ISSN No: 2454-9614

Supportive Data Scheduling and Broadcast through VANET using Batch Signature

R. Janani, P. Sathishkumar*

Department of Computer and Engineering, K.S.Rangasamy College of Technology,
Namakkal, Tamil Nadu, Indi.

*Corresponding Author: R.Janani

E-mail: natarasurasa@gmail.com

Received: 10/11/2015, Revised: 13/11/2015 and Accepted: 05/03/2016

Abstract

Vehicular Ad-hoc network (VANET) is constructed with vehicles and roadside infrastructure. Vehicle location and speed information is collected continuously to manage the VANET communication. On-Board Unit (OBU) processes the data from the various sensors on the inside of the cars, and there are conditions of the vehicles. An on-board unit (OBU) is responsible for the communication with external network, such as with other vehicles and infrastructure. Road side Unit (RSU) is an infrastructure for the communication between the vehicles for sharing and information from different vehicles. The data transfer can be performed with vehicle (V2V) and vehicle-to-infrastructure (V2I). Opponents can track a vehicle by observing their communication and movement patterns. Privacy violation and anonymous communication are some security issues in VANET. Multi Hop broadcasting systems are for the dissemination of safety messages. Freight Forwarder node manages the data transfer process in multi-hop radio protocols. Freight Forwarder node selection process is carried out with reference to the waiting period details. Robust and fast forwarding (ROFF) protocol solves the unnecessary delay and collusion problems in data dissemination process. A freight forwarder candidate is allowed, the waiting time is inversely proportional to its priority forward. The empty space Distribution (ESD) bitmap describes the distribution of spaces between the vehicles. A freight forwarder candidate acquires its priority forward with the concept of the ESD-bitmap. Collisions are avoided by the control the wait time differences than the pre-defined limit.

Keywords—Intelligent transportation systems (ITS), vehicular ad-hoc networks (VANET), multi-hop broadcasting

1. Introduction

The basic application of VANET is that OBUs periodically broadcast information on their present states (e.g., the current time, position, direction, speed and traffic events) to other nearby vehicles and RSUs. For example, the traffic events could be accident location, brake light warning, change lane/merge traffic warning, emergency vehicle warning, etc. After that, other vehicles may change their travelling routers and

RSUs may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. VANET offers various services and benefits to users, and thus deserves deployment efforts.

The security of message exchange plays a key role in VANET applications For example; the information from OBUs has to be identity-authenticated and integrity-checked before it can be relied on. Otherwise, an adversary can replace the information or even impersonate other vehicles to broadcast the wrong information. The wrong information possibly makes some bad situations. For instance, the information of wrong traffic flow may cause the traffic control center to make wrong decisions. The traffic light of the heavy side always stays red and the other side stays green. In addition, an adversary may portray an ambulance to require the traffic light to cooperate with her/him and violate the driving right of other users.

2. Related Work

F. Ahmed-Zaid (2011), stated that over the last two decades, the United States Department of Transportation (USDOT) has conducted extensive research on the effectiveness of vehicle-based collision countermeasures for rear-end, road departure, and lane change crashes. V2V wireless communications and vehicle positioning may enable improved safety system effectiveness by complementing or, in some instances, providing alternative approaches to the traditional, autonomous sensing-based, safety equipment. The goal of the project was to develop and test communications-based vehicle safety systems to determine if Dedicated Short Range Communications (DSRC) at 5.9 GHz, in combination with vehicle positioning, can improve upon autonomous vehicle-based safety systems and/or enable new communications-based safety applications. Internet Service Providers to adopt appropriate administrative, technical, and physical security measures to protect user privacy exists.

