ISSN 2319 - 6629
Volume 8, No.3, April - May 2019
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt07832019.pdf
https://doi.org/10.30534/ijwcnt/2019/07832019

SYBIL ATTACK DETECTION IN VANET USING SPIDER -MONKEY TECHNIQUE AND ECC

Aleena Ann Jose[1], Alisha Pramod[2], Grace Philip[3], Deepika E D[4], Sheba Jiju George[5]
[1]Mangalam College of Engineering, India, aleenaannjose1@gmail.com.
[2] Mangalam College of Engineering, India, alishapramod205@gmail.com.
[3] Mangalam College of Engineering, India, gracephilip08@gmail.com.
[4] Mangalam College of Engineering, India, deepikaed9@gmail.com.
[5]Mangalam College of Engineering, India, shebajikku@gmail.com.

ABSTRACT

Sybil attack in Vehicular Adhoc Networks [VANETs] has more importance in recent times. Malicious node with Multiple identities are introduced by the attacker. Due to this, there are several problems occur in traffic such as accidents, collisions etc. In order to solve the problems in VANETs, this paper proposes a biologically inspired spider monkey time synchronization technique and Elliptic Curve Cryptography[ECC]. Artificial spider Monkey technique is used to detect the Sybil attack on VANETs and to predict the vehicular collision in a challenge zone. ECC method is provide with a key to make each vehicle more secure. This technique detects the malicious vehicles among legitimate vehicle by position verification, message authentication and keys. Spider Monkey time synchronization and ECC help to prevent the attack of the malicious vehicle with legitimate vehicle.

Key words: Elliptic Curve Cryptography(ECC), Spider Monkey Time Synchronization (SMTS), Sybil Attacks, VANET.

1. INTRODUCTION

Road Traffic Plays a vital role in everyday life. In order to improve safety and efficiency of the transportation systems, and to provide innovative services relating to different modes of transport and traffic management. It enables drivers to be better informed and make more coordinated and safer decisions on the road. vehicles communicate to every alternative and pass information to another vehicle. Advantage of VANET communication is the enhanced driver's safety by virtue of exchanging warning messages among vehicles. Security systems have to make sure that transmission comes from an approved source and not interfered in the path by different sources.

Accidents can be avoided if the vehicles follow the traffic rules and road limit. The malicious node could spread out spam messages and send false messages to make matters like false data of collision and theft and heavy traffic. With the expanding amount of the vehicles, streets can most likely get more rushful. Therefore, it is exceptionally important to expand street protection and decrease movement blockage. In VANET, the communication is built up by exchanging the refreshed data about the street and movement conditions to avoid road accidents and efficient result of traffic. VANET is utilized to give the assurance and movement reports to the clients about congested driving conditions, earthquake, tsunami, etc. for lessening the road accidents, fuel consumption and provides safe driving atmosphere.

The distribution and number of roadside units should be relying on the communication protocol is to be used. The inter-vehicle communication design utilizes multihop multi-cast/broadcast to spread traffic activity associated data over numerous hops to an extensive number receiver. The vehicle-to-roadside communication system characterizes one-hop broadcast wherever the roadside unit sends a broadcast message to all or any equipped vehicles in the segment. Vehicle-to-roadside communication configuration offers a high bandwidth link between vehicles and roadside units. Applications of VANETs are (i) Safety Applications: The vehicle-to-vehicle safety communication contains collision warning, road obstacle warning, cooperative driving etc. (ii) Message Dissemination: By means of specific features of safety messages, broadcasting might be the single possible means for message interchange. Therefore, it might be possible to have complete coverage of all or any relevant vehicles. Message sending will enable to spread the warning message to all vehicles outside the radio transmission range of a single hop. (iii) Clustering: A neighbor of the vehicles is grouped into manageable units. It is important to realize economical and reliable safety communication. (iv) Post Crash: Notifications about Vehicles that met with accidents will broadcast messages about its position to neighboring vehicles. Along with that it will also send messages to the highway patrol for seeking more help. (v) Collision Avoidance: To improve collision avoidance application is to reduces road accidents to a great extent. By mounting sensors at the RSU, information that are collected, processed and warning messages are often forwarded to the vehicles to avoid

a collision. There are various ways to avoid collision like to warn vehicles concerning violating traffic signals, low bridge warning, wrong side driving alert etc. (vi) Road Hazard Control Notification: This application informs the vehicles about the geographical features of the road resembling having a pointy curve ahead or occurrence of a landslide, etc. Sensors are often mounted on RSU to capture data about wild animals within the roads running through forests.

