Distributed Sybil Attack Detection in VANET

Reza Mortazavi
Department of Electrical and Computer Engineering,
Tarbiat Modares University
P.O. Box 14155-4838, Tehran, Iran

Maryam Rahbari
Department of Mathematics and Computer Science,
Damghan University

ABSTRACT

Security and Privacy are among the most important concerns in Vehicular Ad-hoc Networks (VANET). Widely accepted privacy preserving communication scheme in VANETcommunity -that is using pseudonyms –has left open doors for some security problems such as Sybil attack. In this paper, we have proposed an efficient approach detecting this attack while preserving privacy of vehicles in the network.

General Terms

Network Security, Ad-hoc Networks

Keywords

Sybil attack, Privacy Preserving, VANET, *Pseudonyms*.

1. INTRODUCTION

VANET is the most known and near to be realizedAd-hoc networks comprising of vehicles as mobile nodes. It is the most important component of Intelligent Transportation System (ITS)[1] in which vehicles act as network nodes and routers and communicate in the ad-hoc manner.The main motive behind VANET is safety on roads. Although many promising safety and entertainment applications are proposed for VANET[2, 3], security and privacy issues remain as concerns. For example, because people usually use their own cars as their proprietaries,it is reasonable the existence of ahigh correlation between a personal car trajectory and its owner private places like home or office.One of the most accepted solutionsfor the problem is to use *pseudonyms*, within which a vehicle *V* is filled with a large number of legal and falsenames, so called *pseudonyms*. These namesare public keys certified by a *Certification Authority (CA)* without any obvious relation between them and real identity of *V*.Each *pseudonym* is used for at most a short period of time and then is discarded. Only *CA* as a trustedcenter knows the exact corresponding real identity for a pseudonym that can be used in case of dispute.

A malicious or misbehaving node can use these certified *pseudonyms* and pretend to be multiple. For example, an attacker can use these legal almost untraceable keys and change the density of traffic for his own profit. This attack in VANET settings is named Sybil attack. Between solutions proposed mitigating the problem[4-6], the most recent one is [7]. However, their approach is not fast enough and may result in an extensive privacy invasion if only one *Road Side Units* (*RSU*) is compromised.In this paper, we propose an efficient approach which can be implemented in a fully distributed manner without privacy breaches problem.

The remainder sections of this paper are as follows. In section 2 the approach used in [7] is introduced briefly. Section 3 explains how an attacker can misuse the approach and invade identity privacy of vehicles. Following, section 4 introduces ourapproach and proves all security requirements are met. Finally, section 5 is devoted to conclusions and future works.

2. P2DAP APPROACH

Tong Zhou et al. [7] have presented a distributed approach in which *RSU* can detect Sybil attacks in conjunction with *CA*,named as Privacy Preserving Detection of Abuses of Pseudonyms (P2DAP). For this purpose, they have suggested to assign*pseudonyms* using a two (or more) –stage approach. After producing a *pseudonymp*, the *CA*[1]applies a hash function $h_{k_c}(p)$, where k_c is a global key known by (semi-)trusted authorities. The results of the function for all *pseudonyms* are classified in coarse-grained groups based on collision on some predefined bits.Then all *pseudonyms* in a group are applied another hash function $H_{k_f}(p)$ where k_f is a secret key known only to*CA*. Again all p in the same subgroup after applying $H_{k_f}(.)$, are classified based on some predefined bits. Then all *pseudonyms* in the same subgroup along with their certificated are assigned to a vehicle.By repeating the above process, large enough number of initial *pseudonyms*is provided and all vehicles can be filled with the desired number of *pseudonyms.* The real identity of the vehicle together with the value of predefined bits for it, is saved that can be used later for tracing purposes. Using hash functions in this scheme results in a considerable space and computation reduction required for *CA* mapping a *pseudonym* to real identity of a vehicle.

The global key k_c is distributed between all *RSU*s. Each *RSU* overhears all the events in communication range produced by vehicles. All the events related to the same time and location, are collected in a list. Any considerable[2]collision after applying h_{k_c}on *pseudonyms* of

[1] Or equally Department of Motor Vehicle (DMV)

[2] Regarding the predefined set of bits in the first level of initialization stage

message senders in a list$L$is a potential Sybil attack and is reported to *CA*for more investigation. Upon receiving such L, the *CA* will apply$h_{k_c}$and then h_{k_f} on received *pseudonyms* and if all (or considerable amounts) of them fallinto the same group, it is Sybil attack and revocation process for misbehaving nodestarts.

