Madhavi Latha Talluri et al. International Journal of Recent Research Aspects ISSN: 2349-7688,
Special Issue: Conscientious Computing Technologies, April 2018, pp. 190-195

Isolation of Sybil Attackers in IOV

Madhavi Latha Talluri[1], Satya Sandeep.Kanumalli[2]

[1]M. tech Scholar, Computer Science & Engineering, Vignan's Nirula Institute of technology & Science for Woman, Pedapalakaluru Guntur, Andhra Pradesh, India

[2]Assistant Professor, Computer Science & Engineering, Vignan's Nirula Institute of technology & Science for Woman, Pedapalakaluru Guntur, Andhra Pradesh, India

Abstract— **Internet of things enabling internet of services is an emerging technology which is enabling the connection with all the smart devices using the internet. IOT helps in interconnecting the devices sharing the realistic information with the users by providing security and efficiency to the users. Whenever these smart devices connected to vehicles and allow the communication between them then it is called Internet of vehicles .The seamless connection between the digital world and physical world helps in order to give the data a purpose to use. Integration with various devices helps in identifying hazard warning and informing the users with the real time instructions. As the connectivity between the vehicles and the smart devices emerging with the new features lead to huge data transfer there is a huge exchange of data between the vehicles there by increasing the usage of new communication technologies . Conventional VANET uses mobile network which makes use of mobility constraints and the number of connected vechiles.It is used to identify traffic jams, emergency vehicles in the urban areas. It cannot provide global application services to the customers. With the increase of data the problem also increases in leakage of information threatening the security of the device. Authentication is need ti provide without leaking the identity of the vehicle and information of the user. One such attach is the Sybil attack in which they are may approaches against Sybil attack in several services, they disregard the presence of different smart devices and have complex solutions. In this paper we develop a mechanism on how to deal with the Sybil attack. Evaluation of our protocol in OMNET+ simulator demonstrates the effectiveness of our approach in identifying and detecting Sybil nodes in IoT network.**

Keywords—RSU, IEEE802.1p, IEEE1609.2, WAVE, DSRC

I. INTRODUCTION

With the usage of internet becoming common new devices are coming with the fastest communication and storage in the devices providing the real time information to the users.

Internet of vehicles is a part of it which is allowing the communication between the devices and the Vehicles providing realistic information to the users ensuring the safety, accuracy, efficiency and realistic information to make decisions.Iov helps in connection the vehicles and also the mobile internet making the user promote the efficiency of transportation, improve the service level, and ensure that the humans are satisfied. Vehicle in IOV terminology refers to all vehicles that consume or provide services/applications of IOV. Thing in IOV terminology refers to any element other than human and vehicle. Things can be inside vehicles or outside, such as AP or road. Environment refers to the combination of human, vehicle and thing. The usage of these mobile networks helps in communication between the devices and provide the realistic information WAVE(Wireless Access in vehicular environment) is used for communication between v2v and v2I .Short range communication is supported by DSRC.WAVE established a certain set of protocols using IEEE 1609p to develop certain standards in communication which supports both IP

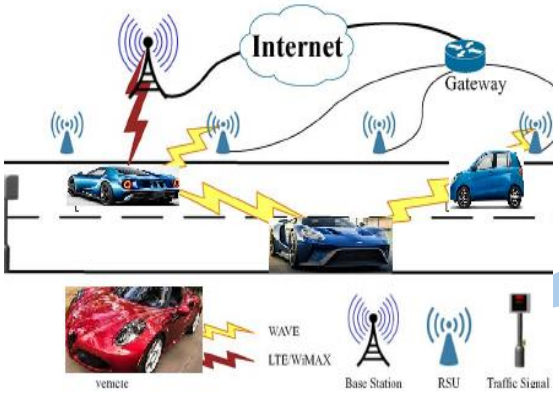
based and non IP based communication. The use of WAVE technology in communication helps in spoofing, eavesdropping alteration and replay. Since there is a huge data exchange there is also exchange of sensitive data .with the exchange of sensitive and accessing of new smart devices

