Exploring 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,
Wagga Wagga, Australia
{mjafer,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 the information cannot be altered by the intruders 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 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 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.

Keywords: VANETs · Secure broadcasting · Network coverage
Information retransmission · Public information

1 Introduction

The revolutionary concept of connecting physical devices to internet is a step towards increasing better services and products for end user satisfaction. Among other devices such as refrigerators, televisions, smart washing machines, etc., vehicles are one of the most important devices for modern day commuters. Therefore, vehicles are at the forefront of new research in connectivity and communication [1–3]. To establish communication, On-Board Units (OBUs) are used in vehicles with most OBUs having limited radio range [4]. In order to overcome this limitation, vehicular communication adopts ad-hoc networks, known

X. Lin et al. (Eds.): SecureComm 2017 Workshops, LNICST 239, pp. 69–84, 2018.
https://doi.org/10.1007/978-3-319-78816-6_6

as Vehicular Ad-hoc Networks (VANET)s. In VANETs, communication link between vehicles change frequently making the topology dynamic and vulnerable to security risks.

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 V2I scenario communication link is established between a vehicle and any roadside infrastructure, commonly known as Road Side Units (RSUs). Further 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 without the aid of another vehicle or fixed infrastructure. 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 vehicle broadcasting 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.

Importance of transmitting authentic information, whether public or private, is very high, therefore, it is crucial to secure the information. Unsecure information specially public information can be misused and can cause mass hysteria and traffic jams. Whereas, when information is secured, it is difficult for intruders to alter the original message and hence lower the risk of creating public panic.

The focus of this paper is to investigate and propose secure broadcasting architecture for VANETs. The proposed secure broadcasting architecture facilitates in 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 learnt from secure P2P communication architectures and apply these ideas in securing 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 to achieve network coverage.

The rest of the paper is organized as follows. Section 2 contains literature review of previous research, whereas Sect. 3 describes the system model that is used in this study. A discussion regarding proposed secure broadcasting architecture is contained in Sect. 4, while operational flow of the architecture is presented in Sect. 5. In Sect. 6, the numerical results are presented in detail. Finally, Sect. 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 communication. 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 for P2P mobile ad-hoc networks. In order to integrate these security features in VANET BC, we can mainly 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 establishing reliability of sender's information and ultimately the mechanism facilitates in preventing Sybil attacks in VANETs. While, 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 if provided with mechanisms 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 that it remains 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 legitimacy of the received information. In [18], trust is based on a process called authentication that help 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 licence number or chaises number of a vehicle, for identification of a vehicle. Whereas, property authentication aid in identifying type of source, e.g. that the source is a vehicle or a traffic signal, on the other hand, location authentication identifies location of a source allowing receiving vehicle to validate received information. Authentication is an effective process of identifying source as well as validating transmitted information. However, this would compromise anonymity of a source vehicle providing convenient way of tracking as well as identifying 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 also introduced by the centralized system for the purpose of validating as well as issuing certificates to registered vehicles. Source vehicles are issued encrypted certificates during transmission of information, while, these certificates are decrypted by providing public key to destination vehicles for validation of transmitted information packets. Furthermore, unique encrypted digital signature generated by the source vehicle and attached to an information packet facilitates in identifying changes in original information by a destination or relay vehicles. Any change in original causes the centralize 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 based on a centralized system implemented through RSUs. Moreover, public nature of information in broadcasting would increase complexity of 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 a RSU. After successful authentication, RSU issue a short-lived anonymous certificate to the vehicle. This certificated as well as public key and signature is broadcasted by the vehicle to all the neighbouring vehicles. The broadcasted information is verified by all the neighbouring vehicles with RSU. Source vehicle in this scenario transmits encrypted information, which is decrypted using public key provided by vehicle to its neighbour. This secure system prevents external attacks by employing encrypting transmitting information as well as registration of vehicles with RSU. However, the system is dependent on availability of RSU and lack mechanism to identify internal attacks.

