Message Dissemination Scheme for Rural Areas Using VANET (Hardware Implementation)

Hassan Mistareehi
Department of Computer Science, University of Kentucky
Lexington, KY 40508, USA
Email: hassan.mistareehi@uky.edu

***Abstract*—Vehicular Ad hoc NETworks (VANETs) are likely to play an important role in Intelligent Transport Systems (ITS). Information collected by On Board Units (OBUs) located in vehicles can help in avoiding congestion, provide useful information to drivers, etc. However, not all drivers on roads can benefit from OBU implementation because OBU is currently not available in all car models. Therefore, in this paper, we designed and built a hardware implementation for OBU which allows to disseminate messages in rural areas. This OBU implementation is simple, efficient, and at low cost. Evaluation results show that our proposed model can transmit and receive plaintext and encrypted messages (e.g., safety messages) to nearby vehicles, Access Point (AP), and destination with acceptable time.**

Keywords: VANET, Arduino microcontroller, Security, OBU

I. Introduction

People living in urban areas receive better connectivity to Internet compared to rural areas due to the lack of infrastructure. The cost of deploying infrastructure to provide complete connectivity is often too expensive for many rural areas. A large number of people still live in the rural areas. In the USA and Canada, around 20% of the total population live in rural areas, while 56% in the European Union (EU) and 60% in China live in rural areas [1], [2].

Delay Tolerant Networks (DTNs) are considered a potential low-cost solution to the problem of connecting devices in rural areas where end-to-end network connectivity is not available. Researchers have done some work to connect rural areas using DTNs [3]–[7]. Authors in [7] showed that DTNs would be a promising solution for remote patient monitoring in low-resource settings for a number of services like notification of lab results and ordering medical supplies. Other schemes used VANETs to disseminate personal health information (PHI) in rural communities [2], [8]. These schemes provide network connectivity to rural areas using vehicles as relay nodes. The sensed data from body sensors of patients can be transferred using VANETs to their health service providers located in city where the data can be collected, stored, and analyzed. These schemes are only useful for non emergency services.

Over the last decade, the researchers and the industry have been working on the deployment of VANETs. In VANETs, vehicles communicate with each other using vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications. VANETs can help in sending alerts to drivers about traffic congestion, accidents, emergency braking, and other road hazards. This helps in saving people lives and makes transportation efficiency [9], [10]. To make this work, we need to implement hardware technology for on-board and road-side units. A number of VANET hardware implementation schemes have been proposed in the literature [11]–[14]. These schemes proposed collision detecting systems to improve traffic efficiency. However, They used sensors in their schemes and not all events can be detected by sensors.

Nowadays, smart devices can provide applications like mobile health (m-health), location-based services, etc. In such applications, smart devices could perform data sensing and processing. Vehicles are not likley to be equipped with OBUs in the near future. Therefore, smart phones could play a key role in vehicular networking as they provide a set of embedded sensors (e.g., accelerometer), computation and communication capabilities that could be used in deployment of VANET applications. Some schemes have been proposed to minimize the risk of accidents using smartphones [15]–[19]. In [17], authors proposed smartphone application called CarSafe, which collects information from both front and back cameras to identify unsafe driving conditions. This application can track and predict whether the driver is disturbed or tired using the front camera. Also, the back camera is used for monitoring road conditions. However, these schemes only provide driver behaviour service and not other services. In addition, since they used sensors in their schemes, not all events can be detected by sensors.

Ensuring security and privacy is an important issue in VANETs. If there are no security and privacy in VANETs, an adversary can gather the transmitted data that contains the private data of the vehicles. In addition, adversary can generate fake messages to misguide the driver to make the wrong decisions. For example, sending falsified warning messages can cause an accident and can damage the lives and properties. Therefore, ensuring security and privacy is an important issue in VANETs. Several schemes [20]–[24] exist in literature for solving authentication and privacy issues in communication.

The contributions of this work are: (1) designing a message dissemination scheme for rural areas using VANET. The scheme provides different services to users in rural areas; (2) using Symmetric Key Cryptography to ensure confidentiality of the sensitive messages; (3) implementing OBU hardware for vehicle and Access Point(AP). This implementation establishes two communication modes; vehicle-to-vehicle, and

978-1-7281-6476-2/21/$31.00 ©2021 IEEE

vehicle-to-infrastructure.

