International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Survey on VANET Protocols and Security Techniques

Ashok Shivaji Dadali[1], Prof. Ram Joshi[2]

[1]Savitribai Phule Pune University
C12/1 Health Camp, Shivaji Nagar
Pune- 411016, India

[2]Savitribai Phule Pune University
Computer Engineering Department
Kothrud, India

Abstract: ***Recently, vehicular ad hoc network (VANET) becomes increasingly popular in many countries. It is an important element of the Intelligent Transportation Systems (ITS). In a typical VANET, each vehicle is assumed to have an on- board unit (OBU) and there are road-side units (RSU) installed along the roads. A trusted authority (TA), a server is installed in the back end. The OBUs and RSUs communicate using the Dedicated Short Range Communications (DSRC) protocol over the wireless channel while the RSUs, TA, and the application servers communicate using a secure fixed network (e.g., the Internet). The basic functionality of a VANET is to allow arbitrary vehicles to broadcast safety messages (e.g., vehicle speed, turning direction, traffic accident information) to other nearby vehicles (denoted as vehicle-vehicle or V2V communications) and to RSU (denoted as vehicle-infrastructure or V2I communications) regularly such that other vehicles may adjust their traveling routes and RSUs may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. As such, a VANET can also be interpreted as a sensor network because the traffic control center or some other central servers can collect lots of useful information about road conditions from vehicles. It is natural to investigate how to utilize the collected real-time road conditions to provide useful applications. In this study, proposed application VANET- based secure and privacy-preserving navigation (VSPN), which makes use of the collected data to provide navigation service to users. Based on the destination and the current location of the driver (the query), the system can automatically search for a route that yields minimum traveling delay using the online information of the road condition. In addition of driving guidance, the navigation results can also be used for other purposes like sharing images and videos.***

Keywords: Navigation, secure vehicular sensor network, signature verification, pseudo identity, anonymous credential, proxy re-encryption.

1. Introduction

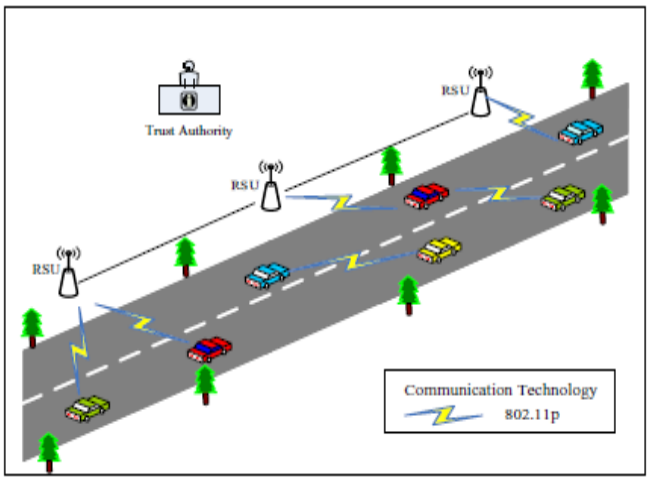

Figure 1: VANET Architecture

India is the second largest country in the world in terms of human population. So it uses large number vehicles in the world, Pune which rank first in the world in terms of two wheeler users. As number of vehicle increase it also increase problems regarding road accident and vehicle traffic congestion and degradation of environment. In India number of people died every year in road accident or they not get medical attention in time because of vehicle traffic. And also when vehicle trapped in traffic it is waste of the user's time and fuel such problem we use Vehicle ad hoc network [VANET] which is the collection of the vehicle on the road, which used to communicate real time traffic and safety information communicate with each other through Road Side Unit [RSU], to help how much road traffic is ahead so user can adjust his route accordingly so it will help user to reach destination in minimum time by avoiding traffic. Global positioning system(GPS) [15] which can help navigation system but it cannot give real time road traffic, it uses predefine data about the road. In VANET network on Board Unit (OBU) is installed on the vehicle which continuously communicate with the RSU, and RSU communicate with Trusted Authority [TA] which give real time road traffic to the VANET user.

VANET has great potential to solve day to day road traffic problem but if any attack happened on the VANET it will be very costly, so security is the main concern in VANET networking. Different kind of attack can occur in the VANET like data modification, data aggregation, data doping and false event generation, black hole, grey hole, message forging on board tempering[7] to avoid this problem we use VANET based privacy and preservation navigation system which effectively handle such attach on the Internet.

VANET applications are divided into two categories safety and non safety messages. Messages like whether information,

music sharing, information about nearby ATM machines etc. And safety messages are which collected from RSU and nearby vehicle which can use to help the human life. Such as emergency speed breaking, real time road traffic which leads travel safety and reduce road traffic. Safety messages can avoid road accident where visibility is low. It can send information to the user by sensing the vehicle through RSU.

