ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DIFFERENT APPROACH FOR SECURE COMMUNICATION OF VANET OVER DSRC WITH 802.11

Harsh Joshi*, Prof. Roopa Nandini

* M.Tech (Student) Dept. Of Electronics and Communication, SRIT, Jabalpur- (M.P.), India
Assistant Professor, Dept. Of Electronics and Communication, SRIT, Jabalpur- (M.P.), India

ABSTRACT

Mobile Ad-Hoc network research has been gaining in last few years. Lot of work has been put into devising routing protocols and secure communication with the development 802.11p standard dedicated to DSRC.VANET is very close to such research. VANETs must be tested thoroughly before they are put in real world as the consequences of failing systems are very high in VANETs. There exist a few simulators like Groove Sim, NS, Which can be used for VANETs but given the popularity and well spread knowledge of MATLAB tool, a simulation environment in MATLAB could be very useful to many researchers. Such environment can be used while designing better MAC protocols, broadcasting schemes, security features in VANETs. In this paper we are surveying different approach like Privacy-preserving schemes, ID-Based Cryptography (IBC), Ad Dissemination Model, FRAMEWORK etc. for secure communion in VANET. Simulation and testing was performed almost in MATLAB.

KEYWORDS: VANET, IBC, MAC, DSRC, NS.

INTRODUCTION

Due to the foreseen impact of the vehicular ad hoc network (VANET) offering a variety of safety applications, extensive attention in industry and academia has been directed toward bringing VANETs into real life and standardizing network operation. DSRC communication relies fundamentally on standards based Inter operability among devices from different manufacturers. The sections that follow examine the major standards for each of the layers in turn: Physical (PHY), Data Link (including medium access control (MAC), Network/Transport, and Application.

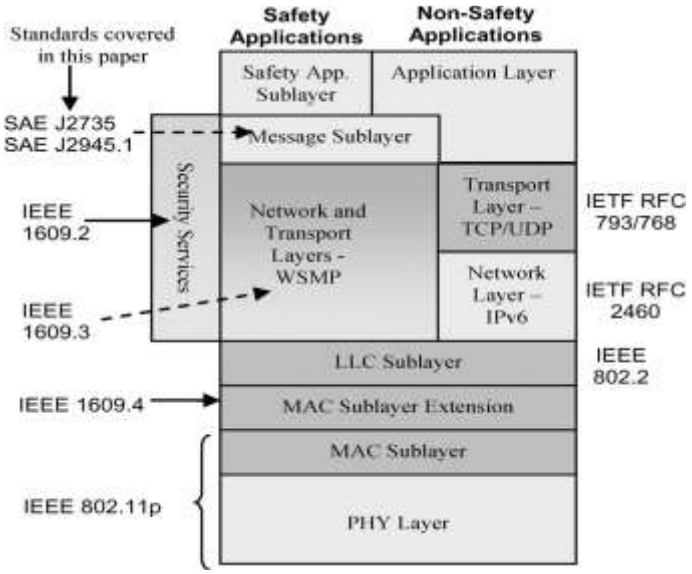

Fig: 1. Layered architecture for DSRC communication

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

Including shorthand names of protocols and standards intended for use at the various layers. At the PHY and MAC layers DSRC utilizes IEEE 802.11p Wireless Access for Vehicular Environments (WAVE), a modified version of the familiar IEEE 802.11 (WiFi) standard. In the middle of the stack DSRC employs a suite of standards defined by the IEEE 1609 Working Group: 1609.4 for Channel Switching, 1609.3 for Network Services (including the WAVE Short Message Protocol (WSMP), and 1609.2 for Security Services. DSRC also supports use of well-known Internet protocols for the Network and Transport layers, i.e., Internet Protocol version 6 (IPv6), User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). These protocols, defined by the Internet Engineering Task Force (IETF), are stable and well documented in other places, so they are not further discussed in this paper. The choice between using WSMP or IPv6+UDP/TCP depends on the requirements of a given application. Single-hop messages, like those upon which collision prevention applications are based, typically use the bandwidth-efficient WSMP, while multi-hop packets use IPv6 for its routing capability.

