EAI Endorsed Transactions
on Security and Safety

Research Article EAI.EU

Secure Communication in VANET Broadcasting

Muhammad Jafer, M. Arif Khan, Sabih ur Rehman and Tanveer A. Zia

School of Computing and Mathematics
Charles Sturt University, Australia
mjafer@ieee.org,{mkhan, sarehman, tzia}@csu.edu.au,

Abstract

Broadcasting is a communication mechanism utilized in VANET architecture that facilitates in disseminated of public information to help reduce traffic jams/congestions. The authentic and genuine nature of public information is required to be maintained to avoid broadcasting of false information causing mass panic and hysteria. Therefore, it is of utmost importance to secure the broadcasting information so that an intruder is unable to alter any information without compromising public nature of the information. In this paper, we have proposed a secure broadcasting architecture consisting of different layers stacked together in different formation according to operating modes. A real-time simulation model is developed in Python, while simulations are run on a supercomputer for the purpose of gathering results for highway environments. We compare the results of the proposed secure highway architecture with unsecure architecture. Overall, the results show delayed propagation time due to the availability of multiple information packets as well as prioritization of these information packets. However, there was no significant difference in retransmission of different information packets when compared with either different broadcasting probability or unsecure highway scenario, which indicates an effective as well as efficient, secure broadcasting architecture.

Received on 15 November 2018; accepted on 11 December 2018; published on 21 December 2018

Keywords: VANETs, Secure Broadcasting, Network Coverage, Information Retransmission, Public Information

doi:10.4108/eai.10-1-2019.156243

1. Introduction

The revolutionary concept of connecting physical devices to the internet is a step towards increasing better services and products for end-user satisfaction. Among these devices, such as refrigerators, televisions, smart washing machines and many more, vehicles are one of the most important devices for modern-day commuters. Therefore, vehicles are at the forefront of new research capable of solving challenges related to traffic safety, congestion, accidents, and pollution [1–3]. The most important concept introduced in recent times is to establish a new type of mobile ad-hoc network for vehicles known as Vehicular Ad-hoc Network (VANET) [4]. In VANETs, the communication link between vehicles change frequently making the topology dynamic and vulnerable to security risks, which are the primary focus of our research.

Moreover, there are two main types of communication supported in VANETS namely: **Vehicle-to-Vehicle** (V2V) and **Vehicle-to-Infrastructure** (V2I) communication. In general, V2V communication is established among vehicles, whereas in the V2I scenario communication link is established between a vehicle and any roadside infrastructure, commonly known as Road Side Units (RSUs). In addition to this, communication scenarios in VANET can also be categorised as **Point-to-Point** (P2P) and **broadcasting** (BC) [5]. P2P communication can be defined as sharing the information between two vehicles. In this scenario, one vehicle acts as a source and the second vehicle acts as a destination. In BC scenario, a vehicle transmits information to all vehicles within a certain geographical area. The BC scenario used in this paper is different than the commonly used BC scenario in mobile wireless communication where a transmitter broadcasts different information for different users. In this paper, we use BC as a source

*Corresponding author. Email: mjafer@ieee.org

vehicle broadcasting the same information for multiple other vehicles.
We also classify the information to be transmitted into two categories **private** and **public** information as explained below.
Private Information :- We consider information as private, transmitted using P2P communication system, if it is intended only for one single vehicle or it requires certain decryption process to extract the information from the transmitted signal. For the sake of simplicity, we assume that private information is intended only between two vehicles that resemble the P2P communication scenario defined above.
Public Information :- On the other hand, public information is defined as the information available for any vehicle within the network and it does not require any decryption process to extract the information from the transmitted signal. This scenario resembles BC communication in VANETs as defined above.
It is of great importance to transmitting authentic information whether public or private, therefore it is crucial to secure the information. Unsecured information especially public information can be misused causing mass hysteria and traffic jams. Whereas, when information is secured, it is difficult for intruders to alter the original message and hence lowering the risk of creating public panic(s).
The focus of this paper is to investigate and propose a secure broadcasting architecture for VANETs. The proposed secure broadcasting architecture facilitates in the implementation of strategies that avoid tempering of information during transmission. To the best of our knowledge, there currently exists no publications related to research studies proposing secure broadcasting systems or architectures. However, there is signification research studies as well as publications in secure P2P communication. This paper builds on the lessons learned from secure P2P communication architectures by applying them to secure public information in VANET broadcasting.
Following list consists of three main contributions put forward in this paper:

- Identification and categorization of security challenges related to broadcasting in VANETs.
- Proposing of a layer based secure broadcasting architecture to counter alteration in information during broadcasting.
- Implementation of the proposed secure broadcasting architecture and collecting results related to credibility index with respect to propagation time required by an information packet, P_{info} to achieve network coverage.

The rest of the paper is organized as follows. Section 2 contains literature review of previous research, whereas Section 3 describes the system model that is used in this study. A discussion regarding proposed secure broadcasting architecture is contained in Section 4, while operational flow of the architecture is presented in Section 5. In section 6, the numerical results are presented in detail. Finally, Section 7 concludes the paper.

2. Related Work

The main focus of this paper is to extend the security principles and techniques available in P2P communication to VANETs BC. Some of the major security challenges in VANET are bogus information, ID disclosure, and Sybil attacks. There are a number of solutions available for these security threats in the literature such as [6–13]. However, one common challenge in the literature is that it is mainly focused on P2P mobile ad-hoc networks. In order to integrate these security features in VANET BC, we have classify these feature into three groups: *Authentication*, *Anonymity* and *Availability of resources*, which is inspired by work put forward in [4, 14–16].
Authentication is a process of validating both sender and associated message by receiving vehicle [14]. The validation process requires sender identification, which is defined by different properties such as location, direction, speed, and owner of the vehicle. The authentication mechanism helps to establish the reliability of the sender's information, which ultimately provides the mechanism facilitating prevention of Sybil attacks in VANETs. In addition to this, the process of *anonymity* dictates hiding sender information as well as encrypting this information to make it unreadable for unintended users. Sender vehicles that are either source or relay vehicles may be willing to share information provided a mechanism to avoid tracking of vehicles or sharing actual vehicle information. On the other hand, a secure system is also required to incorporate fault-tolerant design, resilient to attacks as well as survival protocols so for the purpose of remaining available and operational in the presence of faults or malicious attacks [14, 17]. These three distinct groups of security threats are further explored with respect to P2P and BC systems in the following sections:

2.1. Security in Point-to-Point (P2P) Communication

A Point-to-Point (P2P) communication involves at minimum two vehicles, namely source and destination. Source vehicle transmits information intended for a destination vehicle, which employs a trust mechanism to establish the legitimacy of the received information. In [18], trust is based on a process called authentication that helps in correctly identifying source vehicle. This authentication process consists of three different types, namely ID authentication, property authentication, and

location authentication. ID authentication uses unique IDs, which are either license number or chaises number of a vehicle, for identification of a vehicle. The property authentication facilitates in identifying the type of sources, such as a vehicle or a traffic signal, on the other hand, location authentication identifies the location of a source allowing receiving vehicles to validate received information. Authentication is an effective process of identifying the source as well as validating transmitted information. However, this would compromise the anonymity of a source vehicle providing a convenient way of tracking as well as identifying the vehicle and its passengers.