Encryption mechanisms used for the vehicle authentication as well as encryption purposes play a vital role in creating the 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].

Additionally, 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 pseudonym approach, a vehicle is allotted an alias from a pool of pseudonyms by using different algorithm to achieve vehicle anonymity. Whereas in k-anonymity approach, vehicle information attributes are either suppressed or generalised to avoid identification and tracking of vehicle and its passengers.

2.2 Security in Broadcasting (BC) Communication

In BC, information is shared among all vehicles in a network, therefore, the information is public. Security aspects are relatively new in VANETs broadcasting and to the best of our knowledge, this is the first attempt to propose a secure broadcasting framework. Whereas, the three distinct security parameters of authentication, anonymity and availability of resource remain equally important for 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 authentication mechanism 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 original message cannot be applied in their current form.

3 Generalized VANET System Model

In this section, we present a general 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. The vehicles are randomly distributed where they can communicate with each other using IEEE 802.11p communication protocol. IEEE 802.11p belongs to the family of IEEE 802.11p wireless protocol standards created to support mobile vehicular communication networks [21, 22]. Due to availability of a large number of features in IEEE802.11p, it has become the de facto protocol for VANETs [23, 24]. Among theses 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].

CSMA/CA is a packet collision avoidance process that facilitates in 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 is assigned to the vehicle if network is busy. After expiry of this wait time, the vehicle will check network again and depending on the status of network, vehicle will either transmit or assign another wait time. The process of assigning wait time will continue until information is transmitted. Presence of 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 IEEE802.11p that helps vehicle to maintain an up to date information regarding their neighborhood This information facilitates in accurate calculation of probability of neighborhood, P_{nc}, which is vital in calculating wait time, T_{wr}, of a information packet. P_{nc}, T_{wr} and other variables of the retransmission system are further discussed in Sect. 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 identifying the alteration in public information during broadcasting. The proposed architecture consists of five different layers, namely anonymity, credibility, encryption/decryption, relay vehicle selection method, and transmission layer as shown in Fig. 1. These layers support different operating mode discussed in Sect. 5. A detailed discussion related to functionalities associated with these layers is explained in the following subsections:

