International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

SIGNRECRYPTING PROXY RE-SIGNATURE IN SECURE VANET

C. Suncia Ashrine [1], M. Thurai Pandian[2]

[1]PG Student, Department of CSE, Lord Jagannath College of Engineering and Technology, Tamil Nadu, India
[2]Associate Professor, Department of CSE, Lord Jagannath College of Engineering and Technology, Tamil Nadu, India

---

Abstract - *Vehicular Ad hoc Network is an emerging area as a key component of the intelligent transport system. Despite the immense researches going on in this area, it is yet to be deployed at its full scale due to lack of trust, safety, and condentiality in the network. Moreover, the security algorithms proposed till now are complex, and calculations involved are difficult to be completed within the strict real-time constraints. This paper introduces the SignReCrypting Proxy Re-signature scheme, which reduces the time taken for encryption at sender side as well as for decryption at receiver side. Signcryption reduces the computation cost by converting two steps of signature and encryption into one, whereas re-encryption and re-signature enable Alice to decrypt and sign a message on behalf of Bob. These three terminologies altogether with group signature make the proposed algorithm robust, secure, and efficient. The compromised vehicle is revoked from group using dynamic accumulators, and security is verified using automated validation of Internet security protocols and applications.*

***Key Words*: AVISPA, dynamic accumulator, group signature, proxy re-encryption, proxy re-signature, signcryption, VANET.**

1. INTRODUCTION

Even after several advancements in vehicular technology, road accidents and immense traffic are inevitable fate of the common folks travelling via roadways. Inexperienced driving may not necessarily be the cause; bad weather conditions, health related issues and other uncontrollable situations may cause serious vehicle crashing [1]. The increasing cases of smog in leading cities of world, where drivers are not able to see what lies ahead of them, are very distressing. To control these in an automated way, Vehicular Ad-hoc Network (VANET) is a popular technology in which automobiles can communicate with each other to avoid collisions and jams. Based on the routing scheme used in network, vehicles may send messages only to vehicles/RSUs ahead of them ignoring the behind ones or may communicate only with pre-declared authenticated members e.g., in a group. Whatever the routing technique or channel selecting criteria is, examining it on network before deployment is a necessary overhead, to avoid any unknown interference. Since vehicles need to communicate in real time, even a single minute delay in message delivery is not permissible.

1.1 Cloud Computing

Cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics, intelligence and more over the Internet ("the cloud") to offer faster innovation, flexible resources and economies of scale. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently and scale as your business needs change.

2. PROBLEM DEFINITION

Signcryption is the hot topic since it was introduced in 1997 by Zheng [2]. The clear reduction in computation cost as well as message expansion was shown by the author. According to the paper, the expanded bits added to an original message because of the signature can be shrunk to almost 90% if we use the signcryption technique which also saves 50% of the computation and transmission time invested on that particular message. Later, the prospect diverted from simple composition of encryption with signature to breeding the same with already successful techniques in various areas.

The first ever SignRecryption was mentioned in 2006 by Ateniese et al. Although the proposal was to provide security extension to the original re-encryption scheme given by Blaze, Bleumer, and Strauss (BBS) , signcryption drew many scholar's attention, for which they even got their patent published in the year 2012 . They advanced their research with unidirectional identity based re-encryption, overcoming the BBS's bidirectional perspective, in which the identity of a node can be converted to identity of another node with the help of an authenticated proxy.

3. PROPOSED WORK

In this paper, A signcryption technique along with re-encryption and re-signature schemes, called as SRCPR, stands for SignReCrypting Proxy Re-signature which starts with key generation, followed by vehicle registration, signcryption, message verification at the receiver end, and then decryption. In the system setup phase, CC first selects its master private key and public parameters, computes the corresponding public key, and publishes its public key and public parameters. In the VC registration phase, VCj submits its identity, which serves as the public key, and obtains the corresponding private key generated by CC. In the user registration phase, CC issues a smart card to Ui. In the phase

of authentication between Ui and CC, the SS-3FAKA protocol is executed between Ui and CC. Ui can request a service ticket from CC through the established secure channel in the ticket request phase. In the phase of authentication between Ui and VCj, Ui presents the ticket to VCj to establish a secure channel between Ui and VCj. Finally, the password change and smart card revocation phases can be invoked to change the user password and revoke a lost/stolen smart card without the demand for user identity changing.