In [19], a centralized system is implemented with the help of RSUs providing encryption mechanism for all the vehicles that are registered with the system. An authentication process is employed by the centralized system for the purpose of validating as well as issuing certificates to registered vehicles. Source vehicles are issued encrypted certificates during the transmission of information, while, these certificates are decrypted by providing a public key to destination vehicles. In addition to this, unique encrypted digital signature generated by the source vehicle and attached to a P_{info} facilitates in identifying changes in the original P_{info} by a destination or relay vehicles. Any change in the original P_{info} causes the centralized system to either not issue or validate attached encrypted certificate. The process introduced in this study establish an authentication process without compromising anonymity. However, the process is not applicable in environments lacking RSUs as it is heavily dependent on a centralized system implemented through RSUs. Moreover, public nature of information in broadcasting would increase the complexity of the overall system due to repeated requests for issuing or validation of certification for authentication.

In [6], authentication process based on encrypted vehicle signature is used to establish authentication between a vehicle and an RSU. After successful authentication, RSU issue a short-lived anonymous certificate to the vehicle. This certificated as well as public key and signature are broadcasted by the vehicle to all the neighboring vehicles. The broadcasted P_{info} is verified by all the neighboring vehicles with the RSU. Source vehicle in this scenario transmits encrypted P_{info}, which is decrypted using public key provided by vehicle to its neighbor. This secure system prevents external attacks by employing encrypting transmitting P_{info} as well as registration of vehicles with RSU. However, the system is dependent on the availability of RSU and lack a mechanism to identify internal attacks.

Encryption mechanisms used for vehicle authentication as well as encryption purposes play a vital role in creating secure P2P systems. Both these mechanisms help to establish P2P systems that are robust enough such that they are available to the users even under malicious attacks. For interested readers, a detailed list of literature describing such secure and robust systems based on encryption mechanisms is available at [7–10, 20]. In addition to this, anonymity in P2P communication facilitates in securing confidential information of vehicles such as speed, identity, and location of vehicles. The methodologies used for anonymizing vehicle information in literature of P2P VANETs are based on either pseudonyms of k-anonymity principles [6–13]. In the pseudonym approach, a vehicle is allotted an alias from a pool of pseudonyms by using a different algorithm to achieve vehicle anonymity. On the other hand in k-anonymity approach, vehicle information attributes are either suppressed or generalized to avoid identification and tracking of a vehicle and its passengers.

2.2. Security in Broadcasting (BC) Communication

In the BC, the information is shared among all vehicles in the network, therefore this information is classified as public. Security aspects are relatively new in the VANET broadcasting, consequently the research paper [21] is the only research paper we were able to find. In [21], a detail and analytical discussion related to security perspective of the multi-hop broadcasting message is discussed. The paper identifies and provides possible solutions based on the previous research studies in other wireless networks. A novel methodology or technique has not been proposed in this paper. To the best of our knowledge, there has been no other novel methodology or technique being proposed during the writing process of this paper. On the other hand, the three distinct security parameters of authentication, anonymity, and availability of resource remain equally important for the security of broadcasting. Therefore, we can extend the strategies available in P2P VANET to the security applications in BC.

The concepts and associated principles required for the authentication mechanisms explored in P2P communication are implementable for BC as well. Whereas, anonymity techniques based on either pseudonyms or k-anonymity principles are also effective in case of BC. However, due to public nature of information in BC, encryption and cryptographic techniques used for encryption of the original P_{info} cannot be applied in their current form.

3. Generalized VANET System Model

In this section, we present a general purpose VANET system model with $v = 1, ..., V$ vehicles in the network. These vehicles move with speed, s, of 60 to 100 km/h in the same direction on a highway that consists of multiple lanes. On the other hand, the vehicles on the urban environment travel with the same speed, however these