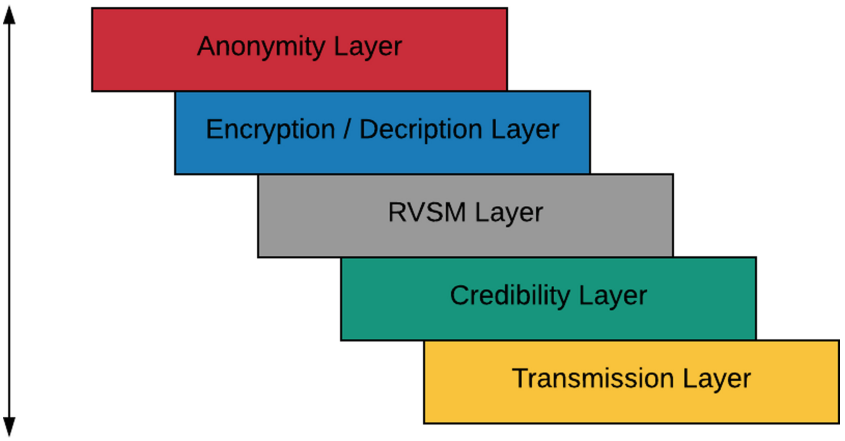

Fig. 1. Layered architecture of the proposed secure broadcasting in VANETs

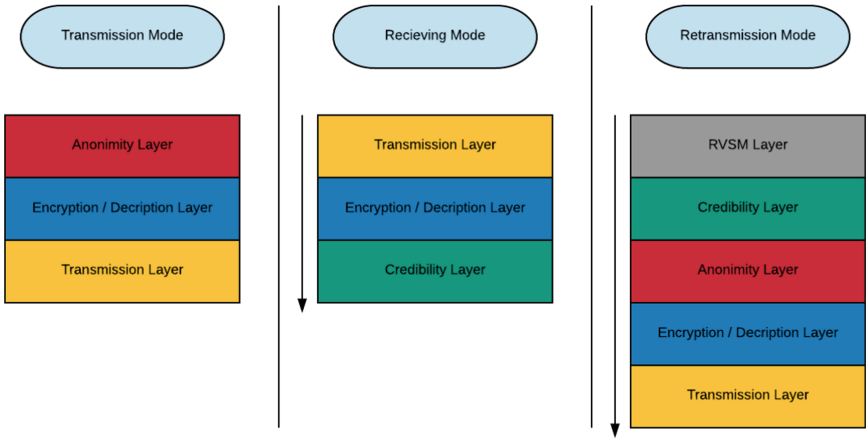

Fig. 2. Operating modes of the proposed secure broadcasting architecture

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 Sect. 2 for P2P can be introduced in anonymity layer to anonymitize 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)

Encryptions is one of the most effective and efficient system to secure information. Therefore, we propose encryption/decryption layer (EDL) to achieve this functionality in our model. This layer can be used to encryption actual information as well as signature of vehicles to preserve authenticity of a information packet, I_p. Due to public nature of I_p, the encryption strategies available in P2P discussed in Sect. 2, such as [8–10], can not be directly applied in VANET broadcasting.

4.3 Relay Vehicle Selection Method (RVSM) Layer

RVSM layer is required during transmission phase for the purpose of avoiding broadcasting storm. Broadcasting storm is caused by blind retransmissions to achieve network coverage, which is a process of achieving propagation of information packet, I_p, to all the vehicles in a network. RVSM layer consisting of a technique, put forward in previous research [23,24], that assigns a wait time, T_{wr}, based on probability of neighbourhood coverage, P_{nc}, to avoid broadcasting storm. An I_p can be broadcast after the assigned T_{wr} expires. Whereas, the probability of neighbourhood coverage, P_{nc}, is determined by all the vehicles, N_{np},