Our scheme depends on humans and their ability to communicate and it doesn't depend on sensors because not all vehicles are equipped with smart sensors and not all events can be detected by sensors. Users could receive information through our application about their surrounding traffic conditions. For example, if someone sees an incident, they can report it by sending a warning message to *other vehicles, access points, and to different departments* such as police, hospital, fire department, etc., to take proper actions. The OBU in our scheme consists of Arduino microcontroller [25]- which acts as the brain of our model, Radio Frequency (RF) module, and bluetooth module. The driver will send the message (e.g., obstacle on the road) using his/her phone through bluetooth module to the OBU. Then the OBU will send the message wirelessly to other vehicles (which have OBUs as well) using Radio Frequency (RF) module. When OBUs receive the message, they will send the message to other drivers' cell phones through bluetooth module, so other drivers can take proper action. The details of the proposed model are explained in detail in the next section of the paper.

The rest of the paper is organized as follows. In Section II, we describe our proposed model. In Section III, we present the hardware implementation and performance evaluation. We discuss and compare some related work in Section IV. Finally, Section V concludes the paper.

II. Proposed Model

In this section, we present our system model and describe the proposed architecture in detail.

A. System Model

Figure. 1 illustrates the proposed architecture which consists of On Board Units (OBUs), Cell Phones, Access Points (APs), and Destinations.

- **On Board Unit (OBU):**
  OBU consists of the following components:
  - **Arduino Microcontroller:**
    Arduino microcontroller is a special purpose mini computer. It has a dedicated input and output device and ports to control the device components. The microcontroller is attached with RF module and bluetooth to send and receive data either from the vehicle or infrastructure [26]. The purpose of the Arduino in our architecture is to transmit and/or receive messages and then forward them to other Arduinos located in other vehicles. We used two types of Arduinos, Arduino nano for vehicles and Arduino mega for access points. The Arduino mega has more storage and computational power than Arduino nano. Table I compares the specification of the two types of Arduinos.
  - **Radio Frequency (RF) module:**
    An RF module is a small electronic device used to transmit and/or receive radio signals between two devices [27]. The transmission range of RF module is 100 m. In our architecture, RF module is used to enable wireless communication between Arduino devices.

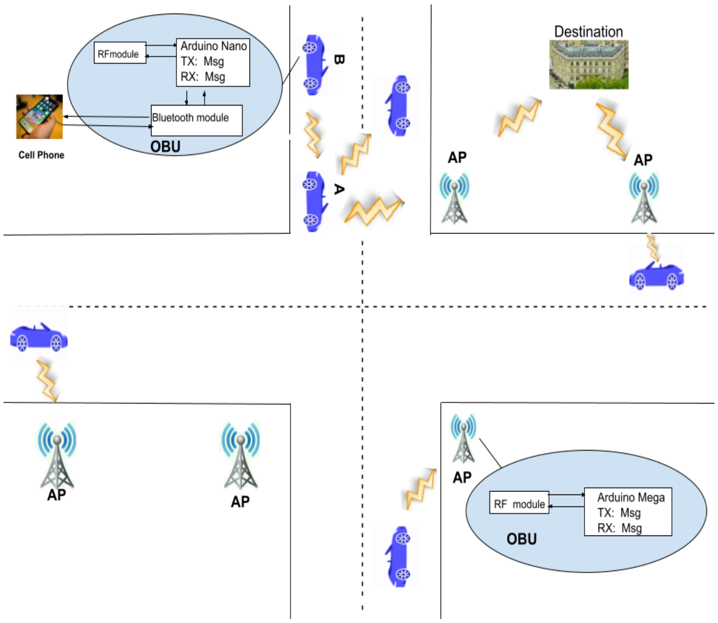

Fig. 1. Message Dissemination Scheme for Rural Areas.