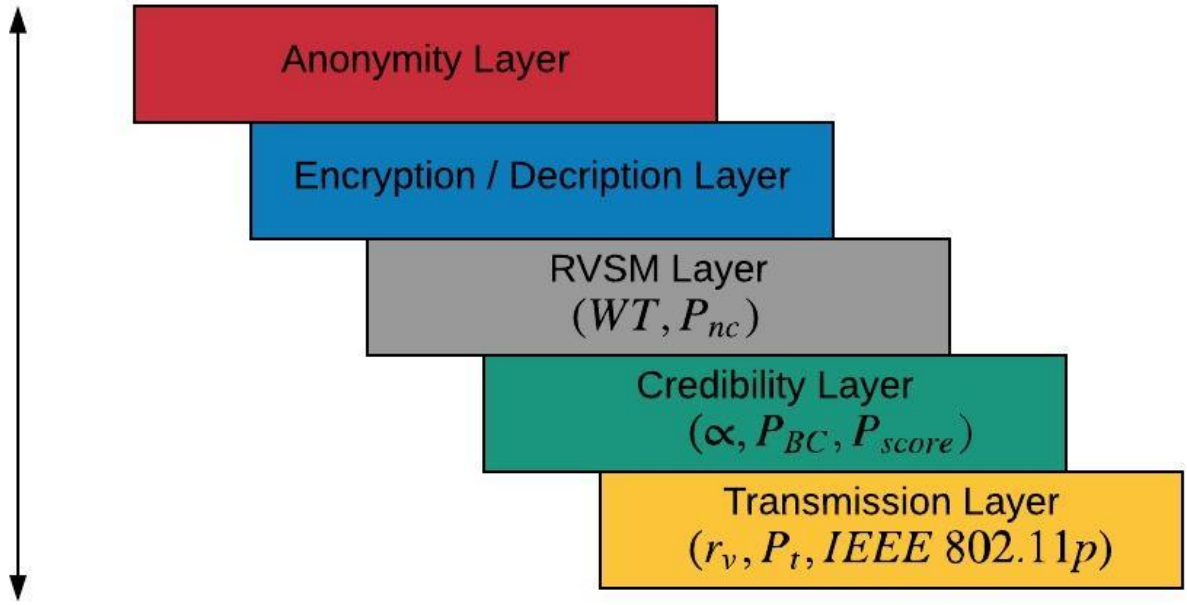

Figure 1. Layered architecture of the proposed secure broadcasting in the VANETs

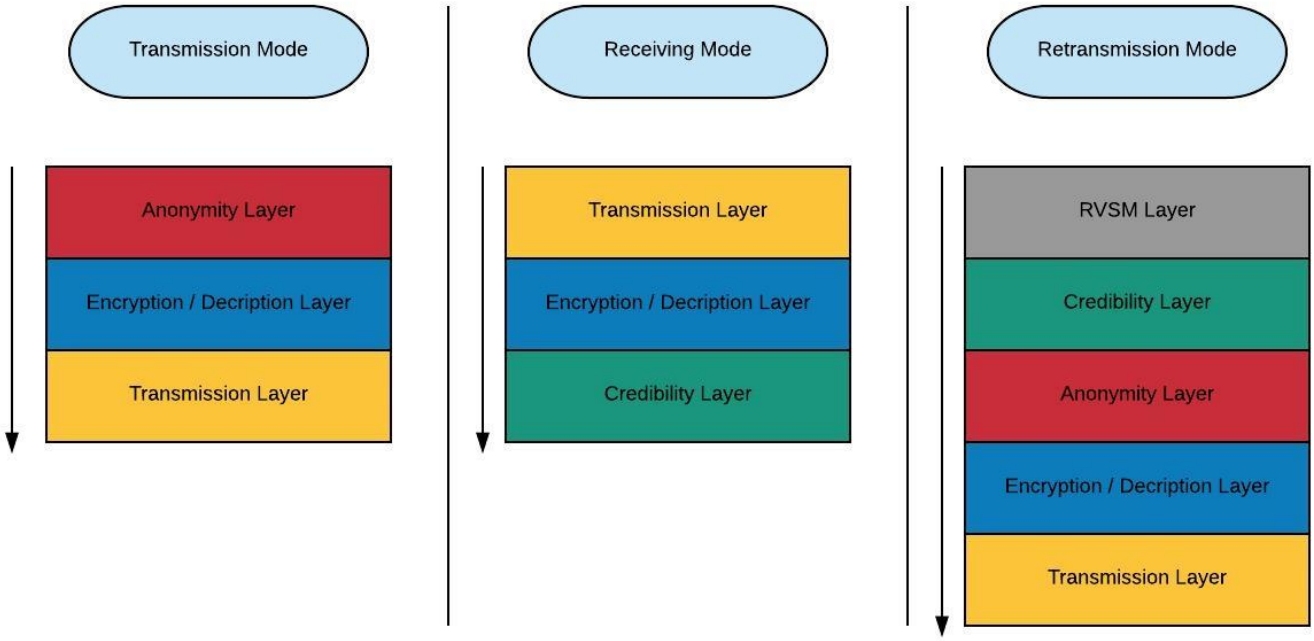

Figure 2. Operating modes of the proposed secure broadcasting architecture

vehicles are able to run left or right depending on the availability of the road. Moreover, the vehicles are randomly distributed capable of communicating with each other using the IEEE 802.11p communication protocol. The IEEE 802.11p belongs to the family of the IEEE 802.11 wireless protocol standards created to support mobile vehicular communication networks [22, 23]. Due to the availability of a large number of features in the IEEE802.11p, it has become the de facto protocol for VANETs [24]. Among these features, Carrier Sense

Multiple Access with Collision Avoidance (CSMA/CA) and beaconing system are the two vital features that play important part in our research [25].
The CSMA/CA is a packet collision avoidance process that facilitates in the seamless transmission of information in a network. In this process, a vehicle, which has a desire to transmit, is required to sense the network for the purpose of establishing network usage. An immediate transmission will proceed when there is no other transmission by any other vehicle in the network. However, a random wait time, formally known as contention window, is assigned to the vehicle if the network is busy. After expiry of this wait time, the vehicle will check the network again and depending on the status of the network, the vehicle will either transmit or assign another wait time. The process of assigning wait time will continue until information is transmitted. Presence of the CSMA/CA helps to avoid implementation of complex collision avoidance and detection system, which would have increased the complexity of our system many folds.
Beaconing system is another feature of the IEEE 802.11p that helps a vehicle to maintain an up to date information regarding their neighborhood This information facilitates accurate calculation of the probability of neighborhood, P_{nc}, which is vital in calculating wait time, WT, of an P_{info}. P_{nc}, WT and other variables of the retransmission system are further discussed in Section 4.

4. Proposed Secure Broadcasting Architecture

A layer based secure broadcasting architecture has been proposed in this Section. The purpose of this proposed architecture is to identify any type of alteration in public information during BC. The proposed architecture consists of five different layers, namely anonymity, credibility, encryption/decryption, relay vehicle selection method, and transmission layer as shown in figure 1. In addition to this, these layers support different operating mode discussed in Section 5. A detailed discussion related to functionalities associated with these layers is explained in the following subsections:

4.1. Anonymity Layer (AL)

Anonymity layer (AL) facilitates in anonymizing information for the purpose of hiding identifiable information of a vehicle. Techniques, such as shared pseudonym pool, put forward in Section 2 for P2P can be introduced in anonymity layer to anonymize vehicle information. In this technique, each network in VANETs has a shared pseudonym pool consisting of unique alias that can be chosen by a vehicle to shield its identity.

4.2. Encryption/Decryption Layer (EDL)

Encryption is one of the most effective and efficient systems to secure information. Therefore, we propose an encryption/decryption layer (EDL) to achieve this functionality in our model. This layer can be used to encryption actual information as well as the signature of vehicles to preserve the authenticity of a P_{info}. Due to public nature of P_{info}, the encryption strategies available in P2P discussed in Section 2, such as [8–10], are not directly applicable in BC.

4.3. Relay Vehicle Selection Method (RVSM) Layer

RVSM layer is required during the transmission phase for the purpose of avoiding the broadcasting storm. The broadcasting storm is caused by blind retransmissions to achieve network coverage, which is a process of achieving propagation of P_{info}, to all the vehicles in a network. The RVSM layer consists of a technique, put forward in previous research [24], that assigns a wait time, WT, based on the probability of neighborhood coverage, P_{nc}, to avoid the broadcasting storm. A P_{info} is broadcasted after the assigned WT has expired. The probability of neighborhood coverage, P_{nc}, is determined by all the vehicles, N_{np}, that have received this information, and all the vehicles in the neighborhood database, N_{vh}, of that vehicle. Mathematically, P_{nc} can be defined as follows:

$$P_{nc} = \begin{cases} 0, & \text{if } N_{np} = 0 \\ 1, & \text{if } N_{vh} = 0 \\ \frac{N_{np}}{N_{vh}}, & \text{otherwise .} \end{cases} \quad (1)$$

