A Data Access Control for Identifying Malicious Node in VANET

A. Biju[1]

Department of Information Technology, Maria College of Engineering and Technology, Tamilnadu, India

Abstract— Vehicular ad hoc networks providing variety of safety events related Application to Vehicular users. There is irregularity vehicle detection in more complex road construction and solutions for cooperative secure (message) data access with the support of roadside Infrastructures. Vehicular communication needs to secure high sensitive data (messages) and identify the malicious vehicles in the Networks during the safety message dissemination over VANET. However, Trusted Authority disseminates sensitive data to all connected Vehicle group within the Network. There are illegal vehicle group could hijack and modify the sensitive data (messages) and disseminate duplicate data (messages) to the other vehicle group. In this paper, proposed, Data Access Control for Identifying Malicious vehicle to prevent duplicate message dissemination from the Unlawfully Vehicle group. And also Revoking malicious vehicle group from the network to protect the legally Vehicle in the Vehicular Ad – hoc Network.

Keywords— Data Access control, Privacy, Revocation Group, Vehicular Ad Hoc Networks.

I. INTRODUCTION

The main application of vehicle-to-vehicle (V2V) communication is to enable the safety application, with in Vehicular Ad-hoc Networks. In Vehicular Ad – hoc Networks communicate the high sensitive data to other vehicle. There is a Trusted Authority and Group Authority, TA disseminate a message to vehicle. Any malicious activities of a user, such as injecting fake information, or modifying and replaying the disseminated messages over this Network, It could be fatal to other lawful users. In addition, users are very conventional about their privacy-related information. The excellence of security message dissemination in vehicular ad hoc Network that traffic generated by event - driven safety method [17]. The security message distribution over VANETs One region finding direction is through a committed routing path, and the other region is pass on to the neighboring vehicles [2][7]. There is more than one source and destination vehicles involved in distribute their data using MAC protocol to access secure information through radio channel access. The vehicle channel access that may not have the timely message dissemination in VANETs [18]. Region based clustering mechanism to be applied in Medium Access Control Protocol to reduce the contention period and also support vehicles to leave and join inter-vehicle communications at high speed [17][18]. The Trusted Authority in vehicle communication revoking an illegal vehicle, Because of this illegal vehicle intention to hijack and modify the Messages. Furthermore, revocation can be achieved by Trusted Authority that is the distributed key management is predictable to facilitate the revocation of malicious vehicles. However road side unit, Here Road side unit acts as the key distributor [19][7], which is containing the identities of misbehaving vehicles. The recipient of each vehicle should verify and receive the messages, check whether the sender is included in the up-to-date details of revocation credential. Using key distribution protocol to preventing RSU [19][7]. However, A misbehaved Road side Unit authorities fail to identify malicious vehicles. Key distribution protocol allows the vehicles to be authenticated with their real identifiers under protection and identities of malicious vehicles if there is a dispute [19].

In Vehicular Ad Hoc Network connections, it is expected that all vehicles will be equipped with a wireless communication device, called an On-Board Unit (OBU), and there will be a number of stationary communication units, called roadside units (RSUs). Both OBUs and RSUs can communicate with each other to improve vehicular safety message dissemination. Such a network that is self-possessed of RSUs and OBUs [7][8]. In VANET facilitate data access. Attribute-Based Access Control System for emergency services with security assurance over Vehicular Ad Hoc Networks to improve the efficiency of rescues assembles via emergency communications over VANETs [12]. Vehicle platoon can communicate with RSU and identified other vehicle platoon. Oped algorithm to identify vehicle platoons from road traffic and optimized the setting of traffic signals [1][12], and also Vehicular networks correspond to an exciting application situation for not only traffic safety and efficiency but more commercial applications[1].

In this paper, goal is to develop a method that produces security message dissemination and avoid the falls and modify messages from the vehicle group Authority, which is misbehaving vehicle in this communications. So that must identifying and revoking a misbehaving vehicle to disseminate security messages over VANET using IEEE 1609.2.

II. Related Works

Vehicular networks represent an attractive application circumstances for not only safety message communication and effectiveness, but more commercial related applications, such as online service, defense, etc. In this paper, Introduce a new techniques relatively different security pattern in VANETs where each vehicle can communicate safety messages and identifying malicious vehicle group revoked from the Network to protect the safety of other legally vehicle. Using IEEE 1609.2 propose sending credential with a vehicle to vehicle communication. [16] The trusted Authority disseminates messages between the vehicle groups. Beneficiary vehicle groups Authority checks the validity of the certificate to decide on accepting/rejecting the message. A certificate could be invalid when the certificate has been revoked by the Trusted Authority. When invalid certificate detected it would be malicious vehicle group because of either a fault or an intentional action, in this process of identifying and revocation of malicious vehicle and dissemination of this revocation information to other lawfully vehicle group. The IEEE1609.2 communication standard requires the Trusted Authority to revoke the certificate of any malicious vehicle group. Once the Trusted Authority revokes a certificate, it is essential for the Trusted Authority to inform the other participating vehicle group of this revocation. The time of revocation of a malicious vehicle that needs to be project some phases for vehicular ad hoc Network communication.

