ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 278 - 281 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

SFT: A Secure and Fast Transmission of Keys to Cooperative Group Communication and Key Management System

[1]Y.SHEILA, [2]Dr.P.HARINI
[1]II year M.Tech, St. Ann's College of Engineering & Technology, India, saec1259@rediffmail.com
[2]Professor and HOD dept. of CSE, St. Ann's College of Engineering & Technology, India, hpogadadanda@gmail.com

ABSTRACT

The problem of efficiently and securely broadcasting to a remote cooperative group occurs in many newly emerging networks. A major challenge in devising such systems is to overcome the obstacles of the potentially limited communication from the group to the sender, the unavailability of that of a fully trusted key generation center and the dynamics of the sender. Here the existing key management paradigms may cannot deal with these challenges effectively. A number of challenges such as efficient certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong dependence on tamper-proof devices arise in existing protocols for securing VANETs. Communication messages in vehicular ad hoc networks (VANET) can be used to locate and track vehicles. While here the tracking can also be beneficial for vehicle navigation, where it can also lead to threats on location privacy of vehicle user. In this paper, we are addressing the problem of mitigating unauthorized tracking of vehicles based on their broadcast communications, where to enhance the user location privacy in VANET. In this paper we propose a novel scheme for both secure and fast transmission of keys to cooperative groups

INTRODUCTION

IN many newly emerging networks, there is a need to broadcast to remote cooperative groups using encrypted transmission. Where the examples can be found in access control in remote group communication arising in wireless mesh networks (WMNs), mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), etc.

Vehicular ad hoc networks (VANETs) are an instance of mobile ad hoc networks that aim to enhance the safety and the efficiency of road traffic. VANETs have a number of distinguishing features and limitations that are related to the very nature of wireless communications and the rapid movement of the vehicles that are involved in those communications.

Compared with wired or other wireless networks, VANETs are very dynamic, and their communications are volatile. In such networks, nodes are vehicles that are equipped with communication devices known as on-board units (OBUs), and depending on the applications, OBUs are used to establish communications with other vehicles or roadside units (RSUs) such as traffic lights or traffic signs. The specific properties of VANETs allow the development of very attractive services such as the so-called comfort services that include traffic information, weather information, location of gas stations or restaurants, price information, and interactive communication such as Internet access.

Also, it is possible to offer safety services such as emergency warnings, lane changing assistance, intersection coordination, traffic-sign violation warnings, and also the road-condition warnings [1]. However, for those new services to make life easier rather than more difficult, they should rely on secure and privacy-preserving protocols that encourage users to participate without fear for their safety or personal privacy

WMNs have been recently suggested as a promising low cost approach to provide last-mile high-speed Internet access. Coming to this a typical WMN is a multi-hop hierarchical wireless network [1].

Where the top layer consists of high-speed wired Internet entry points. The second layer was totally made up of stationary mesh routers serving as a multi-hop backbone to connect to each other and Internet via long-range high-speed wireless techniques.

The bottom layer includes a large number of mobile network users. The end users can easily access the network either by a direct wireless link or through a chain of other peer users leading to a nearby mesh router; the router further connects to remote users through the wireless backbone and Internet. Here Security and privacy issues are of utmost concern in pushing the success of WMNs for their wide deployment and for supporting service oriented applications

A MANET is a system made up of wireless mobile nodes. These nodes which are having wireless communication and networking characteristics. MANETs which have been proposed to serve as an effective networking system facilitating data exchange between mobile devices even without fixed infrastructures.

In MANETs, it is very important for supporting the group-oriented applications, which comes under as audio/video conference and one-to-many data dissemination in battlefield or disaster rescue scenarios.the vehicle's real identity can be passed by the tracing manager (TM) with the help of secret member key also with the RSU,where the trust authority can be checked by the certificate of RSU with that of vehicle certificate too.