4.4. Creditability Layer (CL)

Credibility layer establishes the authenticity of an information packet, P_{info}, which facilitates in the process of prioritization during transmission. The process of establishing authenticity for a vehicle consists of computing and storing historical information related to credibility index, $\propto$, broadcasting probability, P_{BC}, as well as authenticated packet score, P_{score}, of all the vehicles in its neighborhood. The credibility of a vehicle is defined by $\propto$ using historical data consisting of P_{BC} of all the previous retransmissions. Mathematically, $\propto$ is defined as follows:

$$\propto := \begin{cases} 1, & \text{if } B_n = 0 \\ \frac{1}{B_n}\left(\sum_{i=1}^{B_n}(P_{BC})_i\right), & \text{otherwise ,} \end{cases} \quad (2)$$

where B_n is the total number of historical retransmissions. In addition to this, a priority value is assigned to the P_{info} using P_{BC} using Algorithm 1. The P_{BC} relies on a combination of $\propto$ and P_{score}, which consists of an average number of authentic P_{info} received from the

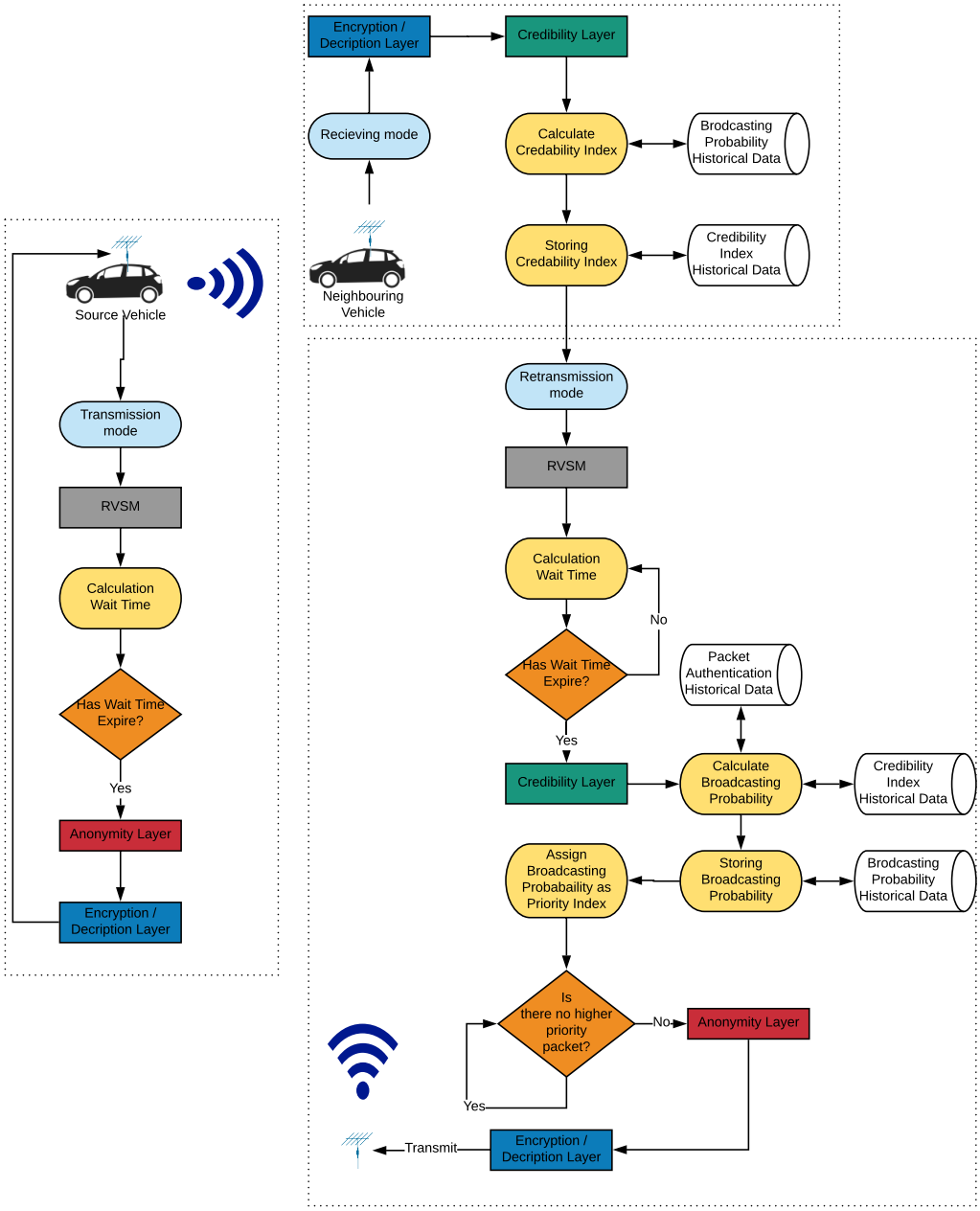

Figure 3. Detail explanation of different layers and transmission modes of the proposed secure broadcasting architecture

source vehicle. Formally, P_{BC} is defined as follows:

$$P_{BC} := \frac{\propto}{P_n}\left(\sum_{i=1}^{P_n}(P_{score})_i\right), \tag{3}$$

where P_{score} ranges between 1 and 0, while P_n are the total number of packets received from the source vehicle. It is important to note that P_{BC} of P_{info} may increase or decrease if another vehicle in the same vicinity either confirms or contradicts the original P_{info} by the source. On the other hand, if a rebuttal is transmitted by source or any other vehicle in the vicinity, the P_{score} transmitted by relay vehicle is decreased by 0.1.

Algorithm 1 Pseudocode of CreditGetPriority function of Credibility Layer

```
function CL_GetPriority(V_id, P^id_info, P_score, isStore)
    if isStore then
        UpdateVehicleHistoricalData(V_id, P_score)
    end if
    Array_P_score ← GetVehicleHistoricalData(V_id)
    P_N ← Length_of_Array_P_score
    Total_P_score ← 0
    for i ← 0 to P_N do
        Total_P_score ← Total_P_score + Array_P_score[i]
    end for
    P_BC ← random(Total_P_score/P_N, 2)
    if isStore then
        UpdateBCHistoricalData(V_id, P^id_info, P_BC)
    end if
    Array_P_BC ← GetBCHistoricalData(V_id, P^id_info)
    B_N ← Length_of_Array_P_BC
    if B_N = 0 then
        return [1, 1]
    end if
    Total_P_BC ← 0
    for i ← 0 to B_N do
        Total_P_BC ← Total_P_BC + Array_P_BC[i]
    end for
    ∝← random(Total_P_BC/B_N, 2)
    return [ ∝ ×10, total_P_score]
end function
```

