AMSE Association for the Advancement of Modelling & Simulation Techniques in Enterprises
IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Advances in Modelling and Analysis B
Vol. 61, No. 1, March, 2018, pp. 5-8
Journal homepage: http://iieta.org/Journals/AMA/AMA_B

An efficient method for detection of Sybil attackers in IOV

Satya Sandeep Kanumalli[1*], Anuradha Ch[2], Patanala Sri Rama Chandra Murty[3]

[1] Research Scholar, CSE Department, Vignan's Nirula Institute of Technology & Science for Women, Acharya Nagarjuna University, Guntur 522009, India
[2] CSE Department, Velagapudi Ramakrishna Sidhartha Engineering College, Vijayawada 52007, India
[3] CSE Department, Acharya Nagarjuna University, Guntur 522510, India

Corresponding Author Email: satyasandeepk@gmail.com

Received: 2 February 2018
Accepted: 10 March 2018

Keywords:
internet of things, internet of vehicles, sybil nodes, K-means, RSU, on board unit, DSRC

ABSTRACT

Brave new world was emerging and chancing its face day by day with the advent of IOT, as a part of it we have IOV which may change the way we are driving our vehicles leading to Autonomous driving, As there is a lot of Buzz on these trends they also comes with security threats of different forms in which Sybil Attack is one in which a malicious vehicle may create multiple identities to a Real one, with which he may circumvent different forms of attacks, We proposed an approach in which we divide the vehicles in to different clusters with their location information and certificate and filter the Sybil nodes with an idea no two nodes with the same identities will have different location ID's or may fall in different clusters at the same time.

1. INTRODUCTION

With the advent of IOT and its real world applications creates a technological shift for costumers and as well as stakeholders. Intelligent Transportation System as an application of IOT helps shaping up the world of Driving with its numerous number of safety applications and making it smart which opens up the new area of Autonomous driving.

With the increasing number of connected cars brings up new set of Vulnerabilities in which Sybil Attack is one of its kind where a node behave like a legitimate one but creates numerous number of false identities which confuses the centralized authority to mistake the attacking node as a real node and vice-versa

For V2V, V2I and V2X [17] communication in IOV need to provide cars identity to the other party in communication in the Figure 1 Car X provide identity I_x to RSU but prior Car Q provide its identity say I_X instead of I_Q, which makes RSU believe that Car Q's Identity is I_X, the same way Q provide its identity I_H instead of I_Q under a different RSU and maintain communication and provide certain privileges of car X and car H which creates a serious problems like Car Y can device various attacks on others ultimately making Car X responsible for everything.

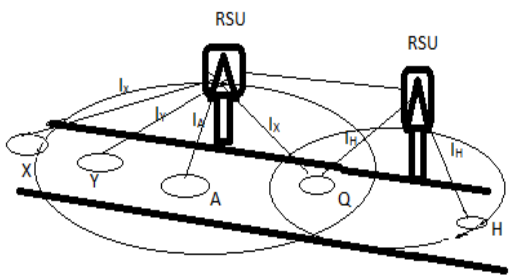

Figure 1. Sybil attack

It is very hard to identify a sible node in such a dynamic heterogeneous as the nodes are always mobile associating with different sets of nodes and as well as different RSU [18], the main problem in identification of a sible node is to differentiate it to a legitimate node, Need to take multiple scenarios of the node and analyze its behavior and filter it out as one scenario may not lead to result. In our approach we devised an approach in which we create clusters of vehicles formed from location information, Certificate and filter out the attacker Node.

2. RELATED WORK

There is lot of work done to detect sybil attacks in WSN and VANET's but very less work done for detection of Sybil attacks in IOV in which certain solutions can be directly inferred from VANET's solutions which are classified in to three category's which includes detection based on certificate, detection based on position, and detection based on resource testing and all of these three and there are different solutions that falls under these mechanisms [15-17] have their own problems.

