ATTACK RESISTANT VANET DATA COMMUNICATION USING VEHICLE MOVEMENT BEHAVIOR ANALYSIS

Ms. K.Girija and Mr. K.S. Saravanan

1PG & Research, Department Of Computer Science & Applications, Vivekanandha College of Arts & Sciences for Women (Autonomous), Namakkal-637 205, Tamil Nadu, India
2Asst. Professor, Department of Computer Science & Applications, Vivekanandha College of Arts & Sciences for Women (Autonomous), Namakkal-637 205, Tamil Nadu, India

Abstract-The vehicular ad-hoc networks are deployed to support data communication over the vehicles. The Sybil attacks are initiated by the malicious nodes to forge the identity of the neighbor nodes. The network layer and application layers are damaged by the Sybil attacks with more channel resource utilization activities. The urban scenario based vehicle pattern discovery model employed for the Sybil attack discovery process. The beacon message based communication process is analyzed to construct the Driving Pattern Matrices (DPMs) for each vehicle. The usual and unusual patterns are distinguished with the support of the minimum distance classifier. The virtual node generation algorithm and virtual node detection algorithm are used to discover the attacker nodes. The VANET attack detection system is enhanced to discover the smart attackers. The vehicle driving pattern discovery process is improved with spatio temporal parameters. The detection model is tuned to discover the attackers in dynamic traffic environment. The Cryptography, Pseudonym and digital signature techniques are integrated to detect and control the malicious node activities. The local and global level driving pattern discovery mechanism is integrated with the system to discover the virtual nodes. The vehicle movement behavior information is maintained in the infrastructure environment to improve the efficiency of the attacker discovery process.

Keywords- Vehicular Ad-hoc Networks, VANET security, Sybil attacks, Driving Pattern Matrix and Minimum distance classifier

I. INTRODUCTION

A number of interesting and desired applications of Intelligent Transportation Systems (ITS) have been stimulating the development of a new kind of ad hoc network: Vehicular Ad Hoc Networks (VANets). In these networks, vehicles are equipped with communication equipment that allows them to exchange messages with each other in Vehicle-to-Vehicle communication (V2V) and also to exchange messages with a roadside network infrastructure (Vehicle-to-Roadside Communication – V2R). A number of applications are envisioned for these networks, some of which are already possible in some recently designed vehicles. They are vehicle collision warning, security distance warning, driver assistance, cooperative driving, cooperative cruise control, Internet access, map location, automatic parking and driverless vehicles.

All of these applications require, or can take advantage of, some sort of localization technique. In the localization problem, the definition of a reference system among nodes is performed by identifying their physical location or their relative spatial distribution in relation to each other. For instance, Map Location is usually done using Global Positioning System (GPS) receivers with a Geographic Information System, while Vehicle Collision Warning Systems can be implemented by comparing distances between nodes’ locations combined with geographic information dissemination.
As ITS and VANets technology advances toward more critical applications such as Vehicle Collision Warning Systems (CWS) and Driverless Vehicles, it is likely that a robust and highly available localization system will be required. Unfortunately, GPS receivers are not the best solution in these cases, since their accuracy range from up to 20 or 30 m and since they cannot work in indoor or dense urban areas where there is no direct visibility to satellites. For these reasons and of course, for security reasons, GPS information is likely to be combined with other localization techniques such as Dead Reckoning, Cellular Localization and Image/Video Localization, to cite a few. This combination of localization information from different sources can be done using such Data Fusion techniques as Kalman Filter and Particle Filter.

The system analysis the localization requirements number of VANet applications. Several localization techniques can be used to estimate the position of a vehicle and their advantages and disadvantages are applied to VANets. None of these techniques can achieve individually the desired localization requirements of critical VANet applications. The localization information from multiple sources can be combined to produce a single position that is more accurate and robust by using Data Fusion techniques.