J.L.Huang, L.Y.Yeh, and H. Y. Chien (2011), stated that an anonymous batch authenticated and key agreement (ABAKA) scheme to authenticate multiple requests sent from different vehicles and establish different session keys for different vehicles at the same time. In vehicular ad hoc networks (VANETs), the speed of a vehicle is changed from 10 to 40 m/s (36–144 km/h); therefore, the need for efficient authentication is inevitable. Compared with the current key agreement scheme, ABAKA can efficiently authenticate multiple requests by one verification operation and negotiate a session key with each vehicle by one broadcast message. Elliptic curve cryptography is adopted to reduce the verification delay and transmission overhead. The security of ABAKA is based on the elliptic curve discrete logarithm problem, which is an unsolved NP complete problem. To deal with the invalid request problem, which may cause the batch verification fail, a detection algorithm has been proposed. Moreover, we demonstrate the efficiency merits of ABAKA through performance evaluations in terms of verification delay, transmission overhead, and cost for re-batch verifications, respectively. Onboard units (OBUs) equipped in vehicles periodically broadcast routine traffic-related messages with information such as position, current time, direction, speed, acceleration/deceleration, and traffic events.

J.Sun, C.Zhang, Y.Zhang, and Y.Fang (2010), stated that Vehicular ad hoc network (VANET) can offer various services and benefits to users and thus deserves deployment effort. Attacking and misusing such network could cause destructive consequences. It is therefore necessary to integrate security requirements into the design of VANETs and defend VANET systems against misbehavior, in order to ensure correct and smooth operations of the network. A security system for VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, non repudiation, message integrity, and confidentiality. Moreover, we propose a privacy-preserving defense technique for network authorities to handle misbehavior in VANET access, considering the challenge that privacy provides avenue for misbehavior.

R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen(2009), stated that Location privacy of mobile users (MUs) in wireless communication networks is very important. Ensuring location privacy for an MU is an effort to prevent any other party from learning the MU’s current and past locations. In this paper, we propose a novel anonymous mutual authentication protocol with provable link-layer location privacy preservation. We first formulate the security model on the link-layer, forward-secure location privacy, which is characterized by the fact that even when an attacker corrupts an MU’s current location privacy, the attacker should be kept from knowing how long the MU has stayed at the current location. Then, based on the newly devised keys with location and time awareness, a novel anonymous mutual authentication protocol between the MUs and the access point (AP) is proposed. To the best of our knowledge, this is the first developed anonymous mutual authentication scheme that can achieve provable link-layer, forward-secure location privacy. To improve efficiency, a Preset in Idle technique is exercised in the proposed scheme, which is further compared with a number of previously reported counterparts through extensive performance analysis.

R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen(2009), stated that Location privacy of mobile users (MUs) in wireless communication networks is very important. Ensuring location privacy for an MU is an effort to prevent any other party from learning the MU’s current and past locations. In this paper, we propose a novel anonymous mutual authentication protocol with provable link-layer location privacy preservation.The first formulate the security model on the link-layer, forward-secure location privacy, which is characterized by the fact that even when an attacker corrupts an MU’s current location privacy, the attacker should be kept from knowing how long the MU has stayed at the current location. Then, based on the newly devised keys with location and time awareness, a novel anonymous mutual authentication protocol between the MUs and the access point (AP) is proposed. To the best of our knowledge, this is the first developed anonymous mutual authentication scheme that can achieve provable link-layer, forward-secure location privacy. To improve efficiency, a Preset in Idle technique is exercised in the proposed scheme, which is further compared with a number of previously reported counterparts through extensive performance analysis.

3. Overview of the Project

3.1 Project Description

The basic application of VANET is that OBUs periodically broadcast information on their present states (e.g., the current time, position, direction, speed and traffic events) to other nearby vehicles and RSUs. For example, the traffic events could be accident location, brake light warning, change lane/merge traffic warning, emergency vehicle warning, etc. After that, other vehicles may change their travelling routers and

RSUs may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. VANET offers various services and benefits to users, and thus deserves deployment efforts.

The security of message exchange plays a key role in VANET applications. For example, the information from OBUs has to be identity-authenticated and integrity-checked before it can be relied on. Otherwise, an adversary can replace the information or even impersonate other vehicles to broadcast the wrong information. The wrong information possibly makes some bad situations. For instance, the information of wrong traffic flow may cause the traffic control center to make wrong decisions. The traffic light of the heavy side always stays red and the other side stays green. In addition, an adversary may portray an ambulance to require the traffic light to cooperate with her/him and violate the driving right of other users.