Xia Feng et al. [1] proposed an event based reputation system in which there is a trusted authority which issues and verifies certificates which are communicated by RSU and there is a event table in OBU which stores different events generated they generate reputation value and event value which incremented for every event occurrence and sybil nodes generates least no of events which can be detected and isolated.

JinTang et al. [2] proposed a solution called DMON, which is based on cryptographic ring signatures, and it replaces vehicle identities by their certificates that are generated using neighbor relationship of RSU. And the Sybil node may not characterize the to have the neighbor relationship of RSU and can be detected by filtering out signatures from certificate.

YunchuanSun et al. [3] have classified Sybil attack as one of the attacks on authentication in which they had not proposed any pin punted mechanism but given its countermeasures in form of Threat models, Intrusion detection system and key management .

Chea et al. [4] have proposed a distributed detection based solution in which anode is detected as Sybil if it is passive in data eet alxchange even the node is in between two other communicating nodes and there will be a voting of Sybil node from the neighborhood information that is collected periodically.

Yuan Yao et al. [5] have proposed a detection mechanism which is based on Received Signal strength Indicator in which each node independently generates a message containing RSSI time series called vascular speech and all of its neighbors exchange such messages and the similarity in the messages are compared between them to filter Sybil node , it does not need any centralized infrastructure for detection.

PengwenlongGu et al. [7] have proposed a solution detection mechanism based on Vehicle driving pattern in which for every vehicle they create a matrix based of driving pattern which is generated by beacon messages they used to exchange, and these matrix are compared with the actual pattern and if an unusual behavior is taken as a Sybil node.

Khaled Rabieh [6] have proposed a solution to detect Sybil vehicles based on their locations in which each of the vehicle is sent challenge and it has to respond with its location as the sybil node most likely to send false data it can be detected using some comparisons, as the challenges can note be sent all the times which creates a lot of overhead, these packets are sent in case of suspicion for Sybil attack.

Many other [7-11] have taken Sybil attack detection with different approaches but every one of them have their own pros and cons resulting no standard way of detection.

3. SYSTEM MODEL

The system model can be described as IOV connects the cars to infrastructure, with the help of cars Onboard Unit (OBU) which is equipped with different integrated technologies like DSRC, GPS, LADER, Optical camera's and various sensors [22] which work independently or together to generate data of the vehicles. The data generated by the vehicles are sent to Road Side Units (RSU) [18] using 4G or existing DSRC [29], These RSUs are connected with other RSU to form a network[12], which takes care of the Handover and Vehicles can communicate with one another using DSRC, which falls in their range.

Every vehicle is holding an unique identity ID_V [13]which is given by the manufacturer and registered under government and also it holds a certificate C_V which is holding ID_V and different parameters of the vehicle which is signed by a global authority.

3.1 Communication model

Figure 2 depicts vehicle V enters an RSU coverage from another RSU it must submit its certificate C_V to RSU and RSU validates it by checking it over the revocation lists and it handovers a temporary certificate TC_V so that the vehicle can communicate with other vehicles using TC_V under a RSU coverage[20] and these temporary certificates may expire soon after the vehicle enters another RSU leaving from current RSU. All the RSUs are interconnected with one another and they do all the necessary knowledge sharing and handover.

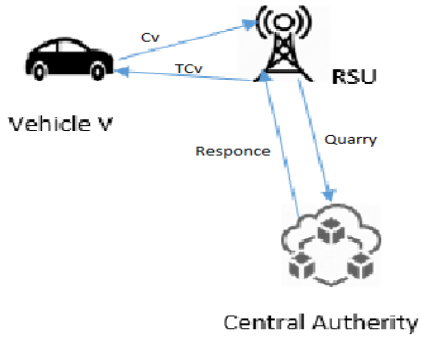

Figure 2. Communication model

RSUs are connected to a secure central authority equipped with Big Data analytics. RSU may transfer information like certificates, Location information, sped and may conduct necessary computation in the form of a Quarry and Central Authority give back the result as a response to requested RSU, the central authority may keep track of certificates and maintain revocation lists and it also maintains a blacklisted vehicles and it keep updating all the information.