Spider Monkey Time Synchronization is used to find the Sybil attacking on VANETs to predict the number of vehicular collisions. Artificial Spider is a packet – controlled like to the insect with controlled memory but able to execute the assigned task. They traverse over fully connected formation graph G(V, E) ;where V is set of sensor nodes and E determines the communication links that mutually connects the vertices of sensor nodes. Artificial spiders move along vertices through edges [1].

Elliptic Curve Cryptography[ECC] is an alternative mechanism for implementing public-key cryptography. It provides with a unique key to each vehicle and to make each vehicle more secure from the attack of the malicious vehicle. The key that is provided to each vehicle is don't disclose with other vehicles.

The remainder of this paper is organized as follows. In section 2, the related works are presented. Section 3 presents the proposed techniques. In section 4, Experiment Result followed by Conclusion.

2. RELATED WORKS

In urban vehicular networks location secrecy of vehicle is great concerned. The RSU provides with the location and timing information to vehicle. Using this message, the verification will be carried out and also it will consider failed RSU for verification. Detecting Sybil attack in urban vehicular networks is very challenging because vehicles are mysterious, location information of vehicles can be very trustworthy [5]. During the design of VANET architecture, the challenges of security must be considered security protocols, cryptographic algorithm etc. The following list presents some security challenges [3]: Real time Constraint: VANET is time critical they save time and also therefore real time operations they support.

• Data Consistency Liability: In VANET even validate node can perform malicious activities. To avoid this inconsistency a mechanism should be designed. Correlation among the received data from different node may avoid this type of inconsistency.

• Low tolerance for error: Some protocols were designed on the basis of probability. VANET uses life critical information on which action is performed in very less time. A small error in probabilistic algorithm may cause some harm.

• Key Distribution: All the security mechanisms implemented in VANET are mostly dependent on keys. Each message is encrypted first and need to decrypt at receiver end either with same key or different key. Also different manufacturer can install keys in different ways and in public key infrastructure trust on CA become the major issues. Therefore, distribution of keys among vehicles is a major task in designing a security protocols.

• Incentives: Manufactures are interested to build applications according to customer concern. Very few consumers may agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of vehicular networks will lead to motivations for vehicle manufacturers, consumers and the government to implement security in VANET.

• High Mobility: The high mobility of VANET nodes requires lesser amount of time for execution of security protocols for same throughput that wired network produces. Hence the design of security protocols must use the methodologies to reduce the execution time.

In urban vehicular networks, where privacy, especially the location privacy of mysterious vehicles is highly concerned, anonymous verification of vehicles is necessary. Consequently, an attacker who succeeds in forging multiple hostile identifies can easily unveiling a Sybil attack, gaining a disproportionately large influence. Here we propose Sybil attack detection mechanism footprint by using this we can preserve the location privacy. When a vehicle approaches road side unit it always senses a authorized message from RSU as the proof of accurate time at this RSU. We design a signer ambiguous so that RSU information is masked from the resultant authorized message. With the temporal limitation on the likability of two authorized messages, authorized messages used for long term identification are prohibited. Therefore, vehicles can generate a location hidden trajectory for location privacy so that no Sybil attack will be there and safe transportation we can have. Rigorous security analysis and extensive trace-driven mock-ups demonstrate the efficacy of Footprint [4].

ECC:

Message authentication in-vehicle communication must be secure so we proposed the scheme called Elliptic Curve Digital Signature Algorithm ECDSA. The scheme works in the following ways:

1. Public and private keys are generated by the vehicle which is going to transfer the information i.e. source vehicle 2. The public key is distributed throughout the network.
3. The secure hash algorithm is used to create the hash of the message to maintain the integrity of the message.
4. A high encryption method is used along with the private key of the sending vehicle and message is send to the destination node.
5. At the receiver side as the publically distributed key is used to decode the message sent by the sending node.
6. The destination vehicle generates the hash using the secure algorithm and compares it with the previously generated hash.

3. PROPOSED TECHNIQUE

The proposed system that deals with the Sybil attacking strategies how to predict the number of Sybil attack on the VANET and detection of malicious nodes among the connected vehicle. It mainly consists of 4 modules are vehicle, Road Side Unit(RSU), Department of Motor Vehicle (DMV), Certificate of Authority(CA). The vehicles can communicate with RSUs and other vehicles as they are equipped global positioning systems (GPS) to authenticate the privacy key preservation to avoid data falsification. Road side unit(RSU) is access points that are installed on the roads. It performs as a medium of communication between the Department of Motor Vehicles (DMV), vehicles and other RSUs. Department of Motor Vehicles (DMV) are in charge for deployment of RSUs, registration of vehicles for the security and safety of VANETs. Certificate of Authority (CA) is mandated for providing and revoking digitally certified pseudonyms issued to vehicles when required. Vehicles periodically received the pseudonyms from CA during the vehicle registration and inspection [1].