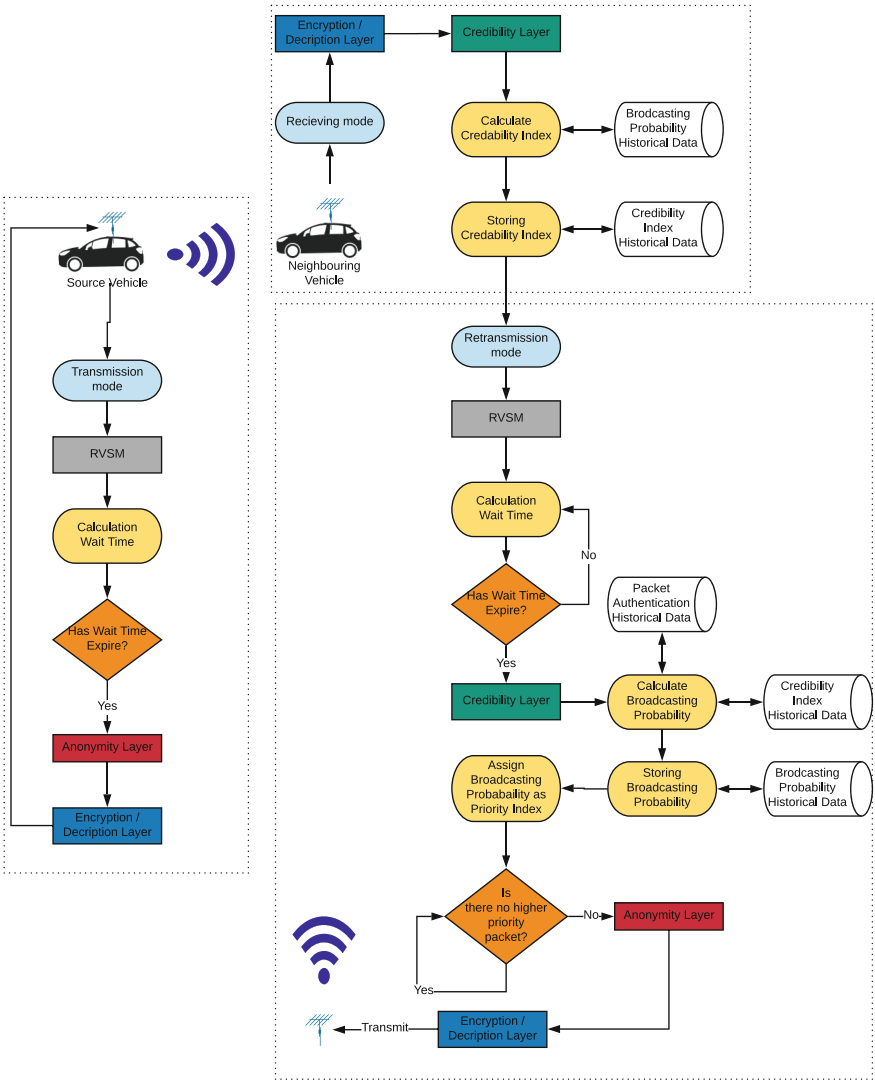

Fig. 3. Detail explanation of different layers and transmission modes of the proposed secure broadcasting architecture

that have received this information, and all the vehicles in the neighbourhood 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 authenticity of an information packet, I_p, which facilitates in process of privatization during transmission. The process of establishing authenticity for a vehicle consists of computing and storing historical information related to credibility index, $\propto$, broadcasting probability, B_p, as well as authenticated packet score, P_a, of all the vehicles in its neighborhood. Credibility of a vehicle is defined by $\propto$ using historical data consisting of B_p of all the previous retransmissions. Mathematically, $\propto$ is defined as following, where B_n is the total number of historical retransmissions:

$$\propto := \begin{cases} 1, & \text{if } B_n = 0 \\ \frac{1}{B_n}\left(\sum_{i=1}^{B_n} B_{pi}\right), & \text{otherwise} \end{cases} \tag{2}$$

While, a priority value is assigned to the information packet, I_p using broadcasting probability, B_p, for the purpose of transmission. B_p relies on combination of $\propto$ and packet authentication score, which consists of average number of authentic packet received from the source vehicle of this current I_p. Formally, B_p is defined as following:

$$B_p := \frac{\propto}{P_n}\left(\sum_{i=1}^{P_n} P_{ai}\right) \tag{3}$$

where P_a is known as packet authentication score ranging 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_a of I_p may increase or decrease by 0.1 respectively, if another vehicle in the same vicinity either confirms or contradicts the reception of original message by the source. Whereas, if a rebuttal is transmitted by source or any other vehicle in the vicinity, one of the P_a transmitted by relay vehicle is decreased by 0.1.

4.5 Transmission Layer (TL)

Transmission layer facilitates in the propagation of information packets, I_p, in a communication network. Transmission of I_p over wireless medium is governed by IEEE802.11p protocol, however, 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 $\mathbf{x}$ such that:

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

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

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

such that $[\mathbf{y}_v]_{N\times 1}$, $[\mathbf{H}]_{N\times N}$, $[\mathbf{n}]_{N\times 1}$ and $\mathbf{x}^\top$ represents transpose of $\mathbf{x}$. We further assume that each element of $\mathbf{H}$ is modelled as a Gaussian random variable and the noise $\mathbf{n}$ is also modelled 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:

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

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 utilize secure broadcasting layers, which are stacked together in different formation according to operating modes shown in Fig. 2. These modes are further discussed in the following sections:

5.1 Transmission Mode

A vehicle, known as source vehicle, is in transmission mode during the process of transmitting original message. The transmission mode requires a combination AL, EDL and TL. AL anonymizes source vehicle information, while, EDL helps in encrypting vehicle signature and other meta data. The encrypted information helps 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 safe guarding the network against spam messages and spamming vehicles.