Besides, privacy is another important issue in recent years. A driver may not want others to know her/his travelling routes by tracing messages sent by OBU. Otherwise, it is difficult to attract users to join the network. Therefore, an anonymous communication is needed. On the contrary, traceability is also required where a vehicle's real identity should be able to be revealed by a trust authority for liability issue when crimes or accidents happen. For example, a driver who sent out fake information causing an accident should not be able to escape by using an anonymous identity. In other words, vehicles in VANET need the conditional privacy.

3.2 Existing System

1) An adversary may modify or replay existing messages, even an adversary may diffuse or impersonate any legitimate vehicle to generate wrong information into the system to affect the behavior of other users or harm the infrastructure of VANET.
2) An adversary may trace the real identity of any vehicle and can reveal the vehicle's real identity by analyzing multiple messages sent by it. The proposing a scheme to prevent all these from happening.

Algorithm

AES (Advanced Encryption Standard)

Identity Based Batch Verification

Disadvantage

- Less Security in existing system
- limited range
- Information should be changed
- Easy to access the information
- Broadcast to duplicate information

3.3 Proposed System

1) TA is completely trusted by everyone and it is powered with sufficient computation and storage capability. The redundant TAs is installed to avoid being a bottleneck or a single point of failure.
2) TA is the only one that can determine the vehicle's real identity but not by others.
3) TA and RSUs communicate through a secure fixed network (e.g. Internet).
4) RSUs are not trusted. Since they are placed along roadside, they can be easily compromised. Also, they are curious about vehicle's privacy.

5) Tamper-proof devices on vehicles are assumed to be credible and its information is never been disclosed. Like the WAVE standard, each OBU is equipped with a hardware security module (HSM), which is a tamper-resistant module used to store the security materials (e.g., master keys). The HSM in each OBU is responsible for performing all the cryptographic operations such as signing messages, keys updating, etc. Thus, it is difficult for legitimate OBUs to extract their master keys from their tamper-proof devices. In addition, the device has its own clock for generating correct timestamp and is able to run on its own battery. TA, RSUs and OBUs have roughly synchronized clocks. This can be done easily by requiring TA to periodically broadcast the current time to all OBUs via RSUs.

Algorithm

Advanced Symmetric key

Novel Identity Based Batch Verification

Advantage

The batch verification process of the proposed IBV scheme needs only a constant number of pairing and point multiplication computations, independent of the number of message signatures. Therefore, the batch verification can dramatically decrease the time cost on verifying a large number of message signatures, which can achieve much better scalability. The security analysis shows that the proposed IBV scheme not only achieves the privacy preserving desired by vehicles and the traceability required by the trust authority, but also satisfies the security issues such as message authentication, integrity, non-repudiation, unlinkability, enforceability and replaying resistance.

Using Project Workspaces, you can customize the user interface for each asset by choosing the fields and list values that display for each project or group of projects. A project workspace will include settings for all configurable fields of all project assets.

Project workspaces may be created for any project. The root/system project always has a project workspace; this workspace may not be deleted. If a project does not define its own project workspace, then it will follow the nearest workspace defined in its parent project hierarchy. Therefore, creating a project workspace will affect the existing project and all child projects that do not define their own workspaces.

4. Modules and Description

4.1 On Board Unit

On-board units (OBUs), to communicate with roadside units (RSUs) located at roadside or street intersection. Vehicles can also use OBUs to communicate with each other. Such a communication network is referred to as vehicular ad hoc network (VANET). VANET can be classified into two types: vehicle-to-infrastructure (V2I) communication or inter-vehicle (V2V) communication. The basic application of VANET is that OBUs periodically broadcast information on their present states (e.g., the current time, position, direction, speed and traffic events) to other nearby vehicles and RSUs. For example, the traffic events could be accident location, brake light warning, change lane/merge traffic warning, emergency vehicle warning, etc. After that, other vehicles may change their travelling routers and RSUs may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. VANET offers various services and benefits to users, and thus deserves deployment efforts.

