Available online at: http://www.ijmtst.com/vol5issue03.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 05, Issue No: 03, March 2019

A Macroscopic Traffic Model-based Approach for Sybil Attack Detection in VANETs

Vikas Kumar Garg | Arshdeep Singh | Pranab Garg

Assistant Professor ,Computer Science and Engineering Department, BGIET Sangrur, Punjab, India.

To Cite this Article

Vikas Kumar Garg, Arshdeep Singh and Pranab Garg, "A Macroscopic Traffic Model-based Approach for Sybil Attack Detection in VANETs", *International Journal for Modern Trends in Science and Technology*, Vol. 05, Issue 03, March 2019, pp.-31-38.

DOI: https://doi.org/10.46501/IJMTST050329

Article Info

Received on 02-March-2019, Revised on 21-March-2019, Accepted on 28-March-2019.

ABSTRACT

Vehicular Ad Hoc Network (VANETs) are required to play a significant job in our lives. They will improve traffic security and welcome an upheaval on the driving experience. In any case, these benefits are balanced conceivable assaults that undermine the vehicle's security, yet additionally travelers lives. One of the most widely recognized ones is the Sybil assault, which is more risky than others since it could be the beginning stage of numerous different assaults in VANETs. This paper proposes a dispersed methodology permitting the discovery of Sybil at tacks utilizing the traffic flow hypothesis. The key thought here is that every vehicle will screen its neighborhood so as to identify a possible Sybil assault. This is accomplished by contrasting between the genuine precise speed of the vehicle and the one evaluated utilizing the V2V correspondences with vehicles in the region. This evaluated speed is acquired utilizing the traffic flow principal chart of the street's segment where the vehicles are moving.

A numerical model that assesses the pace of Sybil assault discovery air conditioning cording to the traffic thickness is proposed. At that point, this model is approved through some broad re-enactments directed utilizing the notable NS3 arrange test system together with SUMO traffic test system.

Keywords

ITS, VANETs, Traffic Model, Sybil assault, CAM

I. INTRODUCTION

The new versatility difficulties of vehicles in Keen Urban communities need the improvement of Intelligent Transportation System (ITS) that assists with diminishing congestion, mishaps, fuel utilization, and so forth. In this manner, Vehicular Ad Hoc Network (VANETs), which are a significant segment of ITS, have been a subject of some 5 serious research and exploratory applications in these most recent two decades. In such systems, vehicles out and about will speak with every others to exchange data about their bearings, their rates, their positions, the condition of street, and so on. Right now, the car business is attempting to outfit new vehicles with Wireless Access Vehicular Environment (WAVE) gadgets. WAVE conventions depend on the IEEE 802.11p standard and give the essential radio standard for committed short-extend correspondence (CSEC).

Since a fruitful assault could have sensational outcomes, security of Vehicular Ad Hoc Network turns into a significant issue. A notable assault is the Sybil one. This assault is considered as one of the most perilous and the premise of numerous different assaults. In Sybil assault, malevolent hub may accept various personalities. The least hurtful target of such assault is to make an figment of traffic blockage so as to reroute different vehicles from the street that the assailant will take. At the opposite end, the assailant could push a specific vehicle to take a specific course so as to trap it or, even, manage it straight to crash in a mishap.

This paper exhibits another procedure permitting the location of Sybil assault in VANETs systems. This methodology misuses some traffic flow hypothesis wonders so as to create a remaining comparing to the difference between the estimated speed of the vehicle and the evaluated speed in a dispersed manner by utilizing the data of its encompassing.

At long last, some sensible recreation utilizing NS3 arrange test system joined with a versatility test system SUMO are given to exhibit the efficiency of our proposed system.

This paper makes the accompanying commitments:

1. Conversely with the current works that are commonly founded on secure key asset testing, notoriety or position verification systems, this paper proposes another methodology dependent on the naturally visible traffic flow hypothesis to distinguish Sybil assaults.
2. It proposes a numerical model permitting to assess the shut type of the Sybil assault likelihood as per the proposed approach.
3. It introduces another procedure which is anything but difficult to be executed and doesn't need neither a focal hub nor extra equipment in the vehicle.
4. It gives practical recreations utilizing notable apparatuses to show the efficiency of our methodology.

