Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 11, November 2017, pg.18 – 24

Security in Vehicular Ad-hoc Network using LiFi

Prakash Tripathi
Department of RDBM & Mahatma Gandhi Chitrakoot Gramodaya University, India
prakashmca.tripathi91@gmail.com

Abstract— Vehicle connectivity can be considered as an emerging technology that provides dissemination of warning messages and traffic information to vehicles running on the road. The deployment of vehicular ad-hoc network communication is strictly dependent on strictly on their security and privacy features. Recent advances in the hardware and software technology, tremendous improvements are made. Emerging Vehicular Ad-hoc Networks have the potential to improve the safety, traffic efficiency and as well as comfort to both drivers and passengers of highways. In the last three decades, various kinds of improvements are made in Wireless Ad-hoc Network and now a day's one of the most attractive research topic is Vehicular Ad-hoc Network (VANET) and become the most relevant form of Mobile Ad-hoc Networks. In this paper we address the Security in Vehicular ad-hoc Network .It contain architecture of LiFi that improves the message dissemination transmission rate than existing architecture.

Keywords— IEEE 802.11, IEEE 802.15, ECDSA, G-Private Key, I-Public Key

I. INTRODUCTION

Vehicular ad-hoc networks (VANETs) are wireless communication networks that do not require any kind of fixed infrastructure. It is based on IEEE 802.11p standard for Wireless Access for Vehicular Environment (WAVE). Vehicular Networks (VNs) consist of vehicles and Road Side Units (RSUs) equipped with on-board processing and wireless communication modules. Europe and US are using the Vehicular Network for safe driving and traffic management. In October 1999, the US Federal Communications Commission (FCC) allocated 75 MHz (the 5.85 –to 5.925-GHz portion) of the spectrum in America for Dedicated Short Range Communications (DSRC) for Vehicle-to-Vehicle or Vehicle-to-Roadside communication [1, 2]. Upcoming Traffic safety initiatives rely heavily on information technology, which means that vehicles must be able to authenticate themselves and be traceable whenever necessary for law enforcement (detection of speed vehicles), crash reconstruction or toll collection. [3]

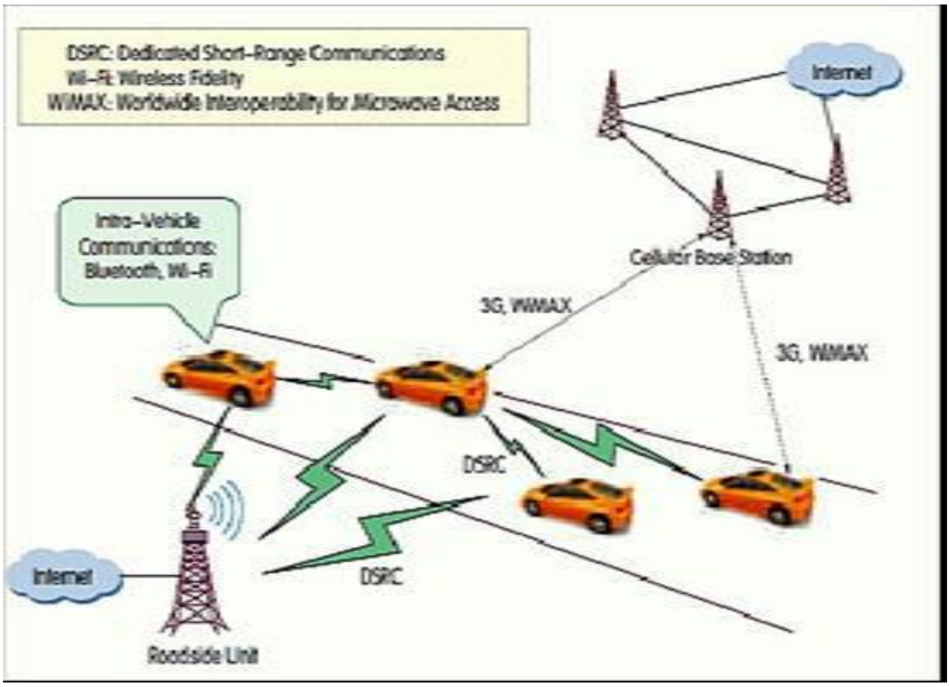
DSRC: Dedicated Short-Range Communications
Wi-Fi: Wireless Fidelity
WiMAX: Worldwide Interoperability for Microwave Access
Internet
Intra-Vehicle Communications: Bluetooth, Wi-Fi
Cellular Base Station
3G, WiMAX
3G, WiMAX
DSRC
DSRC
Internet
Roadside Unit

Fig. 1 Vehicular Ad-hoc Network

II. Review Literature

Vehicular ad-hoc network is emerging research area where most of the scientist, researchers and developers are working to find the solution to increase the security of messages that are passed vehicle-to-vehicle, vehicle-to-roadside unit. In this way some existing protocols are used such as digital signature, public-key-infrastructure and pseudonym. Public-Key-Infrastructure contains public-key-cryptography (PKC) or secret-key-cryptography (SKC) based solutions, the public-key-cryptography (PKC) approach can be further classified into two subcategories: traditional PKI-based digital signature techniques [4], [5] and group-signature-techniques [6].