TABLE I
Comparison of Arduino Nano and Arduino Mega [25]

	Arduino Nano	**Arduino Mega**
Micro-controller	ATmega328	ATmega2560
Digital I/O Pins	14	54
Analog Input Pins	8	16
Flash Memory	32 KB	256 KB
SRAM	2 KB	8 KB
Clock Speed	16 MHz	16MHz

  - **Bluetooth module:**
    Bluetooth is used for communication between Arduinos and cellphones wirelessly. We used bluetooth module HC-05. We created an Arduino-bluetooth interface for exchanging messages between Arduino and the cellphone of a driver. Figure 2 shows the components of OBU of a vehicle as well as an access point.
- **Cell Phone:**
  We use the serial bluetooth application downloaded on the cellphone that allows to write a message and send it to Arduino through the bluetooth module. In addition, serial bluetooth application reads messages that come from Arduino microcontrollers.
- **Access Point (AP):**
  Access points are fixed units that can be deployed along road side (e.g., at major road intersections, gas stations, etc.). The AP collects the messages sent by vehicles and forwards them to the Destination. In addition, it can send

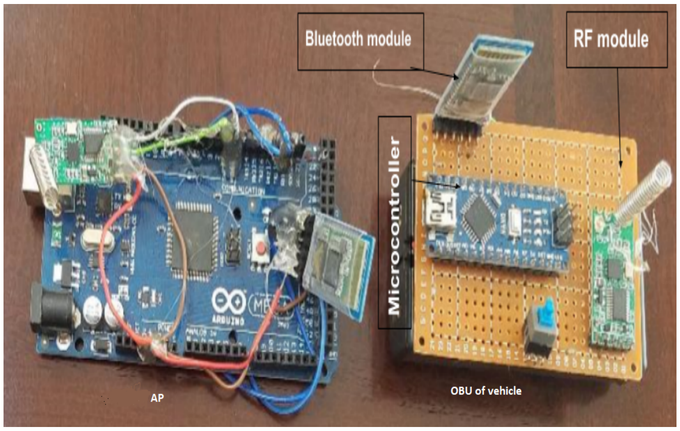

Fig. 2. Components of OBU and Access Point.

messages to vehicles within its transmission range. APs are assumed to be connected to destinations, possibly through Internet.

- **Destination:**
  Destinations in our model could be traffic department, police department, hospital, etc.

B. Proposed Architecture

In this section, we describe our architecture in detail.

In the proposed architecture, information collected by drivers in an area (e.g., driver A sees accident) are sent to other vehicles or nearby access points through the OBU. For example, as shown in Figure 1, driver in vehicle A sends a message (e.g., notifying about an accident) from the driver's cellphone via bluetooth to the OBU of vehicle A. Then, the OBU forwards the message to the nearest vehicle (e.g., vehicle B) using its RF module. When the OBU of vehicle B receives the message, it forwards it to cellphone B using its bluetooth module, and then driver B can take appropriate action. The messages also could be forwarded to access point which will forward them to the destination.

In our scheme, information collected by drivers that are sent to the destination depends on the type of their information. For example, if the information is about an accident, the message should be sent to the police department as well as the fire department. If the message is about a patient, then it should be sent to the nearest hospital and if it is about traffic, then it should be sent to nearby vehicles as well as the traffic department.

We built OBU hardware that can be attached to vehicles and can also be installed in some areas to increase the connectivity; These are called Access Points (APs). These APs will send the messages received from vehicles to the destination. If there are no vehicles or APs within the transmission range of a vehicle, the vehicle stores and carries the message until it gets closer to the next AP or another vehicle. The authenticity and integrity of messages sent by vehicles, APs and destinations should be verified. In addition, all drivers information should be protected and attackers should not be able to trace the routes of the vehicles. This could be achieved by assigning pseudonyms to vehicles in all communications and use them instead of their real identities and keep changing them frequently to maximize privacy. Many researchers in [28], [29] suggest authentication schemes and assigning pseudonyms to vehicles and changing them frequently. These schemes can be incorporated in our architecture to ensure authenticity, integrity, and privacy.

APs are responsible to forward the messages to nearby vehicles and/or the destinations (e.g., police department, traffic department, health department, etc.). The destination is responsible for processing the messages and sending the services that the original source vehicle might need. For example, if someone's car gets out of gas, he/she will send a message that contains the location of the car through vehicles which then will forward the message to the AP. AP in return forwards the message to a destination which provides road side assistance. When the destination that provides road side assistance receives the message, it will take proper action and send help to the source as well as send a message assuring the source that help is on the way. Following Figure 3 shows the flow chart of communication from vehicle to destination.