The token of this paper is as follow. The segment 2 portrays some related works about Sybil assaults location. Segment 3 presents the setting of our investigation by displaying the focused on situation and the utilized traffic flow model. Segment 4 subtleties how our location calculation functions. Segment 5 shows a mathmetical model that assesses the recognition pace of the proposed Sybil assault calculation. Segment 6 approves this calculation utilizing a reasonable system simulation. At last, area 7 finishes up this paper and gives a few viewpoints to this work.

2. RELATED WORKS

A few instruments expecting to distinguish Sybil assaults have been proposed in the writing. Among them, we can make reference to those dependent on asset testing (for example registering capacity, stockpiling capacity, correspondence data transfer capacity, and so forth.). In that case, every vehicle communicates a solicitation to every one of its neighbors, this needs some physical assets to be registered. Subsequently, since assailants need to answer at the same time for them and for the made phony hubs, they won't be capable to answer in the given time interim and just genuine vehicles will be trusted. Be that as it may, this methodology squanders a great deal of processing assets and transfer speed for these tests. In addition, assailants outfitted with incredible registering gadgets can sidestep these tests.

Creators in proposed a RSSI-based limitation system signified INTERLOC, which utilizes the portable hubs as a help to restrict precisely a neighbours. It is utilized chiefly to drop the GPS signal impedance effects, while it can likewise be utilized in identifying Sybil assaults. Versatile hubs help a hub on finding its exact position utilizing the got RSSI. This instrument is in view of the sign quality and its appearance point. This can be utilized to distinguish that the got sign couldn't be the gotten one from a proclaimed position if there should arise an occurrence of a Sybil assault. In this way, this procedure needs to utilize many neighbours, and afterward a high vehicle thickness, so as to precisely restrict a hub. In addition, it doesn't work appropriately in an expressway situation.

Another approach to distinguish Sybil assaults, in light of electro-acoustic situating. Reproductions in indicated that the electro-acoustic situating out performs RSSI-based situating. In spite of its efficiency, electro-acoustic positioning suffers from a significant downside, which is that each vehicle must be furnished with an acoustic ultrasound beeper. This supposition that is exceptionally severe in reality, since barely any vehicles are outfitted with such gadgets.

Introduced an encryption convention to dodge Sybil assaults in VANETs. This convention utilizes the connection between a vehicle and a Street Side Unit (RSU) to trade scrambled messages so as to acquire the system key, that permits it to speak with different vehicles. Since this key is overseen

by the RSU, a hub with a one of a kind ID could get just one system key, and afterward it isn't capable to dispatch Sybil assaults. This convention needs that all messages to be encoded, which is contrary to the worldview of C-ITS where security information need to be traded in an open manner. Also, if a programmer prevails with regards to infiltrating the server where the vehicles' mystery IDs are put away, he could utilize them to produce as much ways of life varying to coordinate a Sybil assault.

Creators in , proposed another completely disseminated secure situating algorithm dependent on a designating number verification and on the shared assurance depending on neighbors for Remote Sensor Systems (WSN). This calculation employments a great deal of messages so as to ensure the right area of hubs, which in wrinkles the expense of such calculation. defined a convention permitting the location and the avoidance from Sybil assaults in Portable Specially appointed Systems (MANETs). This convention is based principally on grouping and way similitude. It utilizes the bundle confirmation by misusing the electronic mark joined with private keys.

The overseement of such keys is extremely testing particularly in a portable networks. Since vehicles are trading data about their status (position, speed, heading, and so forth.), these components can be utilized to recognize Sybil assaults like in the works. creators proposed "Impression", an identifying Sybil assault approach in urban systems. Impression utilizes social relationship among directions to recognize and dispose of sybil hubs. Be that as it may, it assumes that streets are secured with Street Side Units (RSUs), which is over the top expensive for street administrators.

Furthermore, it guesses that all RSUs are considered as legitones, which isn't really valid. The work in examined the driving example similitude in the Sybil assault discovery. It classifies neighbors utilizing the k Closest Neighbors calculation so as to find noxious hubs. This calculation is by all accounts efficient as exhibited by the reenactments, despite the fact that its unpredictability is too high to possibly be utilized continuously in assault discovery inside vehicles. For more Sybil assault recognition related works, perusers are urged to peruse the overview .