III. Preliminaries

A. System Model

In our Vehicular Ad hoc Networks ability to identifying malicious vehicle and revoke from the networks. TA can disseminate messages over the VANET. IEEE 1609.2 security services for Application and Management secure data (message) exchange over this Network. In this Network Secure message formats and processing, also define the circumstances for using secure message Exchanges.

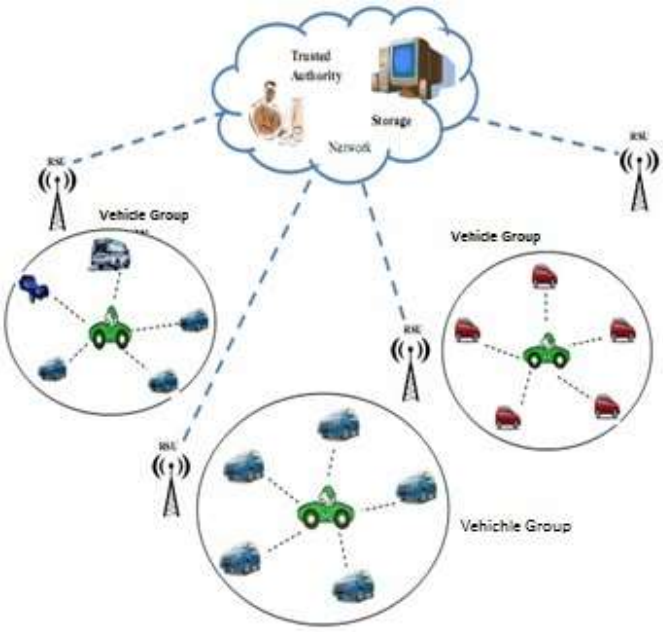

Figure: 1. VANET Architecture

B. Data Access Control

Data Access control is required to illustrate the process that each Vehicular Group can perform in the network. IEEE 1609.2 protocol defines 5.9 GHz DSRC Security.

Anonymity: Anonymity typically refers to the state of an individual vehicle identity. The sender of a safety message should be authenticated to guard against the pretence and

message counterfeit attacks, but the authentic identity of the sender should not be disclosed from message authentication protocol in order to preserve sender's privacy.

Authenticity: Authenticated vehicle should communicate to other vehicle with genuine or original information. Information is authentic when it is the information that was originally created. There is currently requirement for OBU to RSU authentication. The signed and encrypted message type in 1609.2 encrypts the entire message and could be used as a single authenticated response from the OBU. This is the mechanism used to secure transactions over VANET

Confidentiality: Unauthorized vehicle does not access and modify the communication messages. It ensure that only those with the rights and privileges to access Vehicular information. Here Vehicle Group has privileges to access with TA through RSU. Unauthorized vehicle Group cannot view information's. To protect the Confidentiality of Vehicular information, there is number of measures, like Information classification, secure document storage, Application of general security policies, etc….. In addition, if detect any malicious vehicle that should be revoked from the network to protect the safety of other legal vehicles in the system; the actions taken by Trusted Authority while the legal vehicle Group receiving the false message from the misbehaving Vehicle Group. Trusted Authority involves controlling and accessing the Vehicles and receiving the false event report from the Lawfully Vehicle Group. Based on this event TA can take action against the particular Vehicular Group. (i.e., Vehicle revocation)

C. Requirements

This paper aims to prevent the safety messages from the hijackers and identifying misbehaving vehicles revoked from the VANET network. The functional requirements in terms of security and efficiency are presented as follows.

Availability – The real-time interaction between vehicular networks and the physical world, availability is an important factor in VANET system design. This may have a most important impact on the safety and efficiency of future VANET systems.

Security – Communication is mainly performed by exchange of messages. It is largely dependent upon trust worthiness of messages. It can be established by valid communication between trusted vehicle group and group member. Security is one of the main concerns in use of Vehicular ad hoc Networks. and the dissemination of messages from a source must achieve data integrity and identity authentication.

Hands-off –Handoffs occurs when the Vehicle completely breaks connection with the old RSU / OBU before connecting to the new RSU / OBU and synchronizing itself to it.

D. Vehicle Group Registration

RSUs and vehicle group register with the TA to use VANETs. Upon successful registration, a vehicle member issued public/private key pair (mpk; msk) to each RSU and group vehicles. The TA associates the group member's credential and includes this pair of information into a credential ID list. Each vehicle group registers with TA which is required for the threshold-authentication. The registration is carried out by the user.

