GSIS: A Secure and Timed- Efficient Stream Loss-Tolerant Authentication Protocol For Vehicular Communications

R.Suganya
Department of Computer Science, Research scholar, Karpagam University, Coimbatore.
Email:mailtosuha@gmail.com-8870078411
Dr.K.Ravikumar
Department of Computer Science, UGC – NET Coordinator, Asst. Professor, Tamil University, Thanjavur.
Email: ravikasi2001@yahoo.com-9245107548

---ABSTRACT---

In this paper, we first identify some unique design requirements in the aspects of security and TESLA for communication between different communication devices in vehicular ad hoc networks. We propose a Time–Efficient stream Loss –Tolerant Authentication broadcast authentication protocol based on Group signature and Identify (ID) based signature techniques. We demonstrate that the proposed protocol as an efficient protocol with communication and computation overhead, which scales to large number of receiver, and tolerate packet loss. TESLA protocol guarantee the requirements of security can provide the desired traceability of each vehicle in the case where the ID of the message sender has to be receiver by the authority of any dispute event Extensive simulation is conducted to verify the efficiency, effectiveness and applicability of the proposed protocol in various application scenarios under different road systems.

Keywords: **ID – based Signature, TESLA, and Vehicular Communication**

Date of Submission : June 02, 2013 Date of Submission : August 15, 2013

I. Introduction

Broadcast communication is gaining popularity for efficient and large – scale data dissemination. Examples of broadcast distribution networks are satellite broadcasts, wireless radio broadcast, or IP multicast. Because malicious packet injection is easy in many broadcast networks, the receivers want to ensure that the broadcast packets they receive really originate from the claimed source. Simple deploying the standard point – to – point authentication mechanism (i.e., appending a message authentication code (MAC) to each packet, computed using a shared secret key) does not provide secure broadcast authentication. The problem is that any receiver with the secret key can forge data and impersonate the sender. Consequently, it is natural to look for solutions based on asymmetric cryptography to prevent this attack; a digital signature scheme is an example of an asymmetric cryptographic protocol. Indeed, signing each data packet provides secure broadcast authentication; however; however, it has high overhead, both in terms of the time required to sign and verity, and in terms of the bandwidth. Several schemes were proposed that mitigate this overhead by amortizing a single signature over several packets, e.g., [4, 5, 7, 8]. However, none of those schemes is fully satisfactory in terms of bandwidth overhead, processing time, scalability, robustness to denial – of service attacks, and robustness to packet loss. Even though some schemes amortize a digital signature over multiple data packets, a serious denial – of service attack is usually possible where an attacker floods the receiver with bogus packets supposedly containing a signature.TESLA requires that the receivers are loosely time synchronized with the sender. In this section, we receive a simple protocol to achieve this time synchronization. TESLA also needs an efficient mechanism to authenticate keys at the receiver.

Fig: 1 The Network Model (MANET)

Mobile Ad-hoc Networks (MANET – s) are, by their very nature, vulnerable to many types of attacks. Fig.1 The security of MANET –s is often predicated on the availability of efficient key management techniques. However, the usual features of: (1) lack of a centralized authority and (2) dynamic nature of MANET represent major obstacles to providing secure, effective and efficient key management. What further complicates the issue is that, in many applications (such as secure routing, [1, 2, 3] cryptographic keys need to be established prior to communication [9,10, 11, 12]. While these ID – based signatures have improved key management and key recovery, their advantage lies in the fact that the signers' key is shared with the private key generator [13, 10].

The system administration, for the sake of system maintenance and management, has the privilege to check any access point and obtain a list of IP addresses and corresponding MAC (Medium Access Control) addresses of the mobile devices that are connecting to the checked access point. The administration also has the data1 that can indicate a bisection relationship between MAC addresses (or IP addresses) of authorized mobile devices and registered legitimate mobile users.

II. Related Works

A time – efficient and secure vehicular communication scheme (TSVC) based on the TESLA (Timed Efficient Stream Loss – tolerant Authentication) [22]. With TSVC, a vehicle first broadcasts a commitment of hash chain to its neighbors and then uses the elements of the hash chain to generate a message authenticate this vehicles following message.

