International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

The Detection of Sybil Attack by Location Based Privacy System

WilrenD'cruz

M.tech student, Department of Communication Engineering,
Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, Kerala, India

Abstract: ***In this system Sybil attack is detected by localization of nodes by using the infrastructures. Privacy and security are the two important issues in VANETs. Sybil attack is an attack that the malicious user pretends to be multiple vehicles. This reduces the load on the DMV by finding the Sybil vehicle. This is done by the help of RSU that determines the location of the suspicious node andfind the difference from its position.this type of detection need not disclose its identity and privacy is preserved.this is validated by simulating in a realistic test case.***

Keywords: SYBIL ATTACK , VANET, PRIVACY, RSU, DMV.

1. Introduction

As the road accidents are increasing day by day,the government and the automotive industry faces a big challenge in securing the road. A single distraction or a misjudgement can cause road accident that may take human life.Vehicular-ad-hoc-networks(VANET) are being used for traffic control,accident avoidance and management of parking.VANET enables the vehicles to communicate each other by wireless means.VANET faces many security threats that attack on VANET can leadto human life loss. The Sybil attack is very harmful when there is no centralized authority. Sybil attack means the vehicle claims to have many identities and gives an illusion to the driver that there are additional vehicles on the road.thus the malicious vehicle can cause a traffic jam.This method is to enhance security in VANET by detecting the Sybil attack. The proposed scheme is a infrastructure based scheme and a pool of pseudonyms are assigned to the vehicles. That is the vehicles obtain pseudonym from a trusted road side board. These pseudonyms are hashed to a common value so that it can prevent vehicles from Sybil attack. The detection is performed in two steps. In first step the detection is performed by road-side unit which measures the position of each vehicles. This measures a distinguishability degree between the vehicles. If the degree of distinguishability is above the threshold then the RSU report to DMV(central authority). In second step the DMV computes the fine grained hash of the suspicious vehicles.

2. Motivation and Related Works

Zhou et al[3] described a privacy preserving scheme for the detection of Sybil attack by road side unit. and DMV. In this scheme a pool of pseudonyms are hashed to a same value,only with that pseudonym they can communicate. This can increase the privacy but it will be an overload for the DMV to maintain the list,when all the suspicious vehicles, reported to DMV. Studer et al[5] and Tang et al[4] proposed two methods against the Sybil attack by a central authority. One of the scheme described is by assigning tickects to the neighbouring nodes inorder to authenticate them. This is done by central authority which again makes over load to it. Another method is a more distributed scheme, by which a regional authority is assigned to generater (TACKS)temporary anonymous certified keys.

Douceur[2]proposed thesybi attack in peer-to-peer networks,which affects the distributed network. A way to prevent this attack is by assigning a certified authority. If each vehicle had one and only one identity ,they can prevent attack to the VANET as they can be easily tracked.

Resource testing is another way to prevent Sybil attack. Xiao et al[6] and Bouassida et al.[7] described the methods for resources testing. In [9] integrated radar and verification of coherence with the suspected node is done by the received GPS beacon. A spatio-temporal correlation that exists between two vehicle is found as the two vehicles are in same space at the same time by Park et al[10]. This is done ,as the different node assign different timestamp given by the RSU.

3. System Model

3.1 VANET architecture

- The DMV is the trusted authority that maintains the vehicle records and the certified pseudonyms that are assigned to the vehicles. DMV consist of a large resources that can generate pseudonyms for all the vehicles and can store all the information regarding the vehicles.
- RSU is the access point that are scattered on the roads and informations are passed to the DMV by wirred connection. They act as a intermediate to the DMV. Rsu monitor the vehicle activity and if it found to be malicious then it will report to the DMV.
- Vehicles are the untrusted parties and they communicate each other in a multihop manner. They contain wireless devices using 802.11p protocol.