E. Misbehaving Vehicle Detection

Identifying malicious vehicle using cryptographic SHA 1 hash function, that is perceive system in vehicular Network. However, the Vehicular Group disseminates same messages with their own Group vehicle member, which is sent from the RSU to all vehicle groups. The malicious vehicles can disseminate a modified and faked message to other vehicle group member. It can cause safety related events, like false alarm, wrong message updating, and road traffic jam. The vehicle group sent acknowledgement report to RSU about the number of faked messages. RSU calculate the hash value for each false message F ∈ i, j, k, and obtain set of each hash value Hv. if Hv and two or more false message in i, j, k map to the same hash value. The RSU suspect the event to be faked and sent detection message to Trusted Authority to take necessary action.

F. Privacy Preservation

In VANET safety-related applications, Vehicular may take life-critical actions based on messages received from other vehicles. However, any malicious behaviour of a user, such as bring in false information, or modifying and replaying the disseminated messages, could be fatal to other users. In addition, users are very traditional about their privacy-related information. For example, users will not accept if the travelling route and information is revelled to the public. Therefore, security and privacy preservation are satisfied among the critical challenges in the operation of VANETs. It is precondition to elaborately intend a set of mechanisms to

achieve secure communication in VANETs. It guarantees that any additional authentication beyond the threshold will result in the revocation of misbehaving users.

G. Misbehaving Group Revocation

Misbehaving group revocation scheme, each vehicle group maintains the group members to receive and communicate safety messages from the RSU. The Group vehicle header and group vehicle member can periodically exchange their movement details through messages, which is used to avoid misbehaving vehicle cannot enter into the network instead of the group member. Each vehicle maintains a coordinate vehicle, where the moving direction is the x axis, and each vehicle chooses the nearby vehicles as Group. The coordinate of the position vehicle group is represented by its shortest distance to the x – axis and y – axis, which are denoted by Δ_b and Δ_a. The vehicle group header can estimate the relative motion deviation between vehicles and determine whether they are in the same group or not. The stochastic moment series analysis and observed location to provide accurate and automatic group identification.

The TA receives the misbehaving vehicle detection event report from the RSU. TA identifies the group and related vehicles can revoke from the VANET networks. The RSU can send revocation list messages to all connected vehicles and their groups. For that the vehicle cannot communicate with other malicious vehicle and its access between lawfully vehicles.

IV. CONCLUSION

In Vehicular communication needs to secure high sensitive data (messages) and identify the malicious vehicle group in the Networks during the safety message dissemination over VANET. Trusted Authority disseminates sensitive data to all connected Vehicle group within the Network. There are illegal vehicle group could hijack and modify the sensitive data (messages) and disseminate duplicate data (messages) to the other vehicle group. Rectifying above problems, "Data Access Control for Identifying Malicious Vehicle in Vehicular Ad-Hoc Network" techniques used to prevent duplicate message dissemination from the Unlawfully Vehicle group. And also Revoking malicious vehicle group from the network to protect the legally Vehicle in the Vehicular Ad – hoc Network.

REFERENCES

[1] J Yang Zhang, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "V-PADA: Vehicle-Platoon-Aware Data Access in VANETs", IEEE Transaction on Vehicular Technology, vol 60, no. 5, June 2011

[2] Fu-Kuo Tseng, Yung-Hsiang Liu, Jing-Shyang Hwu, and Rong-Jaye Chen, "A Secure Reed–Solomon Code Incentive Scheme for Commercial Ad Dissemination Over VANETs", IEEE Transactions on vehicular technology, vol. 60, no. 9, November 2011

[3] Mate Boban, Tiago T. V. Vinhoza, Michel Ferreira, Jo˜ ao Barros, and Ozan K. Tonguz, "Impact of Vehicles as Obstacles in Vehicular Ad Hoc Networks", IEEE Journal on communication, vol. 29,no.1, Jan 2011

[4] Nikoletta Sofra, Member, IEEE, Athanasios Gkelias, Member, IEEE, and Kin K. Leung, Fellow, IEEE, "Route Construction for Long Lifetime in VANETs", IEEE Tran. on vehicular technology, vol. 60, no.7, Sep 2011

[5] Abderrahim Benslimane, Tarik Taleb, and Rajarajan Sivaraj," Dynamic Clustering-Based Adaptive Mobile Gateway Management in Integrated VANET – 3G Heterogeneous Wireless Networks",IEEE Journal on Communication, vol. 29, no. 3, March 2011

[6] Ying Zhu, Member, IEEE, "Attack Pattern Discovery in Forensic Investigation of Network Attacks", IEEE Journal on Communication, vol. 29, no. 7, Aug 2011