3. BACKGROUND

The traffic flow study is commonly founded on certain models that can be smaller scale scopic or naturally visible. Infinitesimal models center around the individual conduct of drivers, while the naturally visible models consider the flow of vehicles. Infinitesimal models can manage heterogeneous vehicles and stochastic viewpoints to give some exact data about the individual speeds, the space-time chart, and so forth. Be that as it may, since these models require an enormous number of factors and a high count time, they are not appropriate for the improvement of a constant assault location calculation. Then again, plainly visible models require a moderately low calculation time and can be increasingly adjusted for our investigation.

Naturally visible models consider traffic flow as fluid that can be depicted utilizing the hydrodynamic hypothesis and some accumulated amounts, which are the speed (v), the flow (q) and the thickness (d). Besides, all large scale scopic models define a flow-thickness relationship regularly called the Crucial Chart (FD), which is acquired either from the adjustment of a specific infinitesimal model or from the test information. In this way, without loss of generality, the rest of this paper thinks about that the FD has a triangular structure depicted by the accompanying conditions:

$$\begin{cases} \text{if } d < d_c, \text{ then } q = ad \\ \text{if } d_c \leq d < d_{max}, \text{ then } q = bd + c \\ \text{if } d \geq d_{max}, \text{ then } q = 0. \end{cases}$$

where, a,b,c,dc,dmax and qmax are some given parameters that depends on the road's section as depicted by figure 1.

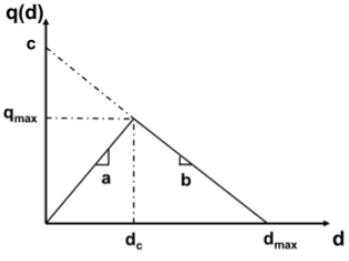


Figure 1: Fundamental diagram example

So as to abuse this traffic model with regards to VANETs, this investigation thinks about every vehicle, as a Helpful Savvy Transportation Framework Station (C-ITSS), trading agreeable messages, meant as Helpful Mindfulness Message (CAM). Each vehicle sends standard CAM messages at a recurrence shifting somewhere in the range of 1 and 10 Hz. This recurrence relies basically upon the vehicles speed. These messages targets advising the neighbors of their nearness.

The fields present in the CAM messages are displayed in the Figure 2.

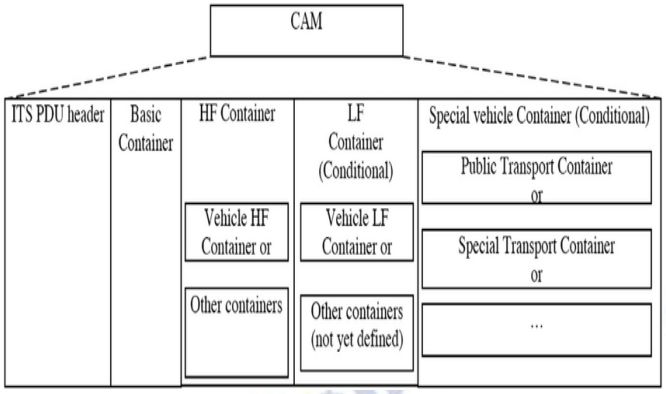


Figure 2: Structure of a CAM packet

As it is appeared from figure 2, the fields which are remembered for the CAM message are basically:

• ITS PDU header: it incorporates chiefly the C-ITS station ID.

• Fundamental Holder: it demonstrates the station type (walker, cyclist, traveler vehicle, transport, and so on.) and the station position (scope, longitude, elevation).

• High Recurrence Holder : it notifies for the information evolving every now and again (speed, direction, ebb and flow, yaw rate, path position, guiding wheel angle, and so forth).

• Low Recurrence Holder : it incorporates the job of the vehicle (open vehicle, uncommon vehicle, risky merchandise, street work, crisis, and so on.), outside light status and the way (history of last put away positions)

• Unique Vehicle Holder : it relies upon the proclaimed job of the vehicle, each job has its own extraordinary compartment, which shows for instance if the light bar and the alarm are utilized or not.