with the evolving technology there can be possibility of attacks on security. The security includes in connecting the vehicle to vehicle, connecting the vehicle to infrastructure that is providing services to other devices and the data. Using of these intelligent devices in communication is providing a threat as they are accessing the passwords and username and can spoof the identity of the vehicles by tampering the information. As the technology is advancing many new threats are coming on the security and privacy of the data.There are variety of attacks done on the data out of which Sybil attack is one of them. Sybil attack is the one which one identity makes a number of various identies resulting the effect on network and breakage of resource utilization, stealing the identies of the owners. Sybil attack is where one identity makes more than one identity on single device. A malicious node makes these identities with the purpose of achieving more benefits from the network or making interrupt in the network. This attacker aims to achieve benefits, such as the usage of unauthorized resources, and getting and publishing private information on network users. [15] When the connectivity to the vehicles is coming from various devices it is difficult to find which is coming to Sybil attack as we need to analyse different scenarios and find the legitimate node and the nodes which are attacked.Sybil attack can be done in various ways either stealing the identity of the vehicle or hampering the network by sending the false images.

Earlier VANET architecture consist of two devices one is the on board unit and Road side unit which is installed in vehicles. The OBU helps in identify the location of devices and establishing the communication between the vehicles in a certain range. The OBU units are connected to the devices which accumulate and calculate the data. The V2I works with communication cars to infrastructure..VANETs allow the direct communication on the vehicles by providing a better road side environment and efficient utilisation. The RSU cover in a certain range helping the vehicles in identifying the nearby areas such as parking or fuel stations. RSU communicate with each other using the wireless technology. In the paper we use a solution which is cost-effective, less time consuming and ease to use for providing the real time data. Certain attributes which influence the decision taking by the

devices and help the driver are used .smart devices help in calculating the information by using these attributes such as network delay or heavy load on the network, increase on the time of communication or communicating with the multiple devices and accessing the privacy information. Falsified data can lead to miscellaneous usage which can cost.

Fig(1) Architecture of IOV



IOV involves not only the communication between vehicles but also the communication with other device and alerting the user by making smart decisions. The OBU in different vehciles is facilitated in communicating with different integrated technologies like DSRC, GPS and various sensors devices. Data generated by the vehicles is sent to RSU using the 4G,Sensor devices which are fixed in communication between the vehicles allows the information to flow .Security is the major concern as many devices involved allow the interexchange of the information easily.

Sybil attack is one attack in which where one node acts as multiple identies resulting in identity theft and breakage of the network. Various cryptographic functions, clustering algorithms, session keys have been used in detection of the Sybil attack .In this approach we propose a light eight approach which is cost effective and can be used easily by the user in detecting the attack. The parameters involved in communication is the connection between the vehicles is secure communication between vehicles and giving the access rights by providing the required information to the devices.

