RESEARCH ARTICLE OPEN ACCESS

Survey on VSPN: VANET-Based Secure and Privacy-Preserving Navigation

Rukaiya Y. Shaikh *, Disha Deotale**
*(ME(Computer Engineering), Savitribai Phule University of Pune, Maharashtra(INDIA))
** (ME(Computer Engineering), Savitribai Phule University of Pune, Maharashtra(INDIA)

ABSTRACT
VANET provide facility for the vehicles on roads to communicate for driving safety. The basic idea is to allow arbitrary vehicles to broadcast ad hoc messages to other vehicles. However, this raises the issue of security and privacy. Here, we have described various existing solutions/protocols that are used in order to satisfy the security and privacy requirement of the vehicular ad hoc network. We have also described security issues and challenges in VANET. We have presented various security attributes that may be considered as criteria to measure security such as availability, confidentiality, integrity, authentication and non-repudiation. This paper also give the detail information of some of the schemes such as RAISE ,IBV with their pros and cons.
Keywords **-** Navigation, On board Unit(OBU), Road Side Unit(RSU), Signature Verification, Tamper Proof Device, Vehicular ad hoc network.

I. INTRODUCTION

Recently, vehicular ad hoc network (VANET) becomes very popular in so many countries. It is an important element of the Intelligent Transportation Systems (ITSs). A vehicular ad hoc network (VANET) is also known as a vehicular sensor network by which we can easily achieve driving safety through inter-vehicle communications or communications with road-side infrastructure.

Basically,Vehicular ad hoc networks (VANETs), is a subset of Mobile Ad hoc NETworks (MANETs), in which vehicles provide communication services among one another or with Road Side Infrastructure (RSU) based on wireless Local Area Network (LAN) technologies.

The primary application of a VANET is to allow vehicles to send safety messages that contain various information like vehicle speed, turning direction of vehicle, traffic accident information etc. to other nearby vehicles . It is denoted as vehicle-vehicle or V2V communications and it also send the information to RSU. It is denoted as vehicle-infrastructure or V2I communications . This information send on regular basis so 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.

The main benefits of VANETs are that they enhance road safety and vehicle security while protecting drivers' privacy from various attacks such as DoS, Sybil, Alteration etc. Security is one of the most critical issues related to VANETs since the information transmitted is distributed in an open access environment.

II. WORKING OF VEHICULAR NETWORKS

Vehicular Networks System consists of large number of nodes (for eg. vehicles).Here, each vehicle can communicate with other vehicle using short radio signals DSRC (5.9 GHz), within 1 KM range area. The communication between each vehicle is an Ad Hoc communication that means each connected node can move freely, there is no any wires required, the routers used is called Road Side Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices.

Typically, in a VANET each vehicle is assumed to have an onboard unit (OBU) and there are road-side units (RSU) that are installed along the roads. A trusted authority (TA) and application servers are installed in the back end. The onboard unit and road-side units communicate with each other by 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 (Internet).

In Vehicular Networks System each vehicle has OBU (on board unit), that is connected to the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device). Tamper Proof Device (TPD) holds the vehicle secrets, that is all the information about the vehicle like keys, drivers identity, trip details of that vehicle, speed of the vehicle, rout etc.

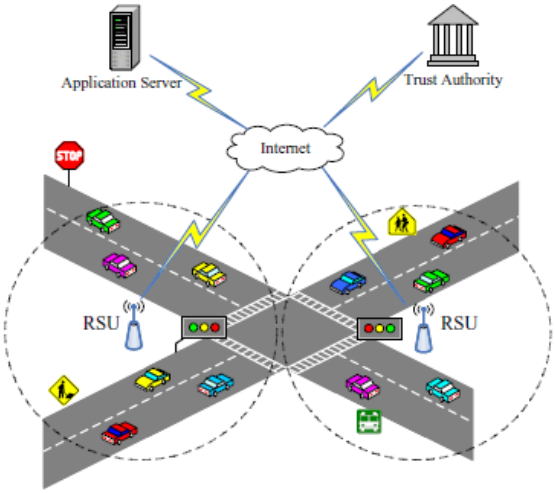

Fig.2.1-VANET Architecture.

III. SECURITY ISSUES AND CHALLENGES OF VANET

3.1 Attacks:

VANET facing many attacks, some of these attacks are as follows.