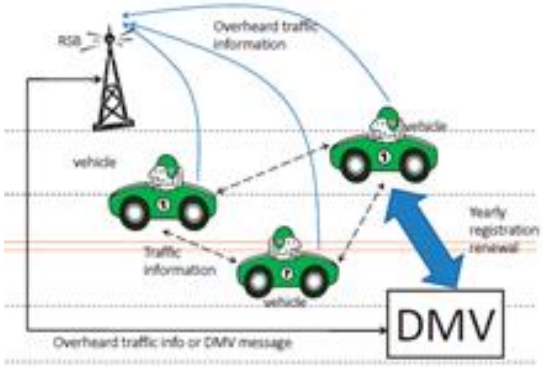


Figure 1 :VANET architecture

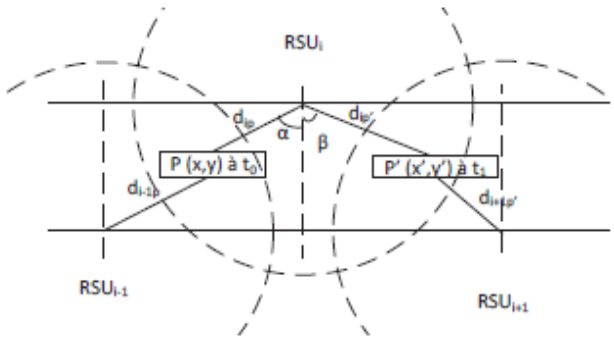


Figure 2: Node localizaion

3.2 Attackers assumption

- Attackers have more computational power and can alter the signal strength.
- Attackers may use more than one certified pseudonym to send the messages.
- Attackers can able to launch Sybil attack.

4. Proposed Scheme

In the proposed scheme, the RSU performs the detection steps. And only if the RSU detect the vehicle to be suspicious, it will report to the DMV. Thus decreasing the over load of DMV. As the RSU's are not the trusted authority they have only the limited information's. The proposed scheme works in three steps. The first is the initialization step the second is the detection step and the third and final step is the verification step

4.1initialization step

In the initialization step , the vehicles are assigned a pool of pseudonyms that are certified. The DMV initially hashes the pseudonyms by a one-way hash function and the outcome is filtered out. It is then assigned as the coarse-grained pseudonyms. In second stage it is passed to a fine grained key.
In other words, for each pseudonym *pl*in the *m*-th coarse-grained group, we have $\boldsymbol{H(pl|\kappa c) = \Gamma m}$, where *H* is a one-way hash function, and Γ*m*is the coarse-grained hash value for group *m*. , the DMV calculates the hash value for the above *p* with a new key *κf*, and selects a set of bits from the result. The bits selected from the new hash value are referred as the "**fine-grained hash value".**

4.2 Detection step

- In the first stage the RSU will go through aa the pseudonyms and checks the coarse grained group. It may either a false alarm or a Sybil attack.
- In second stage a second screening is done to decrease the false alarm. Here the RSU finds the position of the vehicle. It is done by received signal strength and angle of arrival.
- If p and p' are suspicious pseudonyms ,the RSU compares both the pseudonyms and its position to compute the distinguishability degree measure.t0 and t1 be the time when RSU receives the message.

We compute angle and position of p and p' with RSU_i by using the data collected from the neighboring RSUs
The RSU_i(xi,yi) computes the received message and the distance between its sender.the neighboring RSUs(RSU_{i-1}(xi-1,yi-1) and RSU_{i+1}(xi+1,yi+1)) send the distance di-1_p and di+1_p to calculate the p's position.

- Djv= -1 if RSUj fails to receive the message , i.e , It is not in the communication range of RSUj.
- Djv>0 if RSUj received the message. Taking the two distance, we calculate the position P
- $$DD = \frac{\sqrt{(x-x')^2 + (y-y')^2}}{V_{max}|t_1 - t_0|}$$

If DD>>1, propability of two nodes to be malicious is zero which means that they are just two vehicle belonging to same coarse-grained function. Else, the propability of two nodes to be malicious tends to 1 which means the suspected vehicle is malicious and will report to DMV.