II. RELATED WORK

A. *Literature Survey*

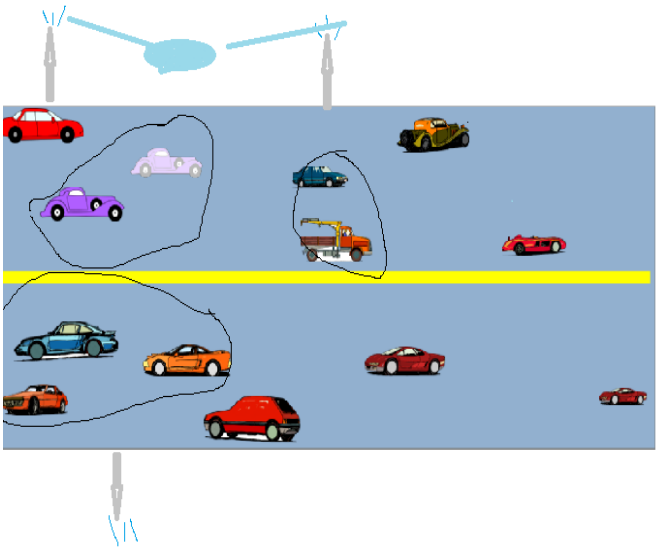
In general the security model followed helps in the detection of the attacks [1], [2], [3].One approach proposed in detecting the Sybil attack in the VANET is using the cryptographic signatures and calculation of the hash algorithm. The hash function [4] is used to verify the the verification time of the vehicle and cryptographic digital signature is used to establish between the communication between the vehicles. An IEEE802.1p is the new standard used for communication which is dedicated to the vehicles.[5] describes a cluster way of communication which is used 8021.p for communicating . The time taken for broad casting, packet delivery and through put are used for various clusters. In this the cluster area is formed by the frequency and a node is elected by using election algorithm for communication of the devices. If any service is not available then all the cluster heads are synchronised and the communication between the vehicles. This paper [6] identifies the potential advantages in internet of vehicles that the traditional IOT approaches in which traffic can be managed and increase the efficiency of the vehcilse.It presents the advantages and disadvantages in IOV allowing the communication between the vehicles.[7] presents the overview of internet of vehcilse.it mentions the objectives of the vehicles using the internet allowing the communication between users and smart devices. Objective to integrate the vehicles ,devices ,human and the transport of the video will yield in the communication .New models have initiated ,may disturb the operations and the quality of the communication so better approaches have to be initiated. In [8] used a a lightweight decentralized Protocol by proposing a trust-extended authentication mechanism (TEAM) for vehicle-to-vehicle (V 2V) communication in VANET.The protocol is insecure against insider attack, impersonation attacks and session key breaking attack[9]. Also, their protocol fails to preserve user traceability, user anonymity and mutual authentication. [10] Provided a comparative study on privacy preserving authentication.[11] IOV an emerging technology with having smart cities making using of global network presents the challenges and the future standard need to be taken between the vehciles.In[12] we discuss a light weight authentication and key agreement approach. In this the clusters are formed using the clustering algorithm and cluster head is elected each time .The vehicles in the cluster communicate with each other using a key agreement protocol generated by the cluster head. The cluster head communicates with the RSU and establishes a secured connection for further communication.[13] the paper reviews the privacy challenges in identifying different areas and the recent privacy preserving techniques proposed.[14] paper proposes the efficiency techniques to support in IOT . The techniques in the detection are classified on the features of network, cryptography and relationship between the neighbours by high lighting the strengths and weakness. [15] Sybil attack detection frame work was evaluate under the SA with fabricate and stolen identities, behaviours churn and multiple identies. JinTanget al[14] used DMON, which is based on cryptographic ring signatures. In this the vehicle identity is replaced by the certificates generated by the RSU.Sybil node is detected by filtering out signatures from certificate

B. *Proposed Work*

In detecting a Sybil attack a new approach has been designed .The approach gives us the quickest response and the detection takes place earlier. Clustering is a method in which vehicles group is denoted by single entity which allow in sharing the load and parallel processing.In this approach we define the authentication between the vehicles and authentication between the RSU .In the model vehicles are denoted by (Vs)

,road side units (RSU) ,application server (S),CA as certificate authority ,CH as cluster head,Ts as the time series stamp. The forming of the cluster is defined by the speed and the ratio of the number of vehicle formed. The communications established in the network are vehicle to vehicle, vehicle to cluster and cluster to road side unit, Road side unit to road side unit. Different authentication mechanisms are need for V2V, V2CH, CH2RSU and RSU to RSU in the network. In this we assume when an attack is done it will tamper the information or modify the network resulting in collapsing the network. Let R1, R2,. . . , Rn be the road side units and vehicles in the network, say V1, V2, . . . , Vi. When the clusters are formed in the vehicles Let CHj is elected as the head of the vehicle .The cluster head is formed using the kmeans algorithm. The vehicles in the cluster establish the communication with the other vehicles using the cluster head which also authenticates the Road side unit. The authentication schemes established in our scheme, the vehicles in a cluster authenticate Vehicle (Vi) to vehicle (Vj) , Vehicle (Vi) to cluster head (CHj), Cluster head (CHj) to road-side unit (Rk).Apart from the authentications and key establishment the RSU establish a key agreement which can communicate secretly using keys. The RSU‘s are uniquely identified and maintain a communication with the cluster head .Tables are maintained to identify the time stamp of each vehicle communicating with the devices and verified if there is any attack. RSU identifies the location of vehicle. The clusters change dynamically with the increase and decrease of the vehicles.As the number of vehciles increses there can be traffic which may lower the speed of the vehicle.

