Detection of Sybil Attacks in Vehicular Ad Hoc Networks based on Road Side Unit Support

R. Keerthana, D. Sarath Kumar, R. Vignesh, N. Vishnu, K. Dinesh Kumar and K. Kumarasan

Abstract---Vehicular Ad-Hoc Networks (VANETs), an emerging profile for the improvement of road safety that has a unique ability to possess inter-vehicle as well as vehicle-to-Road Side Unit communication that is to be implemented all across the globe in coming years. Since the communication is carried out along an open wireless medium this makes the network more vulnerable to attacks. Vulnerability of the network can either be the transmission of false information or vehicles assigned with fake identity, and they can possess identity of authorized vehicles or can even attack anonymously. Several techniques have been developed till date for the detection of unauthorized or illegitimate vehicles that downgrades the security of the network.

Privacy of non-public place information of a vehicle unintended network users are enticing a lot of vital and issue. Services provided by Location primarily based services to VANETs users will breach by Sybil attacks.These papers propose an answer to prevent and observe Sybil attacks in VANETs.The primary use discovery tag embedded within the vehicle to substantiate them to the RSU and procure short period of time certificates. The second uses certificates to substantiate vehicles to their neighbors. The conveyance network is split into numerous zones brought beneath the management of dissimilar guarantee authorities (CAs), forcing a vehicle to vary its credentials at what time touching from a zone to a different. One vital characteristic of the projected answer is that it prevents attackers from following the quality of the vehicles. Avoid false negatives is additionally self-addressed victimization observers in vehicle nodes.

Keywords---Ad-Hoc Networks, Sybil Attack, Vehicular Ad-Hoc Networks, Vehicular Ad-Hoc Network Attacks.

I. INTRODUCTION

Vehicular ad-hoc networks (VANETs) have attracted intensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs carries with it entities together with On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications area unit the two basic communication modes, that severally permit OBUs to speak with one another and with the infrastructure RSUs.

Since vehicles communicate through wireless channels, a range of attacks like injecting false info, modifying and replaying the disseminated messages is simply launched. A security attack on VANETs will have severe harmful or fatal consequences to legitimate users. Consequently, guaranteeing secure conveyance communications should be before any VANET application is place into observe. A well-recognized resolution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate

R. Keerthana, UG Final Year, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India.

D. Sarath Kumar, UG Final Year, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India. E-mail:sarathkumard96@gmail.com

R. Vignesh, UG Final Year, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India.

N. Vishnu, UG Final Year, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India.

K. Dinesh Kumar Assistant Professor, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India.

K. Kumarasan Assistant Professor, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India.

Revocation Lists (CRLs) for managing the revoked certificates. In PKI, every entity within the network holds associate degree authentic certificate, and each message ought to be digitally signed before its transmission. A CRL, sometimes issued by a sure Authority (TA), could be a list containing all the revoked certificates.

A great development can be seen in wireless technology in recent years. Ad – hoc networks is a live example of wireless network in which a user can have access to the facilities of wireless networks within a specified range. Ad-hoc is the most explored branch of wireless infrastructure-less network i.e no infrastructure is required to setup the network. It can be setup anytime and anywhere using pre-installed network hardware in the nodes. Vehicular Ad – hoc networks (VANETs, vehicles on road act as nodes of the network), the subclass of Mobile Ad – hoc networks (MANETs, only smartphones are required to setup the network) have gained much popularity these days. It provides a high speed and high mobility communication to be possible in-between the nodes within a specified range. The vehicles (that act as nodes in the network) can communicate within the range of network either stationary or in motion.

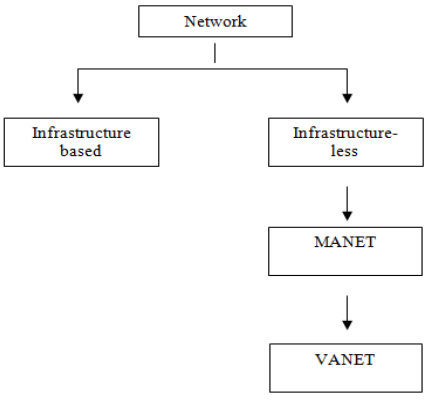

Fig. 1.1: Network Hierarchies

Ad-hoc network is an open communication network, so there is a possibility of breeching inside the network. Therefore, security of this network is the main issue that is to be taken care of.

