ORIGINAL RESEARCH

An Efficient and Secure Vehicular Networks Based on IoT and Cloud Computing

Hesham A. El Zouka[1]

Abstract

Undeniably, the increasing number of vehicles on the roads has automatically led to the unbelievable number of accidents occurring every day and the need for a safe communication system among the vehicles has become quite urgent. Using such systems, vehicles can communicate via wireless communication technologies and protocols like ZigBee, WiMax, Bluetooth, GSM, and RF. This paper introduces a communication system that works on preventing accidents by making all the surrounding vehicles communicate using RF, IoT, and LCD technologies to show all the warnings and the indications sent from other vehicles and a VLC that is connected to every vehicle to detect and send all needed information of occurring accidents on the road to all connected vehicles and to identify the hit or damaged ones. Moreover, the framework proposed in this paper attempts to perform mutual authentication procedures between vehicles and road-side units based on radio frequency identification devices and cloud computing. According to this framework, a low-cost device has been implemented using an LED lamp and an electrical circuit to control the LED luminous flux, and the modulated carrier signal has also been modified to effectively suppress the low-frequency noise. It should be noted that the experiments have shown that vehicular networks must be resilient and self-adapted to failures and potential threats to support coordinated transportation systems. Finally, the security analysis has also shown that the proposed framework is efficient, easily deployed and capable of finding the best routing paths between communicating vehicles.

Keywords Vehicular network security · Identity-based cryptography · Mutual authentication · Conditional privacy · Internet of things · Cloud computing · Anonymity

Introduction

The losses counted every year in Egypt due to road accidents has unbelievably outnumbered those of pandemics and natural disasters over there, bearing in mind that Egypt only possesses less than 2.3% of world's vehicles [1]. However, Egypt has got over 3.5% of total road accidents worldwide and over 5% of road accidents' deaths making the need for safe system on the roads inevitable. The World Health Organization (WHO) estimates that Egypt would jump to 15th worldwide with 539 death per million vehicles. [2] Safety, then, should be guaranteed for drivers and vehicles on the road. Despite the existing adequate levels of safety and health in Egypt, some vehicles there do not follow the proper safety precautions causing countless disasters to follow. In addition, according to the report issued by Central Agency for Public Mobilization and Statistics (CAPMAS), the number of vehicles licensed in Egypt through the end of 2020 reached 11.45 million. There were 2.8 million licensed vehicles (30%) in Upper Egypt governorates, 3.1 million (32.9%) in Lower Egypt governorates, and 2.1 million vehicles (2.6%) in border regions. Cairo governorate ranked highest among others with 2.4 million licensed vehicles (26.2%) followed by Giza governorate with 1.2 million (11.9%).

A safe communication system with affordable cost like the one introduced in this paper is badly needed, then. Previously, Vehicle-to-Infrastructure (V21) had been applied

✉ Hesham A. El Zouka
  helzouka@aast.edu; helzouka@gmail.com

1 Computer Engineering Department, College of Engineering and Technology Arab Academy for Science, Technology, and Maritime Transport, Alexandria, Egypt

where all vehicles communicate through wireless links and traffic control and management system at Intersections. This computerized system is responsible for helping all connected vehicles to make reservations and managing their route till they reach the intersection.

However, this system cannot be described as the best choice in terms of expenses when applying a centralized module for every intersection [3]. Therefore, Vehicle-to-Vehicle (V2V) has been adopted in the proposed module due to its simple design and its ability to use wireless communication. For example, in smart cities, modern transportation systems rely on several technologies to transmit information between vehicles through radio frequencies like visible-light communications (VLC), which have the ability to transmit information through light-emitted diodes usually found in traffic lights and car lamps.

This paper is organized as follows: "Related Work and Motivation" introduces related work and background concepts that have been applied. "Contribution and Proposed System" describes the proposed module. "Methodology and Design Parameters" is where methodology and design parameters are explained. The security requirements according to threat analysis are discussed in "Security Requirements and Threat Analysis", and finally, "Conclusion" concludes the paper.

Related Work and Motivation

Many technologies have shown up recently to handle the incredible increasing number of vehicles on the road. V2V vehicle technology, for example, uses Light Fidelity technology or LiFi as an alternative data transmission medium to send data via optical wireless medium using bulbs with light-emitting diode for signal propagation.

Through LiFi technology, data are deployed in the vehicle environment, taking into account the challenges caused by bandwidth and data latency [4].