Toady every vehicle is registered with its national or regional authority, which allocates a unique identifier to it, but in parts of the US and the EU, registration authorities have used electronically identifying vehicles and similar progress is being made toward machine-readable driving licenses. To allow the wireless authentication of vehicles, these authorities must provide each vehicle with a private/public key pair, along with a shared symmetric key, and a digital certificate of its identity and public key. It will use to sign broadcasted safety messages. This ensures that other vehicles will be able to authenticate a received message if it includes a digital signature and the corresponding certificate issued by a CA (Certification Authority) such authorities will most likely be cross certified, making it possible for any vehicle to check any other vehicle's certificates [3] [4].

In traditional PKI-based digital signature techniques the anonymous public-key certificate of Raya and Hubaux[4] is the first noteworthy attempt to ensure security and privacy in vehicular communications, while also reserving the ability to trace messages back to their senders. Raya and Hubaux [4] proposed a protocol for secure vehicular communication. Each vehicle is preloaded with a large number of private keys, as well as their corresponding anonymous certificates (perhaps approximately 43800). The sending vehicle then randomly selects one of the anonymous certificates, using its corresponding private key to digitally sign messages to be sent. To verify the integrity of the message received, other vehicles use the sender's public key associated with this signature. Each anonymous certificate has only a short lifespan to meet the driver's privacy requirements. Unlike traditional public-key certificates, anonymous certificates are generated using the pseudo-identities of the vehicles, instead of identifying information from the driver. Each driver's entire list of anonymous certificates, which is mapped to the driver's real identity, is kept by the authority, allowing messages to be traced back to the driver in the event of a dispute. In group-signature techniques Lin et al. [6] discovered the fact that the unique characteristics of group signature, which is an important cryptographic primitive, perfectly match the security and privacy requirements in VANETs. By taking different security and privacy requirements of two types of VANET communications namely, vehicle-to-infrastructure and vehicle-to-vehicle communications, they propose a novel secure and privacy-preserving protocol for vehicular communication, based on a combination of group signature and identity (ID)-based signature techniques. Lin et al. [7] developed a time-efficient and secure vehicular communications (TSVC) scheme, based on Timed Efficient Stream Loss-tolerant Authentication (TESLA) [8]. In TSVC, a number of hash chains are generated in advance for a given vehicle. The vehicle selects one chain at random and broadcasts the commitment of the chain to its neighbors, which is simply protected by a traditional PKI-based digital signature. Then, the vehicle uses the elements of the chain to generate message authentication codes (MACs) for messages originating from it. Its neighbors are able to authenticate the messages based on these MACs; however, the high dynamics of topological structure for vehicular network could jeopardize TSVC's effectiveness of message authentication. There have been several proposals for privacy preservation of VANETs. Using pseudonyms is a natural idea. It is preferable to preserve the location privacy of a vehicle by breaking the likability between two locations, for which the vehicle can update its pseudonym after each transmission, while the pure pseudonym schemes do not support the secure functionality of authentication, integrity, and non-repudiation.

A. Communication Protocols for VANETs

A vehicular ad-hoc network uses various kinds of communication protocols such as Cellular networks, IEEE 802.16 (WIMAX), or IEEE 802.11. Cellular or WIMAX based networking is limited to single-hop base station to vehicle communications, and can hardly be applied to ad hoc vehicle to vehicle communications. Moreover, cellular and WIMAX networking heavily depend on the availability of infrastructure, which is normally expensive and might not be available in those underdeveloped areas. The cellular network is further limited with bandwidth and not suitable for large scale multihop vehicle to vehicle networking. The 802.11 based protocol has the flexibility in seamlessly supporting both single-hop RSU to vehicle communications and multi-hop vehicle to vehicle communications. System model in vehicular ad-hoc network classified as follows:

i). Certification Authorities:

Authorities are responsible for key generation and malicious vehicle judgment. Authorities have powerful firewalls and other security protections. Therefore, they have the highest security level. We assume that they cannot be compromised.

ii). Road side infrastructure:

Roadside Infrastructure consists of RSUs deployed at the road sides which are in charge of key management in our framework. Traffic lights or road signs can be used as RSUs after renovation. RSUs communicate with authorities through wired network. We assume a trusted platform module is equipped in each RSU. It can resist software attacks but not sophisticated hardware tampering. The cost of a trusted platform module is only a few tens of dollars which is affordable [1].

iii). Nodes:

Nodes are ordinary vehicles on the road that can communicate with each other and RSUs through radio. We assume that each vehicle is equipped with a GPS receiver using DGPS [9] with accuracy on the order of centimeters and an on board unit (OBU) which is in charge of all communication and computation tasks. Nodes have the lowest security level.

