A Survey : Sybil Attack Detection and Prevention Approach over Network

Swamil Soni*, Prof. Damodar Tiwari** and Dr.Shishir K.Shandilya***
*(0112CS15MT20)
*-***Bansal Institute of Science and Technology, Bhopal

Abstract: VANET is a special type of mobile adhoc network which is specially working towards vehicle entity and its moving knowledge. In such entity and moving scenario further various attack and problems get arise due to multiple interaction in nature. In this paper Sybil user which participate in the network and try to jam peer network through which a processing can get stop or not able to transfer the data via network is presented. This paper contains survey of previous techniques which used in Sybil detection and prevention over VANET. The existing technique associate with the paper makes use of a technique which uses to communicate in between the available vehicle in the network. In the existing paper author proposed a model which make use of technique name “Dynamic certificate generation technique”, which help in making system secure in such a manner in which a Sybil user detection and further prevention optimization is performed over network.

Keywords: VANET (vehicular Ad-hoc network), Sybil Entity, peer network, Trust, RSUs (Road Side Units).

Introduction

VANET is an Ad-hoc network in which various vehicular nodes which equipped with GPS device and road side units are connected to communicate over a wireless channel. In that topology of the network changes frequently which thus to deliver a packet from source to destination a difficult task to do. There are issues like loss of packet, high end to end delay, congestion in wireless channel etc. are generated which degrades the performance of the VANET. Thus efficient routing technique is required to provide better routing mechanism in VANET

Trust is a scenario in which message which comes from the trusted nodes are consider to deliver and message comes from un-trusted nodes are discarded. Thus in that any intruder tries to send any fake information about any event like road accident etc. can be restricted, can provide a better performance to the user. In that way a secure framework is provided to the user to communicate in VANET.

There are various techniques presented by the various researchers to provide better performance to route packets in VANET.

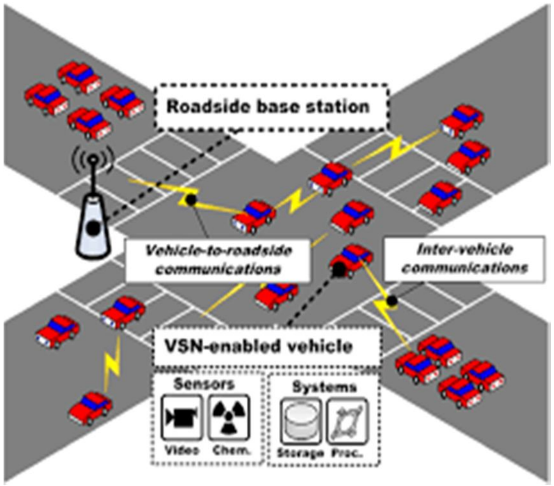

Figure 1.1: Communication Mechanism in VANET

In Figure 1.1, a communication mechanism is presented, in which a communication between road side units and vehicles is presented. Which shows that how vehicle to vehicle and vehicle to roadside unit communication can be performed.

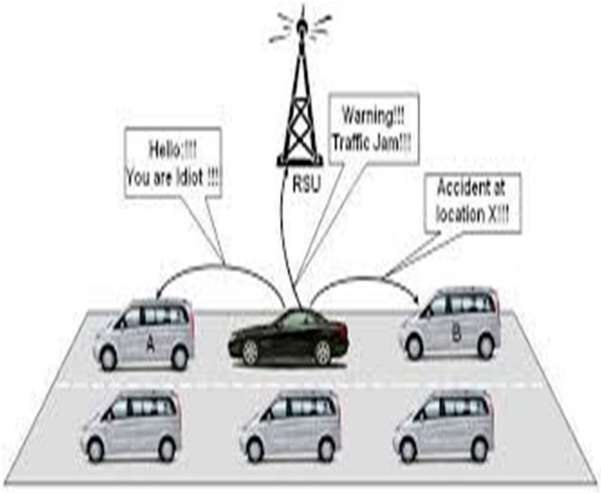

Figure 1.2: Trust Scenario in VANET

In figure 1.2, a description over trust scenario is presented which shows that how an untrusted user can transmit a fake information about traffic jam to the other user. Thus that cause serious effect over the performance of the whole network.

A review over the various techniques which used to provide trust management based routing in VANET is presented.

Literature Survey

In [1] pseudonym based technique to provide anonymity to cars which used to communicate in VANET. In that system pseudonym generation, distribution of the pseudonym and replenishing is done to get an anonymous system to communicate in VANET. In that system roadside units play an important role by collecting all the pseudonyms from the trusted authority. In that system, a vehicle which contains OBU (on board units) which equipped with wireless equipment is used to communicate with the roadside units (RSUs). In that a trust authority and trusted route to communicate with the other vehicles is assumed. In that way a pseudonym based anonymity based system is presented to provide proper communication to the user.

In [2] a data trust algorithm to resolve vulnerability in safety message exchange between vehicles in VANET is presented. A trusted hypothesis is used to provide trust mechanism in VANET. First a packet information message is transmitted frequently between nodes, that message used to identify that the message coming from source node or from a transitional node to restrict the malicious access in that message. At each node a database collection mechanism is provided to collect the information about the nodes. A road segmentation mechanism is used to reduce the overhead of system by dividing that road in to fixed size segments to provide enhanced performance VANET. Accumulation of the road traffic history to provide information of the road traffic to identify the malicious node. A decision node is used to make the decision of which message will be start on the basis of the priority.

In [3] a trust management system which takes care of all the security primitives like encryption and encapsulation is presented. An integration of OSLR routing protocol and that trust management system to provide better performance for the user. In that feasible trust factor collection is used to provide better trust management in VANET is presented. In that system fuzzy logics are used to calculate path trust value. In that way a trust management system to restrict malicious access in VANET is provided.

