Advance Communication Confirmation Protocol for Vehicular Ad Hoc Networks

R.kavitha, Dr N.Rajendran

***Abstract*— A novel Sybil attack detection mechanism Footprint, using the trajectories of vehicles for identification. When a vehicle approaches a road-side unit it actively demands an authorized message from the RSU as the proof of appearance. By utilizing the social relationship among trajectories, Footprint can recognize and dismiss communities of Sybil trajectories. RSU failure is also considered. The received RSU verifies the vehicle on board unit details such as the previous RSU private key and vehicle public key and its distance of previous RSU to received RSU. Due to network issue RSU may goes to failure scenario. Then the Current RSU calculates the Current RSU and neighbor hop RSU along with distance and duration of time slots. The partial signature verification is processed for the new vehicle. The full signature creation is processed for the existing vehicle in the network to analyze the vehicle traversed trajectory information.**

Index Terms— Vehicular networks, communication security, message authentication, certificate revocation.

I. INTRODUCTION

Mobile computing is "taking a computer and all necessary files and software out into the field." Mobile computing: being able to use a computing device even when being mobile and therefore changing location. Portability is one aspect of mobile computing. Mobile computing is the ability to use computing capability without a pre-defined location and connection to a network to publish or subscribe to information.

Mobile Computing is a generic term describing the application of small, portable, and wireless computing and communication devices. This includes devices like laptops with wireless LAN technology, mobile phones, wearable computers and Personal Digital Assistants (PDAs) with Bluetooth or IRDA interfaces, and USB flash drives.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks. A Vehicular Ad-Hoc Network is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created.

VANET defines an intelligent way of using Vehicular Networking. It integrates on multiple ad-hoc networking technologies such as WiFi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Vehicular Ad-hoc Networks are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of WiFi. Other candidate wireless technologies are Cellular, Satellite, and WiMAX. Vehicular Ad-hoc Networks can be viewed as component of the Intelligent Transportation Systems (ITS).As envisioned in ITS is used in vehicles to communicate with each other via Inter-Vehicle Communication (IVC) as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC). The optimal goal is that vehicular networks will contribute to safer and more efficient roads in the future by providing timely information to drivers and concerned authorities. The research on vehicular ad-hoc networks focuses on the optimization of traffic throughput on highways using sensor-enabled cars. Sensor-enabled cars monitor the traffic in their vicinity sensing the distance to the front and rear car as well as their own speed and acceleration. One such network that has received a lot of interest in the last couple of years is VANET. VANET has become an active area of research, standardization, and development because it has tremendous potential to improve vehicle and road safety, traffic efficiency, and convenience as well as comfort to predict the fake identity vehicle list in the vehicle ad-hoc network.

ISSN: 2278 – 7798

II. RELATED WORK

An efficient pseudonymous authentication scheme with strong privacy preservation, named PASS, for vehicular communications. PASS supports Roadside Units-aided distributed certificate service that allows the vehicles to update certificates on road, but the service overhead is almost unrelated to the number of the updated certificates.

Furthermore, PASS provides strong privacy preservation to the vehicles so that the adversaries cannot trace any vehicle even all Roadside Units have been compromised. They concluded that they have proposed an efficient pseudonymous authentication scheme with strong privacy preservation (PASS) for secure vehicular communication. PASS can not only satisfy the security and privacy requirements of VANET but also significantly reduce the revocation cost and the certificate updating overhead. For our future work, the location privacy issue under the context of the proposed PASS scheme.An intelligent secure and privacy-preserving parking scheme through vehicular communications

It is stated that there are always frustrations for drivers in ending parking spaces and being protected from auto theft. In the paper, to minimize the drivers inconvenience, they proposed a new intelligent secure privacy-preserving parking scheme through vehicular communications. The proposed scheme is characterized by employing parking lot RSUs to survey and manage the whole parking lot and is enabled by communication between vehicles and the RSUs. Once vehicles that are equipped with wireless communication devices, which are also known as onboard units, enter the parking lot, the RSUs communicate with them and provide the drivers with real-time parking navigation service, secure intelligent anti-theft protection, and friendly parking information dissemination. In addition, the drivers privacy is not violated. Performance analysis through extensive simulations demonstrates the efficiency and practicality of the proposed scheme.

The Sybil Attack

It is stated that Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. However, if a single faulty entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining this redundancy.

One approach to preventing these "Sybil attacks" is to have a trusted agency certify identities. This paper shows that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities.

Systems that rely upon implicit certification should be acutely mindful of this reliance, since apparently unrelated changes to the relied-upon mechanism can undermine the security of the system. For example, the proposed IPv6 privacy extensions obviate much of the central allocation of IP addresses assumed by CFS. In the absence of an identification authority, a local entity's ability to discriminate among distinct remote entities depends on the assumption that an attacker's resources are limited. Entities can thus issue resource-demanding challenges to validate identities, and entities can collectively pool the identities they have separately validated.

