International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-3)

Research Article | **March 2014**

Multi-Lane Hash Message Authentication Code for Vehicular Ad hoc Networks

Mohanavalli K,
Department of Computer Science,
Adhiparasakthi College of Arts and Science,
Kalavai, Tamilnadu, India.

Dr.G.Arutchelvan,
HOD,Department of Computer Science,
Adhiparasakthi College of Arts and Science,
Kalavai, Tamilnadu, India.

Abstract—

Vehicular Ad Hoc Networks adopt the Public Key Infrastructure and Certificate Revocation Lists for their security. In any PKI system, the authentication of a received message is performed by checking if the certificate of the sender is included in the current CRL, and verifying the authenticity of the certificate and signature of the sender. In my project I replaces the time-consuming CRL checking process by an efficient revocation checking process keyed Multi-Lane Hash Message Authentication Code (Multi-Lane HMAC).Multi-Lane HMAC can significantly decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL. By conducting security analysis and performance evaluation, Multi-Lane HMAC is demonstrated to be secure and efficient.

Keywords— EMAP, Vehicular, HMAC, Ad hoc, Hash

I. INTRODUCTION

Vehicle-to-vehicle (V2V) communications comprises a wireless network where automobiles send messages to each other with information about what they're doing. This data would include speed, location, and direction of travel, braking, and loss of stability. Vehicle-to-vehicle technology uses dedicated short-range communications (DSRC), a standard set forth by bodies like FCC and ISO. Sometimes it's described as being a WiFi network because one of the possible frequencies is 5.9GHz, which is used by WiFi, but it's more accurate to say "WiFi-like." The range is up to 300 meters or 1000 feet or about 10 seconds at highway speeds (not 3 seconds as some reports say). V2V would be a mesh network, meaning every node (car, smart traffic signal, etc.) could send, capture and retransmit signals. Five to 10 hops on the network would gather traffic conditions a mile ahead. That's enough time for even the most distracted driver to take his foot off the gas. HMAC is a popular MAC (Message Authentication Code) that is based on a cryptographic hash function. HMAC is provided with a formal proof of security, in which it is proven to be a PRF (Pseudo-Random Function) under the condition that its underlying compression function is a PRF. Nonetheless, the security of HMAC is limited by a birthday attack, that is, HMAC using a compression function with n-bit output gets forged after about 2 n/2 queries. In this paper we resolve this problem by introducing novel construction we call L-Lane HMAC.

II. ADHOC NETWORK

An ad hoc network is a network that is composed of individual devices communicating with each other directly. The term implies spontaneous or impromptu construction because these networks often bypass the gate keeping hardware or central access point such as a router.

A. Vehicular Adhoc Network

A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres 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. 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. Vehicular networks are a novel class of wireless networks that have emerged thanks to advances in wireless technologies and the automotive industry. Vehicular networks are spontaneously formed between moving vehicles equipped with wireless interfaces that could be of homogeneous or heterogeneous technologies. These networks, also known as VANETs, are considered as one of the ad hoc network real-life application enabling communications among nearby vehicles as well as between vehicles and nearby fixed equipment, usually described as roadside equipment.

B. Internet-Based Mobile Ad hoc Network

Internet-based mobile ad hoc networking is an emerging technology that supports self-organizing, mobile networking infrastructures. The technology enables an autonomous system of mobile nodes, which can operate in isolation or be connected to the greater Internet. Mobile ad hoc networks (Manets) are designed to operate in widely varying environments, from forward-deployed military Manets with hundreds of nodes per mobile domain to applications of low-power sensor networks and other embedded systems. Before Manet technology can be easily deployed, however, improvements must be made in such areas as high-capacity wireless technologies, address and location management,

interoperability and security. A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links.

C. *Intelligent vehicular ad-hoc Network*

Intelligent vehicular ad hoc networks (InVANETs) use WiFi IEEE 802.11p (WAVE standard) and WiMAX IEEE 802.16 for easy and effective communication between vehicles with dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track automotive vehicles. InVANET is not foreseen to replace current mobile (cellular phone) communication standards . Automotive vehicular information can be viewed on electronic maps using the Internet or specialized software. The advantage of WiFi based navigation system function is that it can effectively locate a vehicle which is inside big campuses like universities, airports, and tunnels. InVANET can be used as part of automotive electronics, which has to identify an optimally minimal path for navigation with minimal traffic intensity. The system can also be used as a city guide to locate and identify landmarks in a new city.