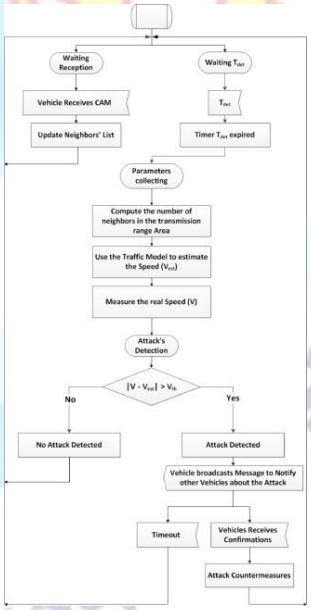
4. PRESENTATION OF THE PROPOSED ALGORITHM

To begin with, we present right now significant level portrayal of our proposed calculation exhibited under a flowchart in the accompanying subsection. Second, each venture of this calculation is itemized as a pseudo-code calculation.

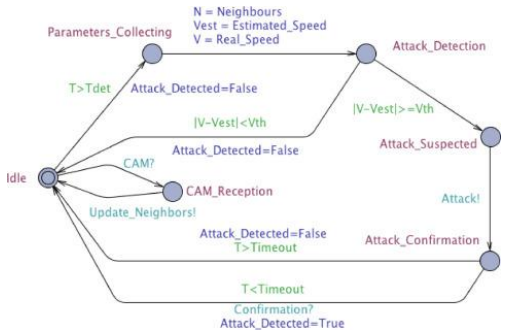
4.1. Calculation significant level portrayal

The Figure 3 portrays a flowchart depicting a significant level perspective on the star presented calculation. The vehicle sits tight for the gathering of a CAM (Helpful Mindfulness Message) to begin refreshing the rundown of its neighbors so as to include the source hub as a neighbor on the off chance that it doesn't as of now exist, since met for the first time. Else, it refreshes the timestamp of this hub. This is finished consistently as expressed by the CAM standard.

So as to decrease the congestion of the vehicle preparing equipment, the Sybil assault identification method is propelled by the predefined period (Δdet). When the identification clock (Tdet) terminates, the vehicle gathers all the handling required information. To start with, it separates from the rundown of its neighbors those that still in its region. To do as such, it revives the rundown by expelling the hub that were not seen for a given time. The pre-owned length for this cleaning could be tuned relying upon the situation and the pre-owned condition (urban, highway,etc.). Furthermore, the central chart is utilized to assess the speed of the vehicle (Vest). Note here that the FD could be now incorporated legitimately inside the On-Board Unit (OBU) of the vehicle or it could be downloaded from a Street Side Unit (RSU) at the city's entrance for instance. At that point, it quantifies the genuine speed (V). From that point onward, location of the Sybil assault is accomplished by an examination of these two rates, as |V −Vest|. On the off chance that this difference is lower than a predefined edge esteem (Vth), at that point no assault is distinguished.



Sybil assault is recognized and the affected vehicle will inform its neighbors of this assault. At long last, if the vehicle gets at any rate a confirmation from another vehicle that has do a similar investigation, it will dispatch some previously arranged countermeasures, which are out of extent of this paper. Else, it will overlook this assault discovery and restart another assault location at the following time frame.



To facilitate the reader's understanding of our contribution, we add a state progress outline, exhibited in the figure 4, to help the Flowchart. This diagram shows that a vehicle begins either by accepting a CAM and afterward refreshing its neighbors or by gathering the parameters that permit to recognize the assault if the identification clock terminates. In the event that the difference between the evaluated and the genuine speeds is higher than Vth, at that point an assault is suspected.

In this manner, a vehicle sends an alarm to its neighbors. In the event that it gets a confirmation, the assault is confirmed. Else, it comes back to the Inactive state to restart another location cycle.

4.2. Algorithm detailed description

To all the more likely comprehend the proposed calculation, we present here its most significant highlights portrayed in the accompanying calculations :

• Calculation 1 subtleties the system of the neighbors' rundown refreshing.

• Calculation 2 displays the technique of the neighbors' number processing.

• Calculation 3 shows the system that utilizes the traffic model to assess the speed of the vehicle.

• Calculation 4 portrays the identification calculation that utilizes the three past calculations.

Algorithm 1 Updating Neighbours' List

1: procedure Neighbours Updating(Packet P, List Neighbours)
2: if (P.Sender / ∈ Neighbours) then
3: Neighbours.Add(Sender);
4: end if 5: Neighbours[Sender].Timestamp ← P.Timestamp;
6: Neighbours[Sender].Location ← P.Location;
7: end procedure

In the Calculation 1, when a vehicle gets a CAM message, it verifies on the off chance that it exists as of now in the neighbour list. On the off chance that it is the situation, it needs to refresh the area and the timestamp of the sender vehicle. Else, it includes the new sender of the message as a neighbor and it embeds the two its area and timestamp.

