Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1342 – 1345

RESEARCH ARTICLE

An Efficient Privacy Preserving Scheme for VANET

[1]BUVANESWARI GANESAN, [2]BENNET PRABHA, [3]MOHANA SUNDARI G

[1]Dept. of Computer Science, SRM University, India
[2]Dept. of Computer Science, SRM University, India
[3]Dept. of Computer Science, SRM University, India
[1] bhuvi.ganesan@gmail.com; [3] prathula.kanishka@gmail.com

Abstract—Vehicular AdHoc Networks (VANETs) scheme help to authenticate messages, identify the valid vehicles and Preserves the privacy of each vehicles.The Objective of PublicKeyInfrastructure (PKI) is to enable secure, convenient and acquisition of public keys and provide functionality using certificates. However, fixed public keys allow an eavesdropper to associate a key with a vehicle and a location, violating drivers' privacy .In this work we propose a VANET time stamped key management scheme based on Temporary Anonymous Certified Keys (TACKs) which replaces the time consuming CRL checking process. To reduce the message overhead substantially and to enhance the effectiveness of the message verification, BSpec's algorithm is used. Our scheme efficiently prevents malevolent vehicles from linking with different keys and provides timely revocation of misbehaving participants while maintaining the same or less overhead for vehicle-to-vehicle communication.

I. INTRODUCTION

In Vehicular Ad Hoc Networks (VANETs), vehicles are equipped with sensors and wireless communication devices, allowing vehicles to sense traffic and road conditions, and warn other nearby vehicles about potential emergency situations and traffic jams. VANETs present a promising approach to reduce the 43,000 traffic fatalities and $260 billion spent annually on traffic-related health care in the US [1], [2]. In addition to helping prevent accidents, VANETs also provide convenience and business services that will help improve a driver's experience [3].

In VANETs, a vehicle's *On Board Unit (OBU)* communicates with other vehicles' OBUs and fixed infrastructure called *Road Side Units (RSUs)*. For VANETs to operate securely and reliably, participants needs to validate received messages; otherwise, an attacker can easily inject bogus messages to disrupt the normal operation of VANETs. To allow authentication, we need to build key management mechanisms that allow senders to establish and update keys for security-sensitive operations. While RSUs can utilize traditional Public Key Infrastructure approaches, designing an OBU key management mechanism for secure VANET operation turns out to be a surprisingly intricate and challenging endeavor, because of multiple seemingly conflicting requirements. Recipients need to authenticate OBUs that they communicate

with; and road authorities would like to trace drivers that abuse the system. However, VANETs need to protect a driver's privacy. In particular, drivers may not wish to be tracked wherever they travel.

II. RELATED WORKS

A. *Distribution of Long-term Keys*

In the TACKs system, each valid OBU has a group user key that is unique to that OBU. This group user key is issued by a trusted group manager (M). This key is stored in the OBU and remains stable over a long period of time, e.g., between annual vehicle inspections. M first initializes the group signature scheme by calling the group key setup algorithm, to generate a group public key gpk and a group master key gmk. It publishes gpk and retains gmk itself. To issue a group user key, M generates the key (guk_i) and sends it to V_i . M also maintains a history of all key/OBU pairs it has issued, so that it can later trace misbehaving OBUs.

B. Authenticating Other OBUs

In VANETs, OBUs broadcast messages to communicate with each other. To allow OBUs to authenticate each other in a broadcast environment, a sender can sign each message using the sender's TACK private key K_S^{-1}, and periodically broadcast the RA signed certificate of its TACK public key K_S^{+}. Receivers know the time and the sender's region and the associated RAs, allowing verification that a valid RA certificate was used. A sender could use the TACK to bootstrap a more efficient broad-cast authentication mechanism (e.g., TESLA [4], [5]). The remainder of this section discusses how OBUs anonymously acquire certificates from RAs and how an authority can track and revoke misbehaving OBUs.

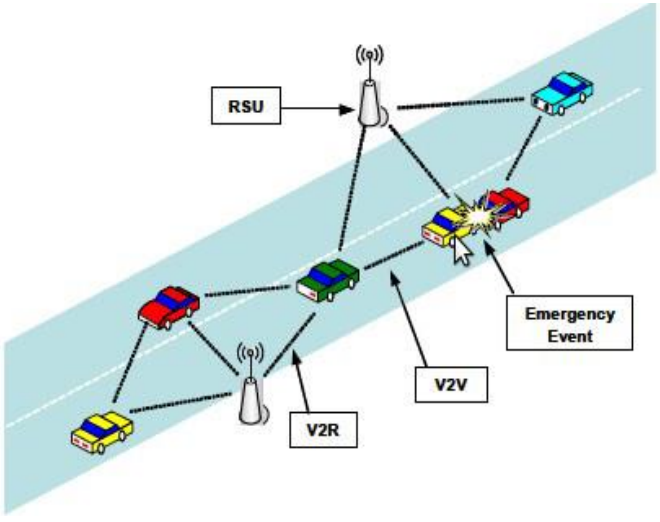
C. Tracking via Online Connections

When OBUs use cellular services to contact online RAs, the cellular provider can identify the source via the SIM card. During a certificate request, the cellular provider (and only the provider) can associate the public key and location with the SIM card. Such associations violate drivers' privacy, but cellular providers can already track users via emergency 911 services or other location specific services. Drivers will have to abandon cell phones in addition to VANETs to prevent tracking by cellular providers.

