ISSN:2320-0790

An International Journal of Advanced Computer Technology

CLUSTER BASED AUTHENTICATION FOR VANET FOR IMPROVING THE SECURITY

[1]Neelambike S, [2]Parashuram Baraki
[1,2]Assistant Professor
[1]Department of Information Science and Engg, [2]Department of Computer Science and Engg
GM Institute of Technology, Davangere
neelais@gmail.com, parashuram.baraki@gmail.com

Abstract: In Vehicular Ad Hoc Networks (VANET), vehicles communicate with another vehicle and also communicate with infrastructure (RSU) points by broadcasting safety and non-safety messages in the network by using the DSRC. In wireless communication, security and privacy are very important issues to avoid threat in the network. Cluster based vehicle to vehicle (V2V) communication scheme is proposed here which prevents vehicle from threat. To achieve security and privacy goals, we propose one time authentication for group and then V2V communication is done using group symmetric key within group. Our scheme satisfies all security and privacy requirements such as authentication, non-repudiation and con- ditional traceability. In case of malicious activity, this scheme can trace malicious vehicle which generates a false message. Computation and communication cost is improved as compared and analyzed with other previous schemes.

Keywords: VANET, V2V communication, Cluster based security, RSU, DSRC

I. INTRODUCTION

Vehicles are becoming important in our day to day life. Therefore, many problems like an accident, traffic congestion etc. are affecting people's life. Government and car manufacturing companies are developing technology which wills minimize all these problems. VANET is new emerging technology which enables vehicular communication to minimize problem. VANET plays effective role in safety on road by introduction of several safety applications. These applications are based on IEEE vehicular communication standards: DSRC and WAVE. Typical structure of VANET is shown in Fig.1.

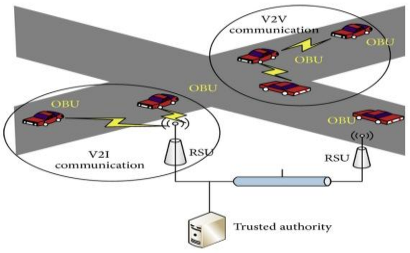

Fig 1: VANET Architecture

VANET has mostly three Network entities [3][9]:

1. Control Center or Authenticated Center (AC): This is very important entity in VANET which manages all network communication. It is trusted authority which has related private information of all vehicles and Roadside Units. It can use this information for security purpose of network. It is more trusted and cannot be compromised.
2. Roadside Unit (RSU): It is an infrastructure which is located along roads and forwards message to TA and vehicles. It has high processing capacity and typical transmission range of 1-3 km.
3. Vehicles: Every vehicle has sensors and an On Board Unit (OBU). OBU has high processing capacity and its transmission range is 100-300m. It exchanges message with vehicles and RSUs [12]. Vehicles send information periodically to neighbors by beacon messages with a frequency of 10 messages per second.

VANET has three communication modes. In V2V communication, vehicles exchange messages among themselves within its range of communication using wireless media. In Infrastructure to Vehicle communication (I2V), infrastructure points in VANET like RSUs communicate with a vehicle to exchange information. In hybrid mode, vehicles communicate with both RSUs and other vehicles [11].

In V2V communication, vehicles communicate through a wireless channel. It requires secure medium to avoid attacks on network. Information exchanged between vehicles may lead to attacks and it can be manipulated by an attacker. An attacker can disclose real identity of a vehicle which creates threat to the privacy of vehicles in the network. An attacker in VANET can classified as external attacker and internal attacker [2]. An external attacker can be prevented by cryptographic operations. It is hard to prevent internal attackers as it has access to cryptographic keys in network. While Securing network, users privacy need to be protected. In this paper, Cluster based V2V communication framework is proposed to secure VANET and preserve privacy. We adopt IEEE 1609.2 [10] security standard for VANET. Cluster of vehicles is formed using location and speed of vehicles and cluster Leader is selected by TA. The rest of the paper is organized as follows: Section II presents overview of previous work. Section III presents system model and assumptions used in this paper. Section IV presents our group based methodology for VANET. Security and performance analysis of proposed scheme is presented in Section V and Section VI. Section VII concludes paper.