3.2 Threat model

To undergo a Sybil attack the attacking nodes must possess different sets of valid certificates, which may be acquired while capturing, or spoofing from the real vehicles while they handshake with RSU and use these fake identities to get the required TC_V form RSU and act and communicate like a legitimate vehicles and they at a given moment of time they may be registered under different RSUs with different TC_Vs.From the set of vehicles, few of them may form as attacking nodes covered under different RSUs can send false information to nearby vehicles and RSU it sends multiple false locations at a given period of time.

4. PROPOSED WORK

Every vehicle sends location information to RSU in regular intervals of time Here we use K Means Clustering algorithm [24-27] to form Vehicular clusters under each RSU which leads in different vehicular clusters. Due to the dynamic nature of the vehicles the clusters may change dynamically which ultimately results in the formation of new clusters with the location change [22].

Algorithm

Step 1 :Apply K-Means
Using location data run K-Means clustering algorithm for n vehicles under RSU, which forms clusters
Step 2: Means are calculated for each cluster
Step 3: Repeat steps 1 and 2 every 0.5 to 2 sec which results in new set of Means and record them
Step 4: Suspicious node detection
If two consecutive Mean variation is more than specified threshold
Read the nodes that caused the variation into a set of

suspicious nodes

Step 5: understand the behavior

For every node in set of set of suspicious nodes

If speed variation is much high or if the node had an angular change

Remove it from suspicious node set

Step 6: Filtering out the Sybil nodes

Take the subset of suspicious node set created under different RSUs under a region

If the nodes having same identities under different cluster identities

Then the resultant nodes are Sybil nodes

4.1 Apply k-means

Under an RSU_A a set of n vehicles sends location data say L_1, L_2, L_3… L_n, and under RSU_B a set of m vehicles sends location data say L_1, L_2, L_3… L_m which are obtained from OBU of the vehicles, Each RSU may locally or remotely runs K-Means algorithm which ultimately forms clusters C_1, C_2…C_k

For each cluster C_i calculate mean using K-Means algorithm which results in mean M and do it independently for each cluster

M= K-Means (L_1, L_2, L_3… L_n)

For every 0.5 to 2 sec we calculate new Means for the new location data as the locations for each vehicle changes periodically which results in new set of means M_{t1}, M_{t2}... M_{ts} of the clusters

4.2 Suspicious node detection:

Once after getting M_{t1}, M_{t2}... M_{ts}calculate the mean variation, which can be drawn from the difference in two consecutive means

$$\delta M_1 = M_{t2} - M_{t1}$$
$$\delta M_2 = M_{t3} - M_{t2}$$
$$\delta M_s = M_{ts} - M_{ts-1}$$

Let λ be the Mean Variation Threshold which can be driven from the previous outcomes, type of the road, speed limitation of the vehicles, line diversions etc. we can set the λ value keeping all these factors combined or individually for example if the road is not having any diversions then it may have average λ value, but if the roads are narrow, having diversions then λ can take high values it also varies with the vehicle density

Once the threshold is fixed then it is compared against the mean change if the mean change is greater than the threshold that is if $\delta M_1 > \lambda, M_2 > \lambda$ … then identify the nodes which caused the variation in to a set called suspicious nodes set.

4.3 Understanding the behavior of suspicious nodes

Once the suspicious nodes are detected then understand their behavior, if the mean variation of the vehicle is due to sudden acceleration which can be directly taken or derived from the speed change over the time periods or if the vehicle is leading to an angular change which can be derived from change in its location then such kind of vehicles are the processing general behavior can be withdrawn from the suspicious set.

4.4 Filtering out the sybil nodes

Same way RSU_A and RSU_B prepare their own suspicious sets they are compared with one another and also with the global set under a region common nodes are filtered out. These node identities are taken along with their cluster identities from which we can figure out Sybil nodes as they possess same identities under different clusters.

