A SURVEY ON SECURE TRANSMISSION ON VECHICLES AND SIGNAL DEVICES

M.JEEVA
Shivani Engineering College
Trichy.
jeejo26@gmail.com

ABSTRACT: Vehicular ad hoc networks (VANETs) enable vehicles to communicate with each other but require efficient and robust routing protocols for their success. In this paper, it makes use of the infrastructure of roadside units (RSUs) to efficiently and reliably route packets in VANETs. In the vehicular adhoc networks operates vehicles to carry and forward messages from a source vehicle to a nearby RSU and, if needed, route this information through the RSU network and, finally send them from an RSU to the particular vehicle. Our system is mostly critical for users who are far apart and want to communicate using their vehicles' onboard units. Many current paradigms, like online networks, will greatly benefit from a system like ours to enable users on the road to exchange different types of data. It evaluates the performance of our system using the simulation process and compares our scheme to old solutions. The results improve the efficiency.

Index Terms—Vehicular networks, communication security, message authentication road side units.

1 INTRODUCTION

Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as

well as communication properties, protocols, data formats and concrete technologies. *(a) Line Parameter Management Including:* Determining QoS and cost parameters, comparing them with given requirements, notifying the user in case of problems and providing a set of alternatives.*(b) Caching:* Copying a certain amount of data (determined directly by the user or by predicted access probabilities) onto the mobile device, providing strategies for situations of simultaneous update or inconsistencies.*(c)Accounting:* Negotiating the costs of the usage of resources in foreign domain

2.LITERATRUESURVEY

2.1 DCS: AN EFFICIENT DISTRIBUTED CERTIFICATE SERVICE SCHEME FOR VEHICULAR NETWORKS

The scheme offers a flexible interoperability for certificate service in heterogeneous administrative authorities, and an efficient way for any OBUs to update its certificate from the available infrastructure RSU in a timely manner. OBU through the available RSUs on the roads. The centralized certificate update process in the classical PKI may be impractical in the large scale VANETs due to the following reasons: Each CA encounters a large number of certificate update requests which can render the CA a bottle-neck. The certificate update delay is long relative to the short V2I communication duration between the immobile RSUs and the highly mobile OBUs during which the new certificate should be delivered to the requesting OBU.

In the Efficient Conditional Privacy Preservation protocol for secure vehicular communications, which allows an OBU to get a short lifetime anonymous certificate from any RSU located in the domain in which the OBU was originally registered.

2.1.1Drawbacks

- The DCS scheme amplifies the capabilities of any entity in the network to simultaneously.
- To verify a relatively large number signatures.
- Certificates compared to the conventional verification method.

2.2 AN EFFICIENT PSEUDONYMOUS AUTHENTICATION SCHEME WITH STRONG PRIVACY PRESERVATION FOR VEHICULAR COMMUNICATIONS

The pseudonymous certificates issued by a legitimate RSU are valid in vehicular communication; PASS allows a vehicle to store a large set of pseudonymous certificates issued by the TA.PASS supports Roadside Unitsaideddistributed certificate service that allows the vehicles toupdate certificates on road, but the service overhead is almostrelated to the number of the updated certificates. Furthermore,PASS provides strong

privacy preservation to the vehicles sothat the adversaries cannot trace any vehicle even all RoadsideUnits have been compromised.

Based on the prxy re-signature cryptography technology where a semi-trusted proxy with given some information can turn a user's signature on a message into another user's signature on the same message, the vehicle only needs to request the re-signature keys from an RSU and re-sign numbers of the certificates issued by the TA to be as same as ones issued by the RSU itself. In this way, the service overhead is almost related to the number of the updated certificates. Although the RSUs act as certificate issuers in PASS, they don't know what certificates are held by a vehicle.

2.2.1 Drawbacks

- CRL is usually transmitted by vehicle-to-vehicle communication.
- Pseudonymous authentication schemes bring large communication cost.
- Larger the CRL size
- Longer the transmission delays to all vehicles.

2.3 CARAVAN: PROVIDING LOCATION PRIVACY FOR VANET

VANET is possible to locate and track a vehicle based on its transmissions, during communication with other vehicles or the road-side infrastructure. Types of tracking leads to threats on the location privacy of the vehicle's user.Problem of providing location privacy in VANET by allowing vehicles to prevent tracking of their broadcast communications. Based on these observations, in the propose a location privacy scheme called CARAVAN,

Injecting false datacompromised vehicle in the VANET can misbehave and broadcast incorrect data, with the malicious intent of attacking its neighboring vehicles. However, since each vehicle signs the broadcast safety messages.