This approach for Sybil attack detection can be improved using more levels in initialization step and equipping *RSU*s by more global keys to reduce false alarms in heavy traffic roads. Such key distribution must consider nearby traffic pattern and load to distributed keys. It is notable that in this plan, *RSU*s are supposed as semi-trusted entities and their knowledge of real mapping is limited. Another improvement is related to shortening validity of pseudonyms' lifetime to a period of τ at which only limited set of pseudonyms are allowed to be used. This results in reducing the effects of privacy attacks and increasing associated cost of attack.

3. PRIVACY AND SECURITY ATTACKS IN P2DAP

It is possible for an attacker to compromise an*RSU* and catch its keys for Sybil attack detection and use them in a low traffic road to correlate messages from vehicles. The authors in [7]suggested to use short-period keys to mitigate the results of such attacks. We believe this is not sufficient, and an irrational attacker can compromise *RSU*s in any time and use it all over the network area. Neither other *pseudonym* distribution scheme nor more adaptive and intelligent key assignment plans to *RSU*s may resolve the problem, because all vehicles use the same *pseudonyms*all over the network.

Another security related problem of the plan is about the required time for the communication between *RSU*sand *CA*. As the authors report based on simulation results, this may last for more than 45 seconds. In case of more attackers, the results will be worse and average detection delay is more than 100 seconds. This time is sufficient for attackers to reshape the traffic pattern of a heavy loaded highway or probably a studied traffic jam as a perquisite to launch metropolitan wide attacks. This type of attack, related to time consuming communications between *RSU*s and CA,is a direct result of untrustworthiness viewpoint to distributed *RSU*s and is strongly related to the first problem above.

4. HBSCG SCHEME

In this section, we introduce our novel proposal to detect Sybil attack named as Homomorphism-Based Signature and Certificate Generation (HBSCG). To our knowledge, this is the first proposal the signatures and certificates of VANET nodes are generated on the fly based on *RSA* homomorphism. Then we analyze and prove that all the security requirements are satisfied.

4.1 Generating Certificates on the fly

In our scheme,fewerprivate and public key pairsas *pseudonyms*are required for a vehicle to communicate privately, because new ones can be generated by the vehicle itself. Each vehicle $v$in a session uses a message format as below to communicate:

$$m, \sigma_{f(k_v^i)}(m), F(K_v^i), cert_{CA}(F(K_v^i)), r'^{e'}, r'r\ , r'K_v^i$$

where m is the message payload, $\sigma_{k_v^i}(m)$denotingthe signature of $m$using i-th private key of v – that is k_v^i, K_v^i is corresponding i-th public *pseudonym* together with its certificate from *CA*.$f$and F are defined as linear functions on private and public key pairs as input respectively in such a way that $f\left(k_v^i\right).F\left(K_v^i\right) = k_v^i.K_v^i\ (mod\ \phi(N))$, where N denotes the modulus in RSA scheme.$r, r' \in_r \mathbb{Z}$are selected by the vehicle for each communication session. The message payload$m$must have enough embedded redundancy that can be easily distinguished from a randomly generated message.

In this paper, we define $F\left(K_v^i\right) = r^{e_{CA}e'}.K_v^i\ (mod\ N)$, and $f\left(k_v^i\right) = (r^{e_{CA}e'})^{-1}.k_v^i\ (mod\ N)$where e_{CA} and e' are public keys of *CA*and nearby *RSU*,respectively[3]. Thanks to multiplicative homomorphismof RSA algorithm, we can easily calculate $cert_{CA}\left(F\left(K_v^i\right)\right)$ as below:

$$\begin{aligned} cert_{CA}\left(F\left(K_v^i\right)\right) &= cert_{CA}\left(r^{e_{CA}e'}K_v^i\right) = (r^{e_{CA}e'}K_v^i)^{d_{CA}} \\ &= r^{e'}.cert\left(K_v^i\right)(mod\ N) \end{aligned}$$

where $d_{CA}$is the private key of *CA*.The value of $cert(K_v^i)$is preloaded by the *CA* in initialization step.Upon receiving the message, a vehicle v' can verify its integrity and correctness using the signature, related certificate, and embedded redundancy.