II. RELATED WORK

There are number of schemes proposed in literature which deals with security and privacy issues in VANET. These schemes satisfy different security and privacy requirements. Group based scheme is proposed in H. Hasrouny [1] where group signature and symmetric key is used to improve performance in authentication delay. Drawback of this scheme is that it cannot detect malicious vehicle which sends false message in V2V communication.

D.He [3] proposed ID based conditional privacy preservation authentication scheme. It uses batch verification of messages to improve performance. A two-level authentication protocol is proposed by U.Rajput in [4]. It uses two pseudonyms to authenticate vehicle. One pseudonym is base pseudonym which is generated by Certified authority and has a longer lifespan. Another pseudonym is generated by RSU and has a shorter lifetime. But the problem with this scheme is that pseudonyms have more size. L. Zhu [2] proposed threshold based message verification scheme. In this prior and posterior countermeasures are used to ensure efficient message verification process. Prior countermeasures are used to check whether the message is sent by vehicle only one time. Group signature is used to preserve the privacy of vehicles. Another group signature scheme is proposed by X.Zhu [6] which uses HMAC to overcome the problem of time-consuming Certificate Revocation List checking process. To improve authentication speed it uses a cooperative authentication method. However, this scheme needs to check CRL every time which degrade the performance of network. Huang Lu [7] proposed ID based authentication with privacy preservation. It uses ID-based cryptography. In this scheme, the vehicle uses self- defined Pseudo ID (PSID) to hide its real identity. It uses two signature schemes depending on communication type. ID- based signature for Vehicle to Roadside authentication (V2R) and Roadside to Vehicle authentication (R2V) is used therein. ID based online and offline scheme is used for Vehicle to Vehicle authentication (V2V).

To further improve the authentication speed and tracing capability of previous schemes, security enhanced group based authentication scheme is proposed in this paper. Pseudo ID generated by TA is used to provide anonymity. Digital sig- nature generation and verification of message in V2V communication requires more time which degrades performance of network. However, this scheme eliminates the need to sign message in V2V communication which leads to faster authentication. In case false message is detected, only TA can trace vehicle using PSID attached at end of message in V2V communication thereby achieving conditional traceability.

III. PRELIMINARIES

In this section, we discuss system model, security and privacy requirements, assumptions and cryptographic tools.

A. System Model

In system model shown in Fig.2, there are three partici-pants namely Trusted Authority(TA), Roadside unit(RSU) and vehicles. Below is the description of each of them. Here, we consider only one group of vehicles for V2V communication.

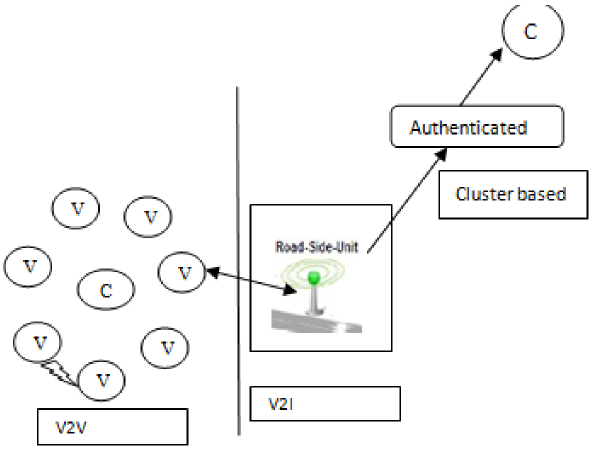

Fig 2: system Model for Proposed work

1. Authenticated Center (AC): Trusted authority is responsible for issuing cryptographic material to other components in the network after vehicle registration. It issues certificate, public and private keys to each vehicle after registration and assigns Pseudo ID, group symmetric key to each vehicle after group formation. In the case of malicious activity, revocation of certificates is done by TA.
2. Roadside units(RSU): Roadside units are infrastructure deployed at road sides which have very high computation capability. They are directly connected to TA. Rsus act as a mediator between AC and vehicles.
3. Vehicles: Each vehicle has On-Board Unit (OBU) and Tamper-Proof Device (TPD). OBU has the high computational capability. Cryptographic materials are stored in TPD which is a very secure device.