[7] Min-Ho Park, Gi-Poong Gwon, Seung-Woo Seo, and Han-You Jeong, Member, IEEE, "RSU-Based Distributed Key Management (RDKM) For Secure Vehicular Multicast Communications", IEEE Journal on Communication,vol. 29, no. 3, March 2011

[8] Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux, "Efficient Certificate Revocation List Organization and Distribution", IEEE Journal on Communication, vol. 29, no. 3, March 2011

[9] Karim El Defrawy, Member, and Gene Tsudik, Senior Member, "Privacy – Preserving Location - Based On-Demand Routing in MANETs", IEEE Journal on Communication, vol. 29, no. 10, Dec 2011

[10] T.W.Chim, S.M.Yiu,LucasC.K.Hui, and Victor O. K. Li, Fellow, IEEE, "OPQ: OT-Based Private Querying in VANETs", IEEE Transaction on Intelligent Transportation system, vol. 12, no. 4, Dec 2011

[11] Jinyuan Sun, Member, IEEE, Xiaoyan Zhu, Chi Zhang, Student Member, IEEE,and Yuguang Fang, Fellow, IEEE, "RescueMe: Location-Based Secure and Dependable VANETs for Disaster Rescue" , IEEE Journal on Communication, Vol. 29, No. 3, March 2011

[12] Lo-Yao Yeh,Yen-Cheng Chen, and Jiun-Long Huang, "ABACS:An Attribute-Based Access Control System for Emergency Services over Vehicular Ad Hoc Networks", IEEE Journal onCommunication,Vol.29,No.3,March 2011

[13] Liqun Chen Member, IEEE, Siaw-Lynn Ng, and Guilin Wang,

"Threshold Anonymous Announcement in VANETs", IEEE Journal onCommunication,Vol.29,No. 3, March 2011

[14] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty, "P2 DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks", IEEE Journal onCommunication,Vol. 29, No. 3, March 2011

[15] Yanyan Zhuang, Jianping Pan, Yuanqian Luo, and Lin Cai, "Time and Location-Critical Emergency Message Dissemination for Vehicular Ad-Hoc Networks" , IEEE Journal onCommunication, Vol. 29, No. 1, Jan 2011.

[16] Arzad Kherani and Ashwin Rao, "Performance of Node-Eviction Schemes in Vehicular Networks" , IEEE Transactions on Vehicular Technology, Vol. 59, No. 2, Feb 2010

[17] Mehdi Khabazian,IEEE,Sonia A¨ ıssa, IEEE, and Mustafa, Mehmet-Ali, Member, IEEE, "Performance Modeling of Message Dissemination In Vehicular Ad Hoc Networks with Priority" , IEEE Journal onCommunication,Vol. 29, No. 1, January 2011

[18] Yen-Cheng Lai, Member, IEEE, Phone Lin, IEEE, Wanjiun Liao, Fellow, IEEE, and Chung-Min Chen, "A Region-Based Clustering Mechanism for Channel Access in Vehicular Ad Hoc Networks" , IEEE Journal onCommunication,Vol. 29, No. 1, Jan 2011

[19] Yong Hao, Student Member, IEEE, Yu Cheng, Senior Member, IEEE,Chi Zhou, Senior Member, IEEE, and Wei Song, "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs" , IEEE Journal on Communication, Vol. 29, No. 3, March 2011

[20] Kannan Govindan, Member IEEE and Prasant Mohapatra, Fellow IEEE, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey" , IEEE, Vol. 14, No. 2, Second Quarter 2012

[21] Osama Bazan, and Muhammad Jaseemuddin, "A Survey On MAC Protocols for Wireless Adhoc Networks with Beam forming Antennas" , IEEE, Vol. 14, No. 2, Second Quarter 2012

[22] Francisco Javier Ros, Pedro Miguel Ruiz, IEEE, and Ivan Stojmenovic, IEEE, "Acknowledgment-Based Broadcast Protocol for Reliable and Efficient Data Dissemination in Vehicular Ad Hoc Networks" , IEEE Transaction on Mobile Computing, Vol. 11, No. 1, January 2012

[23] Rongxing Lu, Xiaodong Lin, Tom H. Luan,iaohui Liang, and Xuemin (Sherman) Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs", IEEE Transactions On Vehicular Technology, Vol. 61, No. 1, January 2012

[24] Shan Chang, Yong Qi, Hongzi Zhu, hong Zhao, and Xuemin (Sherman) Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks" , IEEE Transaction, Vol. 23, No. 6, June 2012

[25] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin (Sherman) Shen, University of Waterloo "Security in Vehicular Ad Hoc Networks" ,IEEE Conference 2011