III. CONCEPT OF STUDY

The aim of this research work is to focus on design of a middleware architectural model for providing safety in Vehicular ad-hoc networks (VANET). Even though a number of safety methods exist, incorporating intelligence is challenging part of this work. This research paper discusses on design and functionality of the model, with simulated results.

A. *SYSTEM DESIGN*

A Trusted Authority (TA), which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. Roadside units (RSUs), which are fixed units distributed all over the network. The RSUs can communicate securely with the TA. On-Board Units (OBUs), which are embedded in vehicles and OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

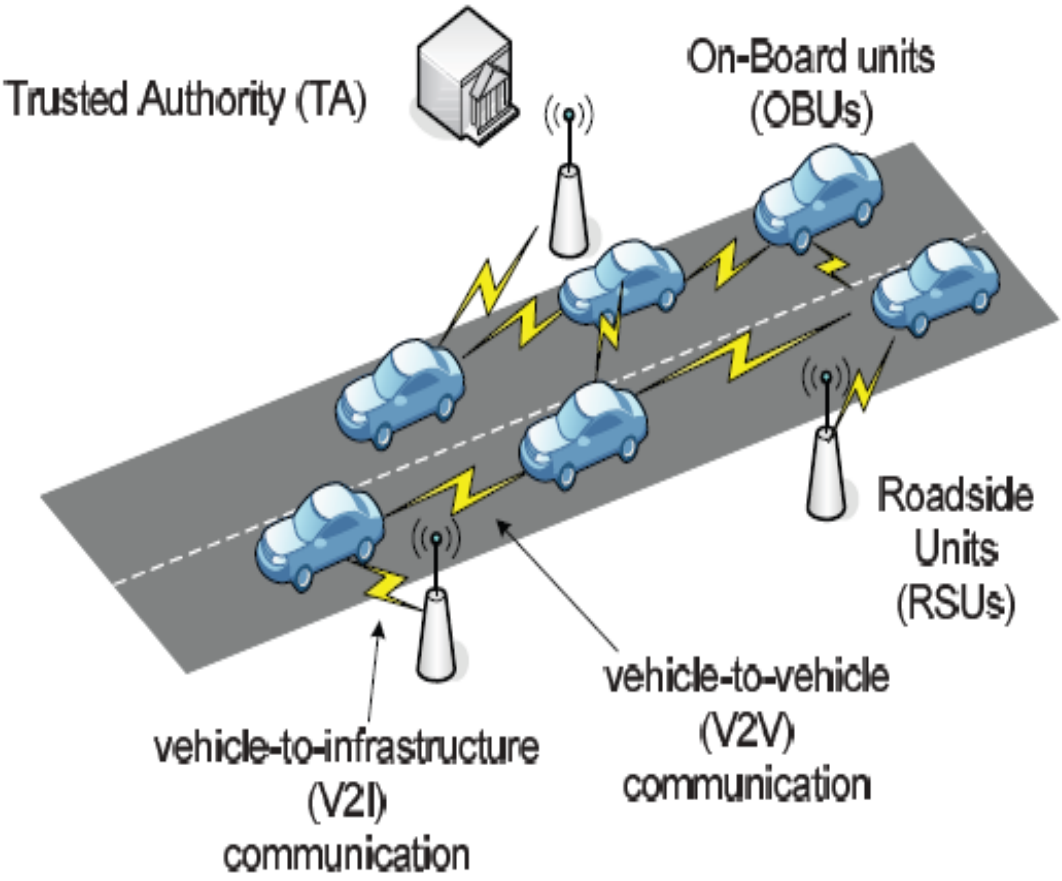

Fig 1. System Design

B. *SYSTEM ARCHITECTURE*

Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to the network. Roadside units (RSUs), which are fixed units distributed all over the network. The RSUs can communicate securely with the TATABLE