As shown in Fig. 1, the LiFi system is composed of light medium which is used to send data and information, where the receiving system relies on the LEDs and a photo detector to perform the necessary processing once the signal is obtained, to obtain the information. Thus, the vehicles will implement actions based on the information obtained, which will be displayed later on the visual screen, which leads to changing the movement of the vehicle or stopping it. . In this case, neither GPS or Wi-Fi are needed as the LiFi technology can simply use programmable interface controller or PIC to send tiny pulses of sound which can be applied in both, T-Junction roads and straight roads.

However, GPS- or RFID-based visibility solutions can be used to prevent many troubles that may face traditional modules, as deciding on the exact location of a vehicle to
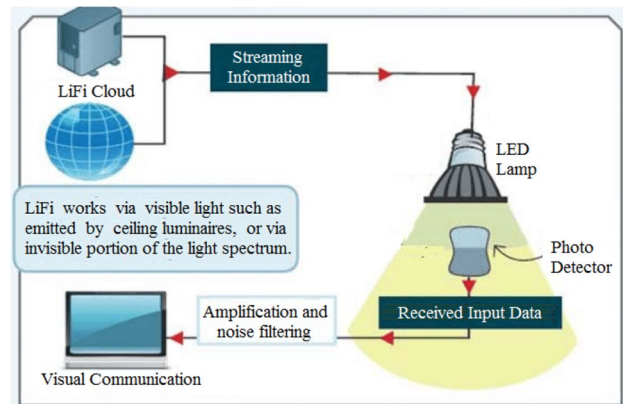

Fig. 1 Overview of LiFi technology

help all the connected vehicles to communicate and decide how they would proceed in case of accidents occurring in the surrounding traffic congestion [5, 6].

On one hand, V2V technology can calculate the exact time of collisions and how severe they are according to a combination of laser range finder or LRF, data from V2V communication, and camera recordings [7]. On the other hand, vehicle-loaded modules will automatically let safety procedures like smart pre-cash systems and air bags work right before the collision takes place. Along with GPS sensors and ultrasonic sensors attached to vehicles, mirrors can measure the distance and detect the visibility of vehicles in detached areas through their mirrors or through the sensor output if it is located in some blind spots to prevent accidents and collisions [8, 9].

Furthermore, communications between vehicles depend on the convergence or divergence between them, as the density of cars on the roads determines the mechanism through which information is transmitted [10]. For example, on crowded roads where traffic density makes the distance between vehicles shorter, bands of higher frequencies (millimeter wave frequencies) can be considered. For visible light, which has 10,000 times the spectrum of radio waves, the data can be transmitted in a single data stream and in a fast manner [11]. Table 1 summarizes the RF techniques used in the different traffic densities.

The proposed system could be of great help to emergency vehicles in avoiding traffic signals and proceeding much faster. Infrared light or any line of sight would not be needed by this system [12]. To prevent accidents and collisions, it adopts VANET technology or Vehicular Ad hoc networks which guarantees safety in vehicles as it sends all the needed information about the routes using RSU or road-side units to which the vehicles are connected to get more information about the traffic and the speed of the vehicle [13].

In VANET domain, several vehicles can be allocated whether with on-board units or road-side units utilizing two

Table 1 RF technology systems in different traffic networks

Traffic networks	RF technology systems	Network overhead
Sparse dense network	Cognitive radio Short range radio	Low
Dense vehicular network	Cognitive radio Short range radio millimeter waves	High
High density network	millimeter waves VLC radio	High
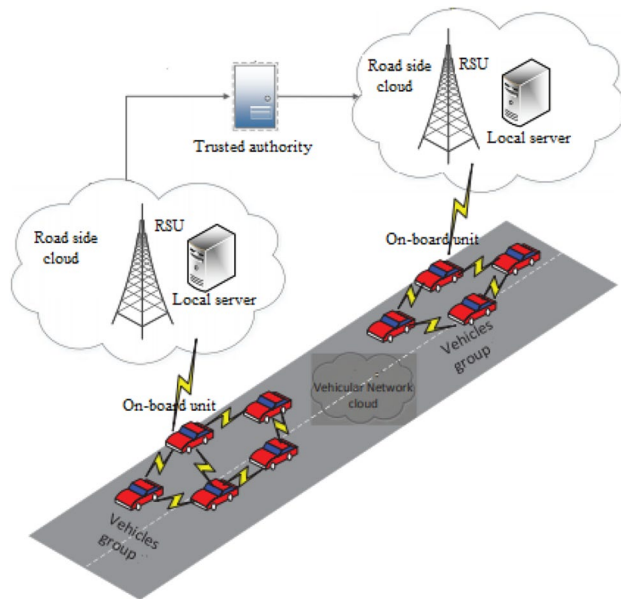
Fig. 2 Communication Domains in VANET

kinds of communication, namely inter-vehicle communication and V2V communication, as illustrated in Fig. 2.