B. Security and Privacy requirements in VANET

1. **Authentication**: This enables receiver to check authentic- ity of message sent by other vehicles.
2. **Message Integrity**: The content of a message sent by sender vehicle should be delivered to receiver vehicle without altering.
3. **Non-repudiation**: Sender vehicle should not be able to deny about a content of the message sent by him. In case of malicious activity, TA checks the origin of a message. So, a sender should not deny it.
4. **Anonymity**: Every vehicle should not display its real identity in VANET. It should use pseudo ID to hide its real identity.
5. **Conditional Traceability**: In case of malicious activity, TA should be able to trace vehicles conditionally.

IV. PROPOSED SCHEME

This section explains the working of proposed scheme. Following are steps involved in this scheme.

A. System Initialization Phase

In this phase AC generates system parameters and pre-loads these into TPD of each vehicle. AC generates public and private key pairs Pui/Pri to vehicle Vi using ECC. It assigns certificate Certi to Vi vehicle. TA pre-loads following parameters in TPD of vehicle Vi at vehicle registration. param =(Pui, Pri, Certi, PuAC)
It also pre-loads standard cryptographic algorithms into TPD.

B. Group Formation

Group of vehicles in particular region is formed by AC based on speed and location of a vehicle and CL is selected by AC.

C. One Time Authentication of Group after its Formation

Step 1: After a group is formed, CL broadcast message ―I am CL‖. Vehicle Vi in the group generates the following message

M1 = (m || Sign(m) || Certi)

This message is encrypted by vehicle Vi using public key of AC (PuAC). Vi send this encrypted message to CL. CL collects all the messages of vehicles in the group and forwards it to AC.

Step 2: AC decrypt these messages and then check certificate of respective vehicles by checking its Certificate Revocation List(CRL) and then verify its signature using public key of vehicle Pui. If all the messages are verified then, AC acknowledges CL that all the vehicles are authenticated.

Step 3: After authenticating all the vehicles in a group, AC generates group symmetric key Ck and Pseudo ID for each vehicle in a group. It calculates hash of Pseudo IDs of vehicles in a group separately and store it in its group hash table. AC sends group parameters by sending message to each vehicle Vi in group through CL or RSUs via secure channel.

Step 4 : After receiving message from AC, vehicle store Hremv in its group hash table HTG. It also store group symmetric key and its Pseudo ID PSIDi in its TPD.

VI. PERFORMANCE ANALYSIS

In this section, we analyze the performance of proposed scheme by analyzing computation cost and communication cost. Later we compare performance of our scheme with other previous schemes.
Proposed scheme is compared with other schemes by find- ing following parameters 1) Message generation time at sender vehicle denoted by (Tg) 2) Message Verification Time at receiving vehicle denoted by (Tv).

To find these parameters, proposed scheme is implemented in JAVA NetBeans IDE 8.1 environment. Java application is created. Cluster of 10 vehicles is formed and we find value of Tg and Tv.

REFERENCES

[1] Global status report on non-communicable diseases 2010. [Online]. Available: https://healthyoupromo.wordpress.com/
[2] Maedeh Kiani Sarkaleh and Asadollah Shahbahrami, ―Classification of ECG arrhythmias

using discrete wavelet transform and neural networks,‖ International Journal of Computer Science, Engineering and Applications (IJCSEA), 2(1): 1-13, 2012.
DOI : 10.5121/ijcsea.2012.2101

[3] Naveen Kumar Dewangan and S.P. Shukla, ―A survey on ECG signal feature extraction and analysis techniques,‖ International journal of innovative research in electrical, electronics, instrumentation and control engineering, 3(6), June 2015.
DOI 10.17148/IJIREEICE.2015.3603.