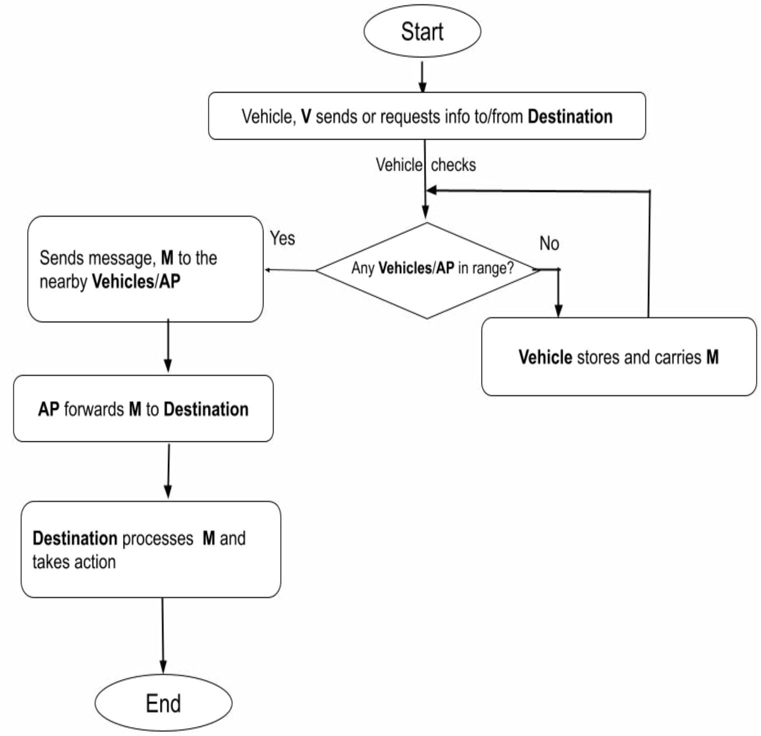
Start
Vehicle, V sends or requests info to/from Destination
Vehicle checks
Any Vehicles/AP in range?
Yes
No
Sends message, M to the nearby Vehicles/AP
Vehicle stores and carries M
AP forwards M to Destination
Destination processes M and takes action
End

Fig. 3. Vehicle Sending or Requesting a Message to/from Destination.

Encryption of Messages. We assume that the APs are trusted and not compromised. In addition, we assume that when vehicles, APs, and destination want to send encrypted messages, they know the symmetric key K that is shared between the communicated parties. Also, we assume every vehicle v knows nearby AP.

In our scheme, not all the messages need to be encrypted;

a vehicle can decide if the message needs to be encrypted or not depending on the type of the message. For example, if a vehicle has to notify about ice on the road, it doesn't need to encrypt the message. On the other hand, if a vehicle wants to send a message about a crime scene, then this message may need to be encrypted. If a vehicle decides to encrypt a message, it encrypts the message using K. This ensures confidentiality. Now, when receiver receives the message, it decrypts the message using the secret key K. We used AES Encrypter/Decrypter application to encrypt and decrypt the messages.

When the driver of a vehicle v_x observes an event, he/she decides whether it is sensitive information or not. If it is not sensitive, he/she assembles the message M_1 without encrypting it, and then sends it to the nearby AP. If it is sensitive information, it assembles M_2 and then sends it to the nearby AP, where M_1 and M_2 are defined as follows:

$M_1 = ID_{AP}, (ID_{v_x}, Type, Loc)$.

$M_2 = ID_{AP}, E((ID_{v_x}, Type, Loc), K))$,

The message M_1 includes the ID of vehicle v_x ID_{v_x}, type of the message $Type$, and the location of phenomena Loc. In message M_2, the symmetric key K is used to encrypt the message. Note that the process of getting K between two parties is not addressed in this paper.

III. Implementation and Evaluation

General overview of our implementation is shown in Figure 4. We built OBU hardware for vehicle and AP. We used 3 OBUs for 3 vehicles, 1 access point and a Personal Computer (PC) for Destination.