Most of the modern vehicles are equipped with LED daytime running light, which can be used to transmit information when vehicles are connected. Euclidean distance tool can be used, then, to calculate the shortest distance between the vehicles and RSUs, and it can send data on road accidents in the surrounding areas to all connected vehicles. As soon as one vehicle detects the accident, it automatically sends the info to the nearby vehicles and, consequently, the traffic will be perfectly managed. In addition to the previously mentioned advantages of the proposed system, it uses ADAS or advanced driving assistance system that helps in navigation and provides road traffic updates and lane changing alerts to guarantee security and privacy in cloud applications [14]. Any sudden changes occurring to a vehicle on the road could be dealt with due to the information exchanged among the vehicles which in return will alert the driver. Vehicle-to-vehicle communication systems are also used

for head-to-head crashes avoidance, as they are responsible for exchanging needed data if the surrounding area has over than 150 vehicles [15]. 802.11p performance is better to be improved, so that the system could be able to send ten frames of data per second at least to the connected vehicles to prevent coming and predicted crashes [16]. To expand communication distance, vehicles will be connected with road-side units through sending, approving, and relaying messages and those units can help vehicles apply special applications [17].

Contribution and Proposed System

In this paper, a modular design of the proposed system is presented based on the integration of the Arduino Nano technology with control networks and communication devices in vehicles to represent and implement a low-cost communication security system on board of the vehicles to carry out the idea of merging Arduino Nano equipped with the microcontroller Atmega328P, vehicle mounted computer, and vibration monitoring sensors [18]. Then, the computer on the back of the vehicles collects the vehicle's kinetic information to control it, and this will be explained in detail in this section.

Along with the Arduino Nano, the Transmitter unit also contains an RF module where radio frequency and baud rate send and transmit signals [19]. Those signals will be received by the receiver in case that it is only configured for the frequency and they can be transmitted even in cases of existing obstacles, as they can cover long intervals rather than IR signals which can only process and communicate if the direct path of vision is available.

Receiver vehicle unit and Transmitter vehicle unit represent the main components of the proposed system. Signals could be sent to the RF receiver included in the Receiver vehicle unit with the help of the Amplitude Shift keying for frequency modulation [20]. It should be also mentioned that RF modules could be included in other boards like the Arduino Uno which is mainly connected to an LCD unit with a crystal display to present a visible image on the surface where the items could be displayed in 2 16-character lines and any further indications or warnings to alert the driver are shown on the LCD unit of the nearby vehicle [21]. Actually the main difference between both boards, the Arduino Nano and the Arduino Uno, is that the former is only available in 32-pin pack called the TQFP or thin quad flat pack, while the latter is only presented in a 30-pin pack called the PDIP or Plastic Dual In-pack Package [22]. Moreover, other units and switches could be connected to the Arduino Uno board like the Relay units which can process electro-mechanically to take over a circuit with the help of low-power signals

and to take over many other circuits with the help of just a single signal.

Sensors attached to communication systems in vehicles are of many advantages and used to prevent accidents [23]; however, roads that lack planned infrastructure and rash driving could, ultimately, lead to many accidents as sensors do not work alone. Therefore, more sophisticated systems are needed like RF modules and vibration sensors to help in raising the quality and the ability of communication systems applied on vehicles, as they are able to exchange data to nearby connected vehicles in a fast yet uninterrupted way.

Methodology and Design Parameters

The goal is to integrate communication systems that operate on the back of the vehicle with the LED technology to transmit data and traffic warnings between vehicles [24]. As previously mentioned, RF transmitter included in the Transmitter vehicle unit is responsible for sending controlled data to nearby vehicles and has three input buttons called Right indicator, Left indicator, and Brake indicator [25]. The sent data are received by a receiver that is connected to the receiver vehicle unit where an LCD unit can display it. In case of braking data, the controller in the receiver unit will have to trigger the relay just to slow down the speed of the vehicle. Vibration sensors, in the transmitter part, on the other hand, are connected to a threshold with certain limits that if exceeded, the controller will send a signal to ESP32 module right away to activate the camera and let it take photographs of the surrounding area to be kept in a Micro SD card as it is considered an accident, then [26].

