*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 3, pp. 829–839
DOI : 10.47974/JDMSC-1759

# Hash function and DSRC based secure communication protocol for VANET-WAVE architecture

Surender Kumar *
Vikram Singh †
*Department of Computer Science & Engineering*
*Chaudhary Devi Lal University*
*Sirsa*
*Haryana*
*India*

**Abstract**

The research and development community has recently become more interested in automotive adhoc networks due to their extensive application possibilities in traffic control and the social networking of automobiles. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication is made possible through vehicular adhoc networks. For safety and other reasons, vehicles connected by vehicular adhoc networks exchange messages. Particularly vulnerable to security and privacy breaches are safety messages. In every vehicle-to-vehicle and vehicle-to-infrastructure communication exchange, information about the vehicle, the driver, and the authentication of transferred information are crucial considerations. A Dedicated Short Range Communication (DSRC) protocol is incorporated with the Wireless Access Vehicular Environments architecture in the current communication. The DSRC protocol incorporates a secure key exchange method to encrypt and decrypt the basic safety messages sent between the vehicles at the receiving end. The end-to-end delay of the communications is barely changed, however the performance of the DSRC is slightly impacted by the encryption and decryption. Our findings demonstrate that, despite a modest drop in DSRC performance, our protocol is too secure for the BSM (Basic Safety Message) to be cracked.

***Subject Classification:*** *68M12.*

***Keywords:*** *Secure Communication, Hash function, VANET and WAVE.*

* *E-mail:* **skgill.ugcnet@gmail.com (Corresponding Author)**
† *E-mail:* **vikramsinghkuk@yahoo.com**

## 1. Introduction

Vehicle-specific adhoc networks (VANETs) are an extension of the idea and concepts of mobile adhoc networks (MANETs), which are wireless networks that spontaneously form between mobile devices. Data is transmitted between cars in VANETs using constant bit rate (CBR) and transmission control protocol (TCP) traffic agents [3]. Vehicular Adhoc networks are divided into two kinds based on the type of communication entities: V2V and V2I.

The cars (also known as nodes) act as routers in a VANET. No "infrastructure" nodes were used when VANET technology was first installed on emergency vehicles to enable them to interact with one another. To self-regulate traffic, the Intelligent Transportation System (ITS) concept was used. It was argued that it might lead to fewer traffic accidents. Although VANETs technically might be considered an extension of MANET technology, the following characteristics set VANETs apart from MANETs [1].

A. Because the nodes (vehicles) in the VANET move very quickly, the topology of the VANET changes more frequently than that of the MANET.
B. While VANET nodes can move along predetermined routes along roads and highways, MANET nodes can be moved at random.

### 1.1 *Dedicated Short-Range Communication (DSRC)*

Figure 1 shows in several countries, like the United States, the European Union, and Japan, DSRC has been standardized. The same 5.850–5.925 GHz spectrum is used by the USA and the EU, albeit with distinct channel definitions. The DSRC spectrum in Japan is in the 5.77-5.850 GHz range. Only V2V and V2I communication is permitted in the free but licensed 75MHz frequency band between 5.850 and 5.925.

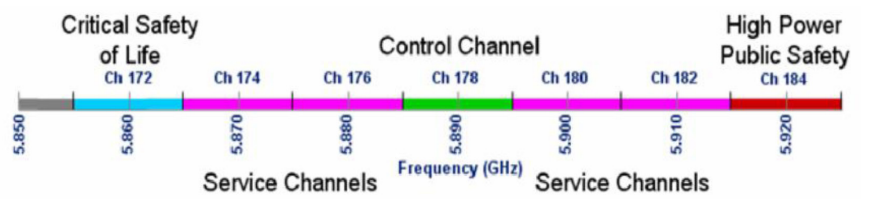


**Figure 1**

**DSRC Spectrum [2]**

[4]. The DSRC standard collection is built on a number of interoperable standards, many of which were created by the IEEE. In particular, Wireless Access in Vehicular Environment is the essential component of the DSRC architecture (WAVE).

### 1.2 *WAVE and Its Architecture*

The DSRC architecture (Figure 2) has several layers, each of which incorporates a unique protocol. IEEE 802.11p is utilised at the Physical and Media Access Control Layers. The upper levels implement the IEEE 1609.2, 1609.3, and 1609.4 protocols. These include IEEE 1609.2, which is in responsibility of offering security services, IEEE 1609.3, which is in duty of offering network security, and IEEE 1609.4, which is in charge of offering channel switching services. WAVE Short Message Protocol (WSMP) is used at the network layer. This layer may use IPv6, TCP, and UDP depending on the requirements of the network's applications.