Lin et at [12], [13] proposed a security protocol, i.e. GSB protocol based on the group signature [14]. With GSB only a private key and the group public key are stored in the vehicle, and the messages are signed according to the group signature scheme without revealing any identity information to the public. Furthermore, when the number of revoked vehicles in the revocation list is larger than some threshold, the protocol requires every remaining vehicle to calculate a new private key and group public key based on the exhaustive list of revoked vehicles whenever a vehicle is revoked. We first outline the main ideas TESLA. Broadcast authentication requires a source of asymmetry, such that the receivers can only verify the authentication information, but not generate valid authentication information. TESLA uses time for asymmetry. We assume that receivers are all loosely time synchronized with the sender - up to sometime synchronized error , all parties agree on the current time. Hence is a sketch of the basic approach.

Each receiver that receives the packet performs the following operation. It knows the schedule for disclosing keys and, since the clocks are loosely synchronized, can check that the key used to compute the MAC is still secret by determining that the sender could not have yet reaches the time interval for disclosing it. If the MAC key is still secret, then the receiver buffers the packet.

The sender distributes a stream of messages $\{M_i\}$, and the sender sends each message M_i in a network packet P_i along with authentication information. The broadcast channel may be loss, but the sender does not retransmit lost packets. Despite packet loss, each receiver needs to authenticate, all the messages it receives.

III. Background and Preliminaries

3.1. ID based signature scheme and attack models for Batch verification:

An ID – based signature scheme consists of four algorithms: Setup, Extract, Signing and Verification.

(i) Setup A key generation center (KGC) sets the system's secret key K_s that is called the master key and the system parameters Param.
(ii) Extract for each identify ID KGC generates the secret key DID corresponding to ID using K_s and Param.
(iii) Signing A user with ID produces a signature (ID), a verifier checks the validity of the using Param.

3.2. Time Synchronization:

TESLA does not need the strong time synchronization properties that sophisticated time synchronization protocols provide [22, 24, 37], but only requires loose time synchronization, and that the receiver knows an upper bound on the sender's local time. We now outline a simple and secure time synchronization protocol that achieves this requirement. This approach does not require any extra infrastructure to perform time synchronization. We present a simple two – round time synchronization protocol that satisfies the requirements for TESLA, which is that the receiver knows an upper bound on the sender's clock. Reiter previously describes this protocol [12, 13].

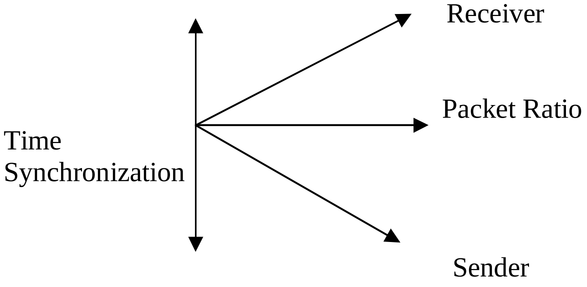


Fig 2. Direct time synchronization between the sender and the receiver.

It shows sample time synchronization between the receiver and the sender. Upon receiving the time synchronization request, the sender records its local time t_S and replies with a signed response packet containing ts and the time synchronization process.

IV. Proposed Secure and Tesla Protocol

4.1. Problem formulation

TESLA is based on loss time synchronization between sender and Receiver. The design of the security communication to face some problems (i.e.) Packet less. We can introduce TESLA Protocol to solve the problems using group and ID – based signature schemes. (Messages)

4.2. Sender Setup

A viable broadcast authentication protocol has the following requirements:

(i) Low computation overhead for generation and verification of authentication information.
(ii) Robustness to packet loss.
(iii) (iv)Scales to a large number of receivers.

4.3. Bootstrapping Receivers

The sender sends the key disclosure schedule by transmitting the following information to the receivers over an authenticated channel (either via a digitally signed broadcast message, or over unicast with each receiver):

4.4. Broadcast Authenticated messages

Every time a sender broadcasts a message, it appends a MAC to the message, using the key corresponding to the current time interval. The key remains secret for the next d – 1 intervals, so messages sent in interval j effectively disclose key Kj-d. We call d the key disclosure delay.