1) Denial Of Service Attack(DoS)

Denial of Service attack happens when the hacker or attacker takes control of a all the vehicle's resources or may be he jams the communication channel that are using by the Vehicular Network, thus it prevents critical information from arriving.

2) Message Suppression.

In this type of attack, an attacker selectively dropping packets from the network, these packets may hold critical information for the receiver. The attacker suppress these packets and he can use that packet again in other time. For example, an attacker may suppress a congestion warning, and use it in another time, so vehicles will not receive the correct warning and it forced to wait in the traffic.

3) Alteration Attack.

In this type of attack, an attacker simply alters an existing data. It includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted. For example, an attacker can alter a message telling other vehicles that the current road is highly congested even if the road is clear.

4) Sybil Attack.

Sybil attack is the creation of multiple fake nodes broadcasting false information. In Sybil attack, a vehicle with On Board Unit(OBU) sends multiple copies of messages to other vehicle and each message contains a different fabricated identity.

3.2 Challenges

1) High Mobility of Nodes:

In VANETs, all nodes are mobile. Vehicles make connections with one another which may last only for a few seconds. Two vehicles which have never crossed one another may never meet again .Vehicles frequently change their point of network attachment when they access Internet services, they need mobility management schemes that provide seamless communication. This mobility management meets requirements such as seamless mobility, support IPV6, scalable overheads and low handoff latency.

2) Volatility

Vehicles traveling in network that makes connection with other vehicles, but these connections will be lost as each car has a high mobility, and maybe will travel in opposite direction. Vehicular networks lacks the relatively long life context, so personal contact of users device to a hot spot will require long life password, and this will be impractical for securing VC.

3) Network Scalability

The scale of this network in the world approximately exceeding the 750 million nodes and this number is still growing, another problem arise when we must know that there is no any global authority govern the standards for this network .For example: the standards used for DSRC in North America is completely different from the DSRC standards used in Europe, the standards for the GM Vehicles is different from the BMW vehicle.

4.Time constraints

An important requirement of VANET is that all the node must capable to transmit messages within an acceptable time limit. Some applications, such as those are related to safety, require strict deadlines .

For example, all of the applications used by the emergency services involve time constraints for mes sage delivery. The driver who receives a warning message must have sufficient time to react. If the arrival deadline is not met, it will be too late and the consequences may be dangerous.

IV. SECURITY REQUIREMENT FOR VANET

Security is an important issue for ad hoc networks, especially for security sensitive applications. To secure an ad hoc network, we need to consider the following attributes as criteria to measure

security such as availability, confidentiality, integrity, authentication and non-repudiation.

1. Availability

Availability is a very important factor for VANET. It guarantees that the network is functional, and useful information is available at any functioning time. Several attacks are in this category, one of the most famous attack is Denial of Service attacks (DoS).

The availability deals with network services for all nodes comprises of bandwidth and connectivity. Group signature scheme has been introduced in order to encounter the availability issues. The scheme is focusing on availability of exchanging the messages between vehicles and RSUs. When the attack causes network unavailability, the proposed technique still survives due to interconnection using public and private keys between RSUs and vehicles.

2. Confidentiality

Confidentiality is an important security requirement for VANETs

communications, it ensures that data are only read by authorized

parties. Confidentiality ensures that classified and important information in the network can never disclosed to unauthorized person. It also prevents unauthorized access to confidential information such as name of the driver, plate number and location of the vcehicle. The most popular technique that are used to preserved privacy in vehicular networks is pseudonyms . Each vehicle node will have multiple key pairs with encryption. Messages are encrypted or signed using different pseudo and these pseudo has not linked to the vehicle node but relevant authority has access to it. Vehicle need to obtain new pseudo from RSUs before the earlier pseudo expires.

3. Authentication

Authentication is a major requirement in VANET as it ensures that the messages are sent by the actual nodes and hence attacks done by the attacker can be reduced easily with greater extent.

In VANET ,authentication is the verification of the identity between vehicles and RSU and the validation of integrity of the information exchange. Additionally, it ensure that all vehicles are the right vehicle to communicate within network.

Public or private keys with CA are proposed to establish connection between vehicles, RSU and AS . On the other hand, password is used to access to the RSU and AS as authentication method.