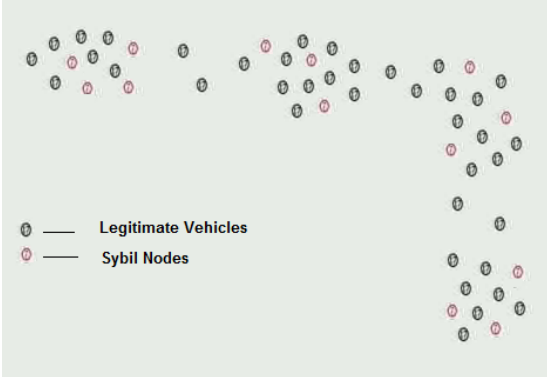

Figure 3. Identification of sybil nodes in a VANET

5. SIMULATION RESULTS

We have simulated our detection mechanism using OMNET++ having Veins extension and the vehicles are simulated using SUMO [19] with 100 cars having 2 RSUs forming 4 clusters with a single diversion in path and with the mean variation threshold λ= 15, K-Means algorithm is called every 0.5 sec, we have assigned 20 Sybil nodes with for every 5 nodes processing same temporary certificates TC_V.

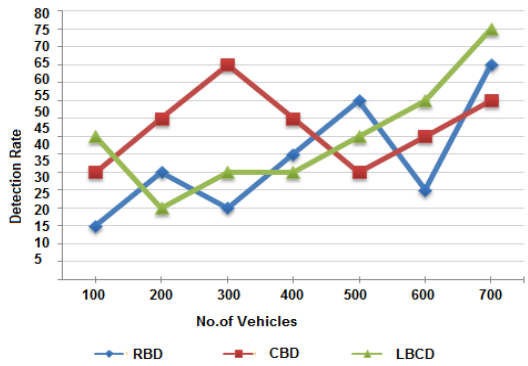

Figure 4. Comparison levels of different detection techniques

The simulation is carried for 10 sec in which our mechanism able to identify the Sybil nodes, as shown in the graph and we have successfully taken the results for different λ values in different traffic scenarios which leads a good detection rates and as shown in Figure 4 the Sybil nodes are shown in red color have been properly identified from legitimate nodes.

We have compared our simulation results with different set of nodes and observed the detection rate and compared it to other existing implementations like certificate based, resource testing based. As shown in Figure 4 our mechanism gave a very good results with a good rate of detection and the result doesn't get much effected as the number of Sybil nodes increased.

6. CONCLUSION AND FUTURE WORK

With new ways to communicate and drive will come with new challenges, Our work deals with detection of Sybil Vehicles considering road safety application in which we have given an Algorithm which uses K-Means algorithm for clustering out the nodes and dynamic filtering of Sybil nodes using behavioral understanding of the vehicles.

We end up with a good results in detecting Sybil nodes without compromising Delay in communication, our work also opens doors to Pure IOV based communication and detection using Global infrastructure without relying on RSU as we use RSU as a key player in our work.

REFERENCES

[1] Feng X, et al. (2017). A method for defensing against multi-source Sybil attacks in VANET. Peer-to-Peer Networking and Applications 10(2): 305-314.

[2] Feng X, Jin T. (2017). Obfuscated RSUs vector based signature scheme for detecting conspiracy Sybil attack in VANETs. Mobile Information Systems.

[3] Sun YC, et al. (2017). Attacks and countermeasures in the internet of vehicles. Annals of Telecommunications 72(5-6): 283-295.

[4] Sowattana C, Wantanee Viriyasitavat, Assadarat Khurat. (2017). Distributed consensus-based Sybil nodes detection in VANETs. Computer Science and Software Engineering (JCSSE), 2017 14th International Joint Conference on. IEEE.

[5] Yao Y, et al. (2017). Voiceprint: a novel Sybil attack detection method based on RSSI for VANETs. Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on. IEEE.