4.5. Transmission Layer (TL)

Transmission layer facilitates in the propagation of P_{info} in a communication network. The IEEE 802.11p protocol governs the transmission of P_{info} over a wireless medium, however, the transmission can also use other established protocols such as Wireless Access in Vehicular Environment (WAVE). We assume that a vehicle, v, transmits its information as a vector $\vec{x}$ such that:

$$\vec{x} = [x_1, x_2, ..., x_n]_{1\times N}, \tag{4}$$

where $x_1, x_2, ..., x_n$ are the coded information alphabets. The transmission vector, $\vec{x}$, is affected by the wireless channel fluctuations, modeled by the channel matrix, $\mathbf{H}$, and the noise vector, $\vec{n}$. The information signal received on a vehicle, v, can be represented by $\vec{y}_v$ and is given as:

$$\vec{y}_v = \mathbf{H}\vec{x}^{\top} + \vec{n}, \tag{5}$$

such that $[\vec{y}_v]_{N\times 1}$, $[\mathbf{H}]_{N\times N}$, $[\vec{n}]_{N\times 1}$ and $\vec{x}^{\top}$ represents transpose of $\vec{x}$. We further assume that each element of $\vec{H}$ is modeled as a Gaussian random variable and the noise $\vec{n}$ is also modeled as uniformly distributed Additive White Gaussian Noise, $AWGN$, with zero mean and unit variance. Such a model is used in most of the VANET communication scenarios such as [26–28]. Furthermore, the data rate at which each vehicle can transmit the packets is denoted by r_v and can be given as:

$$r_v = \eta \log_2\left(1 + \frac{P_t|\mathbf{H}\mathbf{H}^*|^2}{|\vec{n}|^2}\right)bps, \tag{6}$$

where P_t is the transmitted power, η is the bandwidth in Hz and $(.)^*$ denotes the complex conjugate transpose of a matrix.

5. Secure Broadcasting Operating Modes

The proposed secure broadcasting architecture consists of three different operating modes, known as *transmission, receiving and retransmission* modes. These modes operate by utilizing secure broadcasting layers, which are stacked together in different formation according to operating modes shown in figure 2. These modes are further discussed in the following sections:

5.1. Transmission Mode

Algorithm 2 Pseudocode of Transmission Mode

```
function TransmissionMode(Data, V_info)
    WT ← 0
    isTransmit ← False
    Data[P_score] ← 1
    while isTransmit = False do
        if WT = 0 then
            isTransmit ← Check_CSMA_CS(V_info)
            WT ← RSVM()
        end if
        WT ← WT − 1
    end while
    V_AD ← AL(V_info)
    P_info ← EDL(V_AD, Data)
    Transmit(P_info)
end function
```

A vehicle, known as source vehicle, is in transmission mode during the process of transmitting an original P_{info}. The transmission mode requires a combination of AL, EDL, and TL. AL anonymizes source vehicle information, while, EDL helps in encrypting vehicle signature and other metadata. The encrypted information helps a vehicle to identify any message(s) that are circulated with its encryption. The vehicle may identify spam messages and broadcast a rebuttal to that message if needed. This helps to safeguard the network against spam messages and spamming vehicles. Pseudocode of transmission mode is put forward in Algorithm 2.

Algorithm 3 Pseudocode of Receiving Mode

```
function ReceivingMode(P_info)
    [V_info, Data] ← EDL(P_info)
    CL_GetPriority(V^id_Info, Data[id], Data[P_score], True)
end function
```

5.2. Receiving Mode

In receiving mode, a vehicle receives an original or retransmitted P_{info}. This mode consists of EDL and CL. The decryption part of EDL is used to decrypt received P_{info}. The part of the message that is of public nature can be decrypted by this layer. In addition to this, the CL comes after EDL. During receiving mode, the CL computes and updates credibility index of transmitting vehicle based on Eq.2. The Pseudocode of receiving mode is put forward in Algorithm 3.

5.3. Retransmission Mode

Algorithm 4 Pseudocode of Retransmission Mode

```
function RetransmissionMode(Data, V_info)
    [Priority, Data[P_score]] ← CL_GetPriority(V^I_Info, Data[I], Data[P_score], False)
    WT ← 0
    isTransmit ← False
    while isTransmit = False do
        if WT = 0 then
            isTransmit ← Check_CSMA_CS(V_info, Priority)
            WT ← RSVM()
        end if
        WT ← WT − 1
    end while
    V_AD ← AL(V_info)
    P_info ← EDL(V_AD, Data)
    Transmit(P_info)
end function
```

A vehicle is in retransmission mode when it decides to retransmit an original or retransmitted P_{info}. However, before a vehicle decides to retransmit, it has to go through an independent method run by all the vehicles in a network to establish their suitability to retransmit a message using RVSM layer. The RVSM layer provides a WT to all the P_{info} that needs to be transmitted. The transmission of a P_{info} proceeds when WT assigned to it is expired. The CL is involved after the RVSM layer for the purpose of computing P_{BC}. This probability facilitates in prioritizing all the information packets for the purpose of broadcasting. The P_{info} with the highest P_{BC} is then forwarded to the transmission layer for broadcasting over the wireless medium. The Pseudocode of receiving mode is put forward in Algorithm 4.

Table 1. Simulation parameters

Parameters	Values
Simulation Area	Variable
Frequency	5.9 GHz
Type of Road	Highway with multiple lanes
Vehicle Densities	5, 10, 20, 40, 50, 100, 150, 200, 250, 300, 350, 400, 450, 500 vehicles
s	Between 60 and 100 km/h
Protocol	IEEE 802.11p
Transmission Range	1000m [29]

Table 2. Symbols and notations

Symbol	Description
P_{info}	Information Packet
N_R	Number of Retransmissions
WT	Wait Time
TTL	Time To Live
P_{NC}	Probability of Neighborhood Coverage
N_{NP}	Number of vehicles that have received the transmitted packet
N_{VH}	Number of neighboring vehicles in the neighborhood.
V	Total Number of vehicles
s	Speed of vehicles
P_{score}	PacketScore
P_N	Total Number of Packet recieved
P_{BC}	Probability of Broadcast Communication
B_N	Total Number of B_N
V_{info}	Vehicle Information Dataset
V_{id}	Vehicle Identity
V^{id}_{info}	Vehicle Identity Property from Vehicle Information Dataset
P^{id}_{info}	Information Identity Property from P_{info} Dataset
$\propto$	Credibility Index

6. Results and Analysis

The secure broadcasting architecture is implemented using a real-time simulation model of highway and urban environments consisting of a priority queue model. The real-time simulation model is developed in Python are conducted on supercomputer Raijin, located in Canberra, Australia [30]. The machine is equipped with state-of-art Fujitsu high-performance processor and has distributed memory cluster that facilitated in achieving overall lower simulation complexity. Multi and parallel processing is supported by the

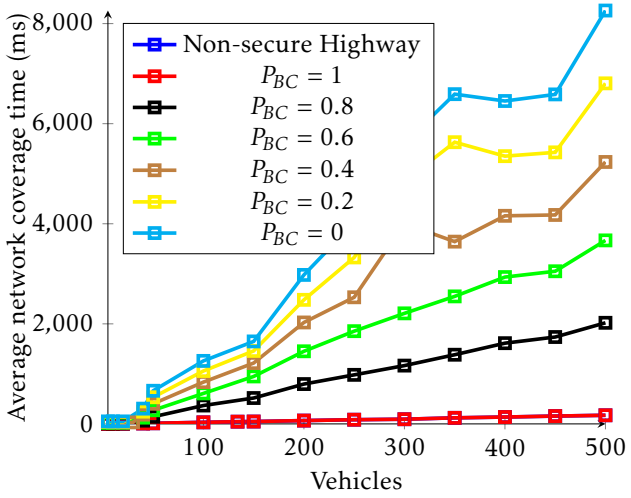

Figure 4. Average network coverage time for different P_{BC} scenarios in vehicular mobile environments for various vehicle densities.