VANET supports real time communication therefore some security techniques such as authentication, privacy, confidentiality, non-repudiation etc. must be followed in order to transmit as well as receive the information correctly and efficiently. Many attacks are possible that can inject fake information, send false alerts which could create delays, congestion or even jam the network or make the network unavailable for the node. There are several attacks possible that affects the safety and privacy of the vehicle, such as Sybil attack, Intrusion, Data fusion, Denial of Service (DoS), Black hole, Illusion etc.

Most of the attacks that are common in VANETs has been discussed in various research papers have been summarized in this paper. Moreover, for securing the network and preventing it from being attacked by any third-party node, several aggregations schemes are described briefly.

A. Overview of VANETs

Vehicular Ad–hoc networks comprises of large no. of mobile nodes that are able to communicate with each other within a specified range. The Federal Communication Commission(FCC) of United States has allocated Dedicated Short Range Communication (DSRC).Licensed spectrum of 75 MHz with a bandwidth of 5.9 GHz and protocol assigned to vehicular networks is IEEE 802.11p as discussed in section I.

In Europe DSRC communication is carried out over a spectrum of 30 MHz over 5.9 GHz band which is used for many applications such as parking management, traffic telematics, transport management etc. As DSRC system of communication across Europe is not standardized, so it is not used in all the countries

VANET Architecture

VANET architecture consists of a Road Side Unit (RSU) and an On-Board Unit (OBU) that is installed in the vehicles. The vehicles transmit messages from OBU to another OBU or from OBU to RSU and messages can be trans-received from RSU to RSU.

If any vehicles transmit a message but there is no other vehicle in the specific range a certain vehicle, then the message is stored at the RSU and can be retrieved when any vehicle comes in the its range.

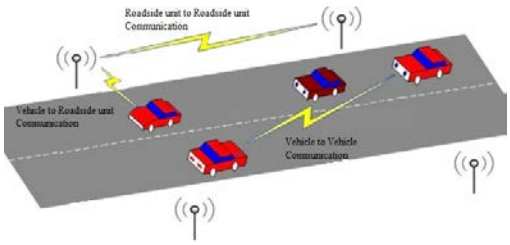

Fig. 1.2: Architecture of VANET

Communication Patterns in VANETs

Schoch et al.provided various communication patterns with purpose, communication mechanism, direction; QoS is all described with an example.

a. **Beaconing:** Information is updated about the speed, position and the nearby vehicles among the nodes. The data packets are broadcasted through link layer over single-hop communication.
b. **Geo broadcast:** Information about sudden occurrence of an even or an abnormality is broadcasted over a larger area in which sender attaches the determined location with message.
c. **Unicast Routing:** Unicast transportation of messages in a specified direction. Multi-hop communication is more suitable for this communication.
d. **Advanced information Dissemination:** Provides information to the vehicles those experiences a delay due to network partitioning. The messages with high priority are handled first when the bandwidth is available for a limited period.
e. **Information Aggregation:** Communication overhead is reduced which in turn decreases the probability of collision and dropping of packets.

B. Threats to Availability

Denial of Service (DoS): The main aim of the attacker is to reduce the performance of the network and overcome the resources of the network available to the nodes, such that the legitimate users of the network cannot utilize the resources.

Black-hole Attack: In this type of attack, when the data packets are directed towards the node that previously existed in the network but presently does not exist.

Malware Attack: In these types of attacks, the attacker injects virus in the network that interrupts the normal procession of the network.

Mischievous Attack: This attack is performed by the legitimate users of the network for their own benefit such as by providing wrong details of traffic jams or route information.