[6] Rabieh K, et al. (2015). Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs. Communications (ICC), 2015 IEEE International Conference on. IEEE.

[7] Gu, PWL, et al. (2016). Vehicle driving pattern based Sybil attack detection. High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on. IEEE.

[8] Chang S, et al. (2012). Footprint: Detecting Sybil attacks in urban vehicular networks. IEEE Transactions on Parallel and Distributed Systems 23(6): 1103-1114.

[9] Grover J, Manoj SG, Vijay L. (2015). Multivariate verification for Sybil attack detection in VANET. Open Computer Science5(1)1.

[10] Hussain R, Heekuck O. (2014). On secure and privacy-aware Sybil attack detection in vehicular communications. Wireless Personal Communications 77(4): 2649-2673.

[11] Kang JW, et al. (2016). Location privacy attacks and defenses in cloud-enabled internet of vehicles. IEEE Wireless Communications 23(5): 52-59.

[12] Liu YB, Wang YH, Chang GH. (2017). Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm. IEEE Transactions on Intelligent Transportation Systems 18(10): 2740-2749.

[13] Sakiz F, Sevil S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Networks 61: 33-50.

[14] Li W, Joshi A, Finin T. SVM-case: ANSVM-based context aware security framework for vehicular ad-hoc networks. In: 82nd IEEE Vehicular Technology Conference. IEEE

[15] Sun YC, et al. (2014). Constructing the web of events from raw data in the web of things. Mobile Information Systems 10(1): 105-125.

[16] Al-Sultan S, et al. (2014). A comprehensive survey on vehicular ad hoc network. Journal of Network and Computer Applications 37: 380-392.

[17] Sowattana C, WantaneeViriyasitavat, and AssadaratKhurat. (2017). Distributed consensus-based Sybil nodes detection in VANETs. Computer Science and Software Engineering (JCSSE), 2017 14th International Joint Conference on. IEEE.

[18] Pattberg B. (2015). DLR-Institute of transportation systems-SUMO–simulation of urban mobility. Sumo-sim. org.

[19] Khatoun R, Zeadally S. (2016). Smart cities: Concepts, architectures, research opportunities. Communications of the ACM 59(8): 46-57.

[20] Khadige A, Zhuang WH. (2014). Stochastic analysis of a single-hop communication link in vehicular ad hoc networks. IEEE transactions on intelligent transportation systems 15(5): 2297-2307.

[21] Gerla M, et al. (2014). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. Internet of Things (WF-IoT), 2014 IEEE World Forum on. IEEE.

[22] Yan SH, et al. (2014). Optimal information-theoretic wireless location verification. IEEE Transactions on Vehicular Technology 63(7): 3410-3422.

[23] Bhargava BK, et al. (2016). A systematic approach for attack analysis and mitigation in V2V Networks. JoWUA 7(7): 79-96.

[24] Jain AK. (2010). Data clustering: 50 years beyond K-means. Pattern recognition letters 31(8): 651-666.

[25] Likas A, Vlassis N, Verbeek JJ. (2003). The global k-means clustering algorithm. Pattern Recognition 36(2): 451-461.

[26] Mahamed GHO, Salman A, Engelbrecht AP. (2006). Dynamic clustering using particle swarm optimization with application in image segmentation. Pattern Analysis and Applications 8(4): 332.

[27] Shafeeq A, Hareesha KS. (2012). Dynamic clustering of data with modified k-means algorithm. Proceedings of the 2012 conference on information and computer networks.

[28] Kenney JB. (2011). Dedicated short-range communications (DSRC) standards in the United States. Proceedings of the IEEE 99(7): 1162-1182.

[29] Eckhoff D, Sommer C. (2012). A multi-channel IEEE 1609.4 and 802.11 p EDCA model for the veins framework. Proceedings of 5th ACM/ICST international conference on simulation tools and techniques for communications, networks and systems: 5th ACM/ICST international workshop on OMNet++. Desenzano, Italy, 19-23.