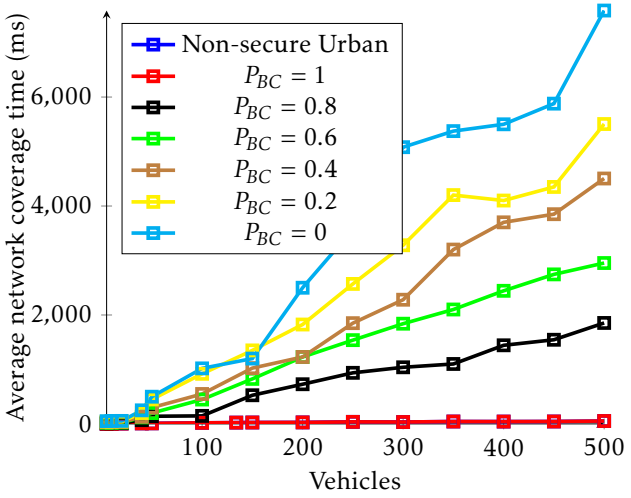

Figure 6. Average network coverage time for different P_{BC} scenarios in vehicular mobile environments for various vehicle densities.

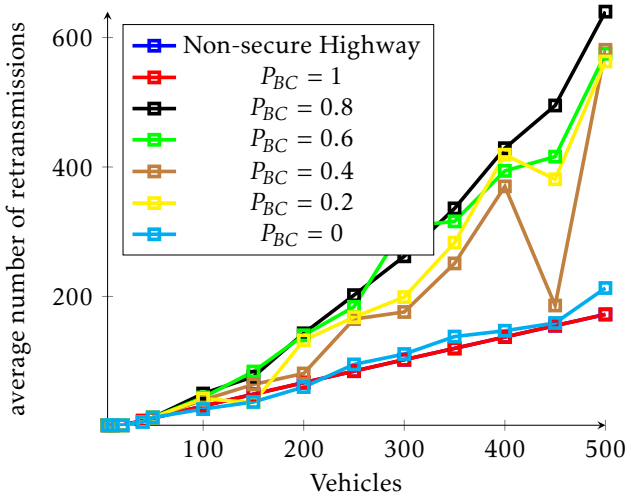

Figure 5. Average number of retransmission in for different P_{BC} scenarios in vehicular mobile environments for varied densities.

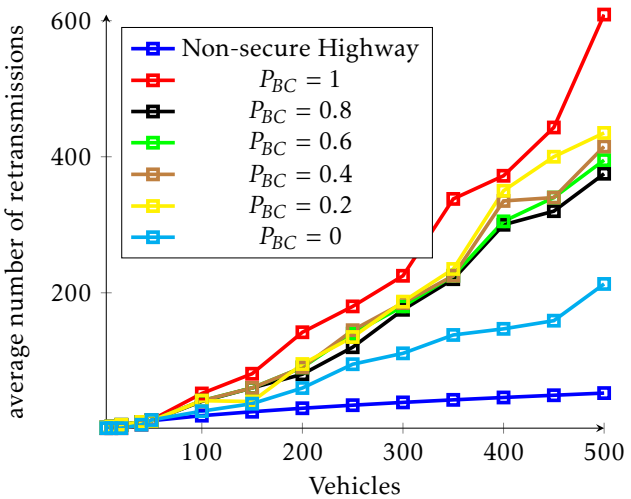

Figure 7. Average number of retransmission in for different P_{BC} scenarios in vehicular mobile environments for varied densities.

supercomputer, which is based on Unix system. Moreover, prioritization of P_{info} in the priority queue is based on Time-To-Live (TTL) and P_{BC}. A P_{info} with a higher value of TTL decreases its priority of retransmission as compared to the lower value of TTL, on the other hand, higher values of P_{BC} increases transmission priority of the P_{info}. The results related to the effect of P_{BC} on network coverage time and the number of transmissions is compared with an unsecure highway and urban environments. The highway and urban scenarios categorized as unsecure lack P_{BC} to establish priority of the P_{info}. In addition to this, the simulation parameters are put forward in Table 1, while Table 2 contains symbols and notations used in this paper.

Additionally, there are different experiment conducted to verify our proposed secure broadcasting architecture discuss concepts discussed in the paper above. The vehicle densities vary between 5 and 500 vehicles travelling on either highway or urban scenarios. In addition to this, vehicles also maintain a safety distance of 70 to 120 meters. The highway scenario consists of 3 lanes and vehicles on highway travel in one direction. On the other hand, there are six roads containing two lanes to allow opposite travel of vehicles in an urban scenario. These roads connect to each other at different points enabling vehicles to turn left or right. In addition to this, the results of the experiments consists of exactly 50 P_{inof} having values of P_{BC} ranging from 1 to 0. Another important parameter is the number of P_{inof}

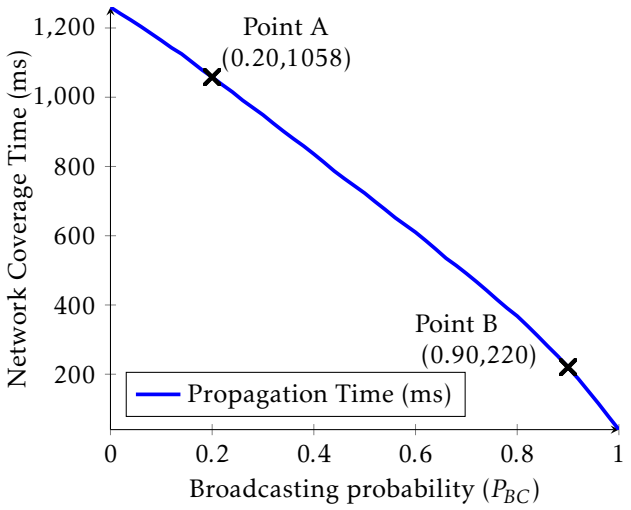

Figure 8. Average number of retransmissions in for different broadcasting probability ,P_{BC}, scenarios in vehicular mobile environments for varied densities.

available for broadcasting at a certain time. In our simulations, the results indicated no significant effect on the experiments for less than 50 P_{inof} in the network. In addition to this, the result show very closely numbers for non-secure and P_{BC} score of 0, therefore the non-secure highway as well as urban scenarios are hidden behind P_BC results of 0. The experiments are further discussed in following two subsections:

6.1. Network Coverage Time

In the first experiment, we investigate network coverage time, which is defined as a time required for propagation of a P_{info} to all the vehicles in the network. The P_{info} that consists of lower values of the P_{BC} are transmitted after those P_{info} with higher values of P_{BC} are transmitted. Therefore, network coverage time of a P_{BC} is directly proportional to the number of P_{info} with higher P_{BC} and vehicle density. The effects of change in network coverage time with respect to the number of P_{info} with different P_{BC} can be observed in figures 4 and 6 for both highway and urban scenarios respectively. The P_{info} network coverage time increases with the decrease of P_{BC}, whereas, an increase in vehicle density also increases network coverage time. In addition to this, an increase in network coverage time due to vehicle density is caused by the increase in the number of vehicles needed to receive P_{info} in a network. On the other hand, network coverage time is quite consistent for the non-secure highway as well as urban environment.

