Journal of Ambient Intelligence and Humanized Computing (2021) 12:9791–9807
https://doi.org/10.1007/s12652-020-02721-5

ORIGINAL RESEARCH

SV2VCS: a secure vehicle-to-vehicle communication scheme based on lightweight authentication and concurrent data collection trees

Righa Tandon[1] · P. K. Gupta[1]

Received: 10 April 2020 / Accepted: 19 November 2020 / Published online: 4 January 2021

Abstract

Vehicle-to-vehicle communication is one of the new paradigms of networking that should be secure, fast, and efficient. In this paper, we have proposed a secure framework that is based on a lightweight authentication scheme for vehicle-to-vehicle communication and established secure communication between the vehicle nodes. Here, we have implemented the concurrent data collection trees that incorporate the lightweight secure message broadcasting protocol to perform secure communication between the vehicles. Furthermore, the proposed scheme ensures fault tolerance during the data collection process between the vehicle nodes and is capable of handling various integrity attacks like Replay, Man-in-the-middle, Modification, and Impersonation. The obtained results represent that the secure network structure reduces the time required for data collection among the vehicle nodes. Results also show that the proposed scheme effectively handles the various integrity attacks and minimizes the time delay during the data collection process in vehicle-to-vehicle communication. A comparative study of results has also been performed with the various other existing schemes.

Keywords Vehicles · Data collection · Secure · Fault-tolerance · Time-delay · Internet-of-vehicles

1 Introduction

With the advancement in vehicular technology, traditional vehicular networks are evolving into the Internet-of-vehicles (IoV) that helps in connecting the vehicles in secure manner. The main aim of the IoV is to acquire the finest communication among vehicles and to fetch the information securely from these vehicles. In IoV, vehicles can communicate with other nearby vehicles, and this process is known as vehicle-to-vehicle communication. The communication link among the vehicles can be established by using some standard networks and internet connectivity to obtain the various benefits. The data that could be shared with the other vehicle nodes in IoV is the vehicle identity, current location of the vehicle, speed of the vehicle, etc. While sharing the data with a large number of vehicles the network can face several security threats that results into loss of data. Therefore, data security forms an integral part in IoV during vehicle-to-vehicle communication.

To establish secure communication among the vehicle nodes in IoV, we have implemented a lightweight authentication scheme (LIAU) (Xu et al. 2019). This scheme uses the combination of single hash functions and keys for authenticating the vehicles. Moreover, this scheme allows vehicles to get themselves registered on to the network. As the registration of a vehicle is successful then a unique ID is assigned to the concerned vehicle. Further, the use of concurrent data collection trees structure with lightweight secure message broadcasting (LSMB) protocol ensures minimizing the time-delay during data collection, and communication process (Cheng et al. 2017; Limbasiya and Das 2020). In concurrent data collection trees, the use of α and β-rings enhances the fault tolerance by reconstructing the network. Furthermore, the LSMB protocol enhances the security of the network by protecting it against several integrity attacks.

The contribution of this research work can be summarized as follows:

✉ Righa Tandon
righatandon@gmail.com

P. K. Gupta
pkgupta@ieee.org

[1] Department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology, Solan, Himachal Pradesh 173 234, India

- Discusses a secure framework for vehicle-to-vehicle communication based on LIAU.
- Implement concurrent data collection tree structure along with LSMB protocol to ensure the security of data during communication and minimizes the time required for data collection.
- LSMB ensures protection against various integrity attacks like replay, man-in-the-middle, modification, and impersonation.
- Enhances fault tolerance of network structure in IoV by reconstructing the network.

This paper is further categorized into various sections where Sect. 2 discusses the existing work for vehicle-to-vehicle communication and data collection processes. Section 3 introduces the framework for vehicle-to-vehicle communication. Section 4 discusses the concurrent data collection trees that reduce the time delay for data collection. It elaborates on the complete scheme for inter-vehicle communication by taking examples. Section 5 provides a detailed security analysis against various integrity attacks. Section 6 focuses on enhancing fault tolerance with concurrent data collection trees and includes various simulation results for the same. Section 7 shows the performance analysis of the proposed scheme. Section 8 includes the simulation results for time-delay minimization, security attacks and also provides the comparative study of obtained results with other schemes. Finally, Sect. 9 concludes this work.