VANETs can improve traffic safety and efficiency only if vehicular messages are correct and precise. Despite the security provided by the combination of TPDs with authenticated messages, an attacker could still manage to transmit valid messages containing false data. It is easy for an attacker to launch such an attack. For instance, putting the vehicle temperature sensor in cold water will let the OBU generate false messages, even if the hardware sensors are tamperproof. Also, one may note that in some cases the sender of the data may not necessarily be malicious, but his vehicle’s sensors may be out of order. To rule out such cases of false data, one needs not only to verify that the sender of the data is legitimate, but also that the data are correct. Therefore some mechanisms for detection of malicious data need to be explored. Such approaches are referred as a priori countermeasures which attempt to prevent the generation of erroneous messages in advance.

The application of information-theoretic measures to anomaly detection was analyzed, but mainly in the context of the wired Internet. Douceur observes that the redundancy checks commonly built into distributed systems to mitigate the threats posed by faulty or malicious participants fail when a single adversary can present multiple distinct identities. The resource testing is used to verify the uniqueness of online identities in a distributed computing environment. Unfortunately, this technique may fail in a VANET if an adversary has more resources than a normal node. Location is very important information shared in a VANET. The first proposal aimed at verifying the position data sent by vehicles is presented.

II. RELATED WORK

Many researchers have proposed different approaches to detect Sybil attack in vehicular ad-hoc network. Sybil attack was introduced and described by Douceur in [14]. Douceur proposed resource testing approach to detect Sybil attack. Resource testing approach is based on an assumption that each vehicle has limited computational resources. If an attacker uses multiple identities, then attacker cannot respond by all Sybil identities, within a fixed time interval. Approach is not suitable for vehicular ad-hoc network due to its assumption that an attacker can easily have more than one computational resource.

Use of temporary identities for short duration communication is another way to prevent Sybil attack [11]. Temporary identity approach preserves privacy and provides anonymity to the user. Although, the scheme is fine but, an attacker can easily get the private key of RSU with the help of temporary identity (TIDI) and actual identity (VIDI) of vehicle.

Soyoung Park discussed time stamp series approach to detect the Sybil attack. Basic idea of time stamp approach is that, whenever vehicle passes across a RSU, vehicles obtain a certified time stamp
signed by RSU. Later on, [10] Sybil attack is detected on the basis of similarity in time stamp series. If a vehicle receives multiple messages with similar time stamp, then it would be a Sybil attack. There are many challenges in this approach. The distance between two RSU is 100 km or more. So detection of Sybil attack takes more time, and if Sybil attacker is stay under in only one RSU, then detection of Sybil attack is impossible. Suppose if a vehicle sends time stamp aggregation request to RSU using multi-hop routing, then receiving time may differ when two node transmit at the same time.

In paper [13] used neighborhood list to identify Sybil nodes. His approach is based on an assumption that if some nodes are simultaneously observed by neighboring nodes for a longer duration of time, then these must be Sybil nodes. Although scheme is fine, but it is putting an extra overload by sharing neighborhood list after each time interval i.e. T₀, T₁, T₂, T₃ etc. So, scheme becomes complex and time consuming for initial deployment of VANET. In Grover [9] approach intersection operation is performed between neighbor lists of all vehicles at each time interval. But, vehicle will not consider himself as his neighbor. So, vehicle will put himself out of his neighbor list i.e. intersection operation will result an empty set of common neighbor at each interval. That means basic assumption of “neighbor approach” proposed by Grover, no longer as set of common neighbor is empty at each time interval.

We are proposing a simple way to detect Sybil attack. In proposed scheme, short lived temporary identities are used to reduce the risk of Sybil attack. Vehicles will use temporary identity provided by RSU [8] for communication with other vehicles, when they are in the range of a particular RSU. For Sybil node detection, we are proposing some modification in Grover [12] scheme. Each vehicle will form a neighborhood list on the basis of beacon packet. Then, instead of sharing neighborhood list after each time interval, vehicle will take the intersection of all neighborhood lists after 4-5 time intervals. If some nodes are continuously observed by vehicle in the neighbor set, then these nodes may belong to Sybil node category.