Table 3. Transmission information and broadcasting over time

Time	V_{id}^r	V_{id}^t	P_{info}^{id}	$\propto$	P_{nc}
t_{40}	V_{22}	V_{18}	2	0.3	0.3
		V_{20}	**1**	**1**	**0.3**
	V_{23}	V_{19}	5	0.9	0.3
		V_{14}	6	0.6	0.3
	V_{24}	V_{17}	8	0.1	0.3
		V_{16}	9	0.2	0.3
t_{41}	V_{22}	V_{18}	2	0.3	0.3
	V_{23}	V_{22}	**1**	**1**	**0.7**
		V_{19}	5	0.9	0.3
		V_{14}	6	0.6	0.3
	V_{24}	V_{22}	1	1	1
		V_{17}	8	0.1	0.3
		V_{16}	9	0.2	0.3

6.2. Number of Retransmission

In the second experiment, we explore the number of retransmissions exhibited by the secure broadcasting architecture for both highway and urban scenarios. The experiments for each vehicle density are repeated at least ten times. The number of retransmissions, N_R, is directly proportional to the distribution of vehicles rather than delay in transmission. Therefore, N_R should exhibit nearly the same values irrespective of the P_{BC}. However, delay in transmission may cause changes in the distribution of vehicles due to the movement of vehicles over time. That is one of the reasons for the different number of average retransmissions observed in figure 5 and 7 for different P_{info} irrespective of their P_{BC}.

6.3. Network Coverage Over Time

In the last experiment consisting of results depicted in Figure 8, we present network coverage over time in a network comprised of 100 vehicles. At point A in the figure, a P_{BC} of 0.2 requires an average of 1058 ms to achieve network coverage, while a P_{BC} of 0.9 requires an average network coverage time of 220 ms at Point B. These results show around 80% decrease in the network coverage, when moving from 0.2 to 0.9 P_{BC}. Therefore, it can be deduced that the network coverage time increase with the decrease of P_B as well as observing of similar tendencies of results compared to the previous discussions regarding the increase in the number of retransmissions and network coverage time. In addition to this, the analysis with respect to differences and similarities of the results produced by highway and urban scenario is put forward in [24].

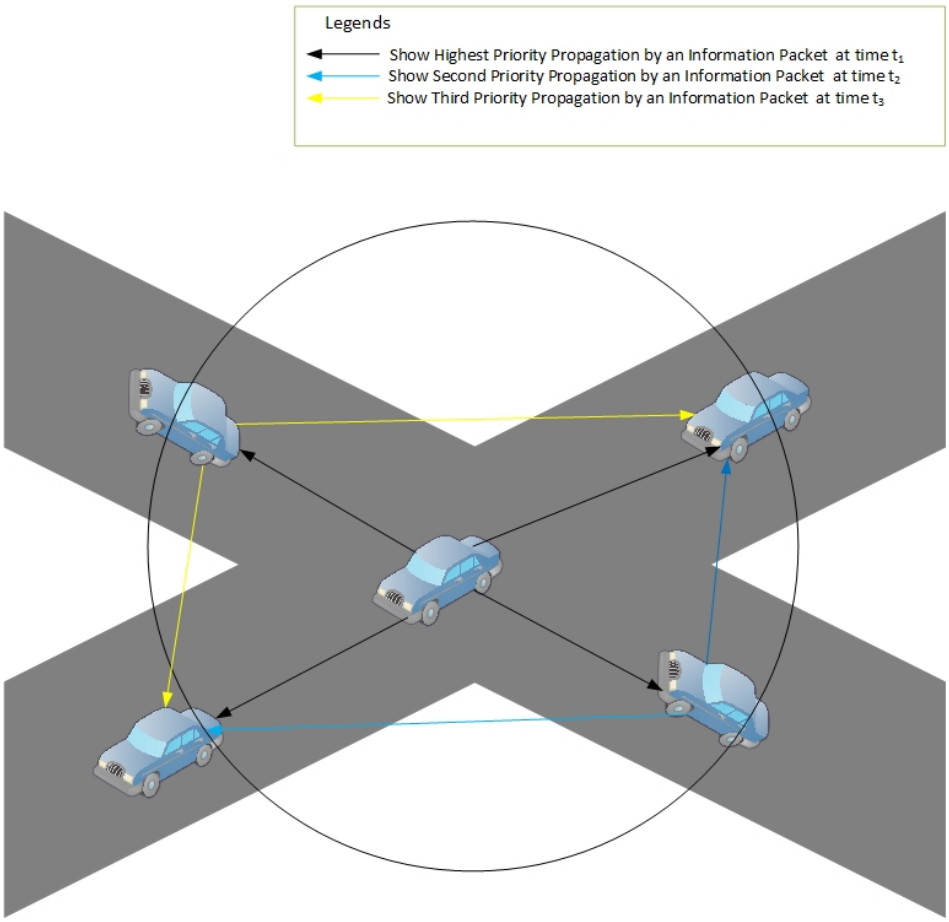

Figure 9. Broadcasting of different packets with different priorities in a network

6.4. Simulation Analysis

In Table 3, a simulation snapshot is present to provide analyses related to the impact of $\propto$ in the transmission process. At the beginning of the simulation, the vehicle in the network does not have enough number of the P_{info} so that the decision of transmitting the P_{info} can be made. In order to present the explanatory numerical results, we start from the vehicle $V_{id}^{r} = V_{22}$. However, the starting vehicle can be any other vehicle in the network. The neighborhood of the $V_2 2$ is depicted in the table, which consists of vehicle 23 and 24. At a time interval t_{40}, the table shows each vehicle containing different P_{info} identified by their identity property, P_{info}^{id}. Each of the P_{info} have different $\propto$ and during transmission, the broadcasting system assigns lower WT to highest $\propto$ in the neighborhood. At t_{40}, the P_{info}^{id} 1 of vehicle 22 is allowed to be broadcasting since its $\propto$ is highest in the neighborhood. On the other hand, At t_{41}, the P_{info}^{id} 1 of vehicle 23 is allowed to be broadcasting, and the same P_{info} is not allowed to broadcast for vehicle 24 due to fact P_{nc} is 1. The 1 value of P_{nc} is achieved when all the neighbors of the vehicle received a P_{info}, therefore there is no need to broadcast this P_{info}.