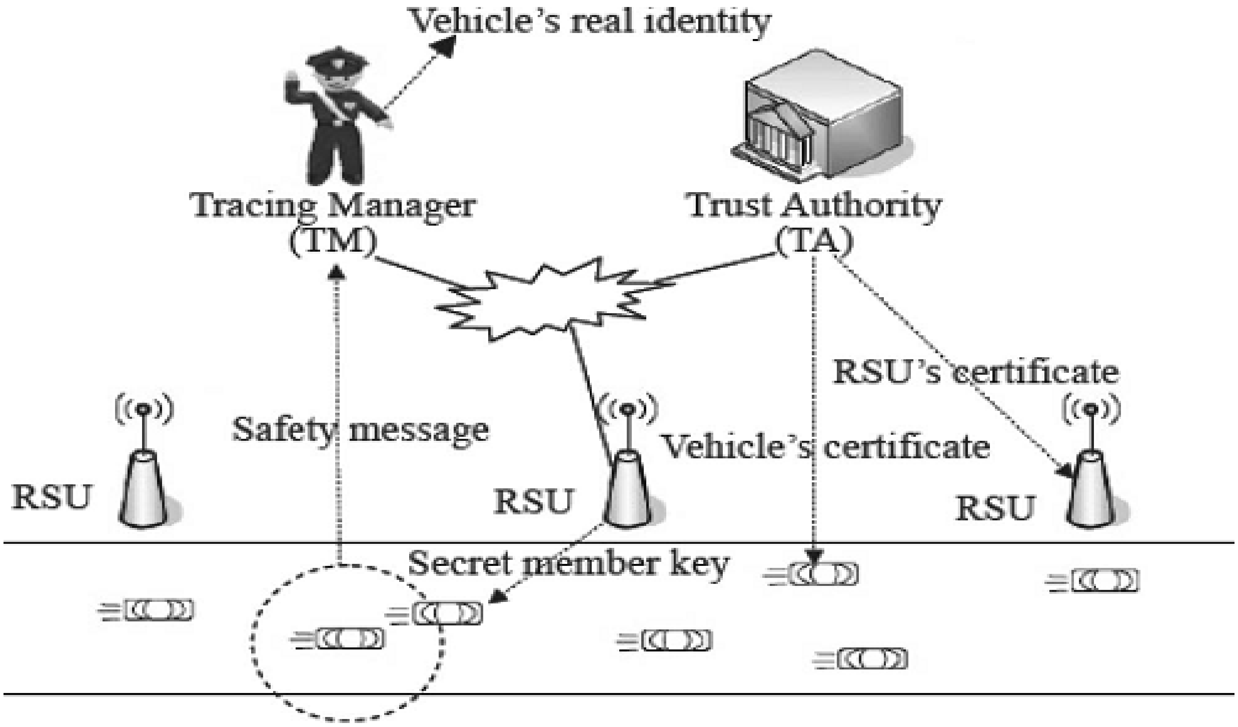

Fig1: Vehicular Network model

It consists of a TA, a tracing manager (TM), RSUs, and vehicles.

• TA: The responsibility of the TA is to issue digital certificates for vehicles and RSUs. Also, it maintains a CRL containing the certificates of revoked vehicles. The TA is assumed to be completely trustable, hard to compromise, and powerful, i.e., with sufficient computation and storage capacity.

• TM: When the content of a safety message broadcast by a vehicle is found to be false, the TM should be able to determine the vehicle's real identity.

• RSU: RSUs are densely distributed in the roadside. In our protocol, RSUs are used to issue secret member keys to vehicles and assist the TM to efficiently track the real identity of a vehicle from any safety message.

• Vehicle: Vehicles move along the roads, sharing collective environmental information contained in safety messages or requesting secret member keys from RSUs. OBUs are assumed to be embedded in each vehicle. By using OBUs, vehicles can communicate with each other as well as with the RSUs. The communication among them is based on the DSRC protocol.

RELATED WORK

Consequently, security and privacy are two critical concerns for the designers of VANETs that, if forgotten, might lead to the deployment of vulnerable VANETs. Unless proper measures are taken, a number of attacks could easily be conducted, namely, message content modification, identity theft, false information generation and propagation, etc. The following are examples of some specific attacks.

- If message integrity is not guaranteed, a malicious vehicle could modify the content of a message that is sent by another vehicle to affect the behavior of other vehicles. By doing so, the malicious vehicle could obtain many benefits while keeping its identity unknown. Moreover, here the vehicle that originally generated the message would be made responsible for the damage caused.
- If authentication is not provided properly, a malicious vehicle might impersonate an emergency vehicle to surpass speed limits without being sanctioned.
- A malicious vehicle could report a false emergency situation to obtain better driving conditions (e.g., deserted roads), and if non repudiation is not supported, it could not be sanctioned even if discovered.