2. Attacks on VANET Network

Table 1: Types of Attacks

Type of Attack	*Description*
privacy leakage	User identity revels to the other user in the network.
Daniel of service attack	A lot of wrong of message are created which kept server busy and service denied to the real user
Confidentiality	A user in VANET may not want vehicle nearby to know his/her destination by eavesdropping.
.Message tempering	Message is modified by the attacker
broadcast Tempering	False safety message into the network.
Malware	Such as viruses or worms can cause problem in to the network.
Spamming	Increase message latency
Black Hole Attack	Established node drops out
Replay attack	Attacker re inject previously received message in to the network
GPS spoofing	Attacker fools vehicle by showing them in different location

- **Denial of Service Attack:** DoS attacks can be carried out by network insiders and outsiders and renders the network unavailable to authentic users by flooding and jamming with likely catastrophic results. Flooding the control channel with high volumes of artificially generated messages, the network's nodes, onboard units and roadside units cannot sufficiently process the surplus data.
- **Broadcast Tampering:** An inside attacker may inject false safety messages into the network to cause damage, such as causing an accident by suppressing traffic warnings or manipulating the flow of traffic around a chosen route.
- **Malware:** The introduction of malware, such as viruses or worms, into VANETs has the potential to cause serious disruption to its operation. Malware attacks are more likely to be carried out by a rogue insider rather than an outsider and may be introduced into the network when the onboard units and roadside units receive software and firmware updates.
- **Spamming:** The presence of spam messages on VANETs elevates the risk of increased transmission latency. Spamming is made more difficult to control because of the absence of a basic infrastructure and centralized administration.
- **Black Hole Attack:** A black hole is formed when nodes refuse to participate in the network or when an established node drops out. When the node drops out, all routes it participated in are broken leading to a failure to propagate messages. Alter or replay legitimate messages, revealing spoofed GPS signals, and impede the introduction of misinformation into the vehicular network. These include:
- **Masquerading:** Masquerading attacks are easy to perform on VANETs as all that is required for an attacker to join the network is a functioning onboard unit. By posing as legitimate vehicles in the network, outsiders can conduct a variety of attacks such as forming black holes or producing false messages.
- **Replay Attack:** In a replay attack the attacker re injects previously received packets back into the network, poisoning a node's location table by replaying beacons. VANETs operating in the WAVE framework are protected from replay attacks but to continue protection an accurate source of time must be maintained as this is used to keep a cache of recently received messages, against which new messages can be compared.
- **Global Positioning System (GPS) Spoofing:** The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite.
- **Tunneling:** An attacker exploits the momentary loss of positioning information when a vehicle enters a tunnel and before it receives the authentic positioning information the attacker injects false data into the onboard unit.
- **Position Faking:** Authentic and accurate reporting of vehicle position information must be ensured. Vehicles are solely responsible for providing their location information and impersonation must be impossible. Unsecured communication can allow attackers to modify or falsify their own position information to other vehicles, create additional vehicle identifiers (also known as Sybil Attack) or block vehicles from receiving vital safety messages.
- **Message Tampering:** A threat to authenticity can result from an attacker modifying the messages exchanged in vehicle-to-vehicle or vehicle-to-roadside unit communication in order to falsify transaction application requests or to forge responses.
- **Message Suppression/Fabrication/Alteration:** In this case an attacker either physically disables inter-vehicle communication or modifies the application to prevent it from sending to, or responding from application beacons.
- **Key and/or Certificate Replication:** Closely related to broadcast tampering is key management and/or certificate replication where an attacker could undermine the system by duplicating a vehicle's identity across several other vehicles. The objective of such an attack would be to confuse authorities and prevent identification of vehicles in hit-and-run events.

3. Literature Survey

Various protocols have applied to the VANET network, to achieve security. Protocols effectiveness is calculated on the basis of minimum delay in response from server, trust of received message, cost and deployment method. Different methods have proposed in the following section to get

security in the VANET such as cryptographic schemes reputation-based systems, and plausibility and sensor-driven techniques.

VSPN: VANET-Based Secure and Privacy-Preserving Navigation

The author in [1] has proposed compute real time road traffic through VSPN protocol. In this system it uses Road side unit (RSU) and Trusted Authority (TA) and on board unit to give real time road traffic. In this system OBU continually communicate with RSU and TA, OBU request for the navigation to RSU, RSU check whether destination is in within his ranger or not and also same time check traffic in that region. if destination is not in current RSU range then it broadcast navigation message to all nearby RSU. This protocol provides security from message integrity and authentication, Identity privacy preserving, traceability and confidentiality. It uses bilinear mapping to map secrete key to public key mapping, and uses Boneh–Lynn–Shacham (BLS) signature scheme [12] to provide security from message forging.