2 Related work

In the past, several studies have been done by the researchers for vehicle-to-vehicle communication in a vehicular network. This section categorizes and includes the various studies about the security-related schemes based on authentication, protocol related schemes, and framework related schemes for the vehicular network.

2.1 Authentication based security-related schemes

Torrent-Moreno et al. (2009) have used the direct radio-based techniques that helps in enhancing vehicle safety on the road. Two categories of the messages are sent between the vehicles. Firstly a periodic message that will tell about the location of the vehicle, and secondly the event-driven message which is sent during the occurrence of a threat. They have controlled the payload of all the periodic messages using distributed fair power adjustment for transportation surroundings. The proposed technique reduces the overall transmission power, and minimizes the communication overhead among the vehicles. Lim and Tuladhar (2019) have proposed an authentication mechanism known as lidar information-based mechanism for vehicle-to-vehicle communication. In this scheme, vehicles can only share their information as they are authenticated. These vehicles are not involved with any trusted authority or infrastructure. The proposed authentication scheme is capable of working against many security threats and therefore, it is considered as one of the robust schemes. Tan et al. (2018) have proposed an authentication protocol for the vehicular environment known as certificate-less authentication. They have used a cryptography-based technique for authentication and distribution of key. For the proposed scenario, vehicles obtain information from other vehicles without any delay. The proposed scheme improves security and overall performance during vehicle to vehicle communication. Timpner et al. (2013) have discussed the vehicle's communication using the cloud and proposed a secure approach that considers the smartphone-based registration, and key deployment. Here, the use of keys provides secure communication among vehicles and establishes trust in vehicular environment. The proposed approach is feasible and secure. Vijayakumar et al. (2016) have provided high-level security by implementing the dual authentication scheme during vehicle communication. They have presented a dual key management scheme for distributing keys among the users. Furthermore, the proposed scheme provides an option for the user to enter and exit from the network with secure transmission of data. Wang et al. (2016) have proposed a two factor-based lightweight authentication scheme for increasing the security of the vehicular network. The proposed scheme reduces the computation cost, and communication overhead among vehicles. Xu et al. (2019) have presented an authentication scheme known as lightweight authentication for the security of vehicles. The proposed scheme prevents any kind of security attacks and it is cost-effective too. Dharminder et al. (2020) have proposed a secure and efficient lightweight authentication scheme that uses mutual authentication, hash functions, and XoR operations while implementing various security measures. The obtained results represent improved security with low computational and communication costs.

2.2 Protocol related schemes

Yasser et al. (2017) have discussed a standalone architecture for vehicle-to-vehicle communication. Two routing protocols i.e. topology-based and position-based, have been used for the implementation of the proposed architecture. They have considered the named data networking (NDN) that ensures several issues while forwarding data through the channel. Kuai et al. (2019) have introduced the delay-tolerant strategy to overcome from the issue of data retrieval in vehicular communication. The proposed scheme provides support in transmitting data to the other vehicles in case of network failure. Mohanakrishnan and Ramakrishnan

(2020) have proposed a technique which includes the use of Genetic Whale Optimization Algorithm. This is done to select a channel for data transmission. This channel will only be active at the time of transmission. Furthermore, modified cognitive tree routing protocol has been proposed that can easily handle any link breakage in the network. The overall scheme reduces the delay in the vehicular network. Zhang et al. (2015) have proposed a protocol which is based on time-division multiple access for the vehicular network. The proposed protocol enhances the overall throughput of the network. Fairness for quality of service has also been assured which in turn increases the performance of the network. Omar et al. (2013) have proposed a protocol based on time-division multiple access which supports one-hop and multi-hop services and also helpful in decreasing collisions during transmission of data.