Application layer IEEE P1609.1, security layer IEEE P1609.2, network layer IEEE P1609.3, upper MAC layer IEEE P1609.4, and bottom MAC and physical layers IEEE 802.11p make up the WAVE architecture.

As shown in Figure 2, the DSRC protocol sits between the Physical and Data Link/MAC layers of the TCP/IP protocol stack. In order to stop information breaches during communication in vehicle Adhoc networks, the current study modified the Dedicated Short Range Communication protocol using hashing.

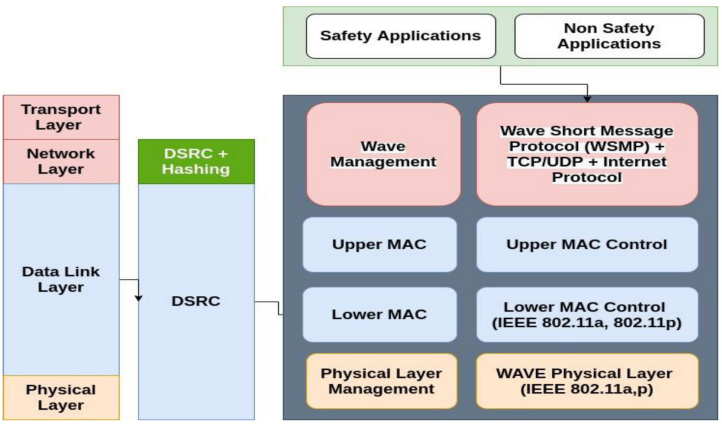


**Figure 2**

**Proposed DSRC/WAVE Architecture**

Application layer IEEE P1609.1, security layer IEEE P1609.2, network layer IEEE P1609.3, upper MAC layer IEEE P1609.4, and bottom MAC and physical layers IEEE 802.11p make up the WAVE architecture. Applications exchange data utilising message sets, data frames, and other data elements that are outlined in the SAE J2735 standard via the DSRC/WAVE and other communication protocols. SAE J2735 [6] additionally covers the message categories general, safety, geolocation, traveller information, and electronic payment. As shown in Figure 2, the DSRC protocol sits between the Physical and Data Link/MAC layers of the TCP/IP protocol stack. The Dedicated Short Range Communication protocol has been changed in the current study using hashing to stop information leakage.

## 2. Related Work

Researchers have carefully surveyed a wide range of authentication and security solutions that have been discussed in many sectors of literature. The list below discusses a few of them.

Hash Message Authentication Code (HMAC) construction to secure vehicle communication has been described by [5]. An HMAC is a collection of pieces of information that validates the message's flow and ensures the message's credibility and veracity. HMAC reduces the amount of time spent checking and the quantity of valid messages in each cluster. As a result, the solution offers secure vehicle authentication and prepares the path for safe and secure driving. [8] elaborate how recommend model uses the received SINR and RSSI value to find its route. They send this RSSI value to the network layer to find distance of node which is in range. It will calculate the optimal path. The focus on parameters like traffic rate of transfer, interruption, packet loss, time, link stableness, for increase overall lifetime of a network through optimal usage of battery.

Three creative contributions by [4] have looked at the effectiveness of multichannel VANET. They first suggested incorporating the present IEEE 802.11 MAC protocol implementation with the IEEE 1609.4 WAVE protocol for the ns2 simulator. [7] also talked about how the protocol is now insufficient to guarantee the strict Quality of Service criteria of safety-related apps in terms of delivery rate and delay. Second, they provided a performance evaluation of multi-channel VANETs based on 1609.4 standards. Third, they have proposed two changes that will hasten the delivery of safety alerts and reduce their latency to the present DSRC 1609.4/802.11p stack.

It was determined from the studies mentioned above that there isn't any detailed research on VANET authentication or key distribution options. It was consequently determined to focus on enhancing authentication and privacy methods for the VANET environment.

The majority of the research asserted that DSRC protocol utilisation is constrained in the absence of vehicle security. Some works of literature handled the safety messages using cellular or WIFI technologies. They have used cellphone networks because they have some level of basic security. Therefore, using DSRC along with hashing to encrypt the safety messages in the vehicular networks is a need.