The data in our model is transferred from a cellphone of driver via serial bluetooth terminal of android application by pairing two bluetooth devices (bluetooth of cell phone and HC-05 bluetooth module of OBU). After pairing the devices, the Arduino nano located in the OBU broadcasts the message to neighbor vehicles (OBUs) or nearby AP via RF module. Figure 4 illustrates the process of sending messages between vehicles, AP and Destination. In our scheme, any vehicle (e.g., vehicle 1) can broadcast a message to neighboring vehicles within its transmission range (e.g., vehicle 2, vehicle 3), as well as AP. Also, the AP could broadcast the message to vehicles within its transmission range (vehicle 1, vehicle 2, and vehicle 3) as well as the Destination (PC). The messages sent/received to/from PC is shown using open terminal software (e.g., putty). For example, if the Destination wants to inform about an incident, Destination (PC) can send a message to AP which in return forwards it to vehicles within its transmission range.

We connected AP with personal computer (PC) to measure the end-to-end delay and the packet delivery ratio using MATLAB environment. The end-to-end delay is the time taken for a packet to reach the destination (see Figure 5). We used AES Encrypter/Decrypter application to encrypt and decrypt the messages. We assumed the symmetric key K is known between the sender and destination. We used 6 data packets sizes 32, 64, 128, 256, 512 and 1024 bytes of data. The message was forwarded wirelessly through bluetooth module HC-05 of vehicle from a smartphone then the vehicle (OBU) received it through RF module and transmitted it to AP, which transmitted it to the PC. In analyzing the end-to-end delay results (Figure 5), we have observed that the transmission times grow with the size of data packet transmitted. For instance, the average delay of data packet size of 64 bytes is longer than that of 32 bytes for plaintext and encrypted messages. In addition, the encrypted messages take more time than plaintext ones due to its size which is bigger than plaintext messages.

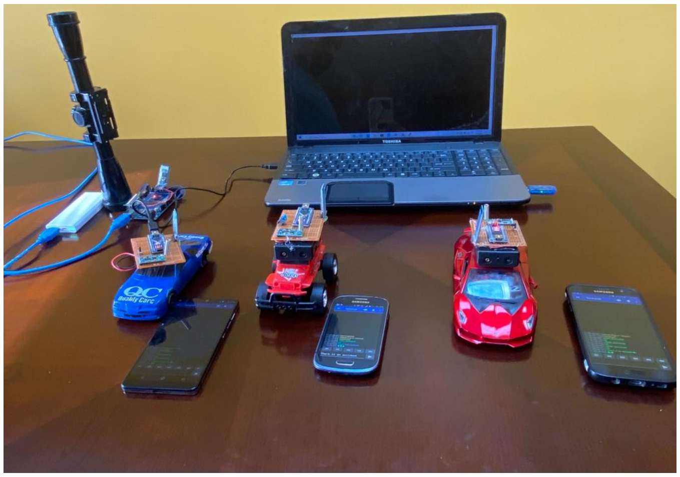

Fig. 4. Sending messages between vehicles, AP and PC.

Figure 6 shows the experimental results in terms of Packet Delivery Ratio (PDR), which refers to the ratio between the packets successfully delivered to the number of packets sent by a source vehicle. Transferring the data of the packets was successfully 100% delivered when the source vehicle and destination were separated by 25m and 50m, and then its PDR decreased to 82% at 75m and below 40% at 100m. When the distance increased to 125m, none of the data packets that were sent reached the destination (PDR=0%) due to the loss of connection - transmission range, which in our scheme is only up to 100m.

IV. Comparison with Related Work

Some VANET schemes have been proposed for transmitting personal health information (PHI) [2], [8], [30]. In [2], extending secure health care to rural areas using VANETs (RCare) has been proposed to minimize the overall health care cost. RCare collects patients' personal health information and provides network connectivity to rural areas using vehicles as relay nodes. These vehicles store, carry and forward the PHI to the health service providers located in the city. However, these schemes focused on transmitting health information and do not address other types of information (e.g., sending warning messages, requesting a service). Additionally, vehicles may rarely visit some areas or vehicles may not exist there, in this case PHI may not get to the destination. Our scheme provides