4.3Verification Step

When the DMV is reported by the RSU that the two vehicle's pseudonyms are of same coarse-grained function i.e, DD between 0 and 1,the DMV checks for the fine-grained group.if it found true then the DMV identify the suspicious vehicle to be malicious

5. Experimental Setup and Result Analysis

In this section, the performance is evaluated by the following steps: detection rate, false positive rate, true positive rate and DMV charge.

Simulation setup
Here NS-2 version 2.35 is used for simulation. 802.11_p MAC and PHY layer protocol is used. The simulation is done in two scenarios, one is of densely distributed vehicles and other is of sparsely distributed vehicles.

- The path loss model:

$$\frac{P_r(d)}{P_r(d_0)} = \left(\frac{d}{d_0}\right)^{\beta}$$

- Relation of the received power and distance:

$$\frac{P_r(d)}{P_r(d_0)_{dB}} = -10\beta \log\left(\frac{d}{d_0}\right) + X_{dB}$$

Simulation result

Simulation result can be evaluated by the following parameters

- Detection rate (DR)

Detection rate is defined by the following expression

$$DR = {}^{TPd}/_{TPr} * 100\%$$

Where TP_d is the number of true positive detected. TP_r is the number of attacks.

- False positive rate(FPR)

It is defined as

$$FPR = {}^{FP}/_{NBm} * 100\%$$

Where FP is the number o false positive reported to DMV

- DMV load

It is defined by the equation

$$DL = {}^{FP + TP}/_{NBm} * 100\%$$

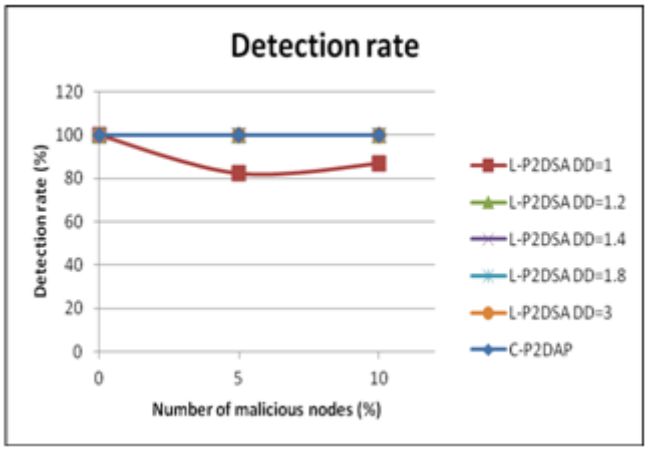
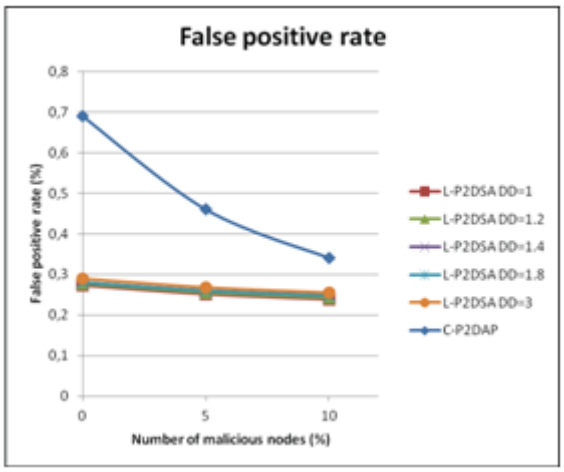
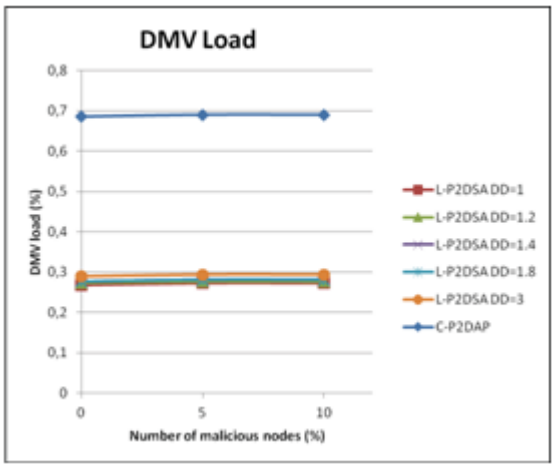