III. PROPOSED MODEL

In this section, we present an overview of our system architecture, assumption and algorithms that derive our design.

System architecture:



Sender Validity. When an OBU requests a certificate from an RA, the RA verifies the group signature and confirms that authorities have not revoked the OBU before returning a TACK certificate. There is a small window of time between when an OBU was revoked and when its TACK certificate expires that allows a revoked OBU to participate in the VANET.

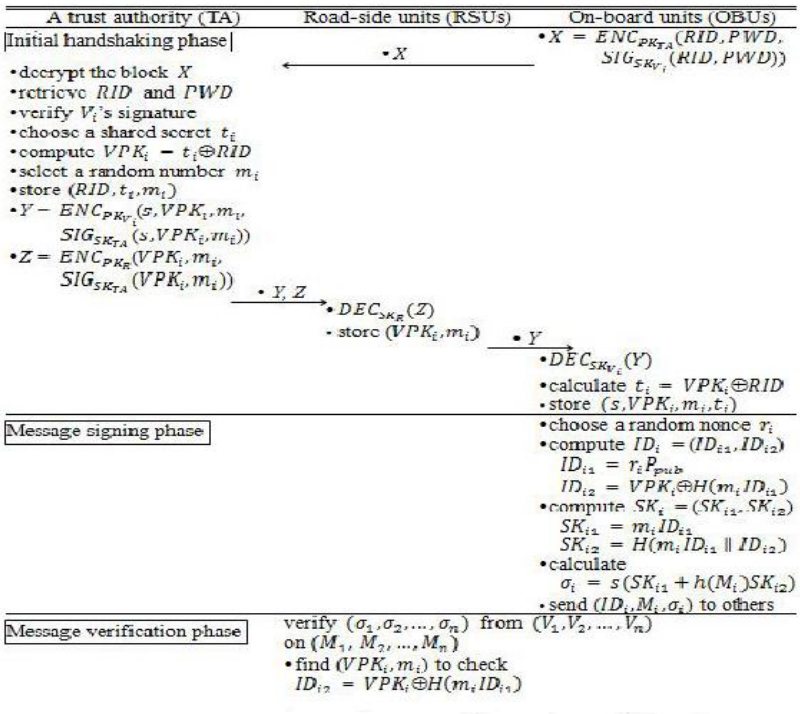
Message Integrity. Provided the underlying cryptography is secure, digital signatures generated using TACK private keys and appended to messages ensure message integrity.

Short-term linkability and Sybil prevention. As an OBU uses the same TACK over a short interval, any messages signed by that TACK can be linked to each other. A malicious OBU cannot perform a Sybil attack and impersonate arbitrarily many OBUs at the same time. As explained in Section IV-D, during a time epoch τ_i , an OBU can only obtain one TACK certificate from an RA for a region.

An attacker who has acquired long-term private keys from multiple OBUs may request multiple TACK certificates from an RA. However, this is equivalent to multiple conspiring vehicles since there still is a one-to-one correspondence between keys and vehicles. In addition, an attacker may request certificates from multiple RAs where each RA controls a different region. However, such an attacker's damage is limited, as the attacker can only use a TACK in its corresponding region.

Long-term unlinkability. To protect drivers' privacy, we require that messages sent by the same vehicle be unlinkable in the long-run. Group signatures and region-based certificates provide long-term unlinkability in TACKs.

BSPECs Algorithm



IV. CONCLUSION

In this work, we presented Temporary Anonymous Certified Keys (TACKs) as an efficient way to fulfill the security and privacy properties necessary for key management in Vehicular Ad Hoc Networks (VANETs). In TACKs, On-Board Units (OBUs) use short-lived keys to sign messages used for VANET communication. These short-lived keys are certified by Regional Authorities (RAs). During key updates, RAs verify that the requesting OBU is a legitimate OBU that has not been revoked; however, the RAs do not learn the OBU's identity. This allows a valid OBU to acquire a certificate for a temporary key and preserve the OBU's privacy. Since RAs' certificates are only valid in their local region, OBUs must update keys upon entering a new region. When a set of OBUs enters the region, all of the OBUs update keys simultaneously, preventing eavesdroppers from tracking drivers across key

changes. If a message is identified as an abuse of the VANET, authorities can trace the certificate request back to the signer. The authorities can revoke the misbehaving OBU so that it is no longer able to participate in the VANET.

REFERENCES

[1] Albert Wasef and Xuemin (Sherman) Shen, IEEE, Fellow " EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks" IEEE JANUARY 2013

[2] J.Duffy . U.S. pitches wireless highway safety plan.Network World,Nov 2005

[3] National Highhway Traffic Safety Administration 2005 state traffic data. http://www-nrd-nhtsa.dot.gov/pdf/nrd-30/NCSA/TSF2005State trafficData05.pdf,sept 2006

[4] F. Bai, T. Elbatt, G. Hollan, H. Krishnan, and V. Sadekar. Towards characterizing and classifying communication-based automotive applica-tions from a wireless networking perspective. In Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet), Dec. 2006.

[5] Y.-C. Hu and K. P. Laberteaux. Strong VANET security on a budget. In Proceedings of Workshop on Embedded Security in Cars (ESCAR), 2006.

[6] J.-P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. IEEE Security & Privacy magazine, 2(3):49–55, 2004

[7] A. Perrig, R. Canetti, J. D. Tygar, and D. Song. The TESLA broadcast authentication protocol. RSA CryptoBytes, 5(Summer), 2002.

