Mr. Mahabaleshwar Kabbur & Dr. V. Arul KumarS, , "MAR_Worm: Secure and Efficient Wormhole Detection Scheme through Trusted Neighbour Nodes in VANETs" in Dec 2019, IJRTE 2278-3075.