Inter node Mobility Correlation for Group Detection and Analysis in VANET, [3] has proposed mobility correlation among the moving vehicle. In VANET network devices communicate with RSU unit through wireless network which leads to connection and disconnection of communication link and network and grouping and dispersion of nodes, which greatly affect the network performance. at the same they also form a group of vehicle which ave similar pattern of movement. To measure correlation among vehicle he uses spatial locality node [SLS] mobility and temporal locality of node pattern [TLS]. And after calculating both values of SLS and TLS he introduces third technique which is dual locality reference [DLR]. Vehicular Security through Reputation and Plausibility Checks [2] uses user's reputation and plausibility to perform security in the VANET network. This technique provides security against data modification, wrong event generation and data collection and data falling. In this protocol faulty nodes identify and remove it from the network. This algorithm mainly targeted on information which transfer on the network it may by single hop or multi-hop network. Efficient Conditional Privacy Preservation Protocol In this proposed system [5] provides two solutions, on anonymous authentication for safety messages with traceability of node who originated the message. The architecture in this method contains Trusted Authority [TA] or main server who constantly communicate with Road Side Unit [RSU], RSU communicate with on board Unit [OBU] to direct location of the message.The OBUs are constantly communicate with the running vehicles and broadcast real traffic information to themselves and also others who request the key.TA: Ta is responsible for registration of RSU and OBU and give key to them. The RSU which can communicate with both OBU and TA has storage capacity. It can tell give message to the user about real time road traffic so user can adjust his route.

Secure Vehicular Communications Systems: Design and Architecture. The authors in [4] have proposed a secure architecture. The architecture consists of the certification authority (CA) where each authority is responsible for assign block or territory. Each authority provides certificates to nodes which are in his territory and also accept nodes out of his nodes which have other certification authority's key nodes enter its territorial boundary. The RSU and on board Unit store the vehicle private key when they enter the other CA's boundary for the signature purpose. It is used as a tamper resistant solution to prevent against physical on-board tampering. Every node utilize high number of public private key for short duration of time (called pseudonyms that hide the real user of the node) instead of just using one public - private key for long term which will easy to crack for attacker. Every node uses a pseudonym for a minimum period of time and then change to next identity. This provides the required privacy Secure Positioning Based Routing (PBR) for VANETs. This protocol [16] depends on asymmetric cryptography and digital signatures. When there is only one node that is transferring the packet then it has to sign in that packet before it can send to the destination. If it dealing with more than one hop then two way signature on the packet is proposed, source signature and sender Signature, in this way we can protect data from modification. When packet reach to the destination it has perform number of checks for packets integrity. In order to check when message is originated time stamp is added with the message. This timestamp is important to check time window of the message. Additional restrictions are added by assuming a peak sending scope of the nodes in the network. Speed of the message is also calculated by time difference between two neighboring nodes and multiplying it with highest speed of the nodes. This protocol set maximum message a node can send so it will restrict malicious nodes to broadcast false message in to the network. If any node is sending more messages than its limit then this protocol will block this node from message transferring. In[13] different groups are formed deepening their geographical location and groups pass messages to the each other. In this method group leader is selected randomly and through group leader messages are passed. In this except group leader all nodes are safe from external attacks only group leader security is in danger. In [19] use hybrid technique to give user real time road traffic to the user. in this method it use both VANET and MANET technologies to give real time road traffic. It proposed real time path planning algorithm to reduce average traveling cost by avoiding vehicle getting stuck in the traffic. It improves overall performance of the VANT network by giving real time road traffic information.