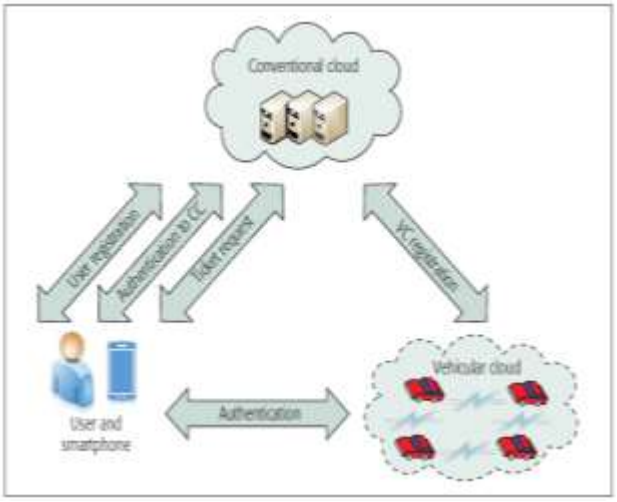

Fig -1: Proposed AKA framework

3.1 User Registration

In this phase, the operations are the same as those in SS-3FAKA.Reg. MM broadcasts its public key in the network, in a fixed period of time. Whenever any vehicle enters in the network, it needs to send its identification details requesting membership registration

3.2 Authentication between User and CC

In this phase, the operations are the same as those in SS-3FAKA.Auth, and the session keys kCC is shared between Ui and CC after the operations.

3.3 Ticket Request

After Ui has been authenticated by CC, Ui can request a ticket from VCj through a secure channel.
Step 1: Ui first sends a ticket request MSG3=<IDi, IDVCj> to CC.
Step 2: Upon receiving the request, CC generates a temporary key tkVCj, defines the validity period of the ticket lifetime, and Ticket VCj= {tkVCj, IDi, lifetime}shkVCj, and sendsMSG4 = <tkVCj, IDVCj, lifetime, Ticket VCj> to Ui. Here, {M}K denotes the cipher text of message M encrypted by a key K.

3.4 Authentication between User and VC

Ui can authenticate VCj using the obtained ticket :

Step 1: Ui generates a one-time random numbernonce1 and computes M1 = h(nonce1||tkVCj)and sends VCj the ticket authentication request MSG5 = <Ticket VCj, nonce1, M1>.
Step 2: VCj decrypts the ticket to obtain(tk'VCj, IDi, lifetime). VCj first verifies whether the ticket is valid. If it is expired, VCj rejects the authentication request; otherwise, it computesM'1 = h(nonce1||tk'VCj). If M'1 = M1,VCj aborts this session; otherwise, Ui is authorized to access its resources and services. VCj generates a nonce nonce2, computes M2= h(nonce1||nonce2||tk'VCj) and the session key skVCj = h(tk'VCj||nonce1||nonce2), and sends the message MSG6 = <nonce2, M2> toUi.
Step 3: Ui computes M'2 = h(nonce1||nonce2||tkVCj). If M'2 = M2, Ui computes skVCj =h(tkVCj||nonce1||nonce2), which is the session key between Ui and VCj; otherwise, Ui terminates this session.
The subsequent phases (i.e., password and biometric change and revocation and re-registration)are the same as those in the SS-3FAKA protocol.

4. RESULTS

Fig -2: Vehicle Registration Page

Fig -3: RSU upload a file

Fig -4: Vehicle(user) Register with a RSU

Fig -5: RSU sends the Request to Admin

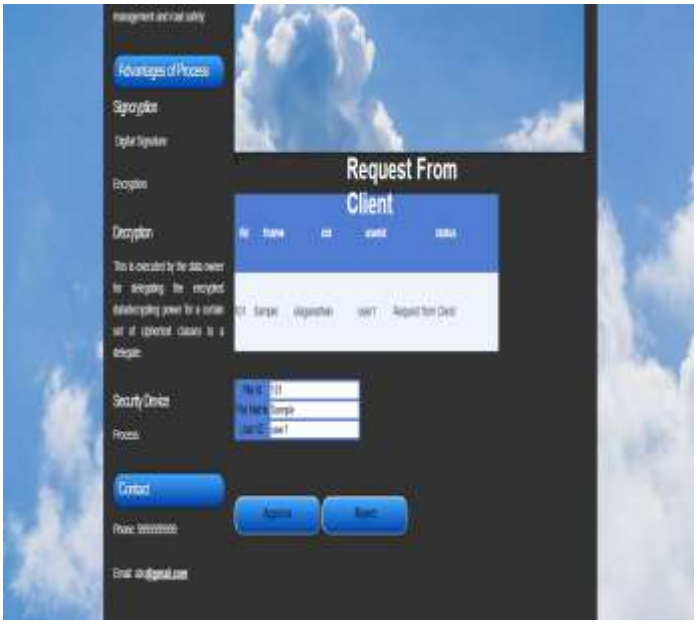

Fig -6: Admin Send the Approval to RSU

Fig -7: File Download

Table -1: Comparison between Proposed and Existing System

Keys for Comparison	SHA	MD5
Security	High secure than MD5	Less secure than SHA
Message Digest Length	160 bits	128 bits
Attacks required to find out Original Message	2^{160} bit operations required to break	2^{128} bit operations required to break
Attacks to try and find two messages producing the same MD	2^{80} bit operations required to break	2^{64} bit operations required to break
Speed	Slower than MD%, Required 80 iterations	Faster, only 64 iterations
Successful attacks so far	No such attack report yet	Attacks reported to some extents