Fig2 Forming of the cluster and establishing the connection with the vehicles is shown below



III. SYSTEM MODEL

Registration phase.

In this the vehicles are registered physically by the government certified user and obtain a secured key (Ks) which is used for communication. The secured key is used to identify the vehciles background and validate them

The Road side units also register and generate CA which is used for communication. As the road side units are deployed with the new wireless technology they need to be registered and get the authorisation certificate for further communication.

A data base table should be maintained by the RSU and the clusters formed by the cluster head which helps in identifying the time for communication and identifying the malicious node.

Electing the Cluster head

In this a cluster is formed based on the region to communicate with the RSU and the cluster head is elected using the kmeans. Electing the cluster head is based on the location and the communication with other vehicles as it responsible for communicating with the cluster as well as the Road side units.The cluster head maintains a table on the communication between the vehicles, RSU and time stamp. Whenever the vehicles communicate they communicate through the cluster head .the communication is noted with the timestamp of vehicles. If vehicles moving at a uniform in speed in cluster try to attack it identifies the flow of the time communication with all the vehicles since the intruder tries to spoof the same identify. If there is sudden increase and decrease it communicates with the neighbouring cluster since the cluster for them increase or decrease so the vehicles identify is noted. If the same vehicle is related in multiple clusters with the same time it will be monitored before confirming the attack.

Authentication and key agreement

The cluster head generates an authentication upon which all the vehicles in the cluster communicate with each other using the cluster head.

The communication between RSU and cluster head is established using the authentication.

The authentication is established between RSU to RSU.RSU when communicate they have their own authentication protocols to filter legitimate vehicles depending on the time of time of communication between them

The vehciles communicate with each other using cluster head elected by the cluster of the vehciles .The cluster head maintains a table with the RSU it is communicate along with the vehicle id and the time stamp .The Sybil node is identified if the communication is occurring from different RSU with the same vehicle id then it is observed for a while by analysing the communication and identify it. If the attack is coming from the same cluster it will validate the communication with the identity of vehicle along with the time stamp. When an malicious attack is done the time stamp of the vehicle and location of the vehicle and the cluster are verified .If the number of vehciles communication with the cluster head at the same time for a certain period and trying to access the information from the infrastructure it is identified as malicious attack. As the time stamp of the vehicle is noted along with the the id of vehicle it is easy to identify.If the number of vehciles are increased at certain time the number of vehicles are categorised and divided into groups.Performance on

froming the clusters and cluster head and the time required for communication is evaluated.

A. Algorithm

Steps:

REGISTER THE VI AND RSUI PHYSICALLY AND GENERATE UNIQUE VALID ID

1. Form the cluster and elect the CHi for each Cluster

2. Generate a key agreement with time TSi ,Vi which communicate with CHi

3. CHi key should be shared with the RSUi and other CHj to communicate with each other.

4. Periodically check the table CHi if the communication with all the vehicles is arriving at once or the time taken to communicate is delayed.

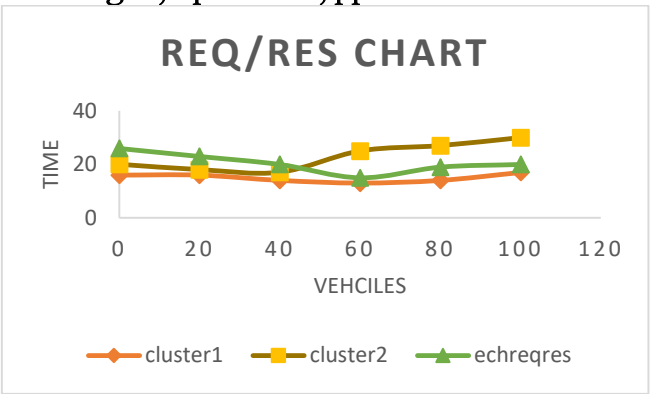
5. Tampering of vehicle from one cluster to another cluster is identified using the ID and time stamp of the vehicle

6. If any suspicious vehicles are identified the timestamp of these vehciles in the cluster and validate with the other RSU .if the same id is identified in different vehicles then it is identified as an attack.