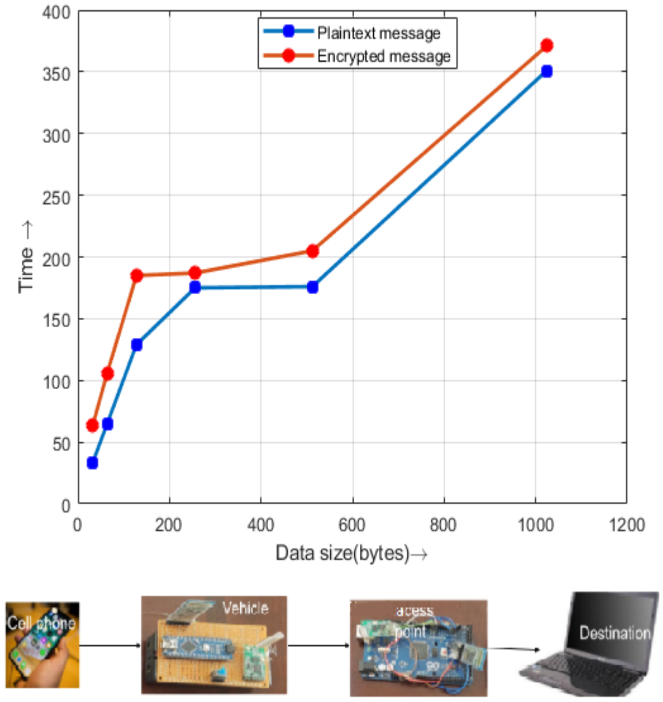

Fig. 5. End-to-end delay (milliseconds) for different data packet sizes.

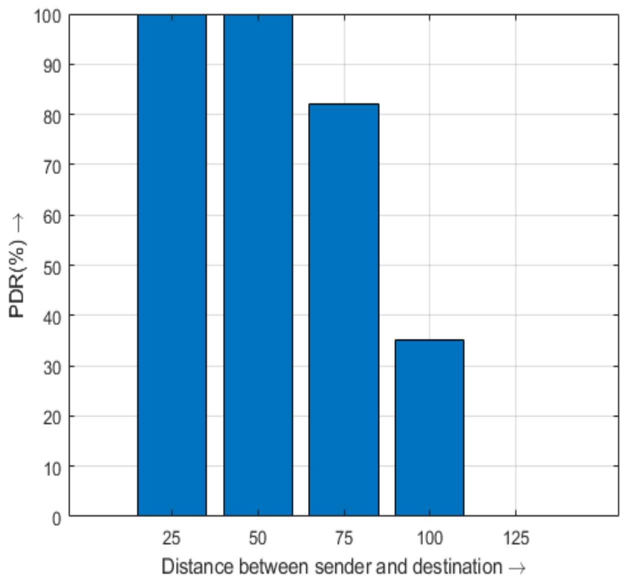

Fig. 6. Packet delivery ratio vs distance between sender and destination.

different services and APs are distributed in these areas to increase the network connectivity.

Some schemes use smartphones to detect transportation modes (e.g., walking, biking, jogging). This data can be used in many different ways, for example, the analysis of traffic patterns and CO2 emissions. Reserchers in [31] designed a smartphone app to detect transportation modes using data collected from GPS, accelerometer, orientation, and magnetic sensors. However, the data were collected from a single user and only two travel modes, walk and automobile, were considered in this scheme. Another scheme collected travel data from different sensors, like accelerometer, gyroscope, and magnetometer [32]. However, no pedestrian, cyclist, or subway is considered in that work. In [33], researchers explored the solutions with a different combination of sensors such as accelerometer, gyroscope and GPS. However they did not include subway as a travel mode.

There are other schemes that have been done to minimize the risk of accidents using smartphones [15]–[19]. In [17], authors proposed smartphone application called CarSafe, which collects information from both front and back cameras to identify unsafe driving conditions. This application can track and predict whether the driver is disturbed or tired using the front camera. Also, the back camera is used for monitoring road conditions. A similar application was proposed in [18]. This application uses the front camera for detection of driver's gaze, yawns, eyes closure and talking on the mobile phone and the back camera for monitoring the driving behaviour. In [19], authors use a set of sensors (e.g., gyroscope, magnetometer, and accelerometer). These sensors used to calculate deflection angle, speed, acceleration, deceleration, and position. These sensors were used for statistically analyzing driver behaviors. However, these schemes provide driver behaviour service only and do not provide other services. In addition, they used sensors in their schemes and not all events can be identified by sensors. Our scheme provides different services and we use humans instead of sensors for detecting events.