This approach entails the following conditions:

• All entities operate under nearly identical resource constraints.

• All presented identities are validated simultaneously by all entities, coordinated across the system.

• When accepting identities that are not directly validated, the required number of vouchers exceeds the number of system-wide failures.

The author claimed that in a large-scale distributed system, these conditions are neither justifiable as assumptions nor practically realizable as system requirements.

Lightweight Key Management In Wireless Sensor Networks By Leveraging Initial Trust

It presented a novel approach for key management in wireless sensor networks. Using initial trust built from a small set of shared keys, low-cost protocols enable neighboring sensors to authenticate and establish secure local links. Once links are established, other security services such as group-key refresh can be provided. The protocols we present require little memory and processing power, and require a small number of shared keys independent of the network size. They have presented a collection of lightweight protocols for authentication and key distribution in resource-constrained sensor networks. These protocols have been implemented on a representative sensor platform. They require only inexpensive cryptographic primitives and use little memory. Security is achieved by taking advantage of

ISSN: 2278 – 7798

bounded periods of trust, just after sensors have been deployed, to quickly and cheaply establish pairwise keys. Bootstrapping keys that enable sensors to authenticate during this trust period are used only within that time, and erased after pairwise keys have been exchanged. In future work, planned to extend these protocols to support authentication and key exchange between distant nodes.

III. SYSTEM METHODOLOGY

RSA Encryption Algorithms

The security of a cryptographic system should not be based on the privacy of its implementation. It should be based on the strength of its underlying mathematical cryptographic algorithm. An algorithm is a procedure or formula. The algorithm is used for encrypting, decrypting bytes and text with public and private keys using asymmetric algorithm RSA. Also enables generate keys. RSA is used for encrypting smaller amount of data. Use GetMaxDataLength method to check maximum data length for specified key size.

Key generation

1) Choose two large random prime numbers P and Q of similar length. Generate two different large odd prime numbers, called P and Q, of about the same size where P is greater than Q that when multiplied together give a product that can be represented by the required bit length you have chosen, e.g. 1024 bits.
2) Compute N = P x Q. N is the modulus for both the Public and Private keys.
3) PSI = (P-1)(Q-1) , PSI is also called the Euler's totient function.
4) Choose an integer E, such that $1 < E < PSI$, making sure that E and PSI are co-prime. E is the Public key exponent.
5) Calculate $D = E^{-1} (\text{mod PSI})$, normally using Extended Euclidean algorithm. D is the Private Key exponent.

When representing the plain-text to plain-text octets in order to secure the message more thoroughly it is usual to add padding characters to make it less susceptible to certain types of attack. After all that has been accomplished you have public and private keys ready for encryption which are then stored as base-64 numbers.

Encryption

1) Convert the data bytes to be encrypted, to a large integer called PlainText.

2) $\text{CipherText} = \text{PlainText}^{E} (\text{mod N})$

3) Convert the integer, CipherText to a byte array, which is the result of the encryption operation.

Decryption

1) Convert encrypted data bytes to a large integer called CipherText.

2) $\text{PlainText} = \text{CipherText}^{D} (\text{mod N})$

3) Convert the integer, Plaintext to a byte array, which is the result of the decryption operation.

Message Verification

As the proof that a vehicle (Vi) was present near certain RSU, an authorized message issued for Vi can be verified by any entity in the system. In case it needs to verify Vi, Vi will sign on an authorized message (**M)** generated by RSU (Rk) using public key and send to the vehicle. These process consists of following steps:

Step 1: Check the Vehicle Id
Step 2: Check the private key of RSU (Rk)
Step 3: Check the public key of Vehicle(Vi)
Step 4: Analyze the Entry time
Step 5: Analyze the message as partial signature or Full Signature creation
Step 6: Verify that the message was signed by legitimate previous RSU

IV. EXPERIMENTS AND RESULTS

The performance of Footprint in recognizing forged trajectories (issued by malicious vehicles) and actual ones (provided by honest vehicles) through trace-driven simulations.

Key Metrics of The Foot Print

In the Sybil attack detection scheme, it is possible that a trajectory of an honest vehicle could be mixed with other trajectories especially when the length of the trajectory is short. This will cause false alarm of Sybil trajectories. This issue can be largely mitigated by comparing multiple sets of trajectories issued in different events. If the probability for an honest trajectory in an event of a vehicle being treated as Sybil.