V. Discussion

5.1. 1 TESLA Security Considerations

A sender sends packet P_j in interval i. When the receiver receives packet Pj, the receiver can use the self – authenticating key K_{i-d} disclosed in P_j to determine i.

The receiver cannot yet verify the authenticity of packet Pj sent in interval. Instead, it adds the triplet (i, M_j, MAC ($K^1{}_i$, M_j) to a buffer, and verifies the authenticity after it learns $k^1{}_i$.

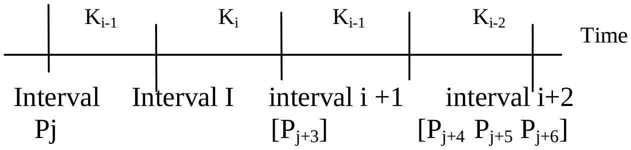


Fig.3 The security of TESLA relies on the following assumptions

The functions F, F1 are secure PRFs, and the function F furthermore provides weak collision resistanc.As long as these assumptions are satisfied, it is computationally intractable for an attacker to forge a TESLA packet that the receivers will authenticate successfully.

As a result, when a node receives a secret token it is able to verify that: (1) the issuing node is a valid authorization node, (2) the token itself is valid (this is important to project against compromised authorization nodes), and (3) in case a token is invalid, its originator can be traced.

VI. Performance Evaluation

We implemented and evaluated the TESLA Protocol in a real MANET environment this section presents the performance of each phases of our scheme. It's also compared them with the performance of the previously proposed previously preservation protocol.

6.1. Experimental setup

We implemented the TESLA protocol on top of the Open SSL library. It's written in Java and consists of about 100 lines of code.

We used laptops and one PDA, a laptop with a P3 – 1. 2GHz, CPU and 512 MB memory, 348 MB memory.

6.2. Comparison Summary

To conclude the discussion of the experiments, we now summarize and compare privacy preservation protocol and TESLA.

The computation costs in terms of basic operations which mostly affect the performance of each scheme.

Table: 1 Privacy preservation protocol

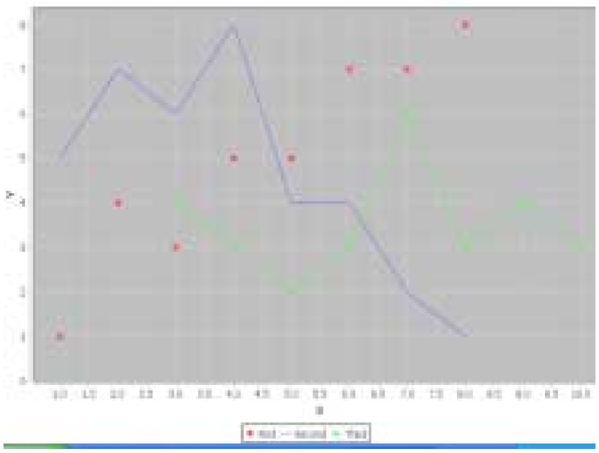
Simulation Scenario	City environment
Communication Range	300 m
Simulation time	100 s
Channel Bandwidth	6 mbs
Packet Size	301 bytes

Table: 2 TESLA Protocol

Simulation Scenario	City environment
Communication Range	300 m
Simulation time	50 s
Channel Bandwidth	6 mbs
Packet Size	301 bytes

6.3. Basic impact of pseudonym changes

The analysis of the section clearly points out which may our when pseudonym changed. We conducted simulation with the Java.



x- Communication Range
y- Packet Ratio

🟥 **TESLA Protocol**
🟩 **Privacy Preservation Protocol**

Fig 4. Packet delivery ratio with influence of pseudonym using Privacy Preservation Protocol& TESLA Protocol.

