© 2017 IJSRST | Volume 3 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

A Review on Group Based Authentication in V2V Communication

Snehal M. Choudhari[1], Hirendra R. Hajare[2]
[1]M. Tech Scholar, Dept of Computer Science and Engineering, Ballarpur Institute of Technology, Ballarpur, Maharashtra, India
[2]HOD, Dept of Computer Science and Engineering, Ballarpur Institute of Technology, Ballarpur, Maharashtra, India

ABSTRACT

Vehicular ad hoc networks (VANET's) are an area of developing techniques. It has become an upcoming technology of this modern world in vehicular communications. We propose group-based V2V authentication and communication for safety message dissemination with lightweight solution, decentralized via group leaders efficient, economical and applicable in real mode. In this paper, we investigate security architecture for V2V communication that ensures integrity, confidentiality, anonymity, authenticity and non-repudiation. We simulate the existing security solutions and we show that our group-based authentication proposal performs better than other schemes.

Keywords: *VANET, V2V Communication, RSU, Communication, PKI, Authentication*

I. INTRODUCTION

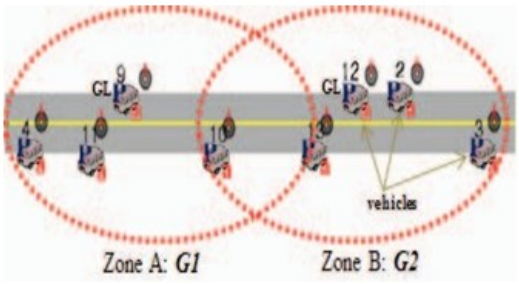
VANETs are ad hoc networks, highly dynamic, with little access to the network infrastructure and offering multiple services. In V2V communication, the exchanged information (emergency message, safety messages etc.) through wireless channels requires a secure environment to avoid attacks on V2V network. In V2V, the communication media used are characterized by a short latency and a high transmission rate. This architecture is used in different scenarios of broadcasting alerts (emergency braking, collision, deceleration, etc.) or in a cooperative driving. In this paper, we consider V2V communications and we propose a framework for group-based V2V authentication adopting the cryptographic components of the security standard for safety message dissemination. For efficient and secure V2V communication, we form vehicular groups and distribute keys for the encryption and the signature per group. The formed groups are based on the current location and speed of the vehicle on the road.

II. LITERATURE SURVEY

Several works investigated the security of VANET and V2V communication. The l609.2 standard [l][2] defines the infrastructure based on PKI [20][2l] for keys and certificates management. Symmetric encryption AES-CCM (Advanced Encryption Standard-Counter with Cipher Block Chaining Message), asymmetric signature ECDSA (Elliptic Curve Digital Signature Algorithm), and asymmetric encryption ECIES (Elliptic Curve Integrated Encryption Scheme) are used for the keys distribution and the safety messages formats. The authentication is studied in [3][7][9][l0][ll][24]. V2I communication is considered in [3] and two successive authentication mechanisms are proposed to reduce overhead on the RSU when authenticating the vehicles. [7] Includes several authentication schemes where anonymity, pseudonyms, trust and privacy are ensured via short-lived keys changing frequently. Symmetric encryption is used to produce an effective delay and RSUs are used for authentication and key distribution. In a decentralized lightweight authentication scheme for V2V is given to protect valid users in VANETs from malicious attacks based on the concept of transitive trust relationships Thus the

amount of their cryptographic calculation is less than in existing schemes. A non-interactive authentication scheme is presented in [l0], providing privacy among drivers in V2V communication networks; Drivers may change their own set of public keys frequently without control from the TTP (Third Trusted Party).

III. PROPOSED WORK



Our main to provide group based security with high speed. For that we are placing the nodes in the networks and performing the communication between them. we use the best nodes are found which will act as decentralized nodes for communication and authentication .these nodes are found using highest energy nodes in the group. We are using the decentralized protocol. This protocol is applied and nodes which are authenticated by the central nodes are used for communication. Using Bicasting we will reduce the delay of the authentication to speed up the communication of the system

IV. CONCLUSION

In this paper, we introduced group-based V2V authentication and communication for safety message dissemination; a security architecture for V2V communication that ensure integrity, confidentiality, anonymity, authenticity and non-repudiation. A lightweight solution, decentralized via GLs, efficient, economical and applicable in real mode

V.REFERENCES

[1] Mayank Verma, Dijiang Huang, "SeGCom: Secure Group Communication in VANETs", published in Communications and Networking, 2009. ComNet 2009. IEEE 2009.

[2] Mahmoud Abuelela, Stephan Olariu, Khaled Ibrahim, "A Secure and Privacy Aware Data Dissemination For The Notification of Traffic Incidents", In *Proceedings of the IEEE Vehicular Technology Conference - Spring*. Barcelona, April 2009.

[3] Dr. Michele Weigle , Standards: WAVE / DSRC / 802.llp, spring 2008

[4] Sandeep K. Harit, Gaurav Singh, Neeraj Tyagi, "Fox-Hole Model for Computer and Communication Technology (ICCCT), 20l2.

[5] Lu Song, Qingtong Han, Jianwei Liu, "Investigate Key Management and Authentication Models in VANETs", Published in: IEEE International Conference on Electronics, Communications and Control (ICECC), 20ll.

[6] Ashwin Rao, Ashish Sangwan, Arzad A. Kherani Anitha Varghese, Bhargav Bellur, Rajeev Shorey , "Secure V2V Communication With Certificate Revocations", Published in IEEE Mobile Networking for Vehicular Environments 2007.

[7] Ming-Chin Chuang, Jeng-Farn Lee,"TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks", Published in: Systems Journal, IEEE (Volume:8 , Issue: 3), 20l3.

[8] Fatty M. Salem, Maged H. Ibrahim, I. I. Ibrahim, " Non-Interactive Authentication Scheme Providing Privacy among Drivers in Vehicle-to-Vehicle Networks", Sixth International Conference on Networking and Services, 20l0.

[9] Rens van der Heijden ,"Security Architectures in V2V and V2I Communication", *13*th *Twente Student Conference on IT* June 2lst, 20l0, Enschede, The Netherlands.

[10] CGI Group Inc, "Public Key Encryption and Digital Signature", 2004. Tim Polk, "Introduction to Public Key Infrastructure", January l3, 2005.

[11] Tim Weil, "Securing Wireless Access in Vehicular Environments (WAVE)", IEEE 2008.

[12] Baber Aslam, Cliff C. Zou, "Distributed Certificate Architecture for VANETs", IEEE Military Communications Conference (MILCOM'09), Boston, Oct. l8-2l, 2009.

[13] Klaus Plößl , Hannes Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks", Computer Standards & Interfaces 30(6): 390-397 (2008).

[14] Maxim Raya, Adel Aziz, Jean-Pierre Hubaux,"Efficient Secure Aggregation in VANETs", VANET '06 Proceedings of the 3rd international workshop on Vehicular ad hoc networks – Pages 67-75.