Modulation Technique	Coded Bit Rate (Mbps)	Coding Rate	Data Rate (Mbps)	Data Bits per OFDM Symbol
BPSK	6	1/2	3	24
BPSK	6	3/4	4.5	36
QPSK	12	1/2	6	48
QPSK	12	3/4	9	72
16-QAM	24	1/2	12	96
16-QAM	24	3/4	18	144
64-QAM	36	2/3	24	192
64-QAM	36	3/4	27	216

Fig: 2. Data Rate Options in a DSRC 10 MHz OFDM Channel

DIFFERENT APPROACHES

Privacy-preserving schemes -

There is a large body of research work related to the security and privacy in VANETs. The most related works are on the design of privacy-preserving schemes. Raya and Hubaux [3] investigated the privacy issue by proposing a pseudonym based approach using anonymous public keys and the public key infrastructure (PKI), where the public key certificate is needed, giving rise to extra communication and storage overhead. The authors also proposed three credential revocation protocols tailored for VANETs, namely RTPD, RC2RL, and DRP [11], considering that the certificate revocation list (CRL) needs to be distributed across the entire network in a timely manner. All the three protocols seem to work well under conventional public key infrastructure (PKI). However, to use frequently updated anonymous public keys to fulfill users' requirement on identity and location privacy. If this privacy preserving technique is used in conjunction withRC2RLand DRP, the CRL produced by the trusted authority will become huge in size, rendering the revocation protocols highly inefficient. A lightweight symmetric-key-based security scheme for balancing auditability and privacy in VANETs is proposed in [4]. It bears the drawback that peer vehicles authenticate each other via a base station, which is unsuitable for inter vehicle communications.

Group signature based schemes are proposed in [8], [10], [11], where signer privacy is conditional on the group manager. As a result, all these schemes have the problem of identity escrow, as a group manager who possesses the group master key can arbitrarily reveal the identity of any group member. In addition, due to the limitation of group formation in VANETs (e.g., too few cars in the vicinity to establish the group), the group-based schemes [8], [10], [11], [12] may not be applied appropriately. The election of group leader will sometimes encounter difficulties since a trusted entity cannot be found amongst peer vehicles. Kamat et al. [11], [12] proposed an ID-based security framework for VANETs to provide authentication, non repudiation, and pseudonymity. However, their framework is limited by the strong dependence on the infrastructure for short-lived pseudonym generation, which renders the signaling overhead overwhelming.There are also a number of defense techniques against misbehavior in VANET literature besides those in [3]. An indirect approach via the aid of infrastructure is used in [8] and [11]. The TA distributes the CRL to the infrastructure points which then take over the TA's responsibility to execute the revocation

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

protocol. The advantage of this approach is that vehicles never need to download the entire CRL. Unfortunately, the conditional anonymity claimed in [8] and [12] only applies to amongst peer vehicles, under the assumption that the infrastructure points (group manager in [8] and base station in [12]) are trusted.

The infrastructure points can reveal the identity of any vehicle at any time even if the vehicle is honest. The scheme in [9] leverages a single TA to recover the identity of a (possibly honest) vehicle, where revocation issues are not discussed. Recently, Tsang et al. [12] proposed a black list able anonymous credential system for blocking misbehavior without the trusted third party (TTP). The blacklisting technique can be applied to VANETs as: if the vehicle fails to prove that it is not on the blacklist of the current authenticator, the authenticator will ignore the messages or requests sent by this vehicle. Although not proposed specifically for VANETs, the proposal in [20] has a similar claim as ours that the capability of a TTP (network authority in our paper) to recover a user's identity in any case is too strong a punishment and highly undesirable in some scenarios. The downside of this technique is the lack of options to trace misbehaving users, since any user in the system (misbehaving or not) will by no means be identified by any entity including the authorities.

ID-Based Cryptography (IBC)

Identity-based or ID-based cryptosystem allows the public key of an entity to be derived from its public identity information such as name, email address, etc., which avoids the use of certificates for public key verification in the conventional PKI. Boneh and Franklin [10] introduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically, let G1 and G2 be an additive group and a multiplicative group, respectively, of the same prime order q. Discrete logarithm problem (DLP) is assumed to be hard in both G1 and G2.An identity-based (ID-based) ring signature scheme to achieve signer ambiguity and hence fulfill the privacy requirement in VANET applications. The disadvantage of the ring signature scheme in the context of VANET applications is the unconditional privacy, resulting in the traceability requirement unattainable.