4.2. Road Side Unit

Message authentication: Any RSU should be able to verify that a message is indeed sent and signed by a certain legitimate vehicle without being modified or forged by anyone. Identity privacy preserving: The real identity of a vehicle should be kept anonymous from RSUs and other vehicles. Any third party should not be able to reveal the vehicle's real identity by analyzing multiple messages sent by it. Traceability: Although the vehicle's real identity should be hidden from RSUs and other vehicles, if necessary, TA should have the ability to retrieve the vehicle's real identity. In addition, once the malicious vehicle wants to escape from its guilty of causing the accident or crime, TA still enable to trace its real identity from its message sent under the proposed scheme. Non-repudiation: A malicious vehicle is unable to broadcast wrong messages to mislead an RSU and deny the behaviors when TA traces it by its message signatures. Unlink ability. A malicious vehicle or RSUs cannot successfully distinguish an anonymous entity by linking some of its message signatures. Replaying resistance: A malicious vehicle cannot collect and store a signed message and attempt to deliver it at a later time when the original message is invalid.

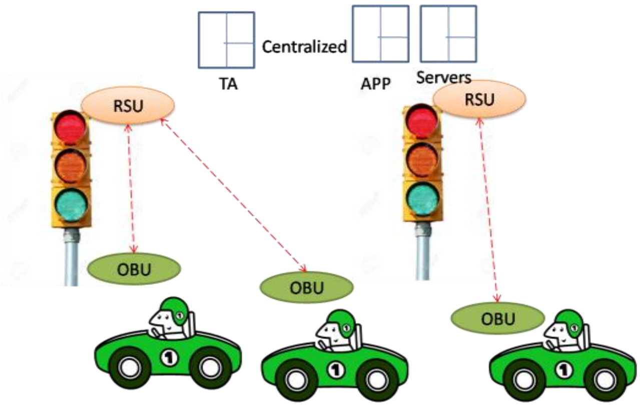

Fig1. VANET Architecture

4.3. Trusted Authority

Privacy is another important issue in recent years. A driver may not want others to know her/his travelling routes by tracing messages sent by OBU. Otherwise, it is difficult to attract users to join the network. Therefore, an anonymous communication is needed. On the contrary, traceability is also required where a vehicle's real identity should be able to be revealed by a trust authority for liability issue when crimes or accidents happen. For example, a driver who sent out fake information causing an accident should not be able to escape by using an anonymous identity. In other words, vehicles in VANET need the conditional privacy the vehicle related information has to be protected from malicious access, while the trust authority can reveal the sender if a dispute appears. The trust authority is capable of tracing a sender's real identity from its pseudo identity. Therefore, the conditional privacy can be achieved. IBV scheme is vulnerable on the replaying attack. An adversary may simulate a fake condition, such as traffic jam, by collecting and storing the vehicle messages and signatures in the corresponding condition. Next, the adversary can replay the information to mislead the traffic control center when she/he wants. IBV scheme does not satisfy the property of non-repudiation. A malicious vehicle can broadcast wrong information to mislead other vehicles and deny the behavior when the trust authority traces her/him by signature.

4.4 Implement Security Message transfer

Each vehicle is preloaded with a large number of anonymous public/private key pairs and the corresponding public key certificates. The conventional public key infrastructure (PKI) is adopted as the security foundation to achieve both message authentication and integrity. In addition, the vehicle takes advantage of a public/private key pair with a short lifetime to avoid movement tracking. However, the main problem is that each vehicle demands a large storage capacity to save a number of key pairs and the corresponding certificates, and incurs the high cost of message verification. The authority also needs to store all anonymous certificates of vehicles, which causes inefficiency for certificate management and is expensive for deployment. Besides, once a malicious message is detected, the authority has to exhaustedly look for in a huge database to find the real identity related with the compromised anonymous public key. a group public key and a private key are stored in the vehicle. The group public key is the same for all vehicles, and the private key of each vehicle is different. Any receiver only confirms the authenticity of the signature by the group public key, and the vehicle has no identity information of the message sender in the transmitted message. Despite decreasing the overhead of pre-loading a large number of anonymous key materials in each vehicle, this scheme increases a large computational overhead through its requirement to maintain a certificate revocation list. In addition, the length of group signature is much longer than one of ordinary signature, and the computational cost of verifying group signature is high.