Algorithm 2 Computing Number of Neighbours

1: procedure NumberNeighbours(List Neighbours)
2: int Tth : freshness of neighbours
3: int N : number of neighbours
4: foreach (n ∈ Neighbours) do
5: if ([Now−Neighbours[n].Timestamp] > Tth) then
6: Neighbours.Remove(n);
7: end if
8: end for
9: N = Neighbours.size();
10: return N;
11: end procedure

At the point when a vehicle needs to register the quantity of its neighbour, it begins by refreshing the rundown of its neighbour as definite in the Calculation 2. To do as such, it verifies if the time since the accepting of the last message is higher than a given edge, indicate Tth. Provided that this is true, it expels the neighbour from the rundown. The quantity of neighbors is then assessed as the cardinality of the inferred refreshed rundown.

Algorithm 3 Estimating Speed

1: procedure SpeedEstimation(List Neighbours)
2: double Vest : estimated speed
3: double a : constant of fluid area
4: double b : constant of congested area
5: double dc : critical density
6: double dmax : maximal density
7: double c = −b∗dmax : second constant of congested area
8: double density : current density
9: int Length : length of the segment
10: density = (NumberNeighbours(Neighbours)+ 1) / Length;
11: if (density < dc) then . Fluid Area
12: flow = a∗density;
13: else if (density < dmax) then . Congested Area
14: flow = b∗density + c;
15: else
16: flow = 0; . Traffic Jam
17: end if
18: V est = flow/density;
19: return Vest;
20: end procedure

Then again, the vehicle's speed is assessed dependent on the full scale scopic traffic model utilizing the Central Graph (FD) as depicted by the Calculation 3. To do this, we misuse the attributes of the FD of the section in which the vehicle moves. This FD should be as of now put away in the vehicle inside the guide or downloaded from some specific RSUs.

Algorithm 4 Attack Detection

1. double Vest : estimated speed
2. double V : real speed
3. double Vth : threshold to detect a Sybil attack
4. List Neighbours : list of Neighbours
5. Time Tdet : timer of periodic attack detection triggering
6. Time DetectionTime : timestamp of the attack detection
7. int Timeout : maximum waiting time for an attack confirmation
8. Packet CAM : packet CAM received
9. while (ReceiveCAM(CAM)) do
10. NeighboursUpdating(CAM,Neighbours);
11. end while
12. if (Tdet is expired) then
13. Vest = SpeedEstimation(Neighbours);
14. V = Node.Mobility.GetSpeed();
15. if (|V −Vest| > Vth) then
16. DetectionTime = Now;
17. BrodcastMessage(\AttackDetected");;
18. Wait(Timeout);
19. if (ReceiveConfirmation()) then
20. LaunchCountermeasures(Sybil);
21. end if
22. end if
23. Tdet is armed
24. end if

The Algorithm 4 presents the Sybil attack detection procedure. When the vehicle receives a CAM messages, it updates the list of neighbours according to Algorithm 1. Simultaneously, it waits for a notification about the expiration of the timer T det. Once this happens, it estimates the speed of the vehicle using the Algorithm 3. The difference between the real measured speed V and the estimated one Vest, which is denoted as |V −Vest|, is computed and then compared with a pre defined threshold Vth, which obviously depends essentially on the road and the traffic model. It could be given also as an input with the FD.

5. SIMULATIONS AND VALIDATION OF THE PROPOSED ALGORITHM

This area exhibits the earth and the aftereffects of the system simulation that we use to assess the efficiency of our proposed calculation.

5.1 Reproductions Condition

The point of these reproductions is to focus on a reasonable situation while utilizing institutionalized CAM messages. The pre-owned rendition of CAM messages compares to the ETSI EN 302 637-2 v1.3.2 refreshed on November 2014 [19] by the standardization association European Broadcast communications Principles Organization (ETSI) Consequently, the proposed calculation was primarily actualized over the application and the offices layers into the ITSS engineering as institutionalized in the ETSI correspondence stack. For the advancement of our assault discovery instrument, we utilize the open-source reenactment system iTETRIS, which is a stage that coordinates a system test system and a traffic flow test system. It is made essentially out of four squares:

• The application square: it contains all the applications that can be devel oped inside the vehicular setting.