B. Group Signature Based Privacy System

In our framework, the communications can be divided into the key distribution phase and the regular broadcast phase. Vehicles get keys dynamically in the key distribution phase and then start to broadcast their geographic and road condition messages periodically in the regular broadcast phase. We resort to the group signature scheme for privacy provision. With group signature, members of a group sign messages under the name of the group. In a group, there are one group public key and many corresponding group private keys. A message that is signed by any group private keys can be verified with the unique group public key, and the signer's identifier will not be revealed. However, authorities hold a tracing key which can be used to retrieve the group private key from the signature. If one group private key is assigned to only one user, the signer can be identified after authorities get its group private key. Those vehicles getting keys from the same RSU form a group, where the communication range of RSUs is 300 meters. We consider that RSUs are only deployed at entrances/exits of the road segments. In a highway scenario, RSUs are normally far away from each other. In the region out of the RSU coverage, vehicles in the same group can communicate with each other in an ad hoc manner. In a city area, RSUs might overlap with each other. We define that a vehicle is only associated with one RSU at a moment to get the service.

C. Distributed Key Management

It has smaller communication overhead than other group signature schemes meanwhile, in the short group signature protocol; there is a group private key generator which can be assigned to key distributors without revealing other secrets. The existence of the generator makes the third party possible to be key distributors. Another attractive feature of the short group signature is that it has a tracing key which can retrieve group private keys from signatures.

III.PROPOSED WORK

Generally a vehicular ad-hoc network consists of vehicles, roadside infrastructure (roadside units), WiMAX (Worldwide Interoperability for Microwave Access), DSRC (Dedicated Short Range Communications), WiFi (Wireless Fidelity), Bluetooth as depicted in figure 1 through which vehicle-to-vehicle and vehicle-to-roadside infrastructure safety messages are transmitted. In our work we use LiFi (Light Fidelity) instead of Wifi and WiMAX since the transmission speed of Lifi is better than Wifi, WiMAX in terms of message dissemination. Generally this research paper is based on secondary data.

Bluetooth, WiFi and WiMAX are wireless technologies that allow devices to interconnect and communicate with each other. Radio waves are electromagnetic waves that have different frequencies. These technologies are radio frequencies similar to analogue radio, FM radio. Bluetooth works on 2.45GHz frequency. WiFi works in two frequency bands 2.4GHz and 5GHz. WiMAX works into two frequency bands 2-11GHz and 10-66GHz. The IEEE standard for Bluetooth is 802.15 data transfer rate is 0.72Mbps (Mega bit per second). It is designed for short range communications with a range of about 10m. It consumes less power so suited for very small battery powered device and portable devices.

Li-Fi stands for Light Fidelity was proposed by the German physicist Harald Haas in 2011 TED (Technology, Entertainment, Design) Global Talk on Visible Light Communication (VLC). Li-Fi is a wireless optical networking technology that uses light emitting diodes (LEDs) for transmission of data. Li-Fi or visible light communication (VLC) technology uses light as medium to deliver high-speed communication. The IEEE standard for LiFi is IEEE 802.15.7. The IEEE 802.15.7 is a high-speed, bidirectional and fully networked wireless communication technology based standard similar to Wi-Fi's IEEE 802.11. Li-Fi is a visible light communication technology (VLC) useful to obtain high speed wireless communication. The difference is WiFi and WiMAX technology uses radio waves for transmission, whereas Li-Fi utilizes light waves. Li-Fi provides better bandwidth, efficiency, connectivity and security than Wi-Fi and has already achieved high speeds larger than 1 Gbps under the laboratory conditions [10].

IV. WORKING OF LIFI

The standard of VLC (IEEE 802.15.7) specifies VLC consisting of mobile-to-mobile (M2M), fixed-to-mobile (F2M) and infrastructure-to-mobile (I2M) communications. The main purpose of VLC standard is to focus on medium-range communications for intelligent traffic systems at low-speed and on short-range mobile to mobile and fixed to mobile communications at high speeds to exchange data. The principle of LiFi is based on sending data by amplitude modulation of the light source in a well-defined and standardized way. LEDs can be switched on and off faster than the human eyes can detect since the operating speed of LEDs is less than 1 microsecond. This invisible on-off activity enables data transmission using binary codes. If the LED is on, a digital '1' is transmitted and if the LED is off, a digital '0' is transmitted. Also these LEDs can be switched on and off very quickly which gives us a very nice opportunity for transmitting data through LED lights, because there are no interfering light frequencies like that of the radio frequencies in Wi-Fi. LiFi is thought to be 80% more efficient, which means it can reach speeds of up to 1Gbps and even beyond. LiFi differs from fibre optic because the LiFi protocol layers are suitable for wireless communication over short distances (up to 10 meters)[10].

