Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC 2018)
IEEE Conference Record # 42656; IEEE Xplore ISBN:978-1-5386-3452-3

Secure Communication and Implementation Technique for Sybil Attack in Vehicular Ad-Hoc Networks

Mukesh Soni
Assistant Professor
Department of Computer Engineering
Smt. S. R. Patel Engineering College
Unjha, India
soni.mukesh15@gmail.com

Anuj Jain
Assistant Professor
Department of Computer Science and Engineering
ITM Universe
Vadodara, India
anujjaingit@gmail.com

***Abstract*— Sybil attack is when one node gains identity of another node. This in one of the dangerous attacks that can give rise to other attacks also. Hence, we present first the implementation of the attack. Secondly, we present the communication and detection algorithm of the sybil attack. In the algorithm, we propose novel approach to solve the problem of communication and detection of sybil attack. Furthermore, we implemented the suggested mechanism to verify the results.**

Keywords— Attack; Communication; Public key; VANET;

I. INTRODUCTION

An applicant can act as several bogus individuals by producing many versions from dissimilar IP addresses. Then, this false personalities can be converted to a huge section of all individualities and legitimate users may not avail required services effortlessly. Sybil attack is defined as a spiteful procedure illegally performing on various vehicle devices. For better understanding the implications of the sybil attack and how to protect against it, scientists designed the categorization for its diverse methods. In a sybil attack, the attacker challenges the name system of a peer-to-peer setup by manufacturing a huge variety of fabricated identities, mistreatment them to achieve a unreasonably massive influence.

A name structure's weakness to a sybil attack depends on the following: how competitively identities are created; the degree to that the name scheme takes inputs from objects that do not have good trusted series link to a trusty individual, and whether or not the name structure considers all bodies identically. One of the major application of sybil attack is in VANETs (vehicular ad-hoc networks). VANET is a category of networks that is shaped from the thought of creating a network of moving devices for precise requirement(s) or circumstances. Vehicles transformed into "Computers on the Wheels" or "Networks on the Wheel". The VANET is the encouraging methodology to offer safety and other applications to the vehicle operators and travelers. Therefore, it converted as a strategic module of the intelligent transport system [8]. Protection from sybil attack in VANETs is very essential due to following reasons:

- For transmission of life-critical information.
- Collision avoidance and co-operative driving.
- Traffic monitoring and optimization.
- Location-based services.
- Infotainment

Sybil attacks are those attacks in which a node obtains multiple fake identities and sends out messages into the network through those identities. These messages can cause Denial of Service, false information spreading which can in turn lead to

accidents and other undesirable situations. To provide a reliable communication for exchange of messages between the nodes. Secure communication between the nodes in VANETs becomes extremely important as life-critical messages are transmitted through them. Various research work have been done in these field but three of the most commonly used methods for sybil attack detection is radio resource testing, registration and detection through position check. These are widely used but they have their own problems which are described later in the section and hence cannot be used for communication and detection of sybil attack in VANETs [9].

A Sybil attack consists numerous fake identities to downfall the faith of the current reputation arrangement. In the vehicular networks, the freedom of movement of devices rises the struggle of classifying the adversary vehicle locality in case of a sybil attack. VANET is a detailed category of mobile ad-hoc network (MANET) where the static nodes are replaced with moving devices equipped with on-board-unit (OBU) and road-side-unit (RSU). The features of VANET are compared with MANETs including express modification in topology, no power limitation, huge scale, flexible network density and high expectable movement (vehicle may move with restricted speed in city areas or on certain unfavorable road conditions). In the past decade, transforming the well-known MANETs to vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications are the witnesses of the development of the vehicular ad-hoc networks.

VANET architecture is designed for V2V and V2I communications with two communication devices called the RSU that is placed on the road side and OBU which is installed in vehicle devices. In vehicular communications, VANET structure may be disturbed by many security vulnerabilities. One of the harmful attacks is a sybil attack. Vehicular ad hoc networks are being progressively be in favor of traffic controller, coincidence avoidance, and managing parking stands at public areas. Security and privacy are two fundamental concerns in VANET. Inappropriately, most of privacy-preserving systems are vulnerable to a sybil attack directly or secondarily in VANET, where an attacker can act to be several bogus vehicles. In sybil attack, an adversary constructs numerous individualities either by counterfeiting new identities or thieving identities from adjacent vehicles [10].

Paper organization: The rest of paper is as follows. The literature survey is discussed in Section II. The problem statement is explained in Section III. We discuss the suggested mechanism in Section IV. The simulation study on the recommended model is explained in Section V. After that, we conclude our work in Section VI. References are at the end.