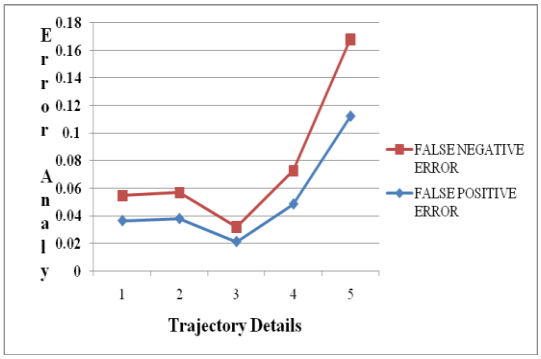
False positive error: is the proportion of all actual trajectories that are incorrectly identified as forged trajectories.

ISSN: 2278 – 7798

False negative error: is the proportion of all forged trajectories that are falsely identified as actual trajectories.

TRAJECTORY	FALSE POSITIVE ERROR	FALSE NEGATIVE ERROR
1	0.0363636363	0.0181818181
2	0.0378787878	0.0189393939
3	0.0212121212	0.0106060606
4	0.0484848484	0.0242424242
5	0.11212121212	0.0560606060

Hop And Neighbour Hop Distance



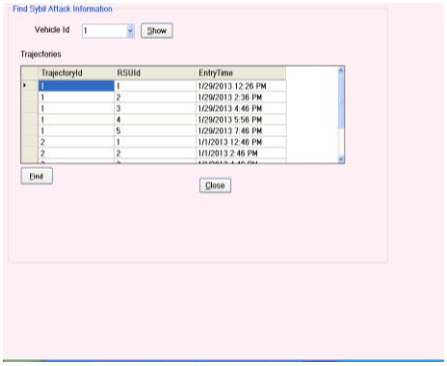
Representation of Trajectory Analysis

Authentication

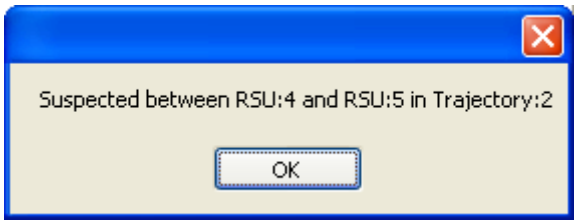
It is used to know how the footprint mechanism evaluated and to detect the Sybil attack in the network in well efficient manner. The attack detected by the three component namely, trusted authority, on board unit and road side unit. The trust authority is the person to analyze the hacking process in the network. Here the detection mechanism utilize the two terms such as distance and time process between the one road side unit and another road side unit.

In this mechanism, the suspected trajectory found in the network using the on board unit traversed path information and crossed time information. Specifically, a trajectory-embedded authorized message has signer-ambiguous and temporarily linkable properties. With the signer-ambiguous property, the RSU signature contained in the message is anonymous which makes an attacker unable to determine which RSU actually signed the message. Thus, no location information can be inferred by knowing a RSU signature.

With the temporarily linkable property, RSUs change their link tags on every new event which means remembering a previous link tag of a RSU does not help an attacker identify this RSU in any other event. Therefore, even if an attacker conducts a field testing by recording the locations of RSUs and their corresponding link tags, it can only log a small number of RSUs for a short period of time.



Sybil Attack Detection

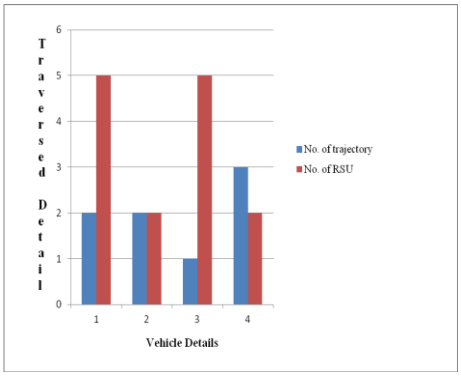


Suspected Trajectory

Vehicle Id	No. of trajectory	No. of RSU
1	2	5
2	2	2
3	1	5
4	3	2

Representation of Authenticated Vehicle Process

ISSN: 2278 – 7798



Representation of Vehicle Traversed Process

Signature Verification

Partial signature verification
Full signature verification

Due to the high mobility of vehicles, the duration of interactions between RSUs and vehicles and between vehicles are very short. This may arouse the scalability concern, how many vehicles a particular RSU or a vehicle is able to interact in a short period of time like seconds. If the generation or verification of signatures is not very efficient, it is possible that a vehicle fails to obtain an authorized message from an RSU before it runs out of the communication range of the RSU. In Footprint, for trajectory verification, only one signature should be verified.

Partial Signature Verification

The partial signature verification is verified depend upon the selection of road side unit and vehicle identity number. The partial signature verification is processed for the new vehicle. The unknown or new vehicle on the network should not contain the previous credential authorization. Here the verification signature is created as encrypted data using the RSA encryption algorithm and the authorized information of the road side unit identity number and on board unit identity number.