[4] B. Castro, D. Kogan and A. B. Geva, ―ECG feature extraction using optimal mother wavelet,‖ The 21st IEEE convention of the Electrical and electronic engineers, Tel Aviv, Israel, 346–350, 2000. doi:10.1109/EEEI.2000.924422.

[5] I. Clarek, R Biscay., M.ía Echeverr and T.és Viru, ―Multiresolution decomposition of non- stationary EEG signals: A preliminary Study,‖ Comput. Biol. Med. 25, 373-382, 1995.

[6] C.Li, C. Zheng, C. Tai, ―Detection of ECG characteristic points using wavelet transform,‖ IEEE Trans. Biomed. Eng. 42, 21-28, 1995.

[7] A. Ahmadian, S. Karimifard, H. Sadoughi and M. Abdoli, ―An Efficient piecewise modeling of ECG signals based on hermitian basis functions,‖ Proceedings of the 29th Annual International Conference of the IEEE EMBS, Lyon, France, pp. 3180-3183, 2007.

[8] K.S. Park, B.H. Cho, D.H. Lee, S.H. Song, ―Hierarchical support vector machine based heartbeat classification using higher order statistics and hermite basis function,‖ Computers in Cardiology Published by IEEE, International Conference at Bologna, 229-232, 2008.

[9] W. Zong, D. Jiang, ―Automated ECG rhythm analysis using fuzzy reasoning,‖ IEEE Conference, Computers in Cardiology, Cleveland, OH, 69–72, 1998.

[10] Rosaria Silipo and Carlo Marchesi, ―Artificial neural networks for automatic ECG analysis‖, IEEE Transcations on Signal Processing, 46(5): 1417-1425, 1998.

[11] Indu Saini and B. S. Saini, ―Cardiac arrhythmia classification using error back propagation method,‖ International Journal of Computer Theory and Engineering, 4(3): 462-464, 2012.

[12] Louis C Pretorius and Cobus Nel, ―Feature extraction from ECG for classification by artificial neural network,‖ University of Pretoria, in IEEE Proceeding, 2002.

[13] A. Coast Douglas, M. Stern Richard, G. Cano Gerald and A. Briller Stanley, ―An approach to cardiac arrhythmia analysis using hidden markov models,‖ IEEE Transaction on Biomed Eng., 37(9): 826-836, 1990.

[14] W. T. Cheng, and K. L. Chan, ―Classification of electrocardiogram using HMMs,‖ Engineering in Medicine and Biology Society, Proceedings of the 20th Annual International Conference of the IEEE, vol.1: 143-146, 1998.

[15] Varejão Andreão Rodrigo, Bernadette Dorizzi, Jérôme Boudy, ―ECG signal analysis through hidden markov models,‖ IEEE Transactions on Biomedical Engineering, 53 (8), 1541-1549, 2006.

[16] M. Lagerholm, C. Peterson, G. Braccini, L. Edenbrandt and L. Sörnmo, ―Clustering ECG Complexes using Hermite Functions and Self-Organizing Maps,‖ IEEE Trans Biomed Eng., 47(7): 838-48, 2000.

[17] Stanislaw Osowski, Linh Tran Hoai, and Tomasz Markiewicz, ―SVM based expert system for reliable heartbeat recognition‖, IEEE Transactions on Biomedical Engineering, 51(4): 582-589, 2004.

[18] Neelambike S, Dr chandrika J---An efficient environmental model considering environmental factor for V2I application services,IEEE, 2015 DOI-10.1109/ICCIC.2015.7435731