II. LITERATURE REVIEW

In 2000, M.E Zarki et al., [1] projected driver ad-hoc networking infrastructure (DAHNI) mechanism for vehicular communication in highways. In this mechanism, cars will be location aware for small area wireless ad hoc networking in V2V communication. The vehicles are interacting through static set-ups to load the statistics among them. The results showed that the mechanism is more suitable to avoid energy problems and increase the speed "Security Issues in a Future Vehicular Network". In 2000, Markus G. Kuhn [2] introduced a protocol using non-uniform one-way hash to decide lesser subcategory of signs that the receivers save. The subclass size turns into a flexible approximation for the logarithm of the quantity of signers. Simply the order-of-magnitude of legal signs is essentially inconstant through test group and not be the accurate figure. The algorithm used in this method is trust placed in collectors for the purpose of a small sample of the signers will turn out to be identical as the exactness of the signature gathering can be diverse by communicating them. However, it is not obligatory to offer a comprehensive record of all signers to create the requested numeral of associate signatures variable "Probabilistic Counting of Large Digital Signature Collections".

In 2000, Markus G. Kuhn [3] proposed a signature collections technique for improving the security in digital signature process. The method uses a small amount of memory for storing the large amount of signature. In this scheme non-uniform

hash function is practiced to choose a lesser subclass of autographs from the collections of signature. Then the size of the subset is verified using probabilistic counting process. The result showed that the method achieved the verification effectively. In 2002, Samuel Madden et al., [4] proposed a sybil attack finding technique for urban road area networks. In these arrangements, position reports statistics for vehicles are essential to validate other vehicle devices. RSUs intermittently broadcast official timestamp to automobiles in its locality. Vehicles collect the authorized timestamps and the same taken into consideration to categorize communications received from other objects in future. Routes prepared up focused on succeeding timestamps and the agreeing public keys of RSUs, which are practiced in multiple actions. On the other hand, the location privacy was not taken into attention since RSUs practice extensive span uniqueness to produce signatures. The localization facts of a vehicle may be conditional from the RSU signatures. In the track, accredited letters distributed by RSUs are ambivalent. It conveys the data about the vehicle position from where the approved message was issued but it is hidden for all other applicants.

In 2002, John R. Douceur, [5] denotes that the Sybil attack, without a logically centralized authority, resource parity and coordination among entities. This method jointly establishes an extensive disseminated structure. There are three main birthplaces of facts about other individuals: a trusted organization, itself, or other (delegated) objects. The absence of any individual is directly liable on the concerned authority or to be checked by only permitted signs or other signs that it has already accepted by the sign accepts to discriminate. All articles should be functioned under nearly same resource limitations. All accessible characteristics are confirmed concurrently by all bodies, synchronized across the arrangement. When accommodating personalities are not openly certified, the requisite number of checks goes beyond the number of scheme wide disasters.

In 2002, S Park et al. [6] proposed a timestamp sequence methodology to secure the VANET against Sybil attack constructed on the roadside unit support. By using this approach, the Sybil attack can easily be discovered the circulation communications, which have almost identical timestamps. The accumulated timestamp displays the supreme fresh path and time for each moving device. The result showed that the proposed method prevented many transportation problems i.e., traffic jamming, difficult highway structures, etc. In 2003, J.Luo and J. P. Habaux [7] proposed the vehicular collision warning communication (VCWC) protocol to take care for driving methods to keep away from road coincidences and reduced the traffic. The protocol uses communication mechanism to warn vehicles when an abnormal situation occurs, in order to stop before crashing. VCWC protocol uses two approaches: active and passive approaches. The passive approach makes vehicles to frequently broadcast their information; whereas the active approach sends the message to the vehicle if any problem occurs. The result showed that the proposed method will reduced the traffic accident and provides maximum the road safety.

III. PROBLEM STATEMENT

There are certain circumstances in which nodes have different threats from a Sybil attack. Our objectives include developing an efficient algorithm to transfer messages and to detect one of the most dangerous attack in VANETs, i.e., Sybil attack, establishing secure V2V communication, to provide a reliable communication for exchange of messages between the nodes. Some of points have been discussed as follows.

- A node can give its various location at same time, this attack becomes very dangerous.
- A node can send out false messages which may cause traffic congestion or in extreme cases, loss of life due to false dissemination of life critical information.

- The sybil attack can loss duplication and division appliances in peer-to-peer database schemes.
- The sybil attack can be used against routing algorithms in sensor network.
- A node can also run denial-of-service attack which can disrupt the network.

IV. PROPOSED FRAMEWORK

In this section, we suggest an effective model to communicate messages and to detect a sybil attack in the VANETs. The public key cryptography is used in the suggested mechanism.

A. *Key Elements in Public Key Architecture*

- **Trusted Authority**: It is a certificate authority (CA), which acts as the essence of faith and delivers amenities that confirm the individuality of people, machines and other objects.
- **Registration Authority**: It is a secondary *CA*, which is licensed by a *CA* to produce different official documents for particular usages, which are legalized by the *CA*.
- **Certificate Database:** It saves certificate applications and generates or withdraws certificates.
- **Certificate Store**: It resides on a local machine to save issued certificates and private keys.
- A *CA* generates digital certificates to objects and people after confirming their uniqueness. It signs these official documents with its private key and a public key will be given to all involved parties in this certificate system. *CAs* practice this important certificate to build a chain of trust. These certificates are embedded in web browsers therefore they have built-in trust of *CAs*.
- Web servers, email consumers, smart devices and various other categories of hardware and software also support this architecture and hold confidential certificates from the major *CAs*.