A number of VANET hardware implementation schemes have been proposed in the literature [11]–[14]. Anadu et al. [11] proposed collision detection system to improve traffic efficiency. Their model consists of a microcontroller, an RGB LCD screen for data display, an Mpu6050 accelerometer, a transmitter on one car and a receiver on the other one. Various parameters of the vehicles such as position and speed are used to create messages for collision detection. The above schemes [11]–[14] provide collision detection and avoidance service only and do not provide other services. In addition, they used sensors in their schemes and not all events can be identified by sensors. Our scheme provides different services and we rely humans instead of sensors for detecting events.

In summary, most of the above mentioned schemes have some drawbacks. As we noticed, many of them use sensors to detect events, and thus in some cases the data that come from sensors may not be sufficient to take a decision or it may lead to a wrong decision. For example, the sensor of camera cannot capture the obstacle on the other side of the road. In addition, not all events can be identified by sensors. Our scheme provides different services and we use humans instead of sensors for detecting events. Our goal is to combine smartphones and OBU of vehicles, so that our scheme get benefits from smartphone applications (e.g., GPS, AES Encrypter/Decrypter, etc) and integrated with OBU of vehicles. In addition, urban areas receive better connectivity to Internet compared to rural areas due to the lack of infrastructure. The cost of deploying infrastructure to provide complete connectivity is often too expensive for many rural areas. Therefore, we design a scheme which provide services to rural areas with low cost. Our scheme also allows drivers to send encrypted messages.

V. Conclusion

In this paper, we proposed message dissemination scheme for rural areas using VANET. Our scheme consists of cell phones, vehicles, access points and destination. The driver in our scheme can send plaintexts and encrypted messages to nearby vehicles, APs and destination. We evaluated our scheme with respect to end-to-end delay and packet delivery ratio. We have observed that the transmission times grow with the size of data packet transmitted. It also shows the packet delivery ratio decreases when the distance between the source and the destination increases. For future work, we will design effective incentive scheme to increase network performance in rural areas.

References

[1] M. Zhang and R. Wolff, “A border node based routing protocol for partially connected vehicular ad hoc networks,” *Journal of Communications*, vol. 5, no. 2, pp. 130–143, February 2010.

[2] M. Barua, X. Liang, R. Lu, and X. Shen, “RCare: Extending secure health care to rural area using VANETs,” *Mobile Netw Appl*, vol. 19, pp. 318–330, 2014.

[3] J. Whitbeck and V. Conan, “HYMAD: Hybrid DTN-MANET routing for dense and highly dynamic wireless networks,” *Computer Communications*, vol. 13, pp. 1483–1492, 2010.

[4] R. F. A. Pentland and A. Hasson, “Daknet: Rethinking connectivity in developing nations,” *Computer*, vol. 33, no. 13, pp. 78–83, 2004.

[5] M. U. A. Doria and D. Pandey, “Providing connectivity to the saami nomadic community,” in *Proceedings of International Conference on Open Collaborative Design for Sustainable Innovation*, 2002.

[6] C. Raffelsberger and H. Hellwagner, “A hybrid MANET-DTN routing scheme for emergency response scenarios,” *IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM workshops)*, pp. 505–510, 2013.

[7] S. Syed-Abdul, J. Scholl, P. Lee, W. Jian, D. Liou, and Y. Li, “Study on the potential for delay tolerant networks by health workers in low resource settings ,” *Computer Methods and Programs in Biomedicine*, vol. 107, no. 3, pp. 557–564, 2012.

[8] M. Murillo and M. Aukin, “Application of wireless sensor nodes to a delay-tolerant health and environmental data communication system in remote communities,” in *Proceedings of IEEE Global Humanitarian Technology Conference*. IEEE, 2009.

[9] N. Cenerario, T. Delot, and S. Ilarri, “A content-based dissemination protocol for VANETs: exploiting the encounter probability,,” *IEEE Transactions on Intelligent Transportation Systems*, October 2011.

[10] H. Mistareehi and D. Manivannan, “ Classification, challenges and critical comparison of proposed solutions for vehicular clouds,” *International Journal of Next-Generation Computing*, vol. 10, no. 1, pp. 1–18, Mar 2019.