5.2 Receiving Mode

In receiving mode, a vehicle receives an original or retransmitted information packet, I_p. This mode consists of EDL and CL. The decryption part of EDL is used to decrypt received I_p. The part of the message that is of public nature can be decrypted by this layer. While, the CL comes after EDL. During receiving mode, the CL computes and updates credibility index of transmitting vehicle based on Eq. 2.

5.3 Retransmission Mode

A vehicle is in retransmission mode when it decides to retransmit an original or retransmitted message. 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. RVSM layer provides a wait time, T_{wr}, to all the information packets, I_p, that needs to be transmitted. The transmission of an I_p proceeds when T_{wr} assigned to it is expired. CL is involved after RVSM layer for the purpose of computing broadcasting probability, B_p. This probability facilitates in prioritizing all the information packets for the purpose of broadcasting. I_p with highest B_p is then forwarded to transmission layer for broadcasting over wireless medium.

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	1000 m [29]

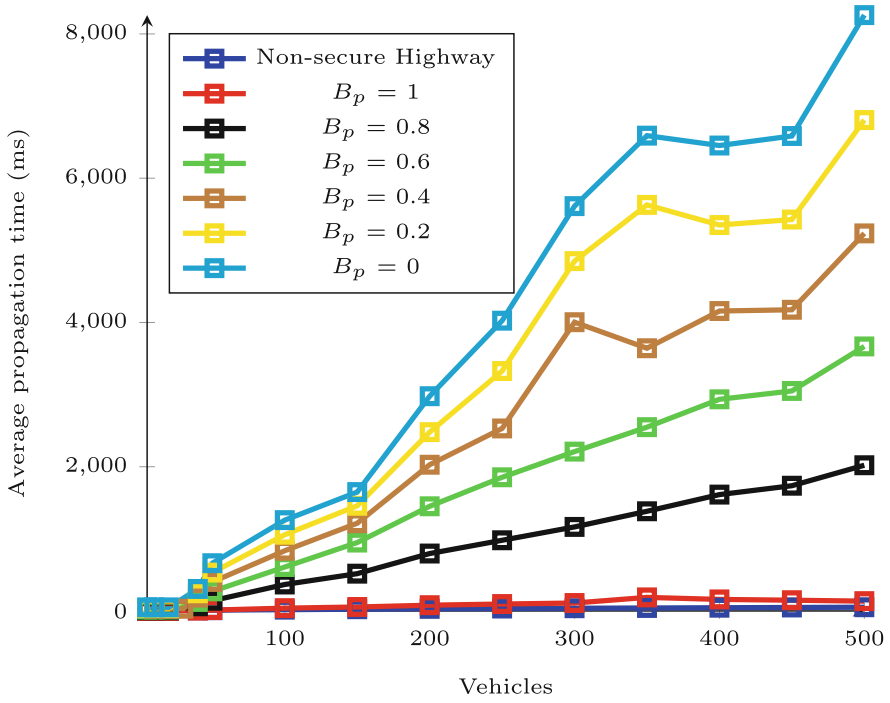

Fig. 4. Average propagation time for different broadcasting probabilities, B_p, scenarios in vehicular mobile environments for various vehicle densities.

6 Numerical Results

The secure broadcasting architecture is implemented by a real time simulation model of highway environment consisting of a priority queue model. The real time simulation model is developed in Python, while privatization of information packets in priority queue is based on Time-To-Live (TTL) and broadcasting probability, B_p. An information packet with higher value of TTL decreases its priority of retransmission as compared to lower value of TTL, on the other hand, higher values of B_p increases transmission priority of the information packet. The results related to effect of B_p on propagation time and number of transmissions are compared with a unsecure highway environment, which lacks B_p to establish priority of the information packet based on the source vehicle. There are different symbols and notations used in the simulation system, which are listed in Table 1. Furthermore, the propagation time in this section is defined as a time required for propagation of an information packets, I_p, to all the vehicles in the network.