B. *Proposed Algorithm*

Sender

1. Takes a message and encrypts using receiver's public key, say it C_1;
2. Performs $C_1 \oplus T_1 \oplus Public\ key\ of\ Receiver$, say it C_S;
3. Send C_S to the receiver;

Receiver

1. Gets C_S at T_2 and checks the validity of the C_S;
2. Computes $C_1 = C_S \oplus T_1 \oplus Own\ Public\ key$;
3. Decrypts C_1 using own Private key;

RSU

1. Record chain timestamps();
2. Compare();
   if(timestamp1=timestamp2)
   sybil attack detected:
   Exit();
   else
   send to receiver();

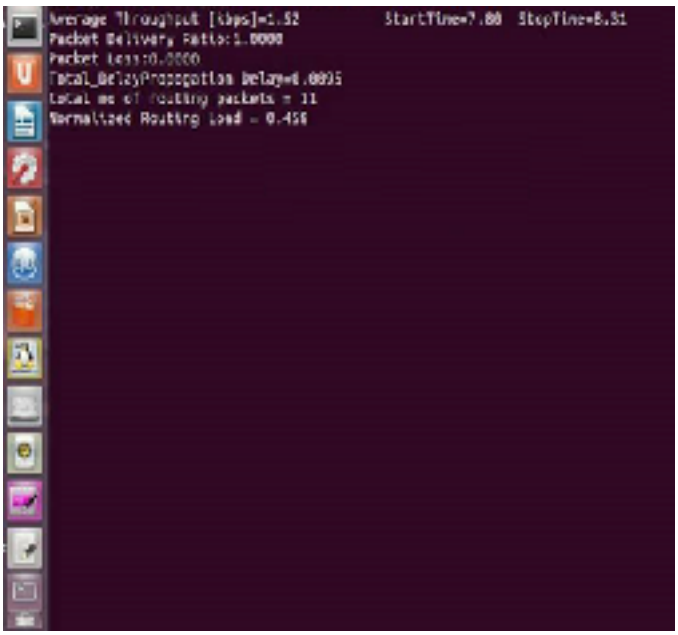

Fig. 1 The proposed framework simulation result

V. SIMULATION RESULTS

In this section, we discuss the outcomes of a recommended scheme to know the practical results. Simulation of key generation and exchange via public key infrastructure algorithm in real-time environment; obtaining real-time certificates of authentication from authority is difficult. Fig. 1 displays a practical outcome of the advised algorithm. In this simulation, it shows that if any node attempts to interrupt the communication between two or more vehicular nodes, then it will be identified based on the suggested model.

VI. CONCLUSION

Security is one of the major issues in wireless ad-hoc networks. This is because the medium is wireless and results in a lot of packet losses. We have proposed an algorithm focused on the hybrid public key infrastructure and chain timestamp concepts to provide communication securely over public environment. After that, we have implemented the mentioned model to know practical outcomes.

REFERENCES

1. El Zarki, M., Mehrotra, S., Tsudik, G., & Venkatasubramanian, N. (2002). Security issues in a future vehicular network. In European Wireless (Vol. 2).
[2] Kuhn, M. G. (2000). Probabilistic counting of large digital signature collections. In Proceedings of the 9th conference on USENIX Security Symposium-Volume 9 (pp. 6-6). USENIX Association.
[3] Markus G. Kuhn. (2000), "Secure and Deducting the Sybil Attack in VANETs," 1st Int'l. Wksp. Peer-to-PeerSystems, pp. 1-12.
[4] Bouassida, M. S., Guette, G., Shawky, M., & Ducourthial, B. (2009). Sybil Nodes Detection Based on Received Signal Strength Variations within VANET. IJ Network Security, 9(1), 22-33.
[5] Douceur, J. R. (2002). The sybil attack. In International Workshop on Peer-to-Peer Systems (pp. 251-260). Springer, Berlin, Heidelberg.
[6] Park, S., Aslam, B., Turgut, D., & Zou, C. C. (2009). Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In Military Communications Conference, 2009. MILCOM 2009. IEEE (pp. 1-7). IEEE.
[7] Luo, J., & Hubaux, J. P. (2004). A survey of inter-vehicle communication (No. LCA-REPORT-2004-013).
[8] Zhang, H., Xu, C., & Zhang, J. (2014,). Exploiting trust and distrust information to combat sybil attack in online social networks. In IFIP International Conference on Trust Management (pp. 77-92). Springer, Berlin, Heidelberg.
[9] Kaur, M., & Mahajan, M. (2015). Movement Abnormality Evaluation Model in the Partially Centralized VANETs for Prevention Against Sybil Attack. International Journal of Modern Education and Computer Science, 7(11), 20.
[10] Hussain, R., & Oh, H. (2014). On secure and privacy-aware sybil attack detection in vehicular communications. Wireless personal communications, 77(4), 2649-2673.