• The system test system square ns-3: it is a notable system test system, which permits to test and approve correspondence conventions.

• The versatility test system square SUMO: it is a notable portability test system, which permits to produce a sensible portability model of the vehicles that will be utilized in the reproduction.

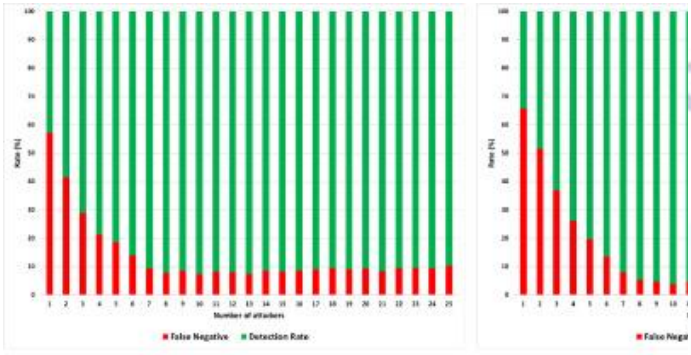
• The controller square iTETRIS Control Framework (iCS): It facilitates the activities between the other three squares. It is some way or another the planning square of this stage. In this way, when an activity is activated by an application direction, ns-3 will recreate a V2X transmission in the correspondence situation inside a remote system. The consequences of this trade are sent by iCS to the application which, thus will deliver a specific activity that will be embraced in the reproduced street traffic situation by SUMO The last ceaselessly encourages others hinders with refreshed vehicle positions through iCS.

5.2. Traffic situation and assault reproduction

Right now, will detail the pre-owned portability model for the assessment of our Sybil assault identification component. The first step comprises in defining the FD qualities. To do that, we utilized a portability situation in SUMO dependent on a 7 fragments in a round street with no off-ramp. At that point, vehicles are presented individually until coming to the traffic jam. Hence, we can go through all the conceivable traffic stages. During this re-enactment, we coordinate sensors (attractive circles), which are situated on the intersections between portions, to gather in a CSV file the required information for the FD parameters identification (for example speed, thickness, inhabitance rate, and so forth.).

The length of the segment has a weak impact on the false positive detection rate. In fact, the

segment with a length of 600m has a higher false positive detection rate. This could be explained by the fact that the fundamental diagram is more accurate with longer segments which allows a better detection rate. Besides, the congestion is smoother in long segment since the traffic is less jerky, and therefore this reduces the false positive detections.



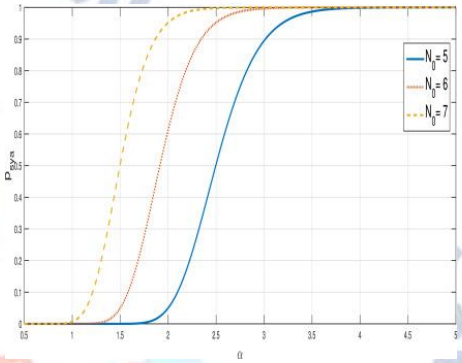
(a) 600m (b)

Attacks detection rate Vs. the speed threshold for different segment lengths

Detection rates compared to the detection speed threshold and the number of the attackers, respectively, for two segments with a length of 600m and 1200m. A false negative detection means that the attack was not detected by the vehicle when it is in progress .To examine the effect of the pre-owned speed edge, figures and present the right identification rates and the bogus negative ones for two fragments with a length of 600m and 1200m individually. It very well may be seen that, when the limit is expanded, the pace of bogus negative discovery is higher. This could be clarified by the way that with a rapid edge, we can miss a great deal of assaults. For instance in the figure , with a limit fixed to 30 Km/h, we had a rate around 25% of bogus negative identification, and with 80 Km/h, this rate increments to 40%.

In figures, we fixed the speed limit to 5 Km/h and we fluctuated the quantity of assailants. With a low number of assailants, the recognition is difficult since the difference between the evaluated speed and the genuine one couldn't be very different, particularly in the fluid zone, the speed remains the same (for example free speed) even with more vehicles. The difference will be more significant in the blocked are. This is appeared by the figure, where, when we have in excess of 8 assaulting vehicles, we will have nearly a similar recognition rate, which is about 90% of right location. From figures , one can comment that the right location rate is marginally higher for a more drawn out portion. Since the section is longer, the congested territory will last more, than a shorter portion, before the all out clog of the street, permitting more efficient assault location. In addition, a vehicle traveling through a long portion will take additional time, and afterward it will have more chances to identify the assault.

