IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

A Memory Efficient Key Management and Distribution Scheme for Vehicular Adhoc Network

Ankur Jain[1], Ratnesh Dubey[2], Vineet Richariya[3]

LNCT Bhopal[1, 2, 3]

Abstract: VANET has lot of security issues. Since evolution of VANET many key management and distribution algorithms have been proposed. In this paper a memory efficient key management and distribution scheme for VANET have been proposed. The proposed scheme is compared with traditional scheme and it is found proposed outperforms the traditional ones.

Keywords: VANET, Vehicular Adhoc Network, Key Management, Distribution Scheme, Memory Efficient.

INTRODUCTION

With the recent developments in computing and wireless communication technologies, networks that can form the basis for such applications can be envisioned. These networks will be completely mobile, require little or no infrastructure, and support the applications in a dynamic, random, and multi-hop topology. Vehicular Network is an envision of ITS. In this network each vehicle is equipped with the technology that allows the vehicle to communicate with other vehicles as well as with the roadside infrastructure. For example, base stations also known as Roadside Units (RSUs) located in some critical sections of the road such as traffic lights, intersections, or stop signs, improve driving experience and make driving safer. By using communication devices, also known as Onboard Units (OBUs), vehicles can communicate with each other as well as with RSUs. A vehicular network is a self-organized network that enables communication between vehicles and RSUs, and the RSUs can be connected to a backbone network, so that many other network applications and services, including internet access, can be provided to the vehicles. Vehicular networks are promising in allowing diverse communication services to drivers and passengers. High interest for these networks is also shown from governmental authorities and standardization organizations. An example of a vehicular network is shown in Figure 1.

The emergence of VANETs through IVC is a form of MANETs, providing communications among nearby vehicles as well as between vehicles without fixed infrastructure support. The term VANET was originally adopted to reflect the ad hoc nature of these highly dynamic networks. The term ad hoc network was associated widely with unicast routing-related research. VANETs comprise Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications based on WLAN technologies. VANETs have similar or different radio interface technologies, employing short-range to medium-range communication systems. Vehicles can be either private, belonging to individuals or private companies, or public transportation means (e.g., buses and public service vehicles such as police cars). There has been significant interest and progress in the field of VANETs over the last several years.

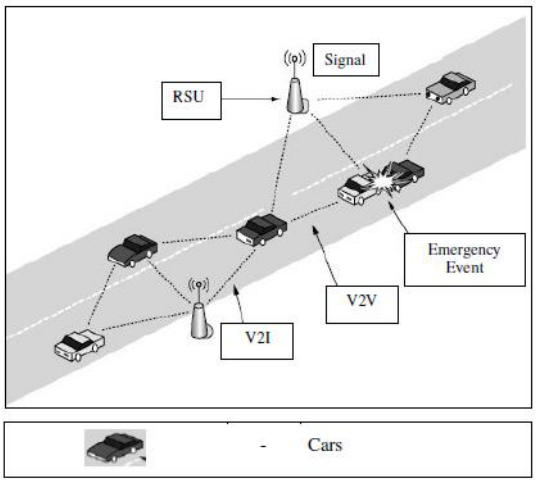


Fig 1.1: Example of VANET

The concept of leveraging wireless communication in vehicles has fascinated researchers since the 1980s and it has been studied in the literature (Kawashima 1990).
Several factors have led to this development, including the wide adoption of Institute of Electrical and Electronics Engineers (IEEE) 802.11 technologies, the embrace of vehicle manufacturers of information technology. It is used to address the safety, environmental, and comfort issues of their vehicles and the commitment of large national and regional governments to allocate wireless spectrum for vehicular wireless communication. Although cellular networks enable convenient voice communication

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

and simple infotainment services to drivers and passengers, they are not well-suited for certain direct V2V or V2I communications. However, VANETs can send and receive hazard warnings or information on the current traffic situation with minimal latency. With the availability since the late 1990s of low-cost GPS receivers and WLAN transceivers, research in the field of IVC gained considerable momentum and it has been studied by Jiang et al (2006). The major goals of these activities are to increase road safety and transportation efficiency. The applications of VANET technology are not completely orthogonal. For example, reducing the number of accidents can in turn reduce the number of traffic jams, which could reduce the level of environmental impact. Due to the importance of these goals for both the individual and the nation, various projects are underway and several consortia have been set up to explore the potential of VANETs.