Figure 3: DR, FPR DL of 20 vehicles/km/lane





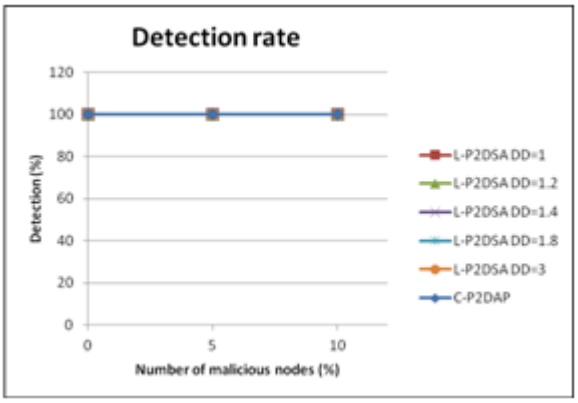


Figure 4: DR,FPR,DL of 50 vehicles/km/lane

6. Conclusion

This paper propose a method to detect the sybil attack in VANET without giving overload to DMV. Here the detection is performed by RSU by decreasing the work of DMV. The addition of second screening that checks the distance between the suspicious nodes decrease the DMV load and false rate detection. One of the interesting future scope is that, to add regional scheme upon entering a region by RSU certified sign. This helps in reducing the cost by reducing the number of RSUs

References

[1] P. Golle GREENE D.et STADDON J. " Detecting and Correcting Malicious Data in VANETs " VANET '04, 1 Octobre 2004.

[2] Douceur J. R. "The Sybil Attack", Microsoft Research, PEER-TO-PEER SYSTEMS Lecture Notes in Computer Science, 2002.

[3] Zhou T., CHOUDHURY R.R., NING P. et CHAKRABARTY K. "P2DAP — Sybil Attacks Detection in Vehicular Ad Hoc Networks" IEEE Journal on selected areas in communications, VOL. 29, NO. 3, Mars 2011.

[4] Tang L., HONG X. et BRADFORD P. G. "Privacy-preserving Secure Relative Localization in Vehicular Networks" Security Comm. Networks, 2008.

[5] studer A., SHI E., BAI F. et PERRIG A. "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs". SECON '09, 2009.

[6] Xiao B., YU B. GAO C. "Detection and Localization of Sybil Nodes in VANETs". DIWANS'06, September 26, 2006.
[7] Bouassida M. S., GUETTE G., SHAWKY M., DUCOURTHIAL B. "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET". Apparu dans : International Journal of Network Security, Vol.9, No.1, PP.22-33, July 2009.
[8] Grover J., GAUR M. S. et LAXMI V. "A Novel Defense Mechanism Against Sybil Attacks in VANET", Sin'10, Russie, 2010.
[9] Yan G., Olariu S., Weigle M.C., "Providing VANET Security Through Active Position Detection", Computer Communications: Special Issue on Mobility Protocols for ITS/VANET, vol. 31, no. 12, 30 July 2008, p. 2883-2897, ISSN 0140-3664.
[10] Park S., ASLAM B., TURGUT D., ZOU C.C. "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support". Military Communications Conference, 2009.

Author Profile

Wilren D'cruz: received the B.Tech degrees in Electronics and Communication Engineering from M.G University, Kerala at Mar Baselios College of Engineering and technology, peermade in 2012. And now she is pursuing her M.Tech degree in Communication Engineering under the same university in Mount Zion College of Engineering.