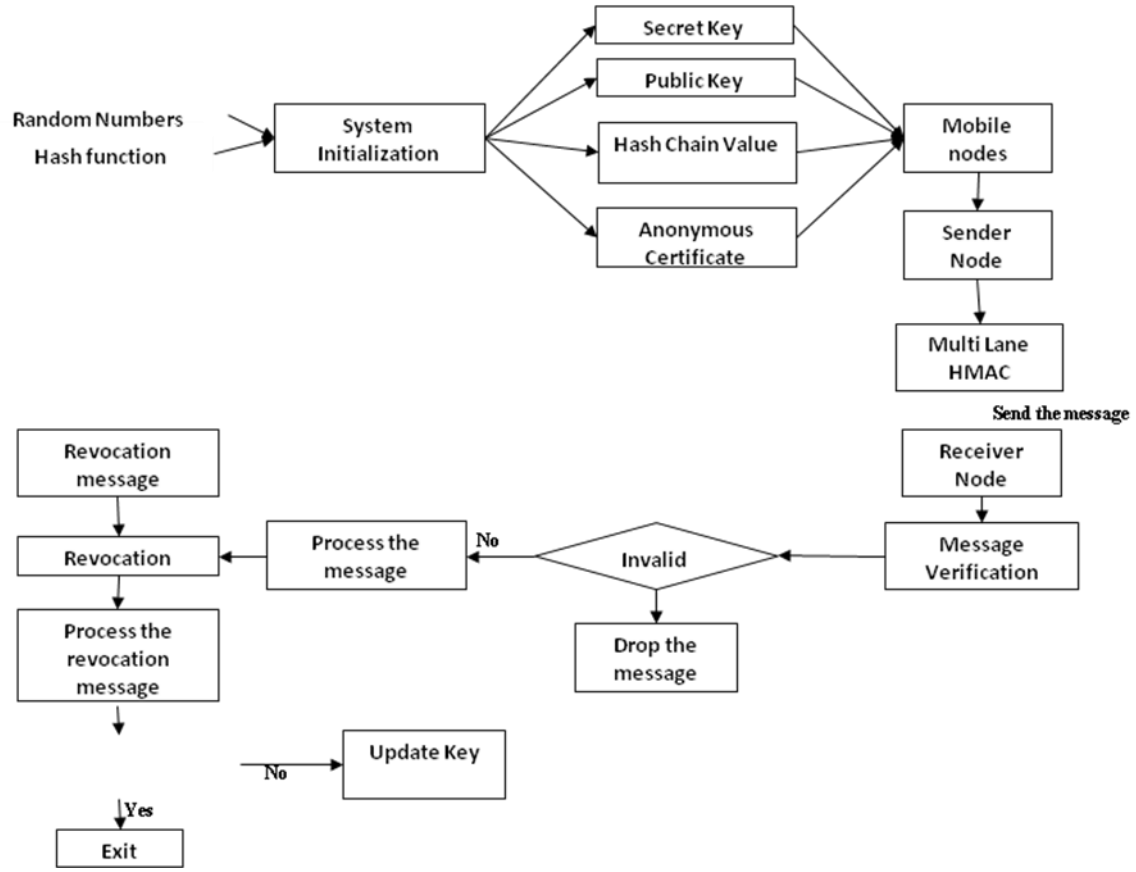

Fig 2. System Architecure

IV. SECURITY ANALYSIS

A. *Hash Chain Values*

Hashing techniques available are based on the concept of a hash function that transforms a given input of arbitrary length to a value of a fixed length, called the hash value. The transformation is done in a manner that it is computationally infeasible to transform the hash value to the original value. Hash functions are very efficient as they do not involve heavy computations and hence are applied in the area of security for message authentication and integrity checks. A hash chain is a successive application of a cryptographic hash function to a string. A hash chain is the successive application of a hash function h: {0; 1}* -> Z * with a secret value as its input. A hash function is easy and efficient to compute, but it is computationally infeasible to invert. A server which needs to provide authentication may store a hash chain rather than a plain text password and prevent theft of the password in transmission or theft from the server. Due to the one-way property of cryptographically secure hash functions, it is infeasible for the eavesdropper to reverse the hash function and obtain an earlier piece of the hash chain. In this example, the user could authenticate 1000 times before the hash chain is exhausted. Each time the hash value is different, and thus cannot be duplicated by an attacker.

Binary hash chains are commonly used in association with a Hash tree. A Binary hash chain takes two hash values as inputs, concatenates them and applies a hash function to the result, thereby producing a third hash value.