Broadcast Tampering: In this the authentic user of the network transmits fake safety messages in the network that could lead to road accidents**.**

C. Sybil Attack

The Sybil attack in laptop security is AN attack whereby a name system is subverted by shaping identities in peer-to-peer networks. In an exceedingly Sybil attack, the assaulter subverts the name system of a peer-to-peer network by making an outsized range of onymous identities, victimise them to realize a disproportionately giant influence. A name system's vulnerability to a Sybil attack depends on however cheaply identities may be generated, the degree to that the name system accepts inputs from entities that don't have a series of trust linking them to a trustworthy entity, and whether or not the name system treats all entities identically.

An entity on a peer-to-peer network could be a piece of software package that has access to native resources. An entity advertises itself on the peer-to-peer network by presenting AN identity. In alternative words, the mapping of identities to entities is several to at least one. Entities in

peer-to-peer networks use multiple identities for functions of redundancy, resource sharing, dependability and integrity. In peer-to-peer networks, the identity is employed as an abstraction of entity may be responsive to identities while not essentially knowing the correspondence of identities to native entities.

A faulty node or a human might gift multiple identities to a peer-to-peer network so as to seem and performance as multiple distinct nodes. Once changing into a part of the peer-to-peer network the human might then take in communications or act maliciously. One approach to preventing these "Sybil attacks" is to own a trustworthy agency certify identities. This paper shows that, while not a logically centralized authority, Sybil attacks area unit invariably doable except below extreme and false assumptions of resource parity and coordination among entities.

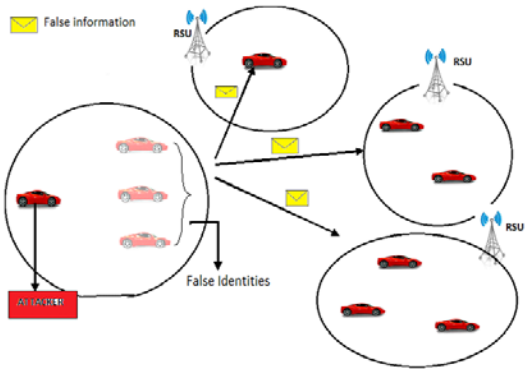

Fig. 1.3: Sybil Attack

As VANET is associate degree rising analysis space then its security problems. There are several security problems in VANET however here during this section we'll be addressing one in all its major security issue i.e. the SYBIL ATTACK. SYBIL attack could be a malicious attack within which the assailant creates multiple identities and uses them to achieve a disproportionately massive influence. SYBIL attack is incredibly grievous because the assailant will play any quite attack with the system cutting down the potency of VANET to a bigger extent and so creating it less possible for sensible approach. These forge identities additionally creates a semblance that there are further vehicles on the road. So the necessity of making certain that associate degree steer is neither changed nor put-upon by an assailant.

Prevent intruders from assaultive the system. A number of it includes resource testing, public key cryptography, Passive Detection through Single Observer, Passive Detection through Multiple Observer, Propagation model, Active Detection by Position Verification, Sensor-Based Position Verification.

D. Security Threats and Attacks

As already discussed in section I briefly about VANET attacks that are classified as follows: threats to:

a. Availability
b. Authentication
c. Confidentiality

All these attacks can be further classified as

a. Network Attacks

These attacks are considered to be of high priority as these directly affect whole of the network and make the network unavailable for the legitimate user. Various attacks that come under this category are Dos, Distributed DoS (DDoS), brute force, malicious node, node impersonation, Sybil attack.

b. Application Attack

The most important application of VANET is safety of the user. This attack affects the safety of the user by changing the content of the actual message and transmitting the fake message. Fake information dissemination and bogus information are some that the attacks that comes under this category.

c. Timing Attack

The main aim of the attacker is to add some time delay in the original message so that the message is not transmitted at the required time but is transmitted after some other instant of time when the information is not required. This could cause misshaping on the road.

d. Social Attack

In this the attacker transmits unnecessary messages in the network to diver the attention of the user. The attacker transmits the information that is not related to the required information such as attacker can send jokes that frustrated the legitimate user which in turn affect the user to user to keep an eye on road.

e. Monitoring Attack

The attacker monitors the network and listens to the conversation messages between the vehicles and misuses the required information shared between the vehicles. All the vehicles have unique identification that helps them to provide the actual location; the attacker can disclose the unique ID of a certain vehicle in the network which affects the privacy of the vehicle.