## 3. Hash Function Based Secure Communication Protocol

Typically, the private key used for key generation is used in the signature generation process. Private and public keys will both be used. Anyone who has access of public key can use it for signature validate. However, the creation of signatures can only be done using a private key. The DSRC protocol is made secure and reliable in this work by the programming of two algorithms. The production of signatures or keys is one of the procedures, as it is demonstrated here. The message and the key are the two inputs, and the outputs are the generation of the signature and the encryption key. The encryption key is obtained by hashing the message and thus generates the signature based on multiple iterations of the algorithm.

### 3.1 *Signature Generation:*

Input: Message (m), key (k)
Output: Signature, encryption (e)
*Algorithm 1:*
Step 1: *Compute : e = Hash (m)*
Step 2: *k ε (1 to n-1), where n is any integer*
Step 3: *Find r = x1 (mod n), where (x1,y1) ε k*
Step 4: *If (r=0) Then goto Step 2*
*Calculate 1/k*
Step 5: *s = (e+r) (mod n)*
*If (s=0) Then goto Step 2*
*Step 6: Signature is (r,s)*

The other process, called signature verification, checks to see if the production of the signature was successful. The resulting signature's validity is determined by this algorithm. Verifying the range between [1, n-1] is a requirement for a signature's authenticity; if the key is outside of this range, the created signature is invalid. Hashing the encrypted message we obtained from the signature generation process is both a necessary and sufficient condition for the signature verification. The performance of these two algorithms is programmed using the DSRC protocol, and the packets are sent from one car to another or from a vehicle to an RSU. However, the messages sent and received by the cars are secure and reliable.

3.2 *Signature Verification:*

Input: Signature pair (r,s)
Output: (r,s) to be valid

Algorithm 2:
Step 1: Verify: If (r,s) ε [1,n-1], Then "Valid" Else "Invalid"
Step 2: Compute e = HASH(m)
Step 3: Compute w = s-1 (mod n)
Step 4: Calculate u1 = e * w (mod n) and u2 = r * w (mod n)
Step 5: *Compute (x1, y1) = u1.G + u2.Q.A*
Step 6: *If x1 = r (mod n) Then "Valid Signature" Else "Invalid"*

The DSRC works closely with the algorithms for signature creation and verification to encrypt or hash the safety messages. These methods are implemented simultaneously with the DSRC in order to maintain DSRC performance. Messages only can be used as a separate module for hashing, allowing the DSRC and hashing to occur in different simulation threads. However, when it is put into practice, we may use the DSRC device and hashing together to encrypt or hash packets before they reach the on board unit (OBU) of the vehicles.

## 4. Experimental Result and Analysis

In this work, the DSRC protocol, which is based on the WAVE 1609 standard for Wireless Access for Vehicular Environment, was implemented and evaluated using the application NS2 (WAVE). The dedicated short-range communication protocol, also known as the Mac layer of the TCP/IP protocol, is positioned between the physical and data link layers. As

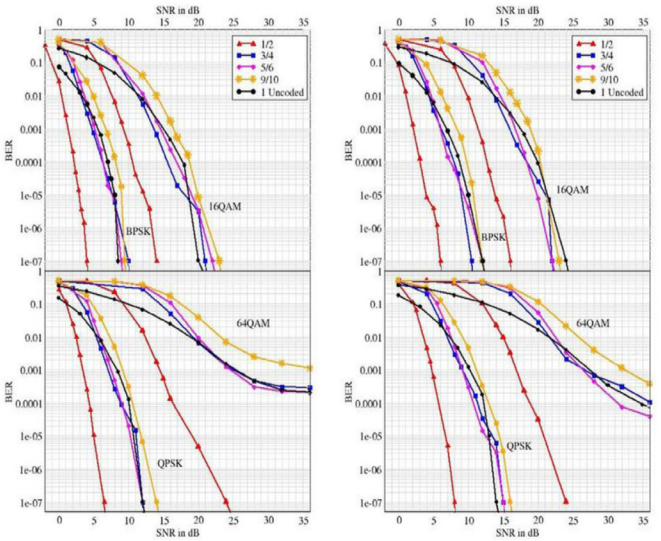


**Figure 3**

**Bit Error Rate of QPSK, BPSK, QAM16 and QAM64**

a result, it is based on real hardware and communication standards like phase-shift keying, quadrature amplitude modulation, and several other networking parameters. According to our findings, the DSRC protocol's modulation schemes play a major role in determining throughput, delay, and other aspects because this protocol primarily relies on faster communication ranges with other vehicles in the network. Figure 4 shows the bit error rate of all the modulations schemes adopted in this work.