Information packets, I_p, that consists of lower values of broadcasting probability, B_p, are transmitted after I_p with higher values of B_p are transmitted. Therefore, propagation time of an I_p is directly proportional to number of I_p with higher B_p and vehicle density. The effects of change in propagation time

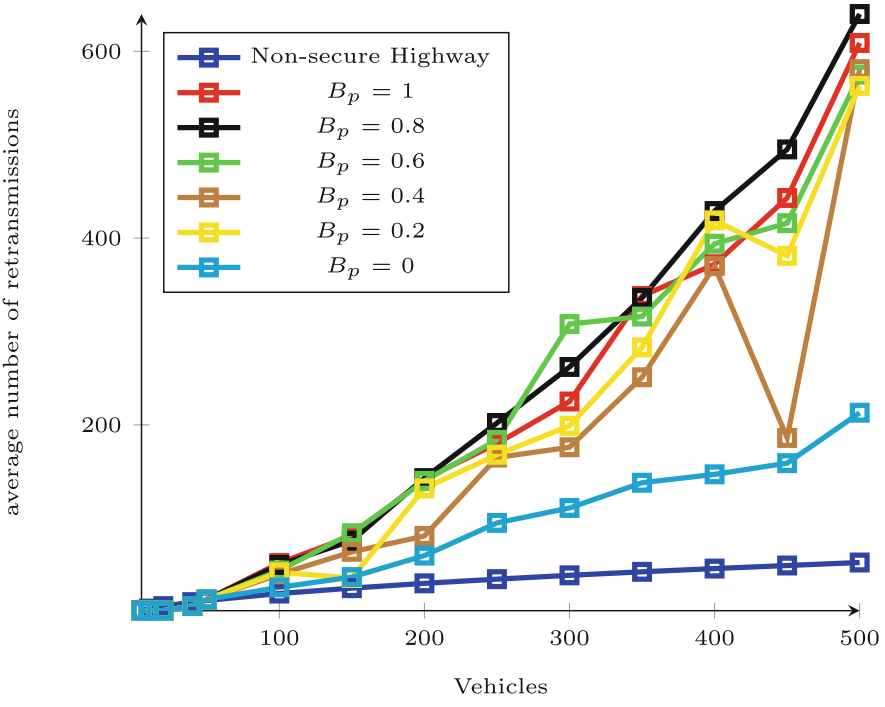

Fig. 5. Average number of retransmission in for different broadcasting probability, B_p, scenarios in vehicular mobile environments for varied densities.