E. Applications

VANET provides a variety of applications that could led to the advancement of standard of vehicles on roads.

This advancement is called as Intelligent Transport Communication (ITC) system; the author classified various applications as follows:

a. Safety

Safety application includes monitoring of vehicles on roads, surface of road, and curves on road. It includes traffic analysis, message transfer, crash notification, hazard control notification, and collision warning.

b. Commercial

Commercial applications provide the vehicle with entertainment services such as audio and video streaming and web access services. The driver can have internet access.

c. Convenience

These increase the efficiency of traffic by traffic management which includes route diversions, electronic toll collections, parking availability etc.

d. Productive

Some positive aspects can be extracted from these productive applications such as environmental benefits, time utilization and fuel saving.

II. SYBIL ATTACK IN VANETS

VANETs consist of two types of vehicles or nodes or users i.e. legitimate user and illegitimate user. Legitimate users are referred to as authentic or valid users of the network whereas illegitimate users are referred to as invalid users in the network. The legitimate are assigned with unique identification number with each vehicle whereas illegitimate user uses the fake identity or unknown identity or the identity of the vehicle that was previously present in the network but currently is out of coverage area of the network or left the network.

The nodes or vehicles i.e. the legitimate users of the network that are able to forge their original identity to acquire an unknown identity or the identity of any other vehicle that is existing or previously existed in the network, are said to Sybil nodes and the attacker is called as Sybil attacker.

The Sybil attacker can also create multiple identities and can disseminate false information in the network for his personal benefits.

III. DETECTION TECHNIQUES

Several techniques have been introduced for the detection of threats in vehicular network. This paper focused on some specific techniques for the detection of sybil nodes that are responsible for fake information dissemination in the network.

Based on some of the attacks, solutions for detection and injection of fake information in the network are provided.

A. Sybil Attack

Trusted certification method presented by Sannella proved to be the most effective method to detect Sybil

attack. Each node in this is issued a certificate for authentication by Centralized Central Authority (CCA). Node with a certificate of authentication is legitimate and other will be fake.

Trusted devices approach by Yu and Lau prevents the attacker node to get mapped with the network hardware. One-to-One mapping of each node in the network is done with a hardware device and assumed that attacker node will not get mapped with the hardware.

Detection approach by Grover J. et al identifies the Sybil attack from the information received from beaconing packets that validates the authenticity of the node in the network and consists of the location coordinates and neighbor information of the node. As no two nodes can possess same location coordinates and same set of neighbors and that too for a time period greater than threshold value. Moreover, the transmit power of the Sybil identities will be different from the legitimate nodes while sending the beaconing packets.

Triki et al (2013)presented a privacy preserving solution to protect against Sybil attack. Author proposed two authentication techniques–RFID tag that are embedded in the vehicle used to get the vehicle authenticated at the nearby RSU. This gets a validation certificate for a shorter lifetime. The other technique uses the certificate obtained in the first technique to validate the vehicles.

A robust detection of Sybil attack by Chen et al (2009**)**, detects the Sybil attack on the basis of motion trajectories of the vehicle. Here each vehicle is assigned different signatures depending upon motion trajectories. The statistical judging is conducted on different set of signatures by using hypothesis testing method that differentiates the vehicles from the Sybil nodes.

A timestamp series approach proposed by Park et al (2009)to secure against Sybil attack in a vehicular specially appointed system taking into account street side unit support. The proposed approach works well when RSU is accessible and vehicle has communication capability. In this methodology RSUs are the main segments giving the endorsements. It is not possible that two vehicles are passing through various PSUs precisely at the same time due to Variance of flow of vehicles. The technique developed as time-stamp arrangement technique needs neither vehicle based open key base nor Internet access at the Road Side Unit.