Figure 3 shows the Bit Error Rate(BER)of QPSK, BPSK, QAM16 and QAM64. Since these modulations schemes are helpful in optimization of the delay between the vehicles, they are used. These simulations were carried out using Monte Carlo Simulations. In the Figure 4, QPSK starts at a Signal to Noise (SNR) at 14 and 16 respectively, whereas the BPSK at 10 and 14, QAM16 at 20 and 25 and finally QAM64 starts at a longer SNR ratio. Using these modulation schemes in DSRC protocol improves the signaling between the vehicles and the infrastructure. The parameters of this work are large and hence the following Table 1 shows the parameters used in the evaluation of DSRC protocol along with hashing with encryption and decryption process along with the modulation schemes. In DSRC protocol, there are two types of packets allowed, service packets and safety packets. The service packets are programmed with the hashing technique and the safety packets are ensured for safety.

**Table 1**
**Parameters taken for evaluation of DSRC**

| Parameter Name | Parameter Value |
|---|---|
| Modulation Index | QPSK, BPSK, QAM16 and QAM64 |
| Number of Cars (Vehicles) | 20,40,60,80,100 (After 100, the simulation abruptly comes to a stop due to the massive processing) |
| Payload in bytes | 100, 200 bytes (The data transferred between nodes are less) |
| Communication Range | 250 Metres (The distance should also be ideal because the cars are travelling quickly.) |
| Random Seed | 0,1 and 2 |
| Data Rate (DR) for Modulation systems | BPSK (1/2 Coding Rate) at 3Mbps<br>QPSK (1/2 Coding Rate) at 6Mbps<br>QAM16 (1/2 Coding Rate) at 12Mbps<br>QAM64 (2/3 Coding Rate) at 24Mbps |
| Propagation Model | Nakagami Model |
| Physical Layer and Mac Layer | Wireless Extended Physical layer & IEEE 802.11P |
| Routing Agent and protocol | DumpAgent |
| Queue length | 20 bytes (50 bytes is the ideal amount, however since this is for vehicles, the queue size is kept to a minimum to prevent packet losses.) |
| Work Area | 1100 metres X 20 metres |
| Parameters of IEEE 802.11P Mac | 5.9GHz Frequency<br>-99dBM for 10Mhz bandwidth (Noise Floor)<br>Window (Min - 15, Max -1023) Congestion |
| Packet kinds or Types | 0 – Safety – Channel (-99) is used.<br>1 – Service and hashing – Channel 1 to 5 can be used |

For every automobile operating in the VANET environment, the aforementioned parameters were configured. The distance versus transmission power in the communication medium has first been calculated. Since distance plays a significant role in how vehicles move, Figure 4 depicts the relationship between transmission power and distance.

Referring to Figure 4, the transmission power increases like an inverted parabola as the distance increases, indicating that if the transmission is too

large, the transmission power will be high to medium. Therefore, while choosing the transmission distance, the optimal distance is the best option. Since the antenna and Nakagami propagation model both support it, the optimal distance that we chose for our simulations is 250 metres. The simulation was based on two DSRC protocol elements:

- Without encryption, decryption, or hashing
- Using Hashing, encryption, and decryption

Figure 5's histogram displays the throughput of various amplitude modulation algorithms when DSRC protocol packets are being sent. When using QAM16, the throughput of BPSK and QPSK modulation techniques decreases slightly, but when using QAM64, the throughput drops considerably and is reduced to a level that is around 50% lower than that of BPSK and QPSK modulation techniques.