Given the simulation parameters , we discovered the ”best” combination of parameter settings in Table 4, where ”best” is defined as a compromise between the performances in terms of false positive, false negative and true positive detection rates. These parameters obviously depend on the fundamental diagram of the road’s segment.



6. CONCLUSION

This paper introduces another Sybil assault location instrument for IoV. This component thinks about every vehicle, as a Helpful Insightful Transportation Framework Station, trading CAM messages. It exploits from a well known perceptible traffic flow models, that should be as of now gave to the vehicles. We first exhibited a calculation that recognizes the Sybil assault utilizing the CAM messages gave by neighbours, which appraises the speed of the vehicle utilizing the major outline of the street's section. On the off chance that this assessed speed is too different from the genuine one, it recognizes an assault and communicates an alarm to different hubs. When the assault is recognized, the trigger hub hangs tight for a confirmation from its neighbours so as to think about it as an assault furthermore, not a bogus location one. This instrument, which is anything but difficult to be actualized furthermore, extremely amazing, has been additionally approved through a numerical model and some reasonable reproductions that demonstrate its efficiency since it recognizes more than 90% of the assaults, when all around tuned.

Our future works will manage the identification of the aggressors and the plan of certain countermeasures to fight against them.

REFERENCES

[1] http://www.ict-itetris.eu/ (access October, 21st 2018)

[2] H. J. Payne, Models of Freeway Traffic and Control. Simulation Councils, Incorporat, 1971.

[3] Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. ETSI EN 302 637-2 v.1.3.2 (2014-11).

[4] European Telecommunications Standards Institute (ETSI), Available at http://www.etsi.org.

[5] Raksha Tiwari, Tripti Saxena. A Review on Sybil and Sinkhole of Service Attack in VANET. Recent Trends in Electronics & Communication Systems. 2018; 5(1): 7–11p.550

[6] Study on the Deployment of C-ITS in Europe: Final Report, Website available at:

[7] https://ec.europa.eu/transport/sites/transport/files/2016-c-its deployment-study-final-report.pdf

[8] M. T. Garip, P. Reiher and M. Gerla, "Ghost: Concealing vehicular botnet communication in the VANET control channel," 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, 2016, pp. 1-6. doi:10.1109/IWCMC.2016.7577024.

[9] A. Zeroual, N. Messai, S. Kechida, F. Hamdi, A Piecewise switched linear approach for traffic flow modeling, International Journal of Automation and Computing, Vol. 14, pp. 729-741, 2017.560

[10] S. Boubaker, F. Rehimi, and A. Kalboussi, "Comparative analysis of microscopic models of road traffic data," in 2011 4th International Conferenceon Logistics, 2011, pp. 474–478.

[11] M. T. Garip, P. H. Kim, P. Reiher and M. Gerla, "INTERLOC: An interference-aware RSSI-based localization and sybil attack detection mechanism for vehicular ad hoc networks," 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, 2017, pp. 1-6. doi: 10.1109/CCNC.2017.8013424.

[12] S. Han, D. Ban, W. Park and M. Gerla, "Localization of Sybil Nodes with Electro-Acoustic Positioning in VANETs," GLOBECOM 2017 - 2017IEEE Global Communications Conference, Singapore,2017,pp.1-6. doi:10.1109/GLOCOM.2017.8253994.

[13] M. Khalil and M. A. Azer, "Sybil attack prevention through identity symmetric scheme in vehicular ad-hoc networks," 2018 Wireless Days (WD),Dubai, 2018,pp. 184-186. doi: 10.1109/WD.2018.8361717.

[14] Q. Tang and J. Wang, "A secure positioning algorithm against Sybil attack in wireless sensor networks based on number allocating," 2017 IEEE 17thInternational Conference on Communication Technology (ICCT), Chengdu, 2017, pp. 932-936. doi: 10.1109/ICCT.2017.8359771

[15] S. Chang, Y. Qi, H. Zhu, J. Zhao and X. Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1103-1114,June 2012. doi:10.1109/TPDS.2011.263.