Visible-light communication systems consist of a transmitter and a receiver, which operate on the photo-voltaic light-emitting diode, as well as SFH309 photo 2detector light Interrupt-driven AVR Microcontroller, which works with the first photovoltaics LED, respectively. All of these sensor diodes are connected to suitably equipped communication capabilities for vehicular networking [27].

Furthermore, both transmitter and receiver modules can work together and communicate if the Arduino is connected to the power supply where input buttons and vibration sensors are connected to the Arduino Nano at the transmitter unit and the LCD unit. On the other hand, the motor and other output buttons are connected to Arduino Uno at the receiver unit.

Then, according to pins configurations, pins in the Arduino board will get connected to the modules. Vehicle-to-vehicle or V2V communication, hence, can develop systems with different functionalities, to provide safety, and which can be used in the following three different scenarios:
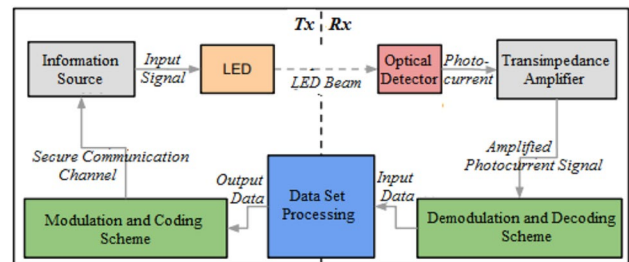

Fig. 3 Construction of transmitting and receiving VLC signal

Scenario 1: The Arduino digital pin receives the Left indicator, as soon as the left button is used, creating a digital pin (RF1) which is marked as High due to its connection to Pin number 7 and the information received is then converted by the encoder from the Arduino to RF signal and sends it to RF receiver which, in return, will connect to the decoder to convert the received signals into Digital format that is marked as Pin High. Arduino will, consequently, send the received data to be displayed on an LED unit that shows "Left Indicator is on" to inform the vehicle at the back that this vehicle is turning left.

Scenario 2: The Arduino digital pin receives the Right indicator, as soon as the right button is used, creating a digital pin (RF2) which is marked as High due to its connection to Pin number 8 and the information received is then converted by the encoder from the Arduino to RF signal and sends it to RF receiver which, in return, will connect to the decoder to convert the received signals into Digital format that is marked as Pin High. Arduino will, consequently, send the received data to be displayed on an LED unit that shows "Right Indicator is on" to inform the vehicle at the back that this vehicle is turning right.

Scenario 3: The Arduino digital pin receives the Brake indicator, as soon as the brake is used, creating a digital pin (RF-3) which is marked as High due to its connection to Pin number 9 and the information received is, then, converted by the encoder from the Arduino to RF signal and sends it to RF receiver which, in return, will connect to the decoder to convert the received signals into Digital format that is marked as Pin High. Arduino will, consequently, send the received data to be displayed on an LED unit that shows "Brakes have been applied" and it will also connect to the driver who is already connected to the Relay where an electrical signal is reduced to a low-power one and, hence, the motor will slow down as well to alert the vehicle at the back that this vehicle has applied brakes and the engine will slow down.

As for the experiments that were used in this research, only RTLSDR 2832 device for spectrum analysis was connected to NI USRP-2922 with a LED lamp to be used in analyzing the spectrum of signal in the frequency domain [28]. The analyzed data are, then, stored in a computer system

for image analysis [29]. The block diagram shown in Fig. 3 illustrates the configurations of transmitting and receiving radio signals.

The high-speed NI USRP-2922 radio frequency transceiver is used to transmit a malicious signal in the selected frequency band [30].

The proposed analog visible-light communication system has been built and tested in an equivalent version of the Delian Gnu/Linux operating system and compiled with the GNU C++Compiler 4.1.2 [31]. A frequency modulation technique has been implemented to enhance the sound waves coming from the computer's microphone.

Then, the transmission process begins through the visible-light channel, where the optical signal emitted by the LED is directly detected and converted into an electrical signal by the used receiver, which is located at a distance of approximately 15 cm from the front of the LED to ensure a direct line of instant communication between the transmitter and the receiver. The complete flow is shown in the flowchart in Fig. 4.