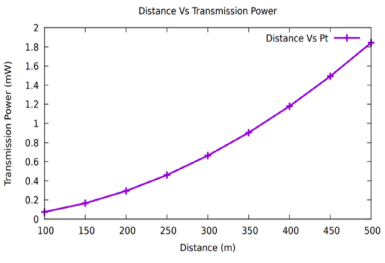


**Figure 4**

**Distance vs. Transmission Power**

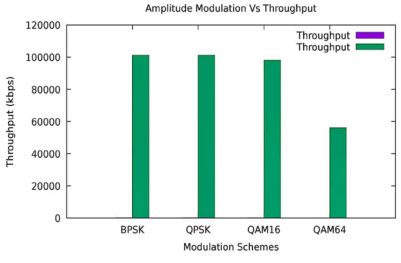


**Figure 5**

**Amplitude Modulation vs. Throughput**

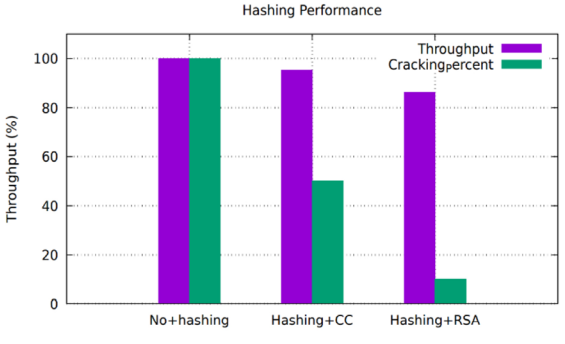


**Figure 6**

**Hashing Performance**

Figure 6's histogram compares the throughput for the DSRC protocol when it is hashed and when it is not hashed. The throughput and likelihood of packet cracking are both 100% when there is no hashing. On a 50-50 scale, it is simpler to break the Caeser Cipher. The packet structure is revealed when the key is given with the same characters, which reduces packet breaking to 50% while maintaining throughput over 95%. In the last scenario, where the throughput is greater than 80% and the cracking rate is incredibly low due to the RSA algorithm-based encryption.

In the Figure 6, the throughput on a normalized scale is 100% when there is no hashing and the cracking percent of the BSM messages are high at 100%. In the Caeser cipher the throughput is relatively high at 95% as the encryption and decryption takes a minimal time as the key size is too small and is also not a complicated process. So the throughput is high as equal as no hashing and CC is taken here only for comparison. The final RSA hashing with DSRC is powerful in the sense that the key is too complex and the operation of RSA also high. Since the mobility of vehicles is high, there would be lot of packet loss and packet drop, hence the average or normalized throughput is 80% when compared to the other two modes. But the main objective of this research is to secure the basic safety messages (BSM) between the V2X and V2V which is achieved with the help of the DSRC protocol.

## 5. Conclusion

The WAVE architecture is used in this work to implement the DSRC protocol. The protocol is hashed using a key generation method, and encryption and decryption are performed using the Caesar cypher and the RSA algorithm. The performance characteristics of different schemes suggest that hashing, encryption, and decryption operations only slightly impair network performance. The RSA method will completely prevent it, but it is extremely unlikely that the packets' structure could be read or cracked. This suggests that the DSRC with hashing and encryption makes the protocol an efficient one when compared to the protocol without hashing. Despite a slight performance hit, there is a very slim chance that the packet can be cracked.

## References

[1] Agarwal, A., Starobinski, D., Thomas, D., and Little, C., "Phase transition of message propagation speed in delaytolerant vehicular

networks", *IEEE transactions on Intelligent Transportation Systems,* Vol. 13, No. 1, pp. 249–263 (Mar. 2012).

[2] Ajami, A. K., & Artail, H. Analyzing the impact of the coexistence with IEEE 802.11 ax Wi-Fi on the performance of DSRC using stochastic geometry modeling. *IEEE transactions on communications*, 67(9), 6343-6359 (2019).

[3] Singh, A., "Simulation and Analysis of AODV, DSDV, ZRP in VANETs, Masters thesis in computer science and engineering", (July 2013).

[4] Gudagudi, S.S. and Desai,V. , "HMAC Based Secure Authentication of VANET's," Vol. 3, No. 8, pp. 1471-1476 (2014).

[5] Jie, C. and Jing, Z., "HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs", Vol. 14 (Sept-2018), https://doi.org/10.1016/j.vehcom.2018.09.003.

[6] Kim, S., & Kim, B. J. Crash Risk-Based Prioritization of Basic Safety Message in DSRC. *IEEE Access*, 8, 211961-211972 (2020).

[7] Ankit Kumar, Pankaj Dadheech, Vijander Singh, Linesh Raja & Ramesh C. Poonia. An enhanced quantum key distribution protocol for security authentication, *Journal of Discrete Mathematical Sciences and Cryptography,* 22:4, 499-507 (2019), DOI: 10.1080/09720529.2019.1637154.

[8] Ankit Kumar, Pankaj Dadheech, Rajani Kumari & Vijander Singh. An enhanced energy efficient routing protocol for VANET using special cross over in genetic algorithm, *Journal of Statistics and Management Systems*, 22:7, 1349-1364 (2019), DOI: 10.1080/09720510.2019.1618519.