It is notable that other vehicles cannot extract K_v^i, $cert(K_v^i)$ because r is selected randomly. However nearby *RSU*overhears all in range messages andcan calculate $r$and K_v^i as below:

$$r' = \left(r'^{e'}\right)^{d'}(mod\ N)$$

$$r = r'r * r'^{-1}(mod\ N)$$

$$K_v^i = r'K_v^i * r'^{-1}(mod\ N).$$

In addition to all steps regular nodes do to verify the message, overhearing *RSU* also checks if other parts of the message are reported correctly or not. In case of an integrity problem, a warning message is broadcast throughout the whole area in the range and a revocation step is requested from the *CA*based on the evidence collected. It is notable that the vehicles' keys are stored in the *On-Board Unit*(*OBU*) of the vehicle using tamper-proof hardware technology.As in[8-10], thistamper-proof hardware, which is also called trusted component, has protected storage for secrets and can performcryptographic operations.

In this schema, we have supposed all *RSU*s are semi-trusted and allowed to know the real *pseudonyms* of vehicles, but not the exact relationship of a vehicle's public and private keys.

[3] Public keys of *RSU*s along with their location on network map are stored on the vehicle.

4.2 Security Requirements

In this section, we show that all security requirements for VANET communication are met in our scheme.

1) **Reliability**: if a vehicle accepts an event, the report must be signed by a legitimate source. The message integrity and redundancy ensure the trustfulness of the sender for the receiver. In case of internal attack, it can be traced based on the collected evidence.
2) **Privacy**: Each vehicle changes its pseudonym on a regular basis, and no other node can link two messages from the same vehicle. An*RSU* as a semi-trusted entity in the network is able to link two messages of a vehicle on an event to some degree of certainty, but the exact correspondence of *pseudonyms* and real identity of a vehicle is only known to *CA*.
3) **Misbehavior Nodes Detection**: As mentioned above, a node is allowed to use multiple legal *pseudonyms* to sign its messages.However faulty or misbehaving nodes misuse this opportunity as in Sybil attack. The proposed scheme can detect such nodes in a fully distributed and hierarchal manner. If number of same reported events in the communication range of an*RSU* is more than a security threshold and applying h_{k_c}on the corresponding pseudonym sender collides on the predefined bits, this is a possible Sybil attack and is reported to *CA* for further investigations. HBSCG outperforms P2DAP by limiting attackers' ability to misuse *pseudonyms*. If attackers in a region compromise an*RSU*, they are unable to use the global private keys from compromised *RSU* out of the region, because all communications are encrypted by public keys of related *RSUs*.

5. CONCLUSION AND FUTURE WORKS

In this paper, we proposed a fully distributed and hierarchal scheme in which all security requirements of VANET communication are met. The proposal is more efficient and robust against possible attacks regarding other similar plans. Scope of attackers is much limited, and a global privacy attack is almost infeasible. Extending our proposal to other communication areas of VANET is intended as our future works.

6. REFERENCES

[1] Akyildiz, I.F., et al., *A survey on sensor networks.* Communications Magazine, IEEE, 2002. **40**(8): p. 102-114.

[2] Lee, U., et al., *Dissemination and harvesting of urban data using vehicular sensing platforms.* Vehicular Technology, IEEE Transactions on, 2009. **58**(2): p. 882-901.

[3] Gerla, M. and M. Gruteser, *Vehicular Networks: Applications, Protocols, and Testbeds.* Emerging Wireless Technologies and the Future Mobile Internet, 2011: p. 201.

[4] Guette, G. and B. Ducourthial. *On the Sybil attack detection in VANET*. 2007: IEEE.

[5] Bouassida, M.S., et al., *Sybil nodes detection based on received signal strength variations within vanet.* International Journal of Network Security, 2009. **9**(1): p. 22–32.

[6] Grover, J., M.S. Gaur, and V. Laxmi. *A novel defense mechanism against sybil attacks in VANET*. 2010: ACM.

[7] Zhou, T., et al., *P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks.* Selected Areas in Communications, IEEE Journal on, 2011. **29**(3): p. 582-594.

[8] Kounga, G., T. Walter, and S. Lachmund, *Proving reliability of anonymous information in VANETs.* Vehicular Technology, IEEE Transactions on, 2009. **58**(6): p. 2977-2989.

[9] Papadimitratos, P., V. Gligor, and J.P. Hubaux. *Securing vehicular communications-assumptions, requirements, and principles*. 2006: Citeseer.

[10] Papadimitratos, P., et al. *Architecture for secure and private vehicular communications*: IEEE.