Full Signature Verification

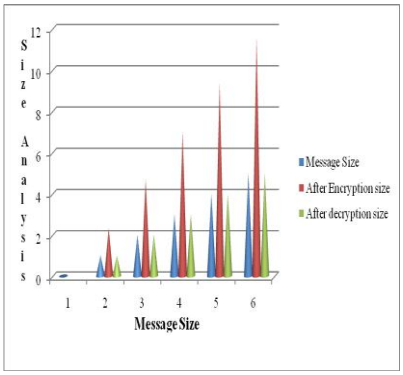
The full signature verification and creation is done by as two pair namely private key of the road side unit and public key of the vehicle and data traversed to road side unit to on board unit for further reference then the output are partial signature value and encrypted message.There are several analysis methods for cryptosystems. Here implemented a new scheme in microcomputer and observed that the file size after the encryption of the plain text increases. Now after decryption, the file size comes to its original size (1MB). This means that RSA algorithm used in new scheme enhances the security level but is also responsible for increase in the File size. This works very well where security is a major concern as the cryptosystem cannot be bypassed.

The results of study are as follows:

- To increase time complexity and space complexity against the exhaustive attack and the time-memory trade off attack, the key length is increased to 504 bits (k1, k2, and k3).
- Te removes the main difficulty arises in Brute-force attack; it almost minimizes the cause of man-in middle attack.
- To improve the security level but File size is increased after encryption is major drawback in this scheme.
- In future, security level is increased but file size remain constant.

Message Size In (KB)	After Encryption size	After decryption size
1	2.33	1
2	4.7	2
3	7.0	3
4	9.4	4
5	11.6	5

RSA Encryption Data



Representation of RSA Algorithm Process

ISSN: 2278 – 7798

V. CONCLUSION

A Sybil attack detection scheme named Footprint is developed for urban vehicular networks. Consecutive authorized messages obtained by an anonymous vehicle from RSUs form a trajectory to identify the corresponding vehicle. Location privacy of vehicles is preserved by realizing a location-hidden signature scheme. Utilizing social relationship among trajectories, Footprint can find and eliminate Sybil trajectories. The Footprint design can be incrementally implemented in a large city. It is also demonstrated by both analysis and extensive trace-driven simulations that Footprint can largely restrict Sybil attacks and can enormously reduce the impact of Sybil attacks in urban settings (above 98 percent detection rate). In this thesis Sybil attack detection mechanism having much space to extend. First, in Footprint, it is assumed that all RSUs are trustworthy. However, if an RSU is compromised, it can help a malicious vehicle generate fake legal trajectories.

Footprint cannot detect such trajectories. However, the corrupted RSU cannot deny a link tag generated by itself nor forge link tags generated by other RSUs, which can be utilized to detect a compromised RSU in the system.

The cost-efficient techniques can be developed to fast detect the failure of an RSU. Second, it will delve into designing better linkable signer-ambiguous signature schemes such that the computation overhead for signature verification and the communication overhead can be reduced.

REFERENCES

[1] Y.Sun,R.Lu,X.Lin,X.Shen,andJ.Su,"AnEfficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[2] R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 6, pp. 2772-2785, July 2010.

[3] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), pp. 251-260, Mar. 2002.

[4] J. Eriksson, H. Balakrishnan, and S. Madden, "Cabernet: Vehicular Content Delivery Using WiFi," Proc. MOBICOM '08, pp. 199-210,Sept. 2008.

[5] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D.S. Wallach, "Secure Routing for Structured Peer-to-Peer Overlay Networks," Proc. Symp. Operating Systems Design and Implementation (OSDI '02), pp. 299-314, Dec. 2002.

[6] B. Dutertre, S. Cheung, and J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust," Technical Report SRI-SDL-04-02, SRI Int'l, ome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Proc. Int'l Symp. Information Processing in Sensor Networks (IPSN '04), pp. 259-268, Apr. 2004. Apr. 2002.

[7] S. Capkun, L. Buttya'n, and J. Hubaux, "Self-Organized Public Key Management for Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.

[8] C. Piro, C. Shields, and B.N. Levine, "Detecting the Sybil Attack in Mobile Ad Hoc Networks," Proc. Securecomm and Workshop, pp. 1-11, Aug. 2006.

[9] N. Borisov, "Computational Puzzles as Sybil Defenses," Proc. Sixth IEEE Int'l Conf. Peer-to-Peer Computing (P2P '06), pp. 171-176, Oct. 2006.

R.Kavitha, currently pursuing M.Phil Computer Science from one of the college affiliated to Periyar University. I also received my B.Sc and M.Sc degrees from affiliated Colleges under Anna University. I have done two projects during my Post Graduate. I am an university rank holder in my PG.

Dr N.Rajendran, currently working as Head of the Department of Computer Science in Vivekanandha College for Women. He has done his Ph.D degree in Data Mining.

ISSN: 2278 – 7798