After Analyzing above attacks, it becomes apparent that message authentication, integrity, and non-repudiation are primary requirements in VANETs. There is a need for mechanisms that provide VANETs with security, i.e., protocols, methods, and procedures that are able to detect whether a message has been modified by an attacker, determine who is the real sender of a message, and avoid identity theft Besides these essential security requirements, privacy is another important issue in VANETs that cannot be forgotten.

If the importance of privacy protection measures is underestimated, the privacy of VANET users could be endangered. For example, an eavesdropper could collect messages that are sent by vehicles and track their locations; by doing so, the eavesdropper could infer sensitive users' data such as their residence and their real identities [2]. Note that these privacy problems are similar to the ones of location-based services. Due to their extraordinary commercial and social potential, VANETs have attracted the attention of industry and academia.

PROPOSED METHOD

In this paper, we are presenting an encryption and decryption scheme to securitize the transmission and communication mechanism between group of vehicles and between vehicle and RSU. For encryption and decryption we use AES algorithm using some substitutions and linear transformations. And the process is encrypted and then broadcast it and only the subscribers who are having the public key can only decrypts the contents.

As the first commercial version of MANETs, VANETs are expected to be deployed in the near future. A VANET consists of on-board units (OBUs) embedded in vehicles serving as mobile computing nodes and road-side units (RSUs) working as the information infrastructure located in the critical points on the road. Mobile vehicles form many cooperative groups in their wireless communication range in the roads, and through roadside infrastructures, vehicles can access other networks such as Internet and satellite communication. VANETs are designed with the primary goal of improving traffic safety and the secondary goal of providing value-added services to vehicles

In our system, vehicles only request a new secret member key when 1) they pass by an RSU for the first time or 2) when their existing secret member keys expire. Since each vehicle only verifies messages from vehicles that have moved into the range of the same RSU and its neighbors, it can easily check whether the anonymous sender was revoked with the help of those RSUs and does not need to retrieve the revocation list from a remote centralized authority. This greatly reduces the certificate management overhead. Compared with the millions of vehicles in a VANET, the number of active vehicles within a range of a single RSU is much smaller. Hence, the system will not suffer from computation and communication bottlenecks. Although each party in our system needs a secret member key, the system's master key is only known and stored by a centralized authority, rather than being stored in each tamperproof device that is embedded in vehicle