SPECIAL CHARACTERISTICS OF VANETS

VANETs have special behaviour and characteristics, distinguishing them from other types of mobile networks (i.e. MANETs). In comparison to other communication networks, VANETs come with unique attractive features which are as follows (Nekovee 2005):

Unlimited transmission power: Mobile device power issues are usually not a significant constraint in VANETs as in the case of classical ad hoc or sensor networks, since the node (vehicle) itself can provide continuous power to computing and communication devices.

Higher computational capability: Operating vehicles can afford significant computing, communication, and sensing capabilities.

Potentially large scale: Unlike most ad hoc networks studied in the literature that usually assume a limited network size, VANETs can extend over the entire road network and include many participants.

High mobility: The environment in which VANETs operate is extremely dynamic and includes extreme configurations. On highways relative speeds of up to 300 km/h may occur, while density of nodes may be 1–2 vehicles/1 km on low busy roads. On the other hand, in the city, relative speeds can reach up to 60 km/h and the nodes density can be very high, especially during the rush hour.

Partitioned network: VANETs will be frequently partitioned. The dynamic nature of traffic may result in large inter-vehicle gaps in sparsely populated scenarios and hence in several isolated clusters of nodes.

Network topology and connectivity: VANET scenarios are very different from classic ad hoc networks. Since vehicles are moving and changing their positions continuously, scenarios are very dynamic. Therefore the network topology changes frequently as links between the nodes connect and disconnect very often. Indeed, the degree to which the network is connected is highly dependent on two factors: the range of wireless links and the fraction of participant vehicles.

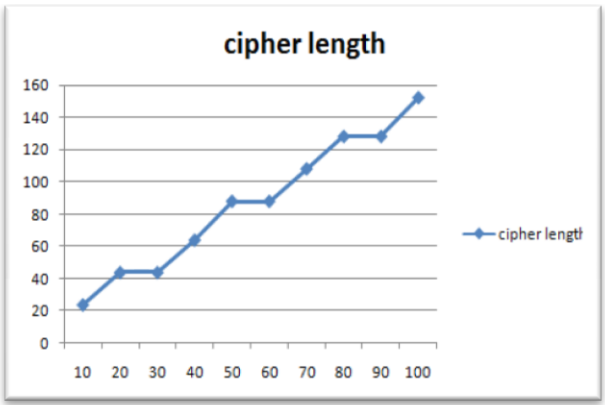
Proposed key distribution and management

Algorithm Main
{
1. Configure mobile ad-hoc network for 50 nodes.
2. Form 2 clusters of 25 nodes each.
3. Form a certification authority (CA) for key generation and management.
4. Generate keys for CA using RSA which will be used for digital signature.
5. Distribute key pairs to all mobile nodes in networks.
6. Encrypt using private key of the sender.
}

Algorithm node_leave
{
1. Key revocation of the node that had left network by CA.
2. Inform all nodes in network so that they can remove that nodes public key from their list.
}

Algorithm node_join
{
1. Generate key pair for new node by CA.
2. Public key distribution for new node in cluster it joined.
}