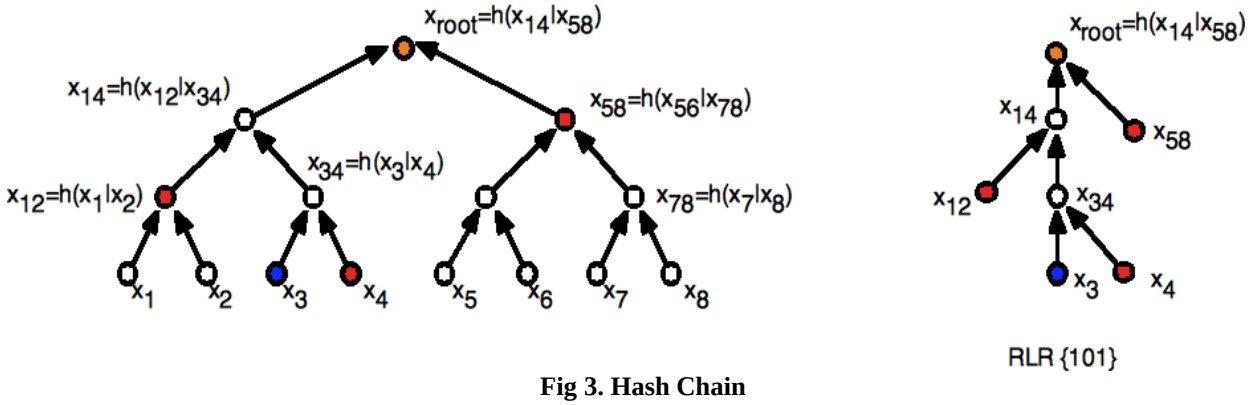

Fig 3. Hash Chain

The problem at hand is to define and implement a mapping from a domain of keys to a domain of locations. From the performance standpoint, the goal is to avoid collisions (A collision occurs when two or more keys map to the same location).From the compactness standpoint, no application ever stores all keys in a domain simultaneously unless the size of the domain is small. The information to be retrieved is stored in a hash table which is best thought of as an array of m locations, called buckets. The mapping between a key and a bucket is called the hash function .The time to store and retrieve data is proportional to the time to compute the hash function. The ideal function, termed a perfect hash function, would distribute all elements across the buckets such that no collisions ever occurred h(v) = f(v) mod m.

B. **Resistance of forging attacks**

To forge the revocation check of any on board unit an attacker has to find the current problem. And find the TA secret key and signature. To the revocation check and TA message and signature are unforgeable.

C. **Resistance of forging attacks**

The values of the hash chain included in the revocation messages are released to non-revoked OBUs starting from the last value of the hash chain, and given the fact that a hash function is irreversible, a revoked OBU cannot use a hash chain value received in a previous revocation process to get the current hash chain value, a revoked OBU cannot update its secret key set.

V. SYSTEM INITIALIZATION

The TA initializes the system by executing Algorithm 1. In step (20), it should be noted that: PKiu denotes the ith public key, where the corresponding secret key is SKiw; PIDiw denotes the ith pseudoidentity (PID), where the TA is the only entity that can relate PIDiw to the real identity of Message Unit; sigTA(PIDi w || PKiu) denotes the TA signature on the concatenation (||) of PIDi w and PKiu ; and C is the number of certificates loaded in each Message Unit.