Table 2: summery of literature survey

Sr. No	*Paper Name*	*Methods*
1	Securing vehicular ad hoc networks, 2006.[16]	Certificate authority (CA) responsible particular region. Each node use short term public private key called pseudonym. Keys revocation function performs by CA.
2	Inter node Mobility Correlation for Group Detection and Analysis in VANET, 2013.	Vehicle groups are formed on the basis of spatial Locality system and temporal Locality system. Combine feature of the system in Dual Locality system[DLS]
3	Vehicular Security Through Reputation and Plausibility Checks, 2007	Vehicle security is achieved by reputation and plausibility is check. Provides security against data modification dual signature sender and receiver checking.
4	ECPP: Efficient condition privacy preservation protocol for secure vehicular communication, 2008	Provides effective communication and location of the vehicle. It can provide real identity of the user at any time.
5	Securing cooperative data downloading in vehicle ad hic network.2013	Develop application layer protocol to share data between vehicles. It is reliable method to share data because after receiving data it also send acknowledgement.
6.	Security without Identification: Transaction Systems to Make Big Brother Obsolete, Comm. 1985	Take navigation credential from one organization and show to other organization. The two separate organizations are not linkable by this anonymous credentials achieved.
7.	An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks, Proc. 2008	Batch verification scheme is known as IBV introduce for verification of large number of RSU. The scheme relies on a temper-proof device to store an unchangeable master secrete key.
8.	A Next-hop Selection Scheme for Emergency Message Propagation in VANETs 2014	Nearest hop is selected when any emergency message has to broadcast. Message is divided in two parts according to their distance from the emergency location spot.
9.	AMOEBA:[13] Robust location privacy scheme for VANET, 2007.	Groups are formed and group leader choose randomly in each group. By group leader all messages and data are transfer..

4. Conclusion

VANET is important technology in vehicle traffic management. It can give safety message to the other vehicle so millions of human life can be saved. To use VANET in daily day to day life, there are different protocols are available, which can provide security to this technology. Different protocols are available to address the security issues, all protocols have their advantage and disadvantage which can handle security related problems. These protocols provide security against above mention security threats.

References

[1] VSPN: VANET-Based Secure and Privacy-Preserving Navigation T.W. Chim, S.M. Yiu, Lucas C.K. Hui, Senior Member, IEEE, and Victor O.K. Li, Fellow, IEEE IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 2, FEBRUARY 2014

[2] Sanjay K. dhurander, Mohammad Obaidat, Amrit Jaiswal, Akasnha Tiwari and Ankur Tyagi "Vehicular Security Through Reputation andPlausibility Checks" june 2014.

[3] Yujin Li, Ming Zhao, Wenye Wang, Internode Mobility Correlation for GroupDetection and Analysis in VANETs IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 9, NOVEMBER 2013.

[4] A. Studer, E. Shi, F. Bai, and A. Perrig, "Tacking Together Efficient Authentication, Revocation, and Privacy in VANETs," Proc. IEEE Sixth Ann. Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), pp. 1-9, June 2009.

[5] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: Efficient condition privacy preservation protocol for secure vehicular communi- cation," in Proc. IEEE 27th Conf. Comput. Commun., Apr. 2008.

[6] B.K. Chaurasia, S. Verma, and S.M. Bhasker, "Message Broadcast in VANETs Using Group Signature," Proc. IEEE Fourth Int'l Conf. Wireless Comm. Sensor Networks (WCSN '09) Dec. 2008

[7] C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM '08, pp. 816-824, Apr. 2008
[8] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68, 2007.
[9] T.W. F. Wang, D. Zeng, and L. Yang, "Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update," IEEEPervasive Computing, vol. 5, no. 4, pp. 68-69, Oct.-Dec. 2006.
[10] E. Fonseca and A. Festag, "A survey of existing approaches for secure ad hoc routing and their applicability to VANETs," NEC Network Laboratories, Heidelberg, Germany, NEC Tech. Rep. NLE-PR-2006-19, Version 1.1, Mar. 2006
[11] G. Philippe, G. Dan, and S. Jessica, "Detecting and correcting malicious data in VANETs," in Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw., 2004.
[12] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. Seventh Int'l Conf. Theory and Application Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '01), 2001.
[13] A. Menezes, "An Introduction to Pairing-Based Cryptography," Math. Subject Classification, Primary 94A60, 1991
[14] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. ACM, vol. 28, pp. 1030-1 044, 1985.
[15] Global Positioning System Standard Positioning Service Signal Specification. Navtech GPS Supply, 1995.
[16] Secure Position-Based Routing for VANETs Charles Harsch,Andreas Festag1, Panos Papadimitratos NEC Deutschland GmbH, 2 EPFL, Switzerland, {charles.harsch|panos.papadimitratos}@epfl.ch
[17] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, AMOEBA: Robust Location Privacy Scheme for VANET," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.
[18] Secure Cooperative Data Downloading in Vehicular Ad Hoc Networks Yong Hao, Jin Tang, Member, IEEE, and Yu Cheng IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS/SUPPLEMENT, VOL. 31, NO. 9, SEPTEMBER 2013.
[19] Real-Time Path Planning Based on Hybrid-VANET-Enhanced Transportation System Miao Wang_, Hangguan Shany, Rongxing Luz, Ran Zhang_, Xuemin (Sherman) Shen_, Fan Baix 2013