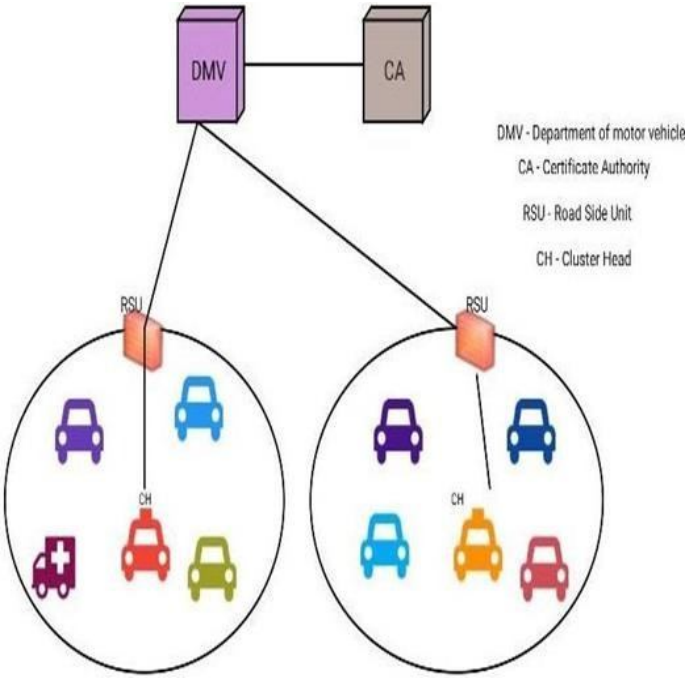


Figure 1: Architecture of VANET

Vehicular Adhoc Network (VANET) is an important component of the Intelligent Transportation System. The system contains a group of vehicles which form as a cluster and each cluster contains a cluster head which is selected according to their performance in the group. The vehicles who travels more time in the route is selected as the cluster head. The cluster head is connected to the Road Side Unit which share the messages with the vehicles within a group. RSUs are immobile and are associated with the backbone network, which should be in place to encourage communication. Each vehicle is connected with other vehicles in the group. Initially all the vehicles should register with the Department of motor Vehicle and the certificate authority and they will provide with a unique key for the secure transaction of messages between the vehicles. Vehicles should even be fitted with hardware that permits the data with the precise location of the vehicle such as Global Positioning System (GPS). To check the authencity of each vehicle, RSUs will send a challenging questions to vehicles. the response from the vehicles are note down. The response should be within a time limit. otherwise it may expire or the response will be false. If the response from the false identity, then it will check the details of the vehicle from the Department of Motor vehicle and to identify the authenticity of that vehicle. If it is a malicious vehicle, then takes necessary actions against it.

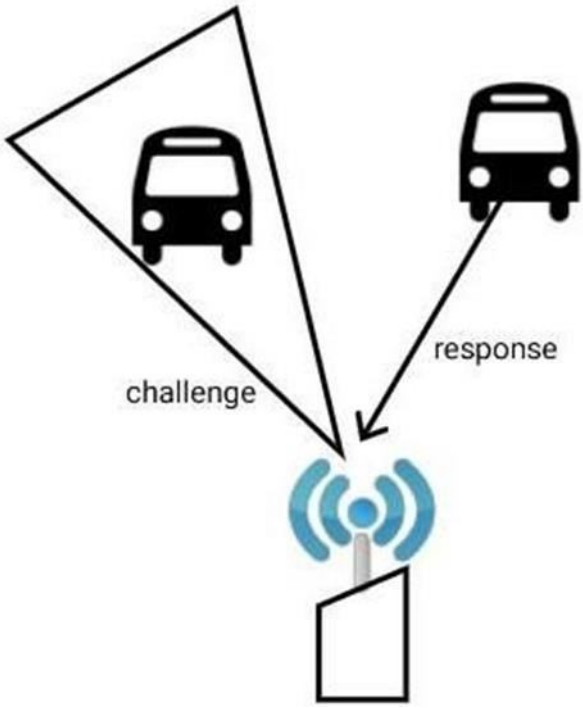
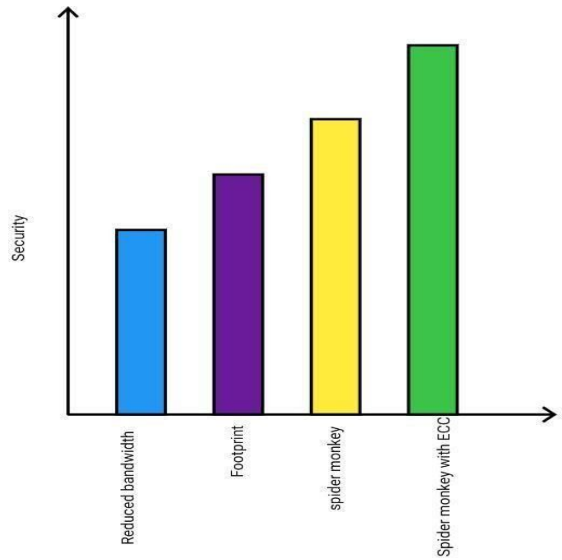