For example, in location based services this property could be that a vehicle is in a particular location from where it claims to be.

4. Integrity

Data integrity is the assurance that the data received by nodes, RSU and AS is the same as what has been originally generated during the exchanges of the message. In order to protect the integrity of the message, digital signature which is integrated

with password access are used

5. Non-Repudiation

Non-repudiation in computer security means the ability to verify that the sender and the receiver are the entities who claim to

have respectively sent or received the message .It ensures that sending and receiving parties cannot deny ever sending and receiving the message such as accident messages.

In a VANET

all the manipulated data related to the safety and

privacy of the users, it should be always possible to verify all hardware and software changes of security settings and applications.

V. PROTOCOLS USED TO ENSURE SECURITY AND PRIVACY

1.VPKI (Vehicular Public Key Infrastructure)

In paper [1], author gave a foundational proposal of using pseudonym based approach using anonymous certificates and the public key infrastructure (PKI).The anonymous certificates are used to hide the real identities of users. This scheme required extra communication and it has large storage overhead. To achieve the privacy requirement of vehicle, the authors proposed to use frequently updated anonymous public keys. But,the problem with this solution is that it required large number of key pairs to be stored, hence making the secure distribution of keys, key management, and storage becomes complex; so practically it is not efficient.

2. Secure Traffic Aggregation

Secure Traffic Aggregation scheme [2] is used to minimize the communication overhead between the vehicles. Firstly, we need to define physical location of cell. When vehicles are located in a cell, the vehicle that is physically closest to the center of the cell is automatically taken as the group leader of the vehicles in the cell, which is delegated to aggregate messages for the whole group when the message is going to be relayed to the leader of the neighbor groups. The aggregation of messages can achieve a significant reduction in the overhead for vehicle to vehicle communications. However, the vehicle closest to the center of a cell could change frequently, leading to a frequent update of the group leader of a cell (e.g., once in a few seconds), which indicates that this approach need to be improved in order to achieve its efficiency and practical applicability.

3.Anonymous-key-based (HAB) security protocol,

In paper [3], author used an anonymous-key-based (HAB) security protocol, which can achieve

anonymous message authentication and conditional privacy preservation. With the HAB solution, a huge set of anonymous keys are preloaded in each vehicle, and each vehicle randomly takes one of the keys in the set to sign a safety message. To further prevent movement tracking, each anonymous key has a short lifetime. The HAB scheme provides an efficient and straightforward way in solving the privacy issues, while the central authority simply keeps all the anonymous certificates of all the vehicles in a certain area in order to maintain the traceability.

4.Group Signature Scheme:

In paper [4], author suggested an idea of using the group signature,but it has a major drawback that it causing a great overhead, every time that any vehicle enters the group area, the group public key and the vehicle session key for each vehicle that belongs to the group must be changed and transmitted, another issue must be considered that the mobility of the VANET prevents the network from making a static group, so the group is changing all the time, and the signatures and keys frequently changed and transmitted.

5.RAISE: RSU-aided Message Authentication

In Vehicular Ad-hoc ,when the traffic density becomes larger, a vehicle cannot verify all signatures of the messages sent by its neighbors in a timely manner, which results in message loss.

Communication overhead as another issue that need to be handle. To deal with these issues, author have introduced a novel RSU-aided messages authentication scheme[5], called RAISE. With RAISE, roadside units (RSUs) are responsible for verifying the authenticity of the messages sent from vehicles and for notifying the results back to vehicles. In addition, author have been used k-anonymity approach to protect user identity privacy, where an adversary cannot associate a message with a particular vehicle.

Advantages:

1.RAISE provide reliable authentication with the help of Road side unit(RSU).

2. Due to the use of symmetric key it is possible to reduce communication overhead.

3.It provide fast vehicle-vehicle (V2V) verification.

4. RAISE can defend against not only the external attacks, but also the internal attacks.RAISE is very strong for spoofing and reply attack.

Limitation:

1.RAISE is totally centralized by RSU. The protocol is software-based. It allows a vehicle to verify the signature of another with the aid of a nearby RSU. However, no batch verification can be done and the RSU has to verify signatures one after another.

2.It required a lot of memory buffer in both RSU and OBU.