III. SYBIL ATTACK DETECTION UNDER VANET

Vehicle communications are becoming increasingly popular with the development of navigation safety requirements as well as the investments of car manufacturers and Public Transport Authorities. Vehicular networks have significant potential to enable diverse applications associated with traffic safety, traffic efficiency and infotainment [1]. Since driving safety is relevant with most of vehicular applications, it is of high importance to implement appropriate security mechanisms. Due to its dynamic and infrastructure-independent nature, vehicular networks are vulnerable to various attacks compared to conventional networks. To ensure the safety and security in vehicular networks, many security mechanisms have been proposed over the past few years and several of them are standardized and recommended by IEEE and ETSI. IEEE 1609.2 standard [2] defines secure message formats and processing for Wireless Access in Vehicular Environments (WAVE) devices. Different from IEEE, in ETSI standards, security services are not defined as sub-functions in management plane [3]. In ETSI TS 102 941 [4] standard, it identifies trust establishment and privacy management required to support security in Intelligent Transport System (ITS) and the relationships between the entities themselves and the elements of the ITS reference architecture. The ETSI TS 103 097 [5] standard specifies different security headers and formats to ensure the interoperability of the different elements and security information that is being exchanged between the ITS stations for security purposes.

In general, the proposed security services based on three major mechanisms: Encryption algorithms, Public Key Infrastructure (PKI) and Pseudonymous. These services can protect the privacy of ITS stations, the authenticity and integrity of messages in vehicular communication environments. However, vehicular networks are still vulnerable to Sybil attacks [6]. Sybil attack happens while different pseudonyms are used by one malicious node at the same time. Each pseudonym acts as a virtual node.
In vehicular networks, Sybil attacks can cause damage in both Networking layer and Application layer. Since the CSMA/CA is implemented in Networking layer, the cooperation among virtual nodes leads to the possibility of using more channel resource than other benign nodes. In Application layer, the virtual nodes also take part in communicating with other ITS stations. Under this circumstance, when a malicious node uses multiple pseudonyms at the same time, the virtual nodes, generated based on the usage of pseudonymous, can help to increase the influence of fake safety messages by broadcasting them to other benign nodes. In addition, several proposed driving safety and traffic efficiency services are based on voting scheme. With the help of virtual nodes, the malicious node can easily take advantage in voting. In this work, we propose a vehicle driving pattern based Sybil attack detection method. Considering virtual nodes have to avoid the positions that are captured by the benign vehicles, their driving patterns become erratic, especially in dynamic traffic environments. Therefore, the main idea of this work is to evaluate the similarity of vehicle driving pattern.

IV. ISSUES ON SYBIL ATTACK DETECTION PROCESS

The Sybil attacks are initiated by the malicious nodes to forge the identity of the neighbor nodes. The network layer and application layers are damaged by the Sybil attacks with more channel resource utilization activities. One malicious node uses different pseudonyms to generate virtual nodes for Sybil attack process. Historical data values are analyzed to estimate the vehicle movement pattern details. The urban scenario based vehicle pattern discovery model is employed for the Sybil attack discovery process. The beacon message based communication process is analyzed to construct the Driving Pattern Matrices (DPMs) for each vehicle. The usual and unusual patterns are distinguished with the support of the minimum distance classifier. The virtual node generation algorithm and virtual node detection algorithm are used to discover the attacker nodes. The following issues are discovered from the current Sybil attack discovery systems under the VANET environment.

- Smart attackers discovery is not supported
- Channel utilization rate is high
- Dynamic traffic conditions are not handled
- Limited attacker discovery rate

V. ATTACK RESISTANT VANET DATA COMMUNICATION FRAMEWORK

The VANET attack detection and control system is enhanced to discover the smart attackers. The vehicle driving pattern discovery process is improved with spatio temporal parameters. The detection model is tuned to discover the attackers in dynamic traffic environment. The local and global level driving pattern discovery mechanism is integrated to discover the virtual nodes.