VII Conclusion

A novel security protocol has been proposed vehicular communication based on group signature and ID – based signature schemes. TESLA is based on 100s time synchronization between the sender and receiver with group signature security and efficient, traceability can be achieved without including the overhead of managing a huge number of shared signatures. Using TESLA with the ID – based signature scheme the management complexity on the public key and certificate can be further reduced the performance valuation on both a city and highway to demonstrate that the message delay and loss ratio can be kept quite low, even in the 100s time synchronization due to the cryptographic operations.

For further work, to generalize the protocols for heterogeneous networking environments (such as hybrid of WLAN, PAN and wide area Network) to a communicate various networking technologies.

Acknowledgements

The authors are grateful to anonyms to referees for invaluable comments.

References

[1]. T.Leighton and S.Micali, “Secret – key agreement without public – key cryptography”, in CRYPTO ‘93, 1993.

[2]. Adi Shamir, “How to share a secret”, Communication of the ACM, vol.22, no.11, pp.612 – 613, Nov.1979.

[3]. Lidong Zhou and Zygmunt J. Haas, “Securing Ad Hoc Networks”, IEEE Network Magnazine, Vol.13, no.6, p. 24 – 30 , 1999.

[4]. Jiejun Kong, Petrol Zerfos, Haiyun Luo, Songwu Lu, and Lixia Zhang, “Providing Robust and Ubiquitous Security Support for MANET,” in IEEE 9th International Conference on Network Protcols (ICNP), 2001.

[5]. X.Boyen Multipurpose Identity – Based Signcryption – A Swiss Army Knife for

Identify – Based Cryptography,, Advances in Cryptology – Crypto 2003, LNCS Vol. 2729, PP.383 – 399, Springer – Verlag, 2003.

[6]. A. Boldyreva, Threshold Signatures, Multi Signatures and Blind Signatures Based LNCS No2567, pp.31-46, Springer – Verlag, 2003.

[7]. C.Boyd and C.Pavlovski.Attacking and Rearranging Batch Verification Schemes. Advances in Cryptology – Asiacrypt 2000, LNCS Vol.1976, pp.58-71, Springer – Verlag, 2000.

[8]. J.Cha and J.Cheon. An ID – based Signature from Gap – Diffie – Hellam Groups. Public Key cryptography – PKC 2003, LNCS Vol.2567, pp.18-30, Springer – verlag, 2003.

[9]. Y.Desmedt and J.Quisqater. Public – key systems based on the Difficulty of Trampering. Advances in Cryptology – Crypto'86, LNCS Vol.263, pp.11-117, Springer – Verlag, 1987.

[10]. Y.Desmedt and M.Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks. In Advances in Cryptology – CRYPTO '9, Volume 537 of Lecture Notes in Computer Science, pages 177 – 188, 1991.

[11]. F.Fujii, W.Kachen, and K.Kuropsawa., Combinatorial bounds and design of broadcast authentication. IEICE Transactions, E769 – A (4) : 502 – 506, 1996.

[12]. R.Gennaro and P.Rohatgi, How to sign digital streams. In Advances in Cryptology – CRYPTO ' 97, volume 1294 of Lecture Notes in Computer Science, pages 180 – 197, 1997.

[13]. R.Gennaro and P.Rohatgi. How to sign digital streams. In Advances in Cryptology – CRYPTO ' 97, volume 1294 of Lecture Notes in Computer Science, pages 180 – 197, 1997.

Authors Biography

Dr.K.Ravikumar working in Tamil university Thanjavur. He is Presented paper in 50 International and National Conferences and Journals. He is Completed UGC Research Project. He is written 16 DDE Books in Tamil University Thanjavur. He is 12 years Teaching and Research Experience. He is having UGC-NET Coaching Co-coordinator for UGC XI Plan.He is a co-ordinator for DDE courses, Tamil University Thanjavur. His Research Areas is Network Security, Cryptography, Mobile Computing,Cloud Computing.

Mrs. R. Suganya, working in T.U.K.Arts College, Karanthai, Thanjavur. She is presented paper in 3 International and National Conference and Journals. She is 8 years teaching experience. Her Research area is Network Security, Cryptography and Mobile computing.