2.3.1 Drawbacks

- Long range communication devices, for example. cellular network.
- Vehicle probe data may include vehicle identity, route segment identity, link time and location and any other data that can be measured and communicated by the vehicles
- The RSU sends probe data requests over a capture range.

2.4. SECURING VEHICULAR AD HOC NETWORKS

VANETs are an emerging research area. Currently, most of the research is focused on the development of a suitable MAC layer, as well as potential applications ranging from collision avoidance to onboard infotainment services. But both academia and the industry have so far largely overlooked the subject of security in VANETs, to later phases of research and development.

Safety-related applications: A collision avoidance and cooperative driving. For example, for lane merging. The common characteristic of this category is the relevance to life-critical situations where the existence of a service may prevent life-endangering accidents.

Other applications: Including traffic optimization, payment services toll collection, location-based services. Obviously, security is also required in this application category, especially in the case of payment services. The security aspects of safety-related applications are the most specific to the automotive domain and because they raise the most challenging problems.

2.4.1 Drawbacks

- To recomputed and redistribute a new key in the case of a leaving member.
- Protocols based on key trees may require the recomputation of only a subset of keys for both operations.
- The management of trees requires higher level of complexity.

2.5. PSEUDONYM CHANGING AT SOCIAL SPOTS: AN EFFECTIVE STRATEGY FOR LOCATION PRIVACY IN VANETS

As a prime target of Quality of Privacy in VANETs, location privacy is imperative for the full flourish of VANETs. Although frequent pseudonym changing provides a promising solution forlocation privacy in VANETs, the pseudonyms are changed in an improper time or location; such a solution may become invalid. By taking the ASS as the location privacy metric, then develop two anonymity set analytic models to quantitatively investigate the location privacy achieved by the PCS strategy.

The ASS asthe location privacy metric, we then develop two anonymity setanalytic models to quantitatively investigate the location privacyachieved by the PCS strategy.

2.5.1 Drawbacks

- In the urban areas, a large number of vehicles are running on the road every day.
- Each vehicle is equipped with an OBU device, which allows them to communicate with other.
- Vehicles for sharing local traffic information to improve the whole safety driving conditions.

5. METHODOLOGY

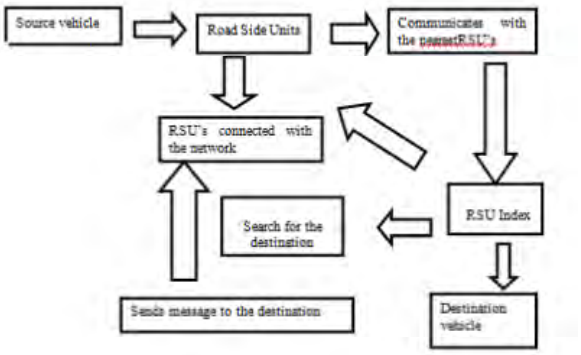

Figure 5.1 System Architecture

The system architecture, the source vehicle transmits the message to the destination vehicle. Using the Road Side units send the message to the destination vehicle and also communicate with the nearest RSU's. In the RSU Index used for search the vehicles.

6. CONCULSION

To present the deliver message, which is part of a complete system that are designing for providing car drivers and passengers pervasive access to needed data while on the road. The proposed system exploits the presence of RSUs to reduce the load on vehicles and to hide the complexity of getting the required data. The evaluation of delivering messages confirmed its effectiveness as compared to recent routing protocols. Ongoing work is focusing on devising secure mechanisms for registering users to the system of RSUs and designating them as proxies to Internet service providers that provide data to these users. A preliminary design and implementation of such mechanisms were published recently.

7. REFERENCE

[1] Albert Wasef and Xuemin (Sherman) Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks" IEEE transactions on Mobile computing, vol. 12, no.1, January2013.
[2] US Bureau of Transit Statistics ,http:// en.wikipedia.org/wiki/assenger_vehicles_in_theUnited _States,2012
[3] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets," IEEE Trans. Vehicular Technology, vol. 61,no. 1, p. 86-96, Jan. 2012.
[4] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl,"Privacy and Identity Management for Vehicular Communication Systems: A Position Paper," Proc Workshop Standards for Privacy in User- Centric Identity Management, July 2006.
[5] M. Raya and J.-P.Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.
[6] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K.Matsuura, and K. Sezaki"CARAVAN:Providing Location Privacy for VANET," Proc. Embedded Security in Car (ESCAR) Conf., Nov. 2005.
[7] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," EEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589- 3603, Sept. 2010.