Security Requirements and Threat Analysis

By moving from main RF technologies model to the visible-light communication concept and using light as a communication medium in VANET, most of the traditional communication aspects will be changed.
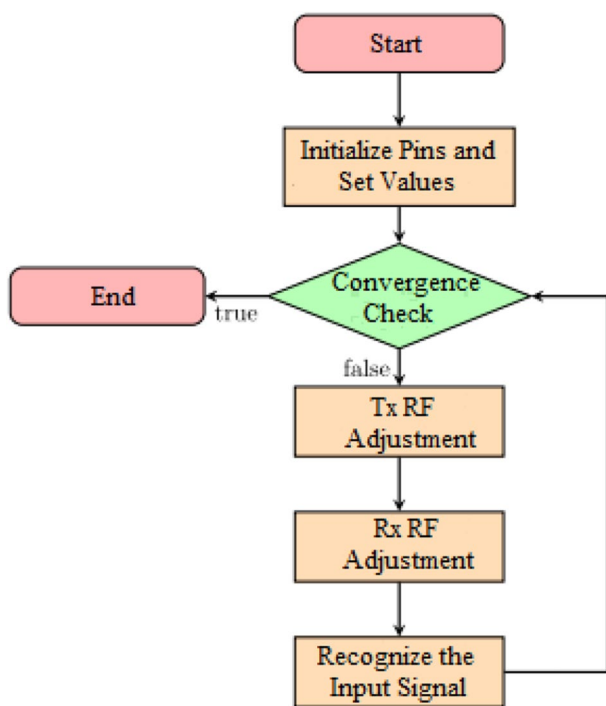

Fig. 4 Flowchart of the design procedure

This will also cause a complete change in privacy and security concerns [32]. Thus, it is very important to focus on privacy and security to ensure secure communication of data between sender and receiver.

In this section, the privacy and security of visible Light Communication are discussed. Privacy and security requirements for VLC fall in line with general security requirements for all wireless systems.

They aim to protect VLC communication against attacks such as denial of service (DoS), eavesdropping, routing and forwarding, node compromise, or jamming attack, etc. These requirements are Authenticity, Confidentiality, Integrity, and Availability, defined as follows:

- Authenticity: To not insert messages into the channel in attempt to deceive the receivers or prevent them from detecting the transmitted messages [33].
- Confidentiality: To impose limits on data access, and prevent the disclosure of the driving routes or senders' identities.
- Integrity: To not alter content of the messages throughout its transmission from source to destination.
- Availability: To imply that information is available to the authorized users anywhere and anytime upon request.

For the proposed VLC system to fulfill the above requirements, a number of critical security issues must be addressed prior to effective implementation of these technologies. In the following sections, most of the security practices are discussed. It was clear for RF systems that the network layer takes the responsibilities for protecting private data from both a legal and a commercial perspective. Like all the wireless and wired networks, VLC channel can be subject to different types of attacks which could affect the performance of the vehicles and privacy of the users or vehicle drivers.

Therefore, the first goal of the security architecture aims to protect the VLC system from various types of network attacks like cache attack, poisoning attack, and flooding attack.

The experiments in this paper have proven that the security breaches in VLC wireless communication with respect to identification are much more critical than the traditional VANET communication. In this research, the sources of security risks were identified and failures in physical infrastructure systems were evaluated.

A matrix-based approach was also used to determine the nature of those threats and the potential to prevent information from being modified or inappropriately accessed. The risky assessment procedure varies depending on the availability of information and the type of task being analyzed in VLC systems, as shown in Figs. 5 and 6, respectively.

The test objective for the validation process is to evaluate the comparative performance analysis of the proposed
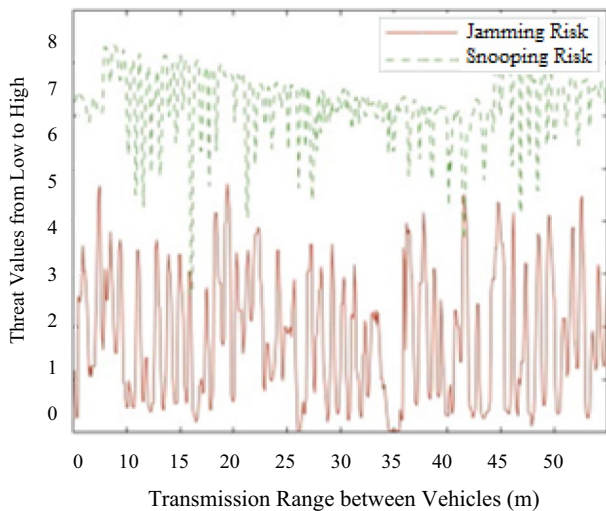
Fig. 5 Risk analysis results for fixed network infrastructure
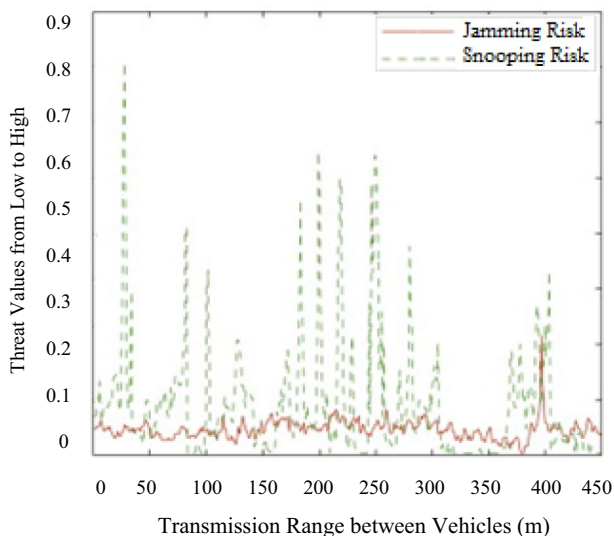