B. Detection of Attack

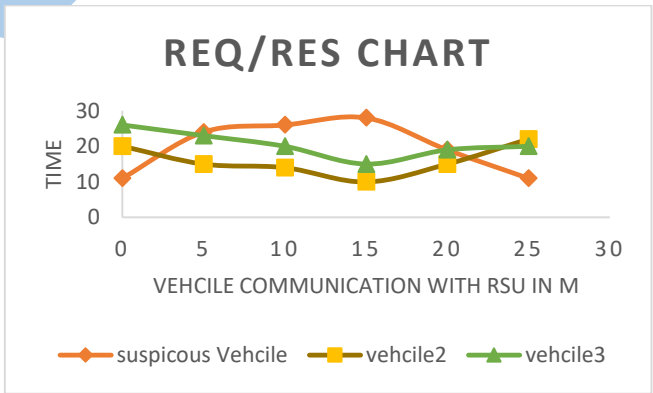
The below graph shows the time series delay on the communication of the vehicles when a malicious attack is done .For this to generate the simulation technique we use the omenet with veins and taken speed and time in counter.

The forming of cluster and vehicles have taken amount time for authentication and communication of packet. In this the vehicles are taken and the throughput time is calculated. . The position as well as the time stamp of the communication is identified .With the help of the time stamp of the communication of the vehicle with RSU we identify the false nodes .As the malicious vehicle communicates with the RSU under the same id or it communicate with only one RSU under different Id.The time required to form the cluster for the vehicles and electing the cluster head to communicate with the RSU is taken .It is compared with the different algorithms such sybil authentication key generation and cluster communication with the vehicle is taken and the time for it represented in the below figure.



Simulation Results

In our simulation detection mechanism using OMNET++ having Veins extension and the vehicles are simulated using SUMO with 100 vehicles and a threshold response of 30sec then the graphical representation is. When a cluster of vehicles starts communication with the RSU the amount of time taken to communicate with the RSU is more. As the cluster is becoming more the amount of the response time by the RSU is increasing since the amount of traffic is increasing .As the amount of traffic increasing the amount of burden also increases on the network which is delaying in the communication. But with our algorithm the time for communication of theo req and res remains the same .Since with increase amount of the traffic the echo response for all the vehicles increase and decrease as they approach near the RSU.A definite study of the curve is maintained for the communication of the vehicle. Since the graph maintains a linear curve the it does not need to calculate the burden on the network.



ACKNOWLEDGMENT

As the availability of new technologies easily available it is necessary to find new methods to identify the attacks. As the current devices are supporting huge data transfer it is necessary to find the smart solutions which are cost effective and ease to use. By using this algorithm we found this algorithm yielded good results and we can use it effectively

REFERENCES

[1] Golle, Philippe, Dan Greene, and Jessica Staddon. "Detecting and correcting malicious data in

VANETs." Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. ACM, 2004.

[2] Grover, Jyoti, et al. "A sybil attack detection approach using neighboring vehicles in VANET." Proceedings of the 4th international conference on Security of information and networks. ACM, 2011

[3] Papadimitratos, Panagiotis, et al. "Secure vehicular communication systems: design and architecture." IEEE Communications Magazine 46.11 (2008).

[4] Reddy, D. Srinivas, et al. "Sybil attack detection technique using session key certificate in vehicular ad hoc networks." Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017 International Conference on. IEEE, 2017.

[5] Prakaulya, Vibhavarsha, Neelu Pareek, and Upendra Singh. "Network performance in IEEE 802.11 and IEEE 802.11 p cluster based on VANET." Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of. Vol. 2. IEEE, 2017.

[6] Dandala, Tej Tharang, Vallidevi Krishnamurthy, and Rajan Alwan. "Internet of Vehicles (IoV) for traffic management." Computer, Communication and Signal Processing (ICCCSP), 2017 International Conference on. IEEE, 2017.