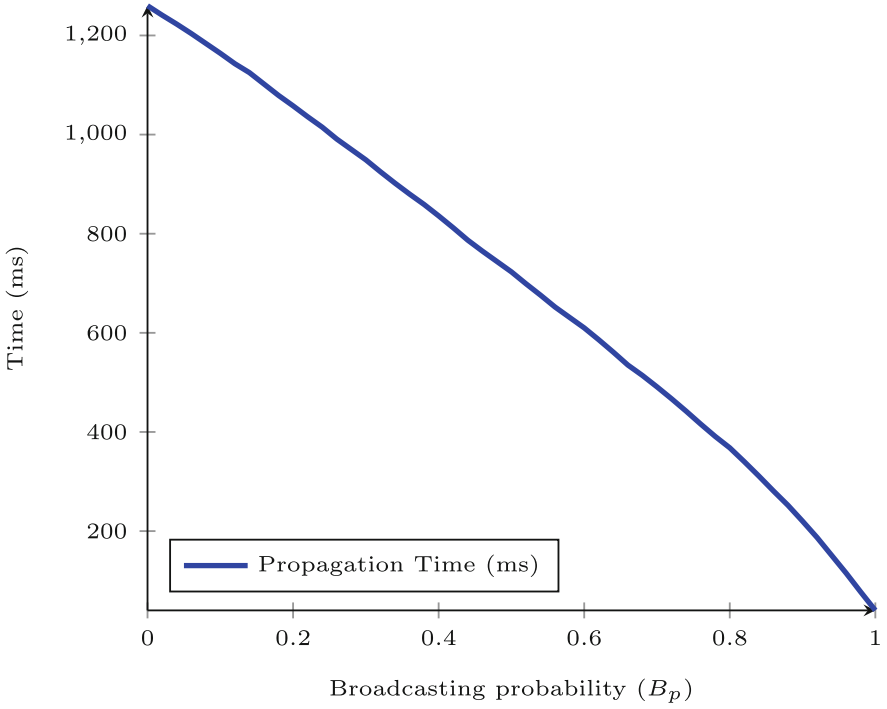

Fig. 6. Average number of retransmissions in for different broadcasting probability, B_p, scenarios in vehicular mobile environments for varied densities.

with respect to number of I_p with different B_p can be observed in Fig. 4. I_p propagation time increases with the decrease of B_p, whereas, increase of vehicle density also increases propagation time. Increase in propagation time due to vehicle density is caused by the increase in the number of vehicles needed to receive I_p in a network. On the other hand, propagation time is quite consistent for non-secure highway environment.

Number of retransmissions, N_R, is directly proportional to distribution of vehicles rather than delay in transmission. Therefore, N_R should exhibit nearly same values irrespective of the probability of retransmission. However, delay in transmission may cause changes in distribution of vehicles due to movement of vehicles over time. That is one of the reasons for different number of average retransmissions can be observed in Fig. 5 for different I_p irrespective of their broadcasting probability. Furthermore, the results in Fig. 6 present propagation time for network coverage over time in a network consisting of 100 vehicles. These results present the similar tendencies compared to the previous discussions regarding increase in $T_w r$.

The results shown in this section consist of exactly 50 I_p having values of B_p ranging from 1 to 0. Another important parameter is the number of I_p available for broadcasting at a certain time. In our simulations, the results indicated no

significant effect on either propagation time or number of retransmissions for less than 50 I_p in the network. The cause of lack of signification variation during broadcasting is caused by quick transmission effect observed and analyzed in our previous work [23,24].

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 are stacked together in different formation according to operating modes. The network computer facility consists of super computer having a real time simulator designed in Python was used for the purpose of collecting results. These results show increase in propagation time to achieve network coverage without having any significant differences in number retransmissions when compare with unsecure highway scenario. The future work of this study is to extend this model to include dynamic readjustment of credibility index and broadcasting probability over 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, K., Saini, M., El Saddik, A.: Toward social internet of vehicles: concept, architecture, and applications. IEEE Access **3**, 343–357 (2015)
3. Gerla, M., Lee, E.-K., Pau, G., Lee, U.: Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds. In: IEEE World Forum on Internet of Things (WF-IoT), pp. 241–246, March 2014
4. ur Rehman, S., Khan, M.A., Zia, T.A., Zheng, L.: Vehicular ad-hoc networks (VANETs)-an overview and challenges. J. Wirel. Netw. Commun. **3**(3), 29–38 (2013)
5. Forouzan, A.B.: Data Communications & Networking (SIE). Tata McGraw-Hill Education, New York City (2006)
6. Choi, H.-K., Kim, I.-H., Yoo, J.-C.: Secure and efficient protocol for vehicular ad hoc network with privacy preservation. EURASIP J. Wirel. Commun. Netw. **2011**, 11 (2011)
7. Armknecht, F., Festag, A., Westhoff, D., Zeng, K.: Cross-layer privacy enhancement and non-repudiation in vehicular communication. In: 2007 ITG-GI Conference Communication in Distributed Systems (KiVS), pp. 1–12 (2007)
8. Hesham, A., Abdel-Hamid, A., El-Nasr, M.A.: A dynamic key distribution protocol for PKI-based VANETs. In: 2011 IFIP Wireless Days (WD), pp. 1–3. IEEE (2011)
9. Al Falasi, H., Barka, E.: Revocation in VANETs: a survey. In: 2011 International Conference on Innovations in Information Technology (IIT), pp. 214–219. IEEE (2011)