In our scenario we use LiFi in Vehicular Ad-hoc Network instead of Bluetooth, DSRC, WiFi and WiMAX because the main objectives of Visible Light Communication (VLC) standard is to focus on medium-range communications for "Intelligent Traffic Systems (ITS)" at low-speed and on short-range mobile to mobile and fixed to mobile communications at high speeds to exchange data so that attacker cannot hack the data/message disseminated between vehicle-to-vehicle and vehicle-to-infrastructure therefore TABLE I and TABLE II show the comparative study between WiFi, WiMAX and LiFi based on their characteristics to prove the result of this paper.

TABLE I
COMPARATIVE STUDY BETWEEN WIFI, WIMAX AND LIFI

Characteristics / Wireless Technology	**WiFi (a)**	**WiMAX**	**LiFi**
Official Release	1997	2004	2011
IEEE Standard	IEEE 802.11 X	IEEE 802.16 Y	IEEE 802.15.7
Spectrum	It uses radio waves (Radio Frequency) of electromagnetic spectrum (electromagnetic waves)	It uses radio waves (RF) of electromagnetic spectrum	It uses Visible Light or optical spectrum i.e. visible light part of electromagnetic spectrum.

Frequency (GHz)	5 GHz	Between 2 -66 i.e. WiMAX operates on two frequency bands 2-11 GHz and 10-66 GHz and has a range of about 50 km with speeds of upto 80 Mbps.	Li-Fi technology is a wireless communication system based on the use of visible light between the red (400 THz(780 nm)) and violet (800 THz(375 nm)).
Range	Based on Radio Propagation and Interference i.e.100 m	Based on Radio Propagation and Interference i.e.50-60 km	Based on Light Intensity i.e.10 m
Data Transfer Rate	54 Mbps	80 Mbps	1 Gbps
Power Consumption	High	High	Low
Cost	High	High	Low
Channel Bandwidth	20 MHz	Between 1.25 MHz – 20 MHz	Unlimited

TABLE III
COMPARATIVE STUDY OF SPEED OF VARIOUS WIRELESS TECHNOLOGIES

Technology	Speed
Lifi	1Gbps
Wifi	150 Mbps
IrDA	4 Mbps
Bluetooth	3 Mbps
NFC	424 Kbps

Source: https://www.ijsr.net/archive/v4i12/NOV151778.pdf

V. CONCLUSIONS

Light Fidelity (LiFi) is emerging area of research. This concept is used in various networking based application such as Mobile Ad-hoc Network (MANET), Vehicular Ad-hoc Network (VANET), Cloud Computing, Cluster Computing etc. LiFi has great potential in the field of wireless data transmission. It is a promising alternative to conventional methods of wireless communications that use radio waves as data carrier. Although this paper is designed to increase the security of vehicular ad-hoc network using LiFi so that intruders cannot hack the message/data disseminated yet many enhancements can be made such as to increase the range and quality of service (QOS) of LiFi. Thus we can achieve more safe communication network.

ACKNOWLEDGEMENT

I would like to thank my father Dr. Rakesh Prasad Tripathi to encouragement for research work.

REFERENCES

[1] Car2Car Consortium. http://www.car-to-car.org/

[2] 5.9GHz DSRC.http://grouper.ieee.org/groups/scc32/dsrc/index.html

[3] Jean-Pierre Hubaux, Srdjan Capkun, And Jun Luo Epfl, “The Security and Privacy of Smart Vehicles”.

[4] Maxim Raya and Jean-Pierre Hubaux, *Laboratory for computer Communications and Applications (LCA), School of Computer and Communication Sciences, EPFL, Switzerland E-mail: {maxim.raya, jean-pierre.hubaux}@epfl.ch* - Securing vehicular ad hoc networks

[5] “Veh. safety commun. project final report. Appendix H: WAVE/DSRC security,” Nat. Highway Traffic Safety Admin., Washington, DC, USA,Apr. 2006.

[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[7] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen,"TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4987–4998, Dec. 2008.
[8]. A. Perrig, R. Canneti, D. Song, and J. D. Tygar, "The TESLA broadcast authentication protocol," *RSA Crypto.*, vol. 5, no. 2, pp. 2–13, Summer/Fall 2002.
[9]. P. Enge, "Retooling the global positioning system," *Scientific American*, May 2004.
[10]. Study Paper on LiFi (Light Fidelity) & its Applications FN Division, TEC.