VI. ALGORITHM

- Select two generators P,Q € G_1 of order q,
- For i □ 1, i do
- Select a random number K_i € Z_q^*
- Set the secret key K_i^- = K_iQ € G_1
- Set the corresponding public key K_i^+ = 1/ki P € G_1
- End for
- Select an initial secret key K_g € G_2 to be shared between all the non-revoked OBSs
- Select a master key s € Z_q^*
- Select the corresponding public key P_o =sP
- Choose hash function H : { 0,1}* □G_1 and h: {0,1}* □ Z*q
- Select a secret value v € Z_q^* and set v_o=v
- For i □ 1,j do to obtain a set V of hash chain values
- Set v_i=h(v_i-1)
- End for
- For all 〖OBU〗_u in the network, TA do
- For i □ 1,m do
- Select a random number a € [1,l]
- Upload the secret key K_a^- = k_aQ and the
- Corresponding public key K_a^- = 1/ka P in 〖HSM〗_u
- Which is the HSM embedded in 〖OBU〗_u
- End for
- Generate a set of anonymous certificates 〖CERT〗_u = 〖cert〗_u^i (〖PID〗_u^i , 〖PK〗_u^i ,sigTA (〖PID〗_u^i|| 〖PK〗_u^i))|1<=i<=C}
- for privacy-preserving authentication
- Upload CERTu in 〖HSM〗_u of 〖OBU〗_u
- End for
- Announce H,h,P,Q, and P_O to all the MOBILENODEs
- After the system is initialized, the TA has the following:
- A secret key pool U_s = { 〖OBU〗_u = k_i | 1 <= i<= l}.
- The corresponding public key set Up={K_i=1/K_i P| 1<=i<=l}.
- A master secret key s and the corresponding public key P_o.
- The secret keyK_g.
- A set of hash chain values V = {v_i |0<=i<=j}, where j is larger enough to accommodate with the number of revocation processes occur during the life time of the network.
- The public parameters H ,h ,P, and Q.

- Also, each MOBILENODE will have the following:
- A set of anonymous certificates (〖CERT〗_u) used to achive privacy-preserving authentication.
- A set of sect=ret keys 〖RS〗_u consisting of m keys randomly selected from U_S,i.e., 〖RS〗_u ⊂ U_S.
- The set of the public keys 〖RP〗_U corresponding to the keys in 〖RS〗_u i.e., 〖RP〗_U ⊂U_P.
- The secret key K_G, which is shared between all the legitimate MOBILENODEs.
- The hash function H, h, P,Q, and the public key P_O.

VII. EXISTING ISSUES

- VANET is vulnerable to variety of attacks such as injecting false information;
- Modifying and replaying the disseminated messages can be easily launched.
- To abstain the leakage of the real identities and location information of the drivers from any external eavesdropper.
- The scale of VANET is very large.
- The security of HMAC is limited by birthday attack.

VIII. PROPOSED WORK

- In this project, I planned to resolve the problem of birthday attack using Multi-Lane Hash
- Message Authentication Code (M-HMAC) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure Multi-Lane HMAC function.
- M-HMAC is suitable not only for VANETs but also for any network employing a PKI system.
- To the best of our knowledge, this is the first solution to reduce the authentication delay resulting from checking the CRL in VANETs.

IX. ADVANTAGES

- Multi-Lane HMAC has the lowest computation complexity
- The number of messages that can be verified using M-HMAC within 300 msec is greater than that using CRL checking process respectively.
- The proposed M-HMAC in authentication reduces the end-to-end delay compared with that using CRL checking process.

X. CONCLUSION

We have proposed EMAP for VANETs, which expedites message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process employing HMAC function. The proposed EMAP uses a novel key sharing mechanism which allows an OBU to update its compromised keys even if it previously missed some revocation messages. In addition, EMAP has a modular feature rendering it integral with any PKI system. Furthermore, it is resistant to common attacks while outperforming the authentication techniques employing the conventional CRL. Therefore, EMAP can significantly decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking. Our future work will focus on the certificate and message signature authentication acceleration.

REFERENCES

[1] [1] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, “Privacy and Identity Management for Vehicular Communication Systems: A Position Paper,” Proc. Workshop Standards for Privacy in User- Centric Identity Management, July 2006.
[2] [2] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, “CARAVAN: Providing Location Privacy for VANET,” Proc. Embedded Security in Cars (ESCAR) Conf., Nov. 2005.
[3] [3] A. Wasef, Y. Jiang, and X. Shen, “DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks,” IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.
[4] [4] M. Raya and J.-P. Hubaux, “Securing Vehicular Ad Hoc Networks,” J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.
[5] [5] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications,” IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.
[6] [6] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, “Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets,” IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012.
[7] [7] US Bureau of Transit Statistics, http://en.wikipedia.org/wiki/ Passenger_vehicles_in_the_United_States, 2012.
[8] [8] J.J. Haas, Y. Hu, and K.P. Laberteaux, “Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET,” Proc. Sixth ACM Int’l Workshop VehiculAr InterNETworking, pp. 89-98, 2009.

[9] [9] IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.
[10] "5.9 GHz DSRC," http://grouper.ieee.org/groups/scc32/dsrc/ index.html, 2012.