Fig. 6 Risk analysis results for mobile network Infrastructure

system in terms of fixed/mobile network infrastructure, power of the received signal and the transmission range. The absence of a proper measure of risk for data snooping or signal jamming could cause a data loss in congested environment which may lead to major vehicle accidents.

IoT Sensors

Developed technology like RF and vibration sensors can work together, as previously mentioned, to provide more sophisticated yet safe communication between vehicles with a single purpose which is reducing car accidents and collisions as much as possible. Even in cases of Hit-and-Run that has already increased in number recently, where driver hits

a passerby without stopping, more developed systems could be applied to help reducing them.

This can take place by attaching vibration sensors and cameras to cars, so when an accident occurs the sensors will receive vibration and the data will be sent automatically to the Arduino to utilize the ESP-32 camera module to take all the needed photographs in the surrounding area to easily find the vehicle that started the whole situation.

Competences

The proposed system is quite liable for improvement and development in the future with excess work and modifications. This system could definitely achieve its target and work brilliantly to reduce car accidents and the camera module attached to it can provide the police with the needed photographs from the nearby vehicles to help them decide the exact reasons behind any accident.

Cloud Server Provider (CSP)

CPSs and their powerful computational services mainly receive location data derived on a wide scale from encrypted aggregated query requests sent by vehicles to be managed and handled by RSUs to calculate the shortest route to the intended destination. However, location data like current user location and the user's query request remain unrevealed to CPS. Vehicles connect and share information among themselves and with the RSUs within an environment where entities controlling traffic and providing access to other services are included.

The kind of info that could be shared by vehicles here are basically collected when OBUs for V2V or V2I communications, sensors, and database units are provided. Moreover, RSUs represent important sources for info when connected to VLC interface and provide vehicles with authentication and authorization, respectively. Undeniably, preserving the confidentiality of the user's personal info is of paramount importance and this kind of info like license plate, speed, traveling routes, and the driver's identity are liable to attacks that could be enlisted as follows:

- Identity Intrusions: within the architecture of authentication, the driver's personal info might be revealed via his vehicle.
- Location Monitoring: The vehicles previously passed by routes or its current location do also go under the sensitive private info that should be preserved [34].
- Frequency Analysis Attack: When some places and locations are frequently visited by the vehicle's user more than others, such behavior could be noticed and detected by CSPs which can get access to those locations by ana-

lyzing the vehicle's access pattern due to their main tasks of recoding and detecting access frequencies.

- Confidentiality Threat: In case of violating confidentiality, the attacker might work on changing the content and the source of the messages mainly protected within the presence of confidentiality during transmission and storage procedures.
- Identification Authentication and Verification: Achieving secure communication in VANET definitely relies on identification authentication, so that the sent messages will not be revealed by the sender nor verified by the receiver and this could be done through two kinds of identification and authentication of a particular vehicle causing impersonation attack, whereas generating multiple identities is called Sybil attack. The first attack works on obtaining a fake ID of other parties after pretending to be a member of the communication process taking place. As for the latter, the attacker appears with several identities to communicate to vital stations like RSUs.

Impact Factors

Despite its ability to achieve reliable communication, RF technology used for communication still has a limited extent for its waves to cross, and the camera module will be attached to a fixed place on the vehicle's body and it will not be able to follow the vehicle from all directions.