[11] D. Anadu, C. Mushagalusa, N. Alsbou, and A. Abuabed, “ Internet of Things: Vehicle collision detection and avoidance in a VANET environment,” *IEEE Instrumentation and Measurement Magazine*, 2018.

[12] G. Rakesh and M. Belwal, “Hardware implementation of VANET communication based collision warning system,” in *Proceedings of International Conference on Communication and Electronics Systems (ICCES)*, 2019.

[13] S. Sharma and S. Sebastian, “IoT based car accident detection and notification algorithm for general road accidents,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 4020–4026, October 2019.

[14] S. Sivakumar, A. Alagumurugan, G. Vignesh, and S. Dhanush, “Accident analysis and avoidance by V2V communication using LIFI technology ,” *International Research Journal of Modernization in Engineering Technology and Science*, vol. 2, March 2020.

[15] Y. Gu, Q. Wang, and S. Kamijo, “Intelligent driving data recorder in smartphone using deep neural network-based speedometer and scene understanding,” *IEEE Sensors*, vol. 19, no. 1, pp. 287–296, Jan 2019.

[16] M. Won, A. Mishra, and S. Son, “HybridBaro: Mining driving routes using barometer sensor of smartphone,” *IEEE Sensors*, vol. 17, no. 19, pp. 6397–6408, Oct 2017.

[17] C. You, M.Oca, T. Bao, N. Lane, G. Cardone, L. Torresani, and A. Campbell, “CarSafe: A driver safety app that detects dangerous driving behavior using dual-cameras on smartphones,” 2012, p. 671–672.

[18] A. Nambi, S. Bannur, I. Mehta, H. Kalra, A. Virmani, V. Padmanabhan, R. Bhandari, and B. Raman, “HAMS: Driver and driving monitoring using a smartphone,” 2018, pp. 840–842.

[19] H. Eren, S. Makinist, E. Akin, and A. Yilmaz, “Estimating driving behavior by a smartphone.” IEEE, Jun 2018, pp. 234–239.

[20] H. Jo, I. Kim, and D. Lee, “Reliable cooperative authentication for vehicular networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 4, pp. 1065–1079, 2018.

[21] S. Mallissery, M. Pai, R. Pai, and A. Smitha, “Cloud enabled secure communication in vehicular ad-hoc networks,” in *Proceedings of IEEE International Conference on Connected Vehicles and Expo (ICCVE)*. IEEE, 2014.

[22] X. Lin and X. Li, “Achieving efficient cooperative message authentication in vehicular ad hoc networks,” *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3339–3348, 2013.

[23] M. Azees, P. Vijayakumar, and L. Deboarh, “EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular adhoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[24] Y. Liu, Y. Wang, and G. Chang, “Efcient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, October 2017.

[25] “Arduino boards, compared,” *https://core-electronics.com.au/tutorials/compare-arduino-boards.html*.

[26] L. Jacioa, “Programming 16-bit microcontrollers in C. Learning to fly the PIC 24,” *I st ed, Newnes Elsevier*, 2007.

[27] Wikipedia, “RF module,” *https://en.wikipedia.org/wiki/RF_ module*.

[28] H. Mistareehi, T. Islam, and D. Manivannan, “ A secure and distributed architecture for vehicular cloud,” *Internet of Things*, Jan 2021.

[29] B. Ying and D. Makrakis, “Pseudonym changes scheme based on candidate-location-list in vehicular networks,” in *Proceedings of IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 7292–7297.

[30] E. Yaacoub, K. Abualsaud, T. Khattab, and A. Chehab, “ Secure transmission of IoT mHealth patient monitoring data from remote areas using DTN,” *IEEE Network*, Oct 2020.

[31] M. Frendberg, “ Determining transportation mode through cellphone sensor fusion,” *Ph.D. dissertation*, 2011.

[32] S. Garg and P. Singh, “ A novel approach for vehicle specific road/traffic congestion,” *MTech Theses*, 2014.

[33] A. Jahangiri and H. Rakha, “ Applying machine learning techniques to transportation mode recognition using mobile phone sensor data,” *IEEE Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2406–2417, Oct 2015.