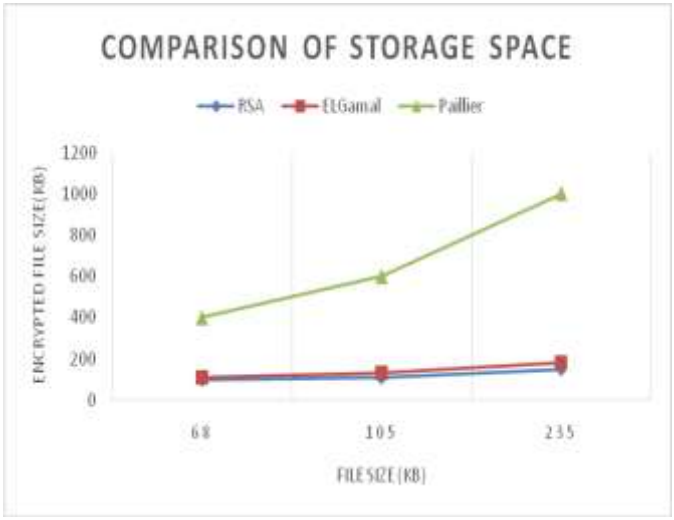

Chart -1: Comparison of RSA required file size with other methods

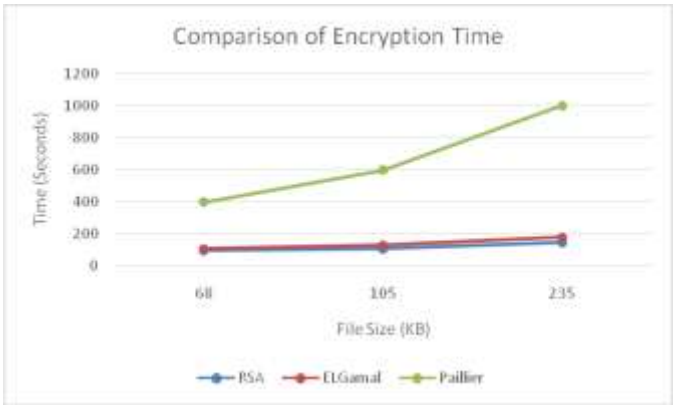

Chart -2: Comparison of RSA computational time with other methods

4. CONCLUSIONS

This project introduces the architecture of VCC and presented the challenges of designing the efficient AKA protocol in VCC to secure the interactions between users and VCs. It proposed an integrated AKA framework that caters for the scalability and flexibility required in VCC. The framework can support single sign-on, such that a user is able to securely access multiple VCs without registering with each VC repeatedly.

The performance analysis demonstrates that the proposed framework provides firm security while ensuring acceptable computational cost and low communication overhead.

REFERENCES

[1] A. H. A. Hanan, M. Y. Idris, O. Kaiwartya, M. Prasad, and R. R. Shah, ``Real traffic-data based evaluation of vehicular traffic environment and state-of-the-art with future issues in location-centric data dissemination for VANETs,'' Digit. Communication. Network., vol. 3, no. 3, pp. 195 210, 2017.

[2] Y. Zheng, ``Digital signcryption or how to achieve cost (signature & encryption)cost(signature)C cost(encryption),'' in Proc. Annu. Int. Cryptol. Conf., 1997, pp. 165 179.

[3] S. Kanchan, G. Singh, and N. S. Chaudhari, ``Re-encrypting secure and efficient routing in VANET groups using sharable clouds,'' in Proc. IEEE 4th Int. Conf. Recent Adv. Inf. Technol. (RAIT), Mar. 2018, pp. 16.

[4] J. Zhang and X. A. Wang, ``Non-transitive bidirectional proxy re-encryption scheme,'' in Proc. IEEE Int. Conf. Netw. Digit. Soc., vol. 1, May 2009, pp. 213 216.

[5] G. Ateniese and S. Hohenberger, ``Proxy re-signatures: New definitions, algorithms, and applications,'' in Proc. 12th ACMConf. Comput. Commun. Secur., 2005, pp. 310–319.

[6] C.-L. Chen, Y.-F. Lin, A. Castiglione, and F. Palmieri, ``A secure payment system for multimedia on demand on mobile VANET clouds,'' Secure. Commun. Network, vol. 9, no. 17, pp. 4378–4390, 2016.

[7] C. Sur, Y. Park, and K. H. Rhee, ``An efficient and secure navigation protocol based on vehicular cloud,'' Int. J. Comput. Math., vol. 93, no. 2, pp. 325344, 2016.

[8] J. Ni, A. Zhang, X. Lin, and X. S. Shen, ``Security, privacy, and fairness in fog-based vehicular crowd sensing,'' IEEE Commun. Mag., vol. 55, no. 6, pp. 146 152, Jun. 2017.

[9] C. Wang, C. Liu, Y. Li, H. Qiao, and L. Chen, ``Multi-message and multi- receiver heterogeneous signcryption scheme for ad-hoc networks,'' Inf. Secure. J., Global Perspective, vol. 26, no. 3, pp. 136 152, 2017.