International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November, 2014
ISSN 2091-2730

An Enhanced Detection of Fake Vehicle Identity in Vanet

M.SAKTHIVEL[1], S.KARTHIKEYINI [2]

[1] ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE, P.G.P ARTS AND SCIENCE, NAMAKKAL.

[2.]M.PHIL FULL-TIME RESEARCH SCHOLAR, DEPARTMENT OF COMPUTER SCIENCE, P.G.P ARTS AND SCIENCE, NAMAKKAL.
msakthivelpgp@gmail.com, keyiniskarthi@gmail.com

ABSTRACT— In vehicular networks, moving vehicles are enabled to communicate with each other via inter-vehicle communications as well as with road-side units (RSUs) in vicinity via roadside-to-vehicle communications. In urban vehicular networks, where privacy, especially the location privacy of secret vehicles is highly concerned, secrets verification of vehicles is indispensable. Consequently, an attacker who succeeds in forging multiple hostile identifies can easily launch a Sybil attack, gaining a disproportionately large influence. A location-hidden authorized message generation scheme is designed for two objectives: first, RSU signatures on messages are signer indistinct so that the RSU location information is concealed from the resulted authorized message; second, two authorized messages signed by the same RSU within the same given period of time (temporarily linkable) are recognizable so that they can be used for identification.

Keywords— RSU location information, RSU private key and vehicle public key, partial signature verification, full signature creation

I. INTRODUCTION

Distributed systems are groups of networked computers, which have the same goal for their work. The terms "concurrent computing", "parallel computing", and "distributed computing"[1] have a lot of overlap, and no clear distinction exists between them. The same system may be characterized both as "parallel" and "distributed"; the processors in a typical distributed system run concurrently in parallel [2]. Parallel computing may be seen as a particular tightly coupled form of distributed computing, and distributed computing may be seen as a loosely coupled form of parallel computing. Nevertheless, it is possible to roughly classify concurrent systems as "parallel" or "distributed" using the following criteria:

- In parallel computing, all processors may have access to a shared memory to exchange information between processors.
- In distributed computing, each processor has its own private memory (distributed memory). Information is exchanged by passing messages between the processors.

The situation is further complicated by the traditional uses of the terms parallel and distributed algorithm that do not quite match the above definitions of parallel and distributed systems; see the section Theoretical foundations below for more detailed discussion[3]. Nevertheless, as a rule of thumb, high-performance parallel computation in a shared-memory multiprocessor uses parallel algorithms while the coordination of a large-scale distributed system uses distributed algorithms. Distributed computing is a field of computer science that studies distributed systems. A distributed system is a software system in which components located on networked computers communicate and coordinate their actions by passing messages. The components interact with each other in order to achieve a common goal [4]. There are many alternatives for the message passing mechanism, including RPC-like connectors and message queues. Three significant characteristics of distributed systems are concurrency of components, lack

of a global clock, and independent failure of components. A computer program that runs in a distributed system is called a distributed program, and distributed programming is the process of writing such programs. Distributed computing also refers to the use of distributed systems to solve computational problems [5]. In distributed computing, a problem is divided into many tasks, each of which is solved by one or more computers, which communicate with each other by message passing. Wireless network [6] refers to any type of computer network that utilizes some form of wireless network connection. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication [7]. A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data.

II. RELATED WORK

In VANET is helps in defining safety measures in vehicles, streaming communication between vehicles, infotainment and telemetric. 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). The research on vehicular ad-hoc networks focuses on the optimization of traffic throughput on highways using sensor- enabled cars. To develop proactive for highway ramps, obstacles, and intersections are used to further analysis. 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. In addition, we also briefly present some of the simulators currently available to VANET researchers for VANET simulations and we assess their benefits and limitations. Finally, we outline some of the VANET research challenges that still need to be addressed to enable the ubiquitous deployment and widespread adoption of scalable, reliable, robust, and secure VANET architectures, protocols, technologies, and services [8].