Zhaou et al (2011)proposed P2DAP strategy for recognition of Sybil attack. Author introduced a lightweight and versatile convention to distinguish Sybil attacks. This strategy does not require any hub in the system to share its personality and hence security of the vehicle is increased.

Xiao, Yu and Gao (2006)proposed a lightweight security strategy for identifying and limiting Sybil nodes in VANETs. This is taken from measurable investigation of sign quality dispersion diagrams. The plan ends up being a method wherein every node in the system can perform the discovery of nodes through area check. With a specific end goal to beat the impediments of the fundamental plan, the author proposed a method to keep Sybil aggressor to conceal for each other. RSU is utilized to have better results. The Accuracy of area confirmation is improved with the help of measurement calculations. The calculations can distinguish Sybil attacks by recognizing the sign quality conveyance with respect to time.

A cooperative Sybil attack in VANETs by Hao Y. et al (2011)proposed a security convention to distinguish Sybil attacks for position based applications. Vehicles in our convention distinguish sybil assaults by looking at the judiciousness of positions of vehicles locally. The attack identification has attributes of correspondence and GPS position of vehicles which are incorporated for message propagation.

No additional equipment and little correspondence and calculation overhead will be acquainted with vehicles. Accordingly, here convention is light weighted and appropriate for genuine applications

Yu B. et al (2013)proposed a strategy to check the positions of potential Sybil nodes. We utilize a Random Sample Consensus (RANSAC)-based calculation to make this strategy more hearty against anomaly information created by Sybil hubs. In any case, a few natural downsides of this technique brief us to investigate extra methodologies. They presented a measurable strategy and configured a framework that can confirm where a vehicle originates from. The framework is has made a Presence Evidence System (PES), with which we can improve the identification precision utilizing investigation over a per-ception period.

IV. CONCLUSION

In VANETs, there is continues transmission and recep-tion of data in between the nodes. For efficient sending and receiving of message, information should be correctly transmitted. Fake information dissemination in the network deteriorates the security of the vehicle and safety of users on roads. Detection of nodes transmitting fake information and solution to prevent such behavior is a much popular topic in research. In this paper different proposed techniques for detection of Sybil Attack are discussed and that have been in the recent researches.

A. Future Work

The research is conducted to improve the security and safety of VANETs. There exists a good trade-off between security and efficiency. Further research could be conducted in vehicular networks to make it more efficient. However, we cannot call a system to be ideal system that can be 100 percent secure, but there might be advanced level techniques to be developed in future to make the vehicular networks secure and safe enough to implement Intelligent Transport Communication (ITC) all across the globe.

REFERENCES

[1] R. Lu, “Security and Privacy Preservation in Vehicular Social Networks”, Doctoral dissertation, University of Waterloo, 2012.

[2] J.R Douceur, “The Sybil attack”, Proceedings of the International Workshop on Peer to Peer Systems, Pp. 251–260, 2002.

[3] M. Sood and A.Vasudeva, “Perspectives of Sybil Attack in Routing Protocols of Mobile AdHoc Network”, Computer Networks& Communications (NetCom), Vol. 131, 2013.

[4] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, Ad hoc Networks Journal Elsevier,Vol. 1, Pp. 293-315, 2003.

[5] J. Newsome, E. Shi, D. Song and A. Perrig, “The Sybil attack in sensor networks: analysis & defenses”, Proceedings of the 3rd international symposium on Information processing in sensor networks, Pp. 259-268, 2004.

[6] G. Yan, S. Olariu and M.C. Weigle, “Providing VANET security through active position detection”, Computer Communications, Vol. 31, No. 12, Pp. 2883-2897, 2008.

[7] B.N. Levine, C. Shields and N.B. Margolin, “A survey of solutions to the Sybil attack”, MA, University of Massachusetts: Amherst, 2006.