10. Al-Kahtani, M.S.: Survey on security attacks in vehicular ad hoc networks (VANETs). In: 2012 6th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1–9. IEEE (2012)
11. Rivas, D.A., Barceló-Ordinas, J.M., Zapata, M.G., Morillo-Pozo, J.D.: Security on VANETs: privacy, misbehaving nodes, false information and secure data aggregation. J. Netw. Comput. Appl. **34**(6), 1942–1955 (2011). 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. Comput. Secur. **60**, 15–36 (2016)
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 Netw. **36**, 482–494 (2016)
14. Engoulou, R.G., Bellaïche, M., Pierre, S., Quintero, A.: Vanet security surveys. Comput. Commun. **44**, 1–13 (2014)
15. Yadav, V., Misra, S., Afaque, M.: Security in vehicular ad hoc networks. In: Security of Self-organizing Networks: MANET, WSN, WMN, VANET, p. 227 (2010)
16. Stampoulis, A., Chai, Z.: A survey of security in vehicular networks. Project CPSC, vol. 534 (2007)
17. Qian, Y., Moayeri, N.: Design of secure and application-oriented VANETs. In: IEEE Vehicular Technology Conference on VTC Spring 2008, pp. 2794–2799 (2008)
18. Kargl, F., Ma, Z., Schoch, E.: Security engineering for VANETs. In: Proceedings of 4th Workshop on Embedded Security in Cars, pp. 15–22 (2006)
19. Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., Hubaux, J.-P.: Secure vehicular communication systems: design and architecture. IEEE Commun. Mag. **46**(11), 100–109 (2008)
20. Isaac, J.T., Zeadally, S., Camara, J.S.: Security attacks and solutions for vehicular ad hoc networks. IET Commun. **4**(7), 894–903 (2010)
21. ur Rehman, S., Khan, M.A., Zia, T.A., Khokhar, R.H.: A synopsis of simulation and mobility modeling in vehicular ad-hoc networks (VANETs). IOSR J. Comput. Eng. (IOSR-JCE) **15**, 1–16 (2013). e-ISSN 2278-0661
22. Jiang, D., Delgrossi, L.: IEEE 802.11p: towards an international standard for wireless access in vehicular environments. In: IEEE Vehicular Technology Conference on VTC Spring 2008, pp. 2036–2040 (2008)
23. Jafer, M., Khan, M.A., Rehman, S.U., Zia, T.A.: Optimizing broadcasting scheme for VANETs using genetic algorithm. In: 2016 IEEE 41st Conference on Local Computer Networks Workshops (LCN Workshops), pp. 222–229, November 2016
24. Jafer, M., Khan, M.A., Rehman, S.U., Zia, T.A.: Broadcasting under highway environment in VANETs using genetic algorithm. In: 2016 IEEE 85th Vehicular Technology Conference (VTC-Spring) (VTC Workshops), June 2017
25. Saeed, R., Naemat, A., Bin Aris, A., Bin Awang, M.: Design and evaluation of lightweight IEEE 802.11p-based TDMA MAC method for road side-to-vehicle communications. In: The 12th International Conference on Advanced Communication Technology (ICACT), vol. 2, pp. 1483–1488, February 2010
26. Goldsmith, A.: Wireless Communications. Cambridge University Press, Cambridge (2005)
27. Hussain, M., Rasheed, H., Ali, N., Saqib, N.: Roadside infrastructure transmission of VANET using power line communication. In: 2017 International Conference on Communication, Computing and Digital Systems (C-CODE), pp. 139–143, March 2017

28. Lazaropoulos, A.G.: 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. Prog. Electromagnetics Res. **44**, 283–307 (2012)
29. Saini, M., Alelaiwi, A., Saddik, A.E.: How close are we to realizing a pragmatic vanet solution? A meta-survey. ACM Comput. Surv. (CSUR) **48**(2), 29 (2015)