[7] Fangchun, Yang, et al. "An overview of internet of vehicles." China communications 11.10 (2014): 1-15.

[8] Yao, Yuan, et al. "Delay analysis and study of IEEE 802.11 p based DSRC safety communication in a highway environment." INFOCOM, 2013 Proceedings IEEE. IEEE, 2013.

[9] Chen, Chao, and Yanmin Zhu. "Augmenting vehicular 3G users through inter-vehicle communications." Wireless Communications and Networking Conference (WCNC), 2013 IEEE. IEEE, 2013.

[10] Zhao, Qingwen, et al. "When 3G meets VANET: 3G-assisted data delivery in VANETs." IEEE Sensors Journal 13.10 (2013): 3575-3584.

[11] Fangchun, Yang, et al. "An overview of internet of vehicles." China communications 11.10 (2014): 1-15.

[12] Wazid, Mohammad, et al. "Design of Lightweight Authentication and Key Agreement Protocol for Vehicular Ad Hoc Networks." IEEE Access 5 (2017): 14966-14980.

[13] Kumar, Nishant, J. Madhuri, and Manjunath ChanneGowda. "Review on security and privacy concerns in internet of things." IoT and Application (ICIOT), 2017 International Conference on. IEEE, 2017.

[14] Feng, Xia, and Jin Tang. "Obfuscated RSUs Vector Based Signature Scheme for Detecting Conspiracy Sybil Attack in VANETs." Mobile Information Systems 2017 (2017).

[15] Pattberg, B. "DLR-Institute of Transportation Systems-SUMO–Simulation of Urban MObility." *Sumo-sim. org* (2015).

[16] B. Ramakrishnan, Dr. R. S. Rajesh and R. S. Shaji, "A Cluster Based Vehicular Ad-hoc Network Model for Simple Highway Communication", International journal of Advanced Networking and Applications, Volume: 02, 2011.

[17] Gu, Pengwenlong, et al. "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, 2016.

[18] Chang, Shan, et al. "Footprint: Detecting sybil attacks in urban vehicular networks." *IEEE Transactions on Parallel and Distributed Systems* 23.6 (2012): 1103-1114.

[19] Silawan, Teerapol, and Chaodit Aswakul. "SybilComm: Sybil community detection using persuading function in IoT system." Electronics, Information, and Communications (ICEIC), 2016 International Conference on. IEEE, 2016.

[20] Chen, Yuzhong, et al. "Distributed multi-hop clustering algorithm for VANETs based on neighborhood follow." Eurasip journal on Wireless communications and networking 2015.1 (2015): 98.

[21] Liu, Yanbing, Yuhang Wang, and Guanghui Chang. "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 (2017): 2740-2749.

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

[23] Sun, Yunchuan, et al. "Attacks and countermeasures in the internet of vehicles." Annals of Telecommunications 72.5-6 (2017): 283-295

[24] Jan, Mian Ahmad, et al. "A robust authentication scheme for observing resources in the internet of things environment." Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on. IEEE, 2014.

[25] Tbatou, S., A. Ramrami, and Y. Tabii. "Security of communications in connected cars Modeling and safety assessment." Proceedings of the 2nd international Conference on Big Data, Cloud and Applications. ACM, 2017.

[26] Florian, Martin, Sören Finster, and Ingmar Baumgart. "Privacy-preserving cooperative route planning." IEEE Internet of Things Journal 1.6 (2014): 590-599.

[27] Sedjelmaci, Hichem, Sidi Mohammed Senouci, and Tarek Bouali. "Predict and prevent from misbehaving intruders in heterogeneous vehicular networks." Vehicular Communications 10 (2017): 74-83.

[28] B. Ramakrishnan, Dr. R. S. Rajesh and R. S. Shaji, "A Cluster Based Vehicular Ad-hoc Network Model for Simple Highway Communication", International journal of Advanced Networking and Applications, Volume: 02, 2011.

[29] Y. Gunter, B. Wiegel, and H.P. Grossmann, "Cluster-based medium access scheme for VANETs" Intelligent Transportation System Conference, 2007. ITSC 2007. IEEE, pp. 343-348, Oct 2007