3.On the other hand, to notify other vehicles whether a message from a certain vehicle is valid, a hash value of 128 bytes needs to be broadcast.

4.There can be tens up to thousands of signatures within a short period of time, thus the notification messages induce a heavy message overhead.

6. IBV: Identity-based Batch Verification Scheme

In paper[6], author introduced an efficient batch signature verification scheme for communications between vehicles and RSUs .Here, RSU can verify multiple received signatures at the same time such that the total verification time can be dramatically reduced. **Identity-based Batch Verification Scheme** can achieve conditional privacy preservation that is essential in VSNs, in which each message launched by a vehicle is mapped to a distinct pseudo identity, while a trust authority can always retrieve the real identity of a vehicle from any pseudo identity.

Identity-based cryptography is used for private keys generation for pseudo identities, certificates are not needed and thus transmission overhead can be significantly reduced.

Advantages

1) Multiple signatures can be verified at the same time instead of one after the other . Therefore, the signature verification time can be dramatically reduced.

2) By generating distinct pseudo identities and the corresponding private keys for signing each message with a tamper-proof device, privacy regarding user identity and location of the vehicles can be protected.

3) The identities of the vehicles can be uniquely revealed by the trusted authorities under exceptional cases.

4) Since identity-based cryptography is employed by the tamper-proof device, efforts on certificate management and the transmission overhead can be significantly reduced.

Limitation

The IBV protocol is designed only for vehicle-to-RSU communications. The RSU can verify a large number of signatures as a batch by using just three pairing operations.

1. IBV protocol relies heavily on a tamper-proof hardware device, installed in each vehicle, which preloads the system-wide secret key. If these devices is cracked, the whole system will be compromised.

2. A vehicle's real identity can be traced easily by anyone, thus this IBV protocol does not satisfy the privacy requirement of the vehicle.
3. IBV protocol has a flaw such that a vehicle can use a fake identity to avoid being traced (anti-traceability attack) or even impersonate another vehicle (impersonation attack1).
4. while using batch verification scheme, if any of the signatures is erroneous, the whole batch will be dropped. This is inefficient because most signatures in the batch may actually be valid,thus this does not give satisfactory successful rate.
5. The IBV protocol is not designed for vehicle-to-vehicle communications.

CONCLUSION:

The security of VANETs is one of the most critical issues because their information transmission is propagated in open access environments. In order to take full advantage of the vehicular networks the communication must be secured meeting all the security requirements. This paper provides a literature survey on various security issues and challenges facing by VANET. Some security requirements such as availability,confidentiality, integrity, authentication and non-repudiation in VANETs have been pointed out. In this paper we have described overview of the various protocols used with their pros and cons in order to handle the security and privacy of VANET.

REFERENCES

[1] J.P.H.M. Raya, P. Papadimitratos, "Securing Vehicular Communications*," IEEE Wireless Comm., vol. 13, no. 5, pp. 8-15, Oct. 2006*.
[2] M. Raya, A. Aziz, and J. P. Hubaux, "Efficient secure aggregation inVANETs*," in Proceedings of International workshop on Vehicular ad hoc networks, pp. 67-75, 2006*
[3] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks,"*Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, 2007*.
[4] W Ren, K Ren, W Lou, Y Zhang,"Efficient user revocation for privacy-aware PKI", *Proceedings of the 5th International ICST Conference, 2008.*
[5] C. Zhang, X. Lin, R. Lu, and P.H. Ho, "RAISE: An Efficient RSU- Aided Message Authentication Scheme in Vehicular Communication Networks," *Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1451-1457, May 2008*.
[6] 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.*
[7] G. Samara, W. Al-Salihy, and R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)," *Proc. IEEE Fourth Int'l Conf. New Trends in Information Science and Service Science (NISS '10), pp. 393-398, May 2010.*
[8] X. Lin, X. Sun, P. Ho, "GSIS: A secure and privacy preserving protocol for vehicular communications*", IEEE Trans. Vehicular Technology 2007, Vol. 56, No. 6, p 3442-3456.*
[9] T.W. Chim, S.M. Yiu, Lucas C.K. Hui,"VSPN: VANET-Based Secure and Privacy-Preserving Navigation" *proc. IEEE TRANSACTIONS ON COMPUTERS,3 VOL. 63, NO. 2,FEBRUARY 2014*