Directions and Future Challenges

A few modifications are highly needed in the near future to this system like using cameras with better and higher quality to have better optical image stabilization and better image resolution than that of the current ones whose images are of low resolution especially when the surrounding natural light is at its minimum level. Moreover, camera modules need a number plate recognition mechanism for a better identification process, especially in hit-and-run cases. Finally, having a GPS module included in the system will definitely help in deciding the exact location of the accident and sending it right away to whom it may concern and the photographs taken by the camera, then, could be used for sending alerts to the nearest police station.

Conclusion

Reducing car accidents and crashes, providing safety, making drivers more alert and more considerate when it comes to following proper lane discipline and having more positive response to any unexpected emergency case or situation could all be achieved when a developed wireless communication between vehicles occurs. In this paper, a low-cost

device was implemented using an LED lamp and an electrical circuit that can control the LED luminous flux. The modulated carrier signal has also been modified to operate at a frequency of 3 MHz, which will effectively suppress the low-frequency noise.

The proposed system has been tested and verified with various vehicle intervals and numbers of vehicles per unit time. To support coordinated transportation systems, the experiments showed that vehicular networks must be resilient and self-adapted to failures and potential threats. The results showed that the ratio between the relative distances between two vehicles with respect to the vehicle's coverage range is 200 m at max and they are moving with a speed varying in the range 10–70 km/h, unlike other systems of VANEt that can deal with greater Euclidean distance and wide variety of cases.

To make the VLC a promising solution for variety of Euclidean distances, it should be supported by a control system that can automatically identify the channels available in the wireless spectrum, especially short-range communications. Simultaneously, an organized network that can be formed by connecting vehicles aiming at analyzing the gathered data without the need for sensors or actuators mounted on board of the vehicle.

Declarations

References

1. CAPMAS. Annual Bulletin of Car and Train Accidents 2020 (Cairo:Central Agency for Public Mobilization, 2020.
2. WHO. Global Status Report on Road Safety 2021 (World Health Organization, 2021), 138. 2021. https://www.who.int/violence_injury_prevention/road_safety_status/2021/en/. Accessed on Apr 2021.

3. Amani AS, Hesham AEZ, Sadek AA-S. Secure and intelligent road traffic management system based on rfid technology. In: World Symposium on Computer Applications and Reserch (WSCAR), Cairo, Egypt, 2016 pp. 41–6.

4. Ifada E, Surajudeen-Bakinde NT, Faruk N, Abubakar A, Mohammed OO, Otuoze AO. Implementation of a data transmission system using Li-Fi technology. In: 2nd International Conference of the IEEE Nigeria Computer Chapter (NigeriaComputConf), 2019, pp. 1–7.

5. Maia G, Aquino ALL, Viana AC, Boukerche A, Loureiro AAF. HyDi: a hybrid data dissemination protocol for highway scenariosin vehicular ad hoc networks. In: Proceedings of the second ACMinternational symposium on Design and analysis of intelligentvehicular networks and applications, 2012, pp. 15–122.

6. Official U.S. Government Information about the Global Positioning System (GPS) and Related Topics 2006. 2020. https://www.gps.gov/applications/marine/. Accessed on 29 Dec 2020.

7. Agarwal Y, Jain K, Karabasoglu O. Smart vehicle monitoring and assistance using cloud computing in vehicular ad hoc networks. Int J Transp Sci Technol. 2018;7(1):60–73.

8. Desai V. Design and implementation of GSM and GPS based vehicle accident detection system. Int J Technol Sci. 2014;1(3):306–3014.

9. Ahmad M, Hameed A, Ikram AA, Wahid I. State-of-the-art clustering schemes in mobile ad hoc networks: objectives, challenges, and future directions. IEEE Access. 2019;7(1):17067–81.

10. Yuan Y, Tasik R, Adhatarao SS, Yuan Y, Liu Z, Fu X. RACE: reinforced cooperative autonomous vehicle collision avoidance. In: IEEE Transactions on Vehicular Technology, 2020, pp. 9279–91.

11. Kumar N, Lourenço N, Terra D, Alves LN, Aguiar RL. Visible light communications in intelligent transportation systems. In: IEEE Intelligent Vehicules Symposium, 2012, pp. 748–3.

12. Abdillah MI, Darlis D. Distance measurement implementation for VLC-based V2V communication on motorbike platooning. In: Presented at International Conference of Engineering Technology Entrepreneurship, Bandung, 2019.

13. Alin-Mihai C, Barthélemy C, Luc C, Suat T, Yasser A, Jean-Marc B. Visible light communications: application to cooperation between vehicles and road infrastructures. In: IEEE Intelligent Vehicles International Symposium, Alcalá de Henares, Spain, (IV'12), 2012.