[8] A. Boukerche, H.A. Oliveira, E.F. Nakamura and A.A. Loureiro, “Vehicular adhoc networks: A new challenge for localization-based systems”, Computer communications, Vol. 31, No. 12, Pp. 2838-2849, 2008.

[9] H. Wang, J. Wan and R. Liu, “A novel ranging method based on RSSI”, Energy Procedia, Vol. 12, No. 1, Pp. 230-235, 2011.

[10] C.H. Ou, “A roadside unit based localization scheme for vehicular ad hoc networks”, Int. J of Communication Systems Wiley, Pp. 123-130, 2012.

[11] J.T. Isaac, S. Zeadally and J.S. Camara, “Security attacks and solutions for vehicular ad hoc networks”, Communications IET, Vol. 4, No. 7, Pp. 894-903, 2010.

[12] K. Ibrahim, “Data aggregation and dissemination in vehicular ad-hoc networks”, Doctoral dissertation, Old Dominion University, Norfolk, Virginia, 2011.

[13] P.Y. Shen, “An efficient public key management regime for vehicular ad hoc networks (VANETS)”, Masters by Research thesis, Queensland University of Technology, 2011.

[14] G. Yan, W. Yang, J. Li and V.G. Ashok, “Active position security through dynamically tunable radar”, IEEE 7th International Conference Mobile Ad hoc and Sensor Systems (MASS), Pp. 733-738, 2010.

[15] B. Xiao, B. Yu and C. Gao, “Detection and localization of Sybil nodes in VANETs”, Proceedings of the workshop on Dependability issues in wireless ad hoc networks and sensor networks, Pp. 1-8, 2006.

[16] B. Yu, C.Z. Xu and B. Xiao, "Detecting Sybil attacks in VANETs", Journal of Parallel and Distributed Computing, Vol. 73, No. 6, Pp. 746–756, 2013.

[17] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks", Proc. Of International Symposium on a World of Wireless, Mobile and Multimedia Networks, Pp. 564–570, 2006.

[18] S. Zhong, L.E. Li, Y.G. Liu and Y.R. Yang, "Privacy-reserving location based services for mobile users in wireless networks", Technical Report. YALEU/DCS/TR-1297, Department of Computer Science, Yale University, 2004.

[19] S. Abbas, M. Merabti, D. Llewellyn-Jones and K. Kifayat, "Lightweight Sybil Attack Detection in MANETs", IEEE, Systems Journal, Vol. 7, No. 2, Pp. 236-248, 2013.

[20] B. Dutertre, S. Cheung and J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust. Technical Report", SRI-SDL-04-02, SRI Int'l 2004.

[21] S. Capkun, L. Buttyán and J.P. Hubaux, "Self-Organized Public Key Management for Mobile Ad Hoc Networks", IEEE Trans. Mobile Computing, Vol. 2, No. 1, Pp. 52-64, 2003.

[22] S. Chang, Y. Qi, H. Zhu, J. Zhao and X. Shen, "Footprint: detecting Sybil attacks in urban vehicular networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 6, Pp. 1103-1114, 2012.

[23] D.P. Bertsekas, J.N. Tsitsiklis, Introduction to Probability, Athena Scientific; 2nd edition, 2008.

[24] J. Blum and A. Eskandarian, "The Threat of Intelligent Collisions", IT Professional, Vol. 6, No. 1, Pp. 24–29, 2004.

[25] J. Douceur, "The Sybil Attack", Proc. of International Workshop on Peer-to-Peer Systems, Pp. 251–260, 2002.

[26] G. Guette and C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)", Proc. of WISTP 08, LNCS 5019, Pp. 106-116, 2008.

[27] G. Guette and B. Ducourthial, "On the Sybil attack detection in VANET", Proc. of IEEE International Conference on Mobile Adhoc and Sensor Systems, 2007.

[28] S. Lv, X. Wang, X Zhao and X Zhou, "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks", Proc. of International Conference on Computational Intelligence and Security, Pp. 442-446, 2008.