Currently, most of the research is focused on the development of a suitable MAC layer, as well as potential applications ranging from collision avoidance to on board infotainment services [9]. In order to avoid transmission collisions in VANETs, a reliable and efficient medium access control protocol is needed. But efficient medium sharing is more difficult due to high node mobility and fast topology changes of VANETs

III. MAIN CONTRIBUTIONS

In this way, the RSU location information is concealed from the final authorized message. Second, authorized messages are temporarily linkable which means two authorized messages issued from the same RSU are recognizable if and only if they are issued within the same period of time. Thus, authorized messages can be used for identification of vehicles even without knowing the specific RSUs who signed these messages. With the temporal limitation on the likeability of two authorized messages, authorized messages used for long-term identification are prohibited. Therefore, using authorized messages for identification of vehicles will not harm anonymity of vehicles.

IV. PROPOSED SCHEME

They proposed a fully self-organized public-key management system that allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services.

Furthermore, their approach does not require any trusted authority, not even in the system initialization phase. By definition, a mobile ad hoc network does not rely on any fixed infrastructure; instead, all networking functions (e.g., routing, mobility management, etc.) are performed by the nodes themselves in a self-organizing manner.

- To find and eliminate Sybil trajectories.
- Location privacy of vehicles is preserved.
- To fast detection of failure RSU details in the network.

PROPOSED ALGORITHM

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 (mod PSI) , normally using Extended Euclidean algorithm. D is the Private key exponent.

Encryption:

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

2) CipherText = PlainText

E

(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) PlainText = CipherText

D

(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 (Rk) at certain time, an authorized message issued for Vi can be verified by any entity (e.g., a vehicle or an RSU) in the system. In the case that an entity needs to verify Vi, Vi will sign on an authorized message (M) generated by RSU (Rk) using public key and then send to the vehicle. The message verification 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

V. PERFORMANCE EVALUATION

In this network creation process is a Typical Vehicular Network (with RSU Installed) is shown graphically. The Fig 1.1 is used to know the RSU deployed and neighbor RSU detail with specified trajectories. Here the figure represents the Vehicular ad-hoc network process with RSU and neighbor RSU connection. The network process is used to know the traverse path of one location to another location.

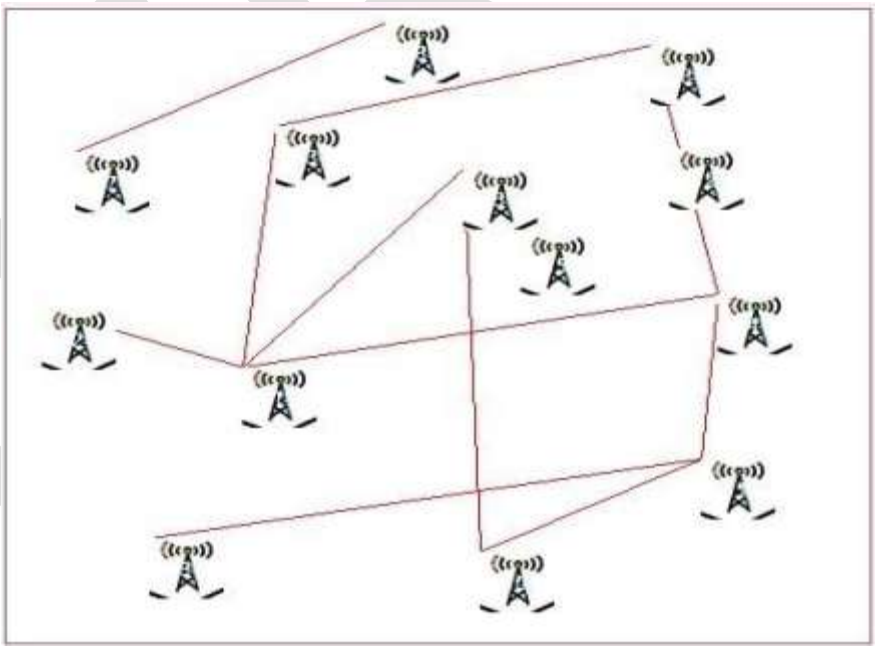

FIGURE: 1.1 NETWORK CREATION

A vehicular ad hoc network, or VANET, is a technology that uses moving vehicles as nodes in a network to create a mobile network. A VANET turns every participating vehicle into a wireless router or node, allowing vehicle approximately traversed of each other to connect and, in turn, create a network with a wide range. As vehicle fall out of the signal range and drop out of the network,

other vehicle can join in, connecting vehicles to one another. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

The message module is used to update the message between Road Side Unit to vehicle On Board Unit. The Fig 1.2 is used to know the trajectory of the desired vehicle, the details contains such as issued vehicle identity number, received road side unit, trajectory id, road side unit number and entry time of the vehicle.