4.5. Batch Verification

An identity-based batch verification (called IBV) scheme for V2I and V2V communications in VANET. They adopted a one-time identity-based signature, which eliminates the verification and transmission costs of certificate for public key. It reduces the overall verification delay of a batch of message signatures, and its batch verification process for signatures from multiple vehicles is much faster than that of other PKI-based schemes, the sender’s real identity can be traced or revealed by anyone who only holds the publicly known system parameters. Thus, their scheme does not achieve the requirement of privacy preserving. Second, a malicious vehicle broadcasts messages on behalf of another legitimate vehicle and even uses a fake identity to avoid being traced. For the above weaknesses, Lee and Lai’s IBV scheme is not secure and suitable for VANET. Moreover, their scheme also lost an advantage. The private keys cannot be generated offline by the temper-proof device. A vehicle cannot get a list of private keys along with the corresponding pseudo identities early. Some computation delays will be caused in the message signing process at the vehicle side. we introduce an enhancing security and privacy for IBV scheme. The proposed IBV scheme can not only support the efficiency of signing and verifying processes for V2I and V2V in VANET, but also withstand the above security threats.

5. Conclusion & Future Work

An efficient identity-based batch verification (NIBV) scheme for vehicle-to-infrastructure and inter-vehicle communications in vehicular ad hoc network (VANET). The batch-based verification for multiple message signatures is more efficient than one-by-one single verification when the receiver has to confirm a large number of messages In particular; the batch verification process of the proposed NIBV scheme needs only a constant number of pairing and point multiplication computations, independent of the number of message signatures. Therefore, the batch verification can dramatically decrease the time cost on verifying a large number of message signatures, which can achieve much better scalability.

The security analysis shows that the proposed IBV scheme not only achieves the privacy preserving desired by vehicles and the traceability required by the trust authority, but also satisfies the security issues such as message authentication, integrity, non-repudiation, unlink ability, un-forge ability and replaying resistance. Also prove that the proposed NIBV scheme is secure against existential forgery in the random oracle model under the computational Diffie-Hellman problem. In the performance analysis, we have evaluated the proposed NIBV scheme with other batch verification schemes in terms of computation delay and transmission overhead. Moreover, we verify the efficiency and practicality of the proposed *scheme by the simulation analysis. Simulation results* show that both the average message delay and message loss rate of the proposed IBV scheme are less than those of the existing schemes.

5.1 Future Work

In the future work, the efforts to enhance the features of IBV scheme for VANET, such as recognizing illegal signatures. When attackers send some invalid messages, the batch verification may lose its efficacy. This problem commonly accompanies other batch-based 4verification schemes. Therefore, thwarting the invalid signature problem is a challenging and a topic for study in our future research.

References

[1] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, "An identity-based ring signature scheme with enhanced privacy," in *Proceeding of Securecomm and Workshops*, 2006, pp. 1-5.

[2] X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442-3456, 2007.

[3] J. Sun, C. Zhang, and Y. Fang, "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks," in *Proceeding of IEEE Military Communications Conference* (*MILCOM '07*), pp. 1-7, 2007.

[4] X. Lin, R. Lu, C. Zhang, H. Zhu, P. H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 88-95, 2008.

[5] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of the 27th IEEE International Conference on Computer Communications* (*INFOCOM'08*), pp. 816-824, 2008.

[6] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transaction on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227-1239, 2010.

[7] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-add services in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248-262, 2011.

[8] T. W. Chim, S. M. Yiu, Lucas C.K. Hui, and O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189-203, 2011.

[9] C. Zhang, P. H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks*, vol. 17, no. 8, pp. 1851-1865, 2011.

[10] K. A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874-1883, 2012.