14. El Zouka HA. A secure interactive architecture for vehicular cloud environment. In: Proceedings of the IEEE conference on Smart Cloud, NY, USA, 2016, pp. 254–61.

15. Hayzmi I, Tutomu M, Kenta W, Kazuyuki S. Crash warning for intersection and head-n car collision in Vehicle-to-Vehicle communication. In: International Conference on Connected Vehicle and Expo, Vol. 1, no.3, Tokyo Institute of technology, 2015.

16. Kawasaki R, Hirai T, et al. Performance evaluation on V2V communications by LTE for crasj warmomh application. IEICE Tech Rep. 2017;116(485):175–80.

17. Lee S, Yoon J, Min S. Study on architecture and application for vehicle to pedestrian communication. In: Proceedings of ITS World Congress 2015, Papernumber ITS-2133, Bordeaux, France, 2015, pp. 5–9.

18. Dinesh R, Swapnil K. Intelligent traffic signal control system using embedded system. In: G.H Raisoni College of Engineering, Nagpur. Innovative Systems Design and Engineering, 2012.

19. Engiz BK, Rakan B. Implementation of a speed control system using Arduino, In: 2019 6th International Conference on Electrical and Electronics Engineering (ICEEE), IEEE, 2019, pp. 294–7.

20. Jha PK, Kachare N, Kalyani K, Kumar DS. Performance analysis of FSO system with spatial diversity and relays for M-QAM over log-normal channel. J Wireless Pers Commun, arXiv preprint arXiv:1709.05488. 2019.

21. Shin W-J, Cho S-Y, Lee J-B, Won T. Numerical 3-D FEM simulation of tensor model for liquid crystal displays. J Mater Process Technol. 2018;20(1–3):60–3.

22. Zheng H, Chang W, Wu J. Traffic flow monitoring systems in smart cities: Coverage and distinguishability among vehicles. J Parallel Distrib Comput. 2019;127:224–37.

23. Agarwal Y, Jain K, Karabasoglu O. Smart vehicle monitoring and assistance using cloud computing in vehicular Ad Hoc networks. Int J Transp Sci Technol. 2018;7:60–73.

24. Guo C, Liang L, Li GY. Resource allocation for vehicular communications with low latency and high reliability. In: IEEE Trans Wireless Communication, 2019, pp. 3887–902.

25. Jernej M, Andrej K, Urban S. Implicit aggressive driving detection in social VANET. In: Proceedings of the 2017 International Conference on Identification, 2017, pp. 348–52.

26. Parthiban KG, Abishek R, Pradeesh S, Kaviarasan K. Wireless notice board with wide range communication. Int J Adv Res Trends Eng Technol. 2020;7(7):93–100.

27. Nasr A, Mohamed S. Accurate distance estimation for VANET using nanointegrated devices. Opt Photon J. 2017;2(2):113–8.

28. Chen C, Chen Y, Qian J, Xu J. Triple-threshold cooperative spectrum sensing algorithm based on energy detection. In: Proceedings of the 2018 5th International Conference on Systems and Informatics (ICSAI), Nanjing, China, 2018, pp. 791–5.

29. Nijsure Y, Kaddoum G, Ghodoosipour G, Cai G, Wang L. A novel spectrum sensing mechanism based on distribution discontinuity estimation within cognitive radio. In: Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 2016, pp. 1–15.

30. Arjoune Y, Kaabouch N. A comprehensive survey on spectrum sensing in cognitive radio networks. Recent advances, new challenges, and future research directions. Sensors. 2019;19(12):107–20.

31. Ettus C. Building and installing the USRP open-source toolchain (UHD and GNU radio) on linux. https://kb.ettus.com/Building_and_Installing_the_USRP_Open-Source_Toolchain_(UHD_and_GNU_Radio)_on_Linux. Accessed on Aug 2020.

32. El Zouka HA. Providing end-to-end secure communications in gsm networks. Int J Netw Secur Appl (IJNSA). 2015;7(4):31–41.

33. El Zouka HA. An efficient lightweight authentication protocol for mobile ad hoc network. In: International conference on wireless and mobile networks (WiMo 2010). Berlin: Springer; 2010. p. 436–44.

34. Abdo MA, Abdel-Hamid AA, El Zouka HA. A cloud-based mobile healthcare monitoring framework with location privacy preservation. In: International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), University of Bahrain, Bahrain, IEEE, 2020.