A similar scenario related to prioritized transmissions of P_{info} in a system is show in figure 9.

7. Conclusion

In this paper, we have identified and categorized security challenges related to broadcasting in VANETs. To counter these security challenges, a secure broadcasting architecture was proposed for the purpose of securing public information from intruders. The secure broadcasting architecture is layered based architecture which is stacked together in different formation according to operating modes. The network computer facility consists of supercomputer having a real-time simulator designed in Python was used for the purpose of collecting results. These results show an increase in network coverage time to achieve network coverage without having any significant differences in number retransmissions when compare with unsecure highway or urban scenarios. The future work of this study is to extend this model to include dynamic readjustment of credibility index and broadcasting probability over the number of time intervals for further verification of the proposed architecture.

References

[1] Kumar N, Misra S, Rodrigues J, Obaidat M. Coalition games for spatio-temporal big data in internet of vehicles environment: a comparative analysis. 2015;.

[2] Alam KM, Saini M, El Saddik A. Toward Social Internet of Vehicles: Concept, Architecture, and Applications. Access, IEEE. 2015;3:343–357.

[3] Gerla M, Lee EK, Pau G, Lee U. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. IEEE World Forum on Internet of Things (WF-IoT). 2014 March;p. 241–246.

[4] ur Rehman S, Khan MA, Zia TA, Zheng L. Vehicular Ad-Hoc Networks (VANETs)-An Overview and Challenges. Journal of Wireless Networking and Communications. 2013;3(3):29–38.

[5] Forouzan AB. Data Communications & Networking (sie). Tata McGraw-Hill Education; 2006.

[6] Choi HK, Kim IH, Yoo JC. Secure and efficient protocol for vehicular ad hoc network with privacy preservation. Journal on Wireless Communications and Networking (EURASIP). 2011;2011:11.

[7] Armknecht F, Festag A, Westhoff D, Zeng K; VDE. Cross-layer privacy enhancement and non-repudiation in vehicular communication. ITG-GI Conference on Communication in Distributed Systems (KiVS). 2007;p. 1–12.

[8] Hesham A, Abdel-Hamid A, El-Nasr MA. A dynamic key distribution protocol for PKI-based VANETs. In: IEEE IFIP Wireless Days (WD). IEEE; 2011. p. 1–3.

[9] Al Falasi H, Barka E. Revocation in VANETs: A survey. In: IEEE International Conference on Innovations in Information Technology (IIT); 2011. p. 214–219.

[10] Al-Kahtani MS. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In: 6th IEEE International Conference on Signal Processing and Communication Systems (ICSPCS); 2012. p. 1–9.

[11] Rivas DA, Barceló-Ordinas JM, Zapata MG, Morillo-Pozo JD. Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation. Journal of Network and Computer Applications. 2011;34(6):1942 – 1955. Control and Optimization over Wireless Networks.

[12] Djamaludin C, Foo E, Camtepe S, Corke P. Revocation and update of trust in autonomous delay tolerant networks. Computers & Security. 2016;60:15–36.

[13] Caballero-Gil C, Molina-Gil J, Hernández-Serrano J, León O, Soriano-Ibanez M. Providing k-anonymity and revocation in ubiquitous VANETs. Ad Hoc Networks. 2016;36:482–494.

[14] Engoulou RG, Bellaïche M, Pierre S, Quintero A. VANET security surveys. Computer Communications. 2014;44:1–13.

[15] Yadav V, Misra S, Afaque M. Security in vehicular ad hoc networks. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. 2010;p. 227.

[16] Stampoulis A, Chai Z. A survey of security in vehicular networks. Project CPSC. 2007;534.

[17] Qian Y, Moayeri N. Design of secure and application-oriented VANETs. IEEE Vehicular Technology Conference (VTC) Spring. 2008;p. 2794–2799.

[18] Kargl F, Ma Z, Schoch E. Security engineering for VANETs. Proc 4th Wksp Embedded Sec in Cars. 2006;p. 15–22.

[19] Papadimitratos P, Buttyan L, Holczer T, Schoch E, Freudiger J, Raya M, et al. Secure vehicular communication systems: design and architecture. IEEE Communications Magazine. 2008;46(11):100–109.

[20] Isaac JT, Zeadally S, Camara JS. Security attacks and solutions for vehicular ad hoc networks. IET communications. 2010;4(7):894–903.

[21] Galaviz-Mosqueda A, Morales-Sandoval M, Villarreal-Reyes S, Galeana-Zapién H, Rivera-Rodríguez R, Alonso-Arévalo MÁ. Multi-hop broadcast message dissemination in vehicular ad hoc networks: A security perspective review. International Journal of Distributed Sensor Networks. 2017;13(11):1550147717741263.

[22] ur Rehman S, Khan MA, Zia TA, Khokhar RH. A synopsis of simulation and mobility modeling in vehicular ad-hoc networks (VANETs). Journal of Computer Engineering (IOSR-JCE), e-ISSN. 2013;p. 2278–0661.

[23] Jiang D, Delgrossi L; IEEE. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. IEEE Vehicular Technology Conference (VTC) Spring. 2008;p. 2036–2040.

[24] Jafer M, Khan MA, Rehman SU, Zia TA. Evolutionary Algorithm based Optimized Relay Vehicle Selection in Vehicular Communication. IEEE Access. 2018;.

[25] Saeed RA, Naemat A, Bin Aris A, Bin Awang MK. Design and evaluation of lightweight IEEE 802.11p-based TDMA MAC method for road side -to-vehicle communications. The 12th International Conference on Advanced Communication Technology (ICACT). 2010 Feb;2:1483–1488.

[26] Goldsmith A. Wireless communications. Cambridge University Press; 2005.

[27] Hussain M, Rasheed H, Ali N, Saqib N. Roadside infrastructure transmission of VANET using Power Line Communication. In: International Conference on Communication, Computing and Digital Systems (C-CODE); 2017. p. 139–143.

[28] Lazaropoulos AG. Deployment concepts for overhead high voltage broadband over power lines connections with two-hop repeater system: Capacity countermeasures against aggravated topologies and high noise environments. Progress in Electromagnetics Research. 2012;p. 283–307.

[29] Saini M, Alelaiwi A, Saddik AE. How Close are We to Realizing a Pragmatic VANET Solution? A Meta-Survey. ACM Computing Surveys (CSUR). 2015;48(2):29.

[30] Intersect Australia Limited; 2017. (Accessed on 17/06/2018). http://www.intersect.org.au/time/raijin/primer.