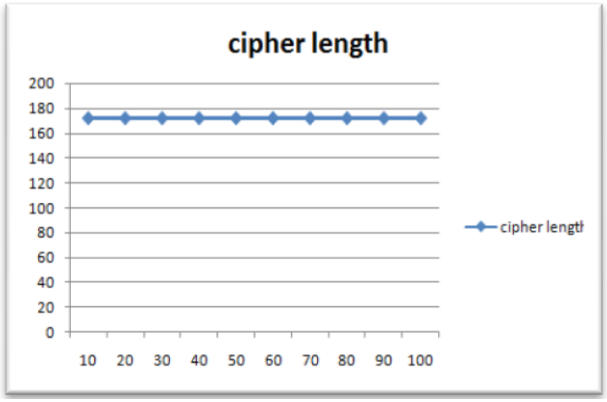
First of all a 50 vehicle network is configured here. 2 Clusters are formed with each having 25 vehicles. A certification authority is formed which placed at the center of the road map. Keys generated by multi group key management algorithm are distributed to all vehicles by CA. All the vehicles communicate by encrypting messages before sending and messages are decrypted by public key of sender.



IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016



CONCLUSION

In this paper a key management and distribution scheme is proposed with two variants one is fixed length encryption and second is variable length encryption. It is found for a network like VANET variable length cipher is more memory efficient than fixed length.

REFERENCES

[1] N. Kumar, N. Chilamkurti, J.P.C. Rodrigues, Learning automata-based opportunistic data aggregation and forwarding scheme for alert generation in vehicular ad hoc networks, Comput. Commun. 39(1) (2014) 22–32.
[2] A. Kontorovich, A. Trachtenberg, Deciding unique decodability of bigram counts via finite automata, J. Comput. Syst. Sci. 80(2) (2014) 450–456.
[3] N. Kumar, J. Kim, ELACCA: efficient learning automata based cell clustering algorithm for wireless sensor networks, Wirel. Pers. Commun. 73(4) (2013) 1495–1512.
[4] N. Kumar, N. Chilamkurti, J.H. Park, ALCA: agent learning based clustering algorithm in vehicular ad hocnetworks, Pers. Ubiquitous Comput. 18(8) (2013) 1683–1692.
[5] K.A. Shim, CPAS: an efficient conditional-privacy authentication scheme for vehicular sensor networks, IEEE Trans. Veh. Technol. 61(4) (2012) 1874–1883.
[6] F. Ipate, Learning finite cover automata from queries, J. Comput. Syst. Sci. 78(1) (2012) 221–244.
[7] S. Misra, V. Krishna, V. Saritha, LACAV: an energy efficient channel assignment mechanism for vehicular ad hoc networks, J. Supercomput. 62(3) (2012) 1241–1262.
[8] P.B.F. Duarte, Z.M. Fadlullah, A.V. Vasilakos, N. Kato, On the partially overlapped channel assignment on wireless mesh network backbone: a game theoretic approach, IEEE J. Sel. Areas Commun. 30(1) (2012) 119–127.
[9] T.W. Chim, S.M. Yiu, L.C. Hui, O.K. Li, SPECS: secure and privacy enhancing communication schemes for VANETs, Ad Hoc Netw. 9(2) (2011) 189–203.
[10] Y. Hao, Y. Cheng, Ch. Zhou, W. Song, A distributed key management framework with cooperative message authentication in VANETs, IEEE J. Sel. Areas Commun. 29(3) (2011) 616–629.
[11] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, in: Proceedings of Asiacrypt, vol.2248, 2011, pp.514–532.
[12] Y.S. Yen, C.H. Chao, R.S. Chang, A.V. Vasilakos, Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs, Math. Comput. Model. 53(11–12) (2011) 2238–2250.
[13] Q. Wu, J.D. Ferrer, G. Nicolás, Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications, IEEE Trans. Veh. Technol. 59(2) (2010) 559–573.
[14] J. Torkestani, M. Meybodi, Mobility-based multicast routing algorithm for wireless mobile ad-hoc networks: a learning automata approach, Comput. Commun. 33(6) (2010) 721–735.
[15] Ch. Li, M. Hwang, Y. Chu, A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc network, Comput. Commun. 31(12) (2008) 2803–2814.
[16] A. Wasef, Y. Jiang, X. Shen, and ECMV: efficient certificate revocation management scheme for vehicular ad hocnetworks, in: Proceedingsof IEEE Globecom, 2008.