The VANET data communication system is constructed to discover and control the Sybil attacks. The Cryptography, Pseudonym and digital signature techniques are integrated to detect and control the malicious node activities. The vehicle movement behavior information is maintained in the infrastructure environment to improve the attacker discovery process. The system is partitioned into six major modules. They are VANET deployment process, Historical data management, Driving Pattern Matrix (DPM) construction, Local and global pattern discovery, Sybil attack discovery process and Communication security process.

The VANET is constructed under the deployment process. Historical data management maintains the vehicle movement information in urban scenario. Vehicle driving details are analyzed under the Driving Pattern Matrix (DPM) construction process. Local and global patterns are extracted with spatial and temporal details. The Sybil attack discovery process is initiated to fetch the attackers in the VANET. Attacker operations are controlled in the communication security process.
The Vehicular Ad-hoc Network is build with vehicles and Road Side Infrastructures (RSI). The VANET is deployed with vehicle and RSI count details. Data providers are placed to provide shared data values. Vehicles are initialized with associated RSI environment. The urban vehicle movement data values are maintained under the log files. The vehicle location details are updated with GPS information. The vehicle movement details are arranged with time information. The historical data values are collected from the T-Drive data set for Taxi driving data in Beijing, China. The historical data values are used to construct the Driving Pattern Matrix (DPM) for the vehicles. The Driving Pattern Matrix (DPM) is build for each vehicle. Vehicle movement information are arranged with its spatial and temporal sequences. The DPM is constructed for a selected time period.

The local and global patterns are extracted using the Driving Pattern Matrices (DPM). Spatial and temporal parameters are used for the local and global pattern discovery process. The local patterns are extracted with the vehicle and region information. The global pattern is extracted for all the vehicles with entire network area.

The virtual node generation and virtual node detection algorithms are used in the Sybil attack discovery process. Minimum distance classifier is applied to identify the attackers. Optimal threshold based virtual node detection algorithm is adapted to discover the smart attackers. Dynamic traffic conditions are analyzed in the attacker discovery process. The attack control process uses the Cryptography, Pseudonym and digital signature techniques. The vehicles are authenticated using three certificate authorities (CA). Root CA (RCA), Long Term Certificate Authority (LTCA) and Pseudonym Certificate Authority (PCA) are employed for the security process. The malicious node activities are controlled with digital signature based certificates.

VI. EXPERIMENTAL ANALYSIS

The VANET security system is build to detect and control the Sybil attacks in data communication process. The Virtual Node Detection (VND) scheme is build to analyze the historical data for attack discovery process. The attack discovery and control operation are supported in the Optimal Threshold based Virtual Node Detection (OTVND) scheme. The system is tested with three performance measures. They are Detection Latency, Detection Rate and Virtual Nodes Frequency.

**Figure No: 6.1. Detection Latency Analysis between Virtual Node Detection (VND) algorithm and Optimal Threshold based Virtual Node Detection (OTVND) algorithm**
The attack detection latency is estimated with the time period taken to detect the Sybil attacks in the VANET environment. The attack detection latency analysis between Virtual Node Detection (VND) and Optimal Threshold based Virtual Node Detection (OTVND) scheme is shown in figure 6.1. The Optimal Threshold based Virtual Node Detection (OTVND) scheme reduces the attack detection latency 30% than Virtual Node Detection (VND) scheme. The attack detection accuracy is analyzed with the actual attacks and detected attack ratio levels. The Attack Detection Rate analysis between Virtual Node Detection (VND) and Optimal Threshold based Virtual Node Detection (OTVND) scheme is shown in figure 6.2. The Optimal Threshold based Virtual Node Detection (OTVND) scheme increases the Attack Detection Rate 15% than Virtual Node Detection (VND) scheme. The virtual node frequency is calculated to identify the attack generation node levels. The security scheme protects the generation of virtual nodes in the VANET data communication environment. The virtual node frequency level analysis between Virtual Node Detection (VND) and Optimal Threshold based Virtual Node Detection (OTVND) scheme is shown in figure 6.3. The Optimal Threshold based Virtual Node Detection (OTVND) scheme controls the Virtual Nodes Frequency 40% than Virtual Node Detection (VND) scheme.
VII. CONCLUSION