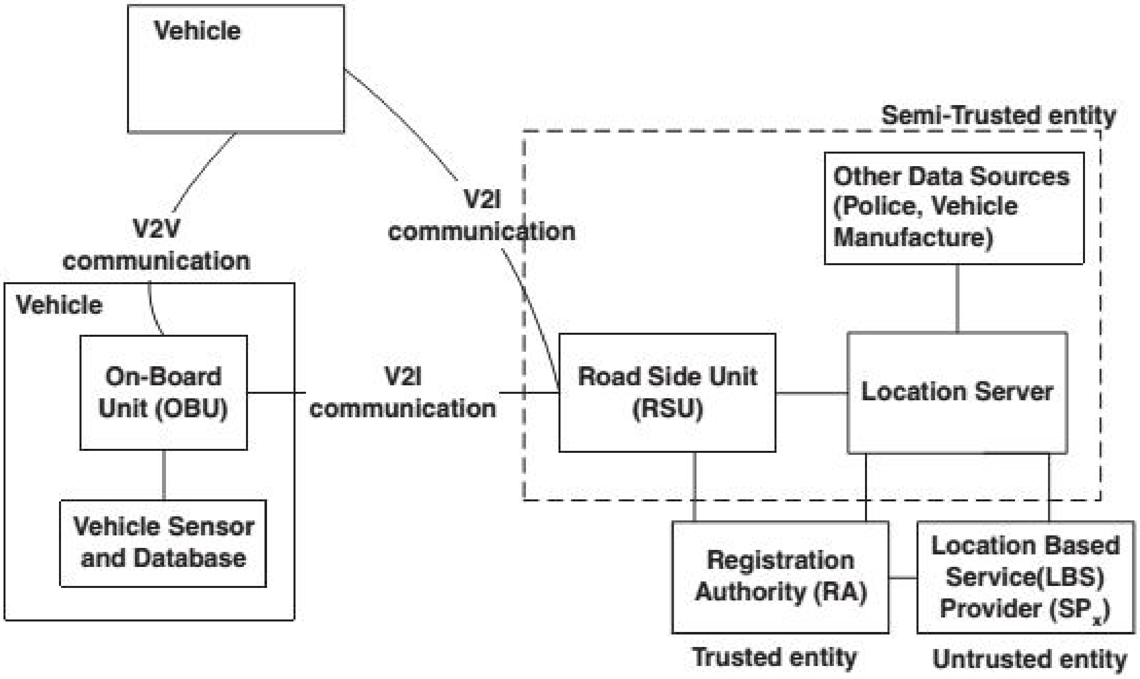

Fig2: Tamperproof device that is embedded in vehicle

A typical VANET that consists of vehicles, access points on the road side, and a collection of location servers. Vehicles move on roads, sharing collective environmental information between themselves, and with the servers via access points.

In this paper, we consider several security requirements

- **Confidential communication**. When a vehicle communicates with an RSU, only that vehicle and that RSU are aware of the information exchange. In our protocol, this implies that vehicles send a request to an RSU for a secret member key without being detected by other vehicles and secretly receive a secret member key from the RSU.

- **Message authentication**. If a message has been modified after being sent, this modification is observable by a legitimate receiver. In addition, if the message has never been modified, it confirms to the legitimate receiver that the message is from a legitimate entity.

- **Privacy protection**. As mentioned above, privacy is an important concern in VANETs. In this paper, we consider the following two cases .i.e.vehicle and RSU and vehicle and vehicle

- **Anonymity revocability**. The TM has the ability to retrieve the real identity of dishonest vehicles that are sending fake messages to other vehicles to disrupt traffic.

CONCLUSION

Finally we conclude that we addressed the location privacy threats and security threats that emerge in VANET due to unauthorized tracking of vehicles based on their broadcasts, as well as potential user privacy threats due to identification of LBS applications accessed from vehicle. For future work, we intend to use formal modeling as a methodology to verify security properties of the proposed group protocols

REFERENCES

[1] Y. Zhang and Y. Fang, "ARSA: An Attack-Resilient Security Architecture for Multi-Hop Wireless Mesh Networks," IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1916-1928, Oct. 2006.

[2] K. Ren, S. Yu, W. Lou and Y. Zhang, "PEACE: A Novel PrivacyEnhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 2, pp. 203-215, Feb. 2010.

[3] B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu and S. Guizani, "A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study,"IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 398-408, Jan. 2009.

[4] Y-M. Huang, C.-H. Yeh, T.-I. Wang and H.-C. Chao, "Constructing Secure Group Communication over Wireless Ad Hoc Networks Based on a Virtual Subnet Model,"IEEE Wireless Comm., vol. 14, no. 5, pp. 71-75, Oct. 2007.

[5] Q. Wu, J. Domingo-Ferrer and U. Gonz´ alez-Nicol´ as, "Balanced Trustworthiness, Safety and Privacy in Vehicle-to-vehicle Communications," IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559-573, Feb. 2010.

[6] L. Zhang, Q. Wu, A. Solanas and J. Domingo-Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications,"IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606 - 1617, May 2010.

[7] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET,"IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

[8] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System," inAdvances in Cryptology–EUROCRYPT'94, LNCS, vol. 950, pp. 275-286, 1995

AUTHORS:

Yendrapati Sheila Krupamai received the B.Tech degree in Information Technology from JNTU Kakinada, in 2012. & pursuing her M.Tech in Software Engineering from JNTU Kakinada.

Dr. P. Harini is presently working as a professor and HOD, Dept. of Computer Science and engineering, in St. Ann's College of Engineering and Technology, Chirala.She obtained Ph.D. in distributed and Mobile Computing from JNTUA, nanthapur. She Guided Many UG and PG Students. She has More than 18 Years of Excellence in Teaching and 2 Years of Industry Experience. She published more than 20 International Journals and 25 Research Oriented Papers in Various Areas. She was awarded Certificate of Merit by JNTUK, Kakinada on the University Formation Day on 21 - August - 2012.