Figure 2: Challenge-response among RSU and vehicle

4. EXPERIMENT RESULT

The Sybil attack detection in VANET using Spider monkey time synchronization technique and ECC provide security from malicious vehicle. It determines the malicious vehicle by using challenge and response message. ECC provides a unique key to all registered vehicle. Therefore, all vehicles registered in the department of motor vehicle is secured.



When we compare the proposed technique with other techniques then the security of the system is high. Reduced bandwidth has least security followed by footprint which provides less function with other techniques. spider Monkey with ECC provides more security when compared with spider monkey technique because ECC provides more security by the usage of the unique key.

5.CONCLUSION

This paper proposes a biologically inspired spider monkey time synchronization technique and Elliptic Curve Cryptography[ECC]. Artificial spider Monkey technique is used to examine the Sybil attack on VANETs to predict the number of vehicular collision in a challenge zone. ECC method is provide with a key to make each vehicle more secure. This technique detects the malicious vehicles among legitimate vehicle by position verification, message authentication and keys. Spider Monkey time synchronization and ECC help to prevent the attack of the malicious vehicle with legitimate vehicle. The Sybil attack detection in VANET using Spider monkey time synchronization technique and ECC provide security from malicious vehicle. It determines the malicious vehicle by using challenge and response message. ECC provides a unique key to all registered vehicle so all vehicles registered in the department of motor vehicle is secured.

REFERENCES

[1] Celestine Iwendi, Mueen Uddin, James A. Ansere, P. Nkurunziza, J.H. Anajemba, and Ali kashif Bashir, **"on detection of Sybil attack in large-scale Vanet using spider-monkey technique"** IEEE Journal, Sept 2018. https://doi.org/10.1109/ACCESS.2018.2864111

[2] Nitish Kumar Bharti and Manoj Sindhwani **"Enhancing the Message Authentication Process in VANET under High Traffic Condition using the PBAS Approach"** Indian Journal of Science and Technology, Vol 9(47), December 2016. https://doi.org/10.17485/ijst/2015/v8i1/106794

[3] Ram Shringar Raw, Manish Kumar, Nanhay Singh **"Security challenges, issues and their solutions for VANET"** International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013. https://doi.org/10.5121/ijnsa.2013.5508

[4] Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao and Xuemin Shen **"Footprint: Detecting Sybil Attacks in Urban Vehicular Networks"** IEEE Transactions on parallel and distributed systems, vol.23, No.6, June 2012. https://doi.org/10.1109/TPDS.2011.263

[5] D. Balamahalakshmi, K.N Vimal Shankar**" Sybil attack detection with reduced bandwidth overhead in urban vehicular networks"** IJCMC, Issue.1, January 2014, pg.578-584.

[6] Y. Sun, R. Lu, X. Shen and J. Su, **An Efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications"**, IEEE Trans- Vehicular Technology, vol.59.n0.7, sept,2010. https://doi.org/10.1109/TVT.2010.2051468

[7] R. Lu, X. Lin, H. Zhu, and X. Shen **"An intelligent secure and privacy-preserving parking scheme using vehicular communications",** IEEE Trans vehicular Technology, vol.59, no.6, pp.2772-2785, July 2010. https://doi.org/10.1109/TVT.2010.2049390

[8] Nageswara Reddy Karukula, Sunar Mohammed Farooq **"A route map for detecting Sybil attack in urban vehicular network"** vol.02,0975-6760, Nov 12 to Oct 2013.