2.3 Framework and model based schemes

In the vehicular network, communication of confidential messages between vehicles is one of the major concern. He et al. (2014) have proposed the use of emergency slots for sending of various confidential messages with reduced waiting time during transmission. Furthermore, vehicles can exploit their normal slots without any interruption. This will enhance the overall performance, and reduces the time delay. The proposed propagation model reduces the large vehicle obstruction. In many vehicular networks, Dedicated short-range communication has been used. Ahmad et al. (2019) have proposed a congestion control test-bed for controlling the network congestion that overcomes the limitations of dedicated short-range communication. This involves many vehicles to vehicle communications and also legitimize congestion control. Improvement in the overall performance of the network can be witnessed by controlling network congestion. Dey et al. (2016) have proposed a heterogeneous network structure for inter-vehicle communication by using wireless technologies. This helps in safety applications and reduces the traffic data collection. This network works with a large number of vehicles without compromising the performance and with reduced packet delivery errors. Boban et al. (2014) have focused on the effect of shadowing of other vehicles. Real measurement data of vehicles have been considered which is further divided into three groups i.e. line-of-sight, obstructed line-of-sight, and non-line-of-sight. They have used the geometry-based model that enhances the performance of the network. Huang et al. (2018) have focused on the security of electric vehicles and presented a security model known as the lightning network and smart contract. The proposed model includes the registration process, scheduling process, authentication process, and the charging process. Security of vehicles can easily be improvised by using the scheduling mechanisms. Chinnasamy et al. (2019) have proposed smart cloud vehicles of dominating sets that form a basic backbone of the wireless vehicular network. A dominating set consists of a one-hop connection in which nodes are connected. Smart cloud vehicles circulate periodic messages containing the current location of the vehicles to the roadside unit. The main purpose is to find minimal connected dominating sets to enhance speed, processing power, and reducing time delay. Li et al. (2015) have proposed a framework in which privacy preservation and non-repudiation scheme have been used for the vehicular network. They have implemented the public key cryptography for generating pseudonyms to allow authorized users to access vehicles with their real identities. The proposed scheme can also be reused with other security frameworks for improving performance. Dharminder and Mishra (2020) have proposed a framework for vehicular communication. The proposed framework ensures that only authorised users can access the information in the vehicular network. The proposed framework employs a batch verification method and hence it is considered as one of the secure and efficient. It also satisfies security attributes that are suitable for VANET. Mishra et al. (2020) have proposed a security framework for effective vehicular communication. They have used a chaotic map-based authentication scheme. The proposed scheme is secure as it is resistant to many security attacks, and improves the performance of the overall system.

3 Proposed framework

The proposed framework of vehicle-to-vehicle communication network is shown in Fig. 1. Here, vehicles communicate by using wireless connectivity for sending and receiving of data to/from other vehicles in a secure manner. For the secure wireless network, we have used concurrent data collection trees along with LSMB protocol.

3.1 Authentication and registration process

For secure communication among vehicle nodes, we have used the LIAU scheme. This scheme generates a unique key using a hash function for each vehicle. Vehicles can register themselves onto the network by making use of unique keys generated. The overall registration process is managed by the vehicle registration authority (VRA) that assigns unique identities to each requesting vehicle nodes. The VRA puts in a sensor on to the vehicle nodes with essential parameters. Only registered and authenticated vehicles are allowed to transmit the data among themselves. Further, the proposed authentication scheme uses a single hash function which reduces the overall communication costs.

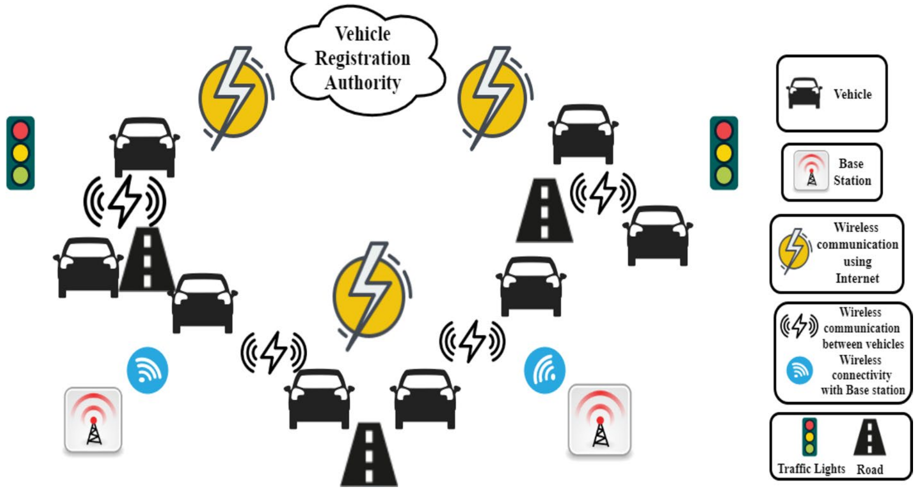


Fig. 1 Framework for vehicle-to-vehicle communication

3.2 Communication and data collection process

In the proposed vehicle-to-vehicle communication network, two types of communication i.e. vehicle-to-vehicle, and vehicle-to-base station in concurrent data collection trees, has been performed. Authenticated vehicle on the road can send information that consist the vehicle identity, data, and time-slot to the other authenticated vehicle. After vehicle-to-vehicle communication, the vehicle node sends the data to the base station. The overall connectivity of this framework is made possible using internet connectivity.