The Vehicular Ad-hoc Networks are build to handle the data transmission over the vehicles. The Sybil attack detection mechanism uses the vehicle driving patterns in urban scenario. Virtual node generation algorithm, virtual node detection algorithm and Minimum distance classifiers are employed in the detection process. Smarter attacker discovery, dynamic traffic management and attack control methods are used to improve the vehicle data communication. The vehicle data communication system is build with Sybil attack discovery and control mechanism. The attack discovery process is improved with smarter attacker detection process. The pattern discovery process is improved with local and global level analysis. The system achieves high detection accuracy with minimum detection intervals.

REFERENCES

[1] R. Khatoun, P. Gu, R. Doulami, L. Khoukhi and A. Serhrouchni, “A reputation system for detection of black hole attack in vehicular networking,” in Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015.
[2] “IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages,” IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006), pp. 1–289, April 2013.
[3] “Intelligent Transport Systems (ITS); Communications Architecture,” ETSI EN 302 665 V1.1.1, pp. 1–44, Spt 2010.
[4] “Intelligent Transport Systems (ITS); Security; Trust and Privacy Management,” ETSI TS 102 941 V1.1.1, pp. 1–30, June 2012.
[5] “Intelligent Transport Systems (ITS); Security; Security header and certificate formats,” ETSI TS 103 097 V1.1.1, pp. 1–33, April 2013.
[6] M. Ben Sinai, N. Partush, S. Yadid and E. Yahav, “Exploiting Social Navigation,” ArXiv e-prints, Oct. 2014.
[7] Aravendra Kumar Sharma, Sushil Kumar Saroj, Sanjeev Kumar Chauhan and Sachin Kumar Saini, “Sybil Attack Prevention and Detection in Vehicular Ad hoc Network”, International Conference on Computing, Communication and Automation (ICCCA2016), IEEE, 2016.
[8] H. Weerasinghe, H. Fu, S. Leng and Y. Zhu, “Enhancing unlinkability in Vehicular Ad Hoc Networks,” Intelligence and Security Informatics (ISI), IEEE International Conference on, vol. no., pp.161-166, 10-12 July 2011.
[9] J. Grover, M. S. Gaur, V. Laxmi and N. K. Prajapati,”A sybil attack detection approach using neighboring vehicles in VANET,” In Proceedings of the 4th international conference on Security of information and networks, ACM, New York, NY, USA, pp. 151-158, 2011.
[10] Y. Hao, J. Tang and Y. Cheng, “Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs,” Global Telecommunications Conference, IEEE, vol. no., pp.1-5, 5-9 Dec. 2011.
[11] B. Mishra, S. K. Panigrahy, T.C. Tripathy, D. Jena and S. K. Jena, “A secure and efficient message authentication protocol for VANETs with privacy preservation,” Information and Communication Technologies, World Congress on, vol. no., pp.880-885, 11-14 Dec. 2011.
[12] J. Grover, M. S. Gaur and V. Laxmi, “A novel defense mechanism against Sybil attacks in VANET,” In Proceedings of the 3rd international conference on Security of information and networks, ACM, USA, pp. 249-255, 2010.
[13] S. k. Harit, S. K. Saini, Dr. N. tyagi and K. K. Mishra “RSA Threshold Signature Based Node Eviction in Vehicular Ad Hoc Network, Information technology journal, in Asian network for system information, 2011.
[14] J. R. Douceur, “The Sybil Attack, IPTPS 01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251260, London, UK Springer-Verlag, 2012.