Ad Dissemination Model

According to this approach we leave mobile SPs, such as vehicles that are willing to share music, to service discovery schemes [5]–[8]. To impress more customers, an SP may disseminate one ad multiple times with a certain frequency, where each is denoted as an ad rebroadcast. Due to the location relevance of most ads in VANETs, the SP will request one specific RSU1 (usually the RSU nearest to itself) to act as its source RSU (SRSU) and broadcast its ad to the nearby vehicles. To cover a larger area than the communication range of the SRSU, the ad needs to be forwarded by vehicular nodes over multiple hops. Therefore, ad dissemination involves three parties with conflicting requirements: First, each SP intends to maximize its advertising effect by disseminating ads to as many nodes as possible. Second, as an ad receiver, each node would like to learn of the local services without being distracted by excessive ads. In addition, being selfish, each node forwarding one ad expects to receive certain incentive in return. Third, VANETs as a whole need to ensure ad dissemination is under control in the face of increasingly more ads to avoid message storms. Meantime, the infrastructure entities may also expect to obtain incentives for supporting ad disseminations. All these conflicting requirements need to be balanced in VAAD.

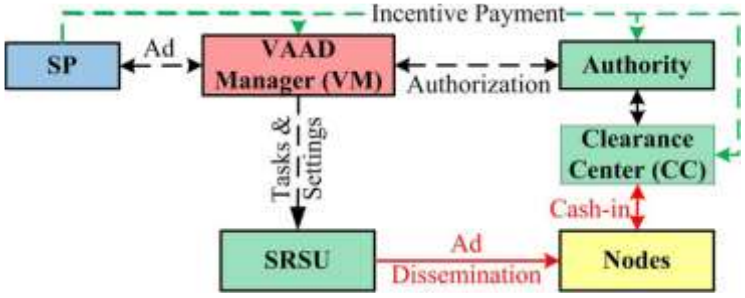

Fig: 3. Overview of VAAD

Evidence and Token for Fairness

The basic principal of the evidence-token mechanism is to balance the effort that vehicles make over time with the advantages that vehicles take from others. The mechanism requires time to be slotted. The TA will be responsible for maintaining the balance according to the time slots. It receives the evidences from vehicles via RSUs when vehicles

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

pass by the RSUs, and it sends the tokens back to the vehicles based on the evaluation of their authentication efforts in the past time slots. The evidences will not be repeatedly used to count their effort. The TA generates and distributes tokens to vehicles to enable them to verify other vehicles' integrated signatures. The tokens must be of timeliness; otherwise, vehicles may disconnect from RSUs after obtaining enough tokens.

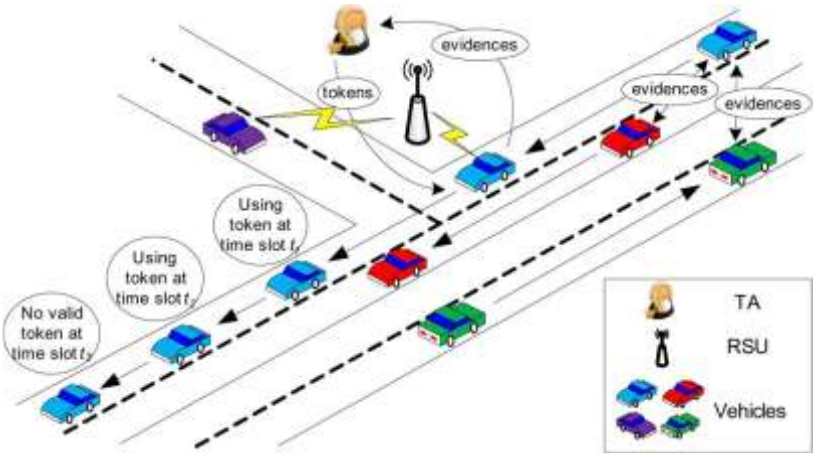

Fig: 3. Evidence-token mechanism.