For ensuring secure communication among vehicles, we have used the LSMB protocol that ensures data transmission to be carried out at a faster pace. Furthermore, this protocol can tackle several integrity attacks like replay, man-in-the-middle, modification, and impersonation attacks. This protocol also reduces the data collection time required by vehicles.

4 Secure vehicles-to-vehicle communication using concurrent data collection trees

When a large number of vehicles are involved, the data collection tree structure is more effective and efficient. We have considered a network in which vehicles are assumed as nodes $VN = [\ VN_1, VN_2, VN_3, \ldots, VN_{|N|}]$ and base stations are considered as $BS = [BS_1, BS_2, BS_3, \ldots, BS_{|S|}]$. All the vehicles in the network communicate and send data to each other. A single stream of data gets one unit of time-slot. For maintaining fairness among all the vehicles, the data streams must begin and end at the same time-slot. Considered network $|N|$ in which vehicle nodes is VN, the data stream is DS and the number of vehicles that communicate at a particular time-slot is given as:

$$w_{max} = \left\lfloor \frac{|VN|}{DS} \right\rfloor. \tag{1}$$

Consider w_i as the vehicles that are used by data streams for $i\ th$ time-slot. If w_i is an odd number it represents two types of communication i.e., vehicle-to-base station, and vehicle-to-vehicle. Whereas, if w_i is an even number, it represents vehicle-to-vehicle communication only. We have obtained the mentioned value of w_i as per following:

$$w_i = min \left[w_{max}, |VN| - \sum_{j=1}^{i-1} w_j^{'} \right]. \tag{2}$$

After $j\ th$ time-slot, number of vehicles that have completed transmissions can be represented as $w_j^{'}$ and are given as follows:

$$w_j^{'} = \left\lceil \frac{w_j}{2} \right\rceil. \tag{3}$$

In the first time slot, w_{max} nodes have been utilised by the data streams that have taken part in the data collection process. This results in the formation of two cases where the value of w_{max} can be even or odd. Depending upon the value of w_{max}, the value of time slot $T1$ can be calculated as per following:

$$T1 = \begin{cases} \left\lfloor \frac{2|VN| - w_{max}}{(w_{max}+1)} \right\rfloor + 1, \ if \ w_{max} \ is \ odd, \\ \left\lfloor \frac{2|VN| - w_{max}}{w_{max}} \right\rfloor + 1, \ if \ w_{max} \ is \ even \end{cases} \tag{4}$$

After $(T1 + 1)th$ time-slot, the number of vehicles waiting for data transmission are

$|VN| - T1\left\lceil \frac{w_{max}}{2} \right\rceil$

For completing the remaining process, these vehicles require $T2$ time-slots. Depending upon the number of vehicles, waiting for data transmission, the value of $T2$ time-slot can calculated as per following:

$$T2 = \begin{cases} \left\lfloor log_2(|VN| - T1\left\lceil \frac{w_{max}}{2} \right\rceil) \right\rfloor + 1, \\ if |VN| - T1\left\lceil \frac{w_{max}}{2} \right\rceil > 0, \\ \\ 0, \qquad\qquad otherwise \end{cases} \tag{5}$$

If the obtained value of w_{max} is odd or even then the value of $T2$ time-slot is calculated as per following:

$$T2 = \begin{cases} \left\lfloor log_2(|VN| - T1\left\lceil \frac{w_{max}+1}{2} \right\rceil) \right\rfloor + 1, \\ if |VN| - T1\left\lceil \frac{w_{max}+1}{2} \right\rceil > 0 \;\; and \;\; w_{max} \;\; is \;\; odd \\ \\ \left\lfloor log_2(|VN| - T1\left\lceil \frac{w_{max}}{2} \right\rceil) \right\rfloor + 1, \\ if |VN| - T1\left\lceil \frac{w_{max}}{2} \right\rceil > 0 \;\; and \;\; w_{max} \;\; is \;\; even \\ \\ 0, \qquad\qquad otherwise \end{cases} \tag{6}$$

For the given network topology, we have considered two rings known as α-rings and β-rings. If the value of w_{max} is 1 then the vehicle can directly collect the data from the base station by using star topology. Whereas, for the considered network the value of w_{max} is 2, or w_{max}=3 for data collection and transmission among vehicles by using α-rings or β-rings respectively.