As the proof that a vehicle was present near certain Road Side Unit (RSU) at certain time, an authorized message issued for specified vehicle can be verified by any entity (e.g., a vehicle or an RSU) in the system. If the authorized message passes the ownership verification, the entity further examines whether the signature contained in the authorized message is signed by a legitimate RSU in the system.

The vehicle can use this sequence of authorized messages to identify itself. This method is simple but inefficient because each time when the vehicle needs to be identified in a conversation, all messages in the sequence should be sent to the conversation holder for verification

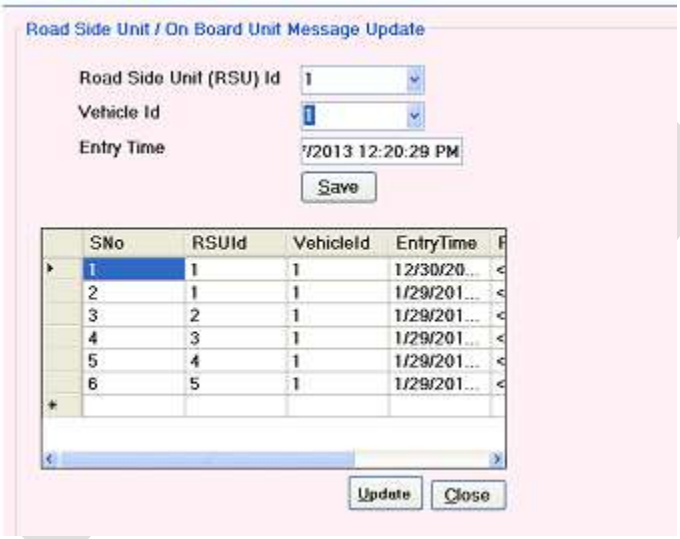

FIGURE: 1.2 MESSAGE UPDATION

ACKNOWLEDGMENT

My abundant thanks to Dr.R.K.Vaithiyanathan, Principal, PGP Arts and Science College, Namakkal who gave this opportunity to do this presentation paper work. I express my deep gratitude and sincere thanks to my supervision M.SAKTHIVEL MCA., M.Phil., Assistant Professor, Department of Computer Science at PGP Arts and Science College, Namakkal for her valuable, suggestion, innovative ideas, constructive, criticisms and inspiring guidance had enabled me to complete the presentation paper work successfully.

VI.CONCLUSION

In this paper Sybil attack detection mechanism having much space to extend. First, in this paper it is assumed that all RSUs

are trustworthy. However, if an RSU is compromised, it can help a malicious vehicle generate fake legal trajectories (e.g., by inserting link tags of other RSUs into a forged trajectory). In that case, duplicated node id cannot detect such trajectories. However, the corrupted RSU cannot deny a link tag generated by it 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 develop into designing better linkable signer-ambiguous signature schemes such that the computation overhead for signature verification and the communication overhead can be reduced.

VII. FUTURE ENHANCEMENTS

In future work, the scenario where a small fraction of RSUs are compromised will be considered. Last, the future work can validate the design and study its performance under real-complex environments. Improvements will be made based on the realistic studies before it comes to be deployed in large-scale systems. The future work is to continue to work on several directions.

REFERENCES:

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

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

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

[4]. Dodis, Kiayias. A, Nicolosi. A, and Shoup. V, "Anonymous Identification in Ad Hoc Groups," Proc. Int'l Conf. Theory and Applicat ions o f C rypto g ra phi c Techniques (EUR OCRYPT ' 04) , pp. 609-626, 2004.

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

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

[8] Fukuhara.T, Warabino. T, Ohseki. T, Saito K, Sugiyama K, Nishida. T, Eguchi. K. "Broadcast methods for inter-vehicle communications system," Proceedings of IEEE Wireless Communications and Networking Conference, pp. 2252-2257, 2005.

[9] Liu. J.K, Wei. V.K, and Wong. D.S, "Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract)," Proc. Ninth Australasian Conf. Information Security and Privacy (ACISP '04), pp. 325-335, 2004.