Frame Work

System and Security Models The last decade has witnessed a rising interest in vehicular networks and their numerous applications. Although the primary purpose of VANET standards is to enable communication-based automotive safety applications, they allow for a range of comfort applications. Many services could be provided by exploiting RSUs as delegates to obtain data on the user's behalf. These services span many fields, from office on- wheels to entertainment, downloading files, reading e-mail while on the move, and chatting within social networks. In this approach, we design a service-oriented vehicular security system that allows VANET users to exploit RSUs in obtaining various types of data. In REACT, users register once with the RSUs online (through the Internet) before they start connecting to the RSUs from their vehicle. After registration, the RSUs obtain from a trusted authority (TA) a master key (Km) for the user. The users get their Km the first time they connect to an RSU from their vehicle. We describe a AES algorithm that uses the users' password from their account to securely transfer their Km to them. Km will be used to encrypt the initial packet key, which is assigned to the user at the beginning of each session. Then, each packet will be encrypted by a set of derived keys. With regard to the assumptions, we presume that each vehicle is equipped with a positioning system (e.g., Global Positioning System) and a digital map and has an Electronic License Plate (ELP) [3] installed. We also assume a hybrid RSU architecture in which some RSUs are directly wired to each other, others connect to the RSU network through the Internet (using gateways), whereas a third group is both wired to other RSUs and has an Internet connection. In all cases, however, each RSU has a way of connecting to any other RSU (possibly through other RSUs). In addition, several TAs are connected to the RSUs through secure wired links. Similar to [11], we assume that TAs have powerful firewalls and other protections that prevent them from being compromised. In addition, the RSUs are supposedly equipped with trusted platform modules (TPMs), intrusion detection systems, and firewalls that enable them to resist software attacks. These assumptions were made by several works such as [11] and [12], which showed that RSUs can be well defended against software attacks. With respect to hardware attacks, RSUs can be monitored using hidden surveillance cameras such as digital video or analog CCTV cameras that report to a central station, in which observers can immediately notice a hardware attack and take the appropriate actions. The RSUs do not store sensitive data, but each RSU has a secure connection to a database server that stores the RSUs' private information. Each RSU will have its own database to avoid the effect of failures. In addition, we assume that each RSU will be monitored by a TA, which, upon detecting a malicious behavior from the RSU, will isolate it from the network by informing other RSUs, which inform vehicles that are connecting to them. A secure protocol (such as IP tunneling) is assumed to connect RSUs to one another. For VANET users, we assume that each user will connect to a single RSU at a single time (to reduce overhead). Vehicles and RSUs exchange messages using uncast when they are within direct range and depend on the network-layer routing protocol when they are apart.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

PERFORMANCE ANALYSIS AND SIMULATIONS

In this section, the performance of all the approaches will be analyzed and compared. To examine the performance in various environmental scenarios, it is necessary to implement a large geographical deployment, which requires numerous vehicles and is generally too costly. Thus, instead of field test experiments, the theoretical analysis and simulations are usually applied to evaluate the protocol performance in VANETs.

CONCLUSION

How we can ensure security and privacy in service-oriented VANETs represents a challenging issue. We have presented the VANET security system mainly achieving privacy, traceability, non frame ability, and privacy preserving defense against misbehavior. These functionalities are realized by the pseudonym-based technique, the threshold signature, and the threshold authentication based defense scheme. The ID-based cryptosystem facilitates us to design communication and storage efficient schemes. Through security and efficiency analysis, our system is shown to satisfy the predefined security objectives and desirable efficiencies. VAAD supports secure ad dissemination in VANETs with pragmatic cost and effect control. Being more cost effective and efficient than existing advertising methods, e.g., ad dissemination based on cellular communications and roadside ad posters, VAAD shows appealing application potential in future VANETs. The TA strategically adjusts the valid period (lifetime) of tokens for each vehicle user based on the collected evidence, thereby periodically controlling vehicle users' cooperation capabilities. Finally we find encryption based secure communication is more reliable in every point of view so our future work consists of simulating best security system and experimenting it in real VANET settings.

REFERENCES

[1] E. Coronado and S. Cherkaoui, "Service discovery and service access in wireless vehicular networks," in Proc. IEEE GLOBECOM Workshops, 2008, pp. 1–6.
[2] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616 629, Mar. 2011.
[3] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," IEEE Wireless Commun., vol. 16, no. 4, pp. 16–22, Aug. 2009.
[4] O. Trullols, M. Fiore, C. Casetti, C. Chiasserini, and J. Ordinas, "Planning roadside infrastructure for information dissemination in intelligent transportation systems," Comput. Commun., vol. 33, no. 4, pp. 432–442, Mar. 2010.
[5] IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 2, FEBRUARY 2013 A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks Khaleel Mershad and Hassan Artail.
[6] IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 9, SEPTEMBER 2010 An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, Fellow, IEEE.
[7] IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 7, SEPTEMBER 2013 Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks Xiaodong Lin, Senior Member, IEEE, and Xu Li.
[8] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," in Proc. 27th IEEE INFOCOM, Phoenix, AZ, USA, 2008, pp. 246–250.
[9] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[10] X. Liang, R. Lu, X. Lin, and X. Shen, "PPC: Privacy-preserving chatting in vehicular peer-to-peer networks," in Proc. 72nd IEEE VTC, Ottawa, ON, Canada, 2010, pp. 1–5.
[11] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs," in Proc. 30th IEEE INFOCOM, Shanghai, China, 2011, pp. 2147–2155.
[12] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68, Jan. 2007. IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 14, NO. 1, MARCH 2013.