In [4] an attack resilient trust mechanism is presented. That provide a detection mechanism to detect various attacks in the VANET and malicious access from the nodes, in that system node trust is evaluated on the basis of the data collected from the various nodes that can be measured in two dimensions called functional trust and recommendation trust to know how node can be satisfied the functional requirement and how much the truth-worthy the recommendation is which provided by the node. In that technique two models called research model and adversary model are used to provide proper search mechanism for the user.

In [5] a trust structure in VANET is presented, which uses short time certificate and Merkle signature scheme to provide an enhanced search mechanism in VANET. In that a pseudo id for the vehicles is generated and a short time certificate is issued to the user to provide better communication to the user. In that certificate a pair of private and public key is provided to the user to uses as per their need. In existing techniques a check for the revocation of the sender vehicles is performed which generate overhead for the process thus a short time certificate based technique reduces that overhead. And Merkle tree based technique is used to provide a trusted path to the user.

In [6] a similarity mining technique is used to provide a trust mechanism in VANET. In that technique similar message or similar vehicles are identified using that technique. And a trust value or a reputation for the new vehicles is calculated on the basis of to provide a better trust mechanism in VANET. That technique is used to decide that message coming from a trustworthy vehicle or not, in that a trust value for vehicle is calculated to recommend trust reputation for the vehicle. Firstly similarity for the vehicle is calculated then calculation of the reputation is conducted to assign reputation for that vehicle then that reputation is updated to provide updated information about the reputation to the other vehicles in VANET.

In [7] a similarity based trust management scheme is used to assign trust rating for the vehicles. In that Apriori based data mining technique is used to calculate similarity among the various vehicles. In that technique, calculation for the trust rank is conducted at receiver's end which provides information about the similarity relationships of the various neighbors in the VANET. Then that information used to restrict any false message about the event in the VANET. Provide a way restrict abnormal behaviors in the VANET.

Problem Identification

We investigated the main factors affecting the performance of network and attacks using Sybil in vehicular networks.

Here are some problem formulations being monitored with the existing approach:

1. Limited bandwidth, protocol used should not allow the redundant packets so that maximum data can be disseminated over the network, which is a big challenge.
2. Each vehicle having the limited resource to respond and process the Sybil, thus a system can't respond in case of more Sybil than the available resources. In such case an enhance resource model or manage technique is required.
3. Temporal identity used by several devices such that it is a challenge to detect the further identification of the user.
4. An assumption based scheme is used by author which is complex and time consuming approach.
5. A node detection and prevention in between the large number of node face the accuracy issue while large node in range.

Proposed Work

Sybil attack detection is performed by existing scheme with the given challenges in the VANET system, the algorithm certificate generation techniques is used by the recent approach.

In VANET exiting MANET routing protocols used but their performance is not effective. After study it shows that particular road situation and the vehicle condition, the protocol is changing as every protocol has its own advantages and disadvantages. Some protocol needs high priority as they are providing safety to the vehicles in which packet forwarding delay is not allowed, on the other hand several other protocols may be used at the situation where slight delay is tolerable. Simultaneously since there is limited bandwidth, protocol used should not allow the redundant packets so that maximum data can be disseminated over the network, which is a big challenge.

In future we will try to device an algorithm which can work for Sybil detection with trust management and signature based scheme.

Conclusion

VANET (Vehicular Ad-hoc network) is a network in which various vehicular nodes which equipped with GPS devices and Road Side Units are connected to in an infrastructure-less environment to communicate with one another over a wireless channel. A Sybil message and attack is being performed by the multiple nodes over the network. If there is any false message is broadcasted in the network that create serious trouble for the whole network. Thus to restrict such messages and such nodes, trust among the vehicles is required in which each message rely from trusted node or vehicle. A review over the various techniques which used for trust management and Sybil detection in the VANET is presented in the existing systems. There are various techniques like similarity based trust management is provided to the trust management in the VANET. An enhanced technique is needed in future to provide better trust management in VANET such that a proper Sybil detection can be performed over the available node.

References

[1] Aravendra Kumar Sharma, Sushil Kumar Saroj, Sanjeev Kumar Chauhan, Sachin Kumar Saini," Sybil Attack Prevention and Detection in Vehicular Ad hoc Network", International Conference on Computing, Communication and Automation (ICCCA2016).

[2] Hassan Artail, and Noor Abbani "A pseudonym management system to achieve anonymity in vehicular Ad hoc networks" IEEE, 2015.

[3] Hanaa S. Basheer, Carole Bassil, Bilal Chebaro "Toward Using Data Trust Model in VANETs" IEEE, 2015.

[4] Shuaishuai Tan, Xiaoping Li, and Qingkuan Dong "A Trust Management System for Securing Data Plane of Ad Hoc Networks" IEEE, 2015.

[5] Wenjia Li, and Houbing Song "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks" IEEE, 2015.

[6] SanoopMallissery, ManoharaPai M.M., Smitha A., Radhika M. Pai, Joseph Mouzna “improving the public key infrastructure to build trust architecture for VANET by using short time certificate management and merkle signature scheme” IEEE, 2014.
[7] Brijesh Kumar Chaurasia, ShekharVerma, Geetam S Tomar “Trust Computation in VANETs” IEEE, 2013.
[8] Kavitha .M ,ShrikantS.Tangade , SunilKumarS.Manvi “Distributed Trust & Time Management Strategy in VANETs” IEEE, 2013.
[9] Ali Akbar Pouyan, Mahdiyeh Alimohammadi,” Sybil Attack Detection in Vehicular Networks”, 2014.
[10] Lu, R., Security and Privacy Preservation in Vehicular Social Networks, Doctoral dissertation, University of Waterloo, 2012.