4.1 α-rings

In this structure, $|VN_\alpha|$ represents the number of vehicles that are participating in the network. Where $|VN_\alpha| \geq$ 2DS. In an α-ring having $|VN_\alpha|$ vehicles, a data stream requires T1 time-slot to gather data from $|VN_\alpha|$-1 vehicle. This vehicle considers only one time-slot for combining and forwarding the data to the base station. Let us assume, the number of vehicles in an α-ring are assigned with arbitrary node numbers, i.e., VN_1,VN_2, VN_3,...,$VN_{|N_\alpha|}$. For the vehicle-to-vehicle communication ($VN2VN$ communication), vehicle VN_{k1} communicate and send its data to vehicle VN_{k2} at time-slot 0 < t ≤ T1, where t is the time-slot number and k1 and k2 are the arbitrary node numbers in an α-ring.

$$k1 = (1 + mod(2(DS - 1) + t - 1, |VN_\alpha|)), \tag{8}$$

$$k2 = (1 + mod(2(DS - 1) + t, |VN_\alpha|)). \tag{9}$$

The complete process of formation of an α-ring is shown in Algorithm 1.

Algorithm 1 $\alpha - rings$

```
Procedure:1. Input the number of vehicle nodes $VN_\alpha$.
2. Input the number of data streams $DS$.
3. Calculate $w_{max}$.
4. If $w_{max} = 2$
5. Calculate T1 and T2 using equations (4) and (6).
6. To find which two vehicles are participating in $VN2VN$ communication
   6.1. Calculate k1 and k2 using equations (8) and (9).
END
```

Now, the overall time duration for data collection in vehicle-to-vehicle communication network can be represented as per following:

$$T = T1 + T2. \tag{7}$$

Let's consider an example of α-ring in which the number of vehicles are 6 and data streams are 3. i.e., VN_α=6 and DS=3. Therefore, the value of w_{max} can be calculated using the following:

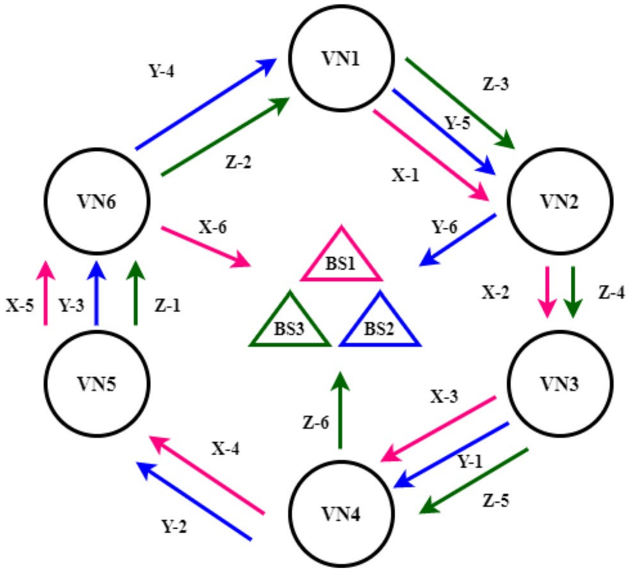


Fig. 2 Vehicle communication and data collection in the network having VN_α=6 and DS=3 (X,Y,Z). Arrows are showing flow of different data streams

$$w_{max} = \left\lfloor \frac{|VN_\alpha|}{DS} \right\rfloor = 2$$

The total time taken is calculated using equations (4) and (6). Hence,

$$T = T1 + T2 = 5 + 1 = 6.$$

Here, the Fig. 2. describes the vehicle communication in which circles are used to represent the vehicles, triangles are used to represent the base stations, and arrows represents the flow of different data streams.

4.2 β-rings

In this structure, a network has been considered in which $|VN_\beta|$ vehicles are participating. Where $|VN_\beta| \geq$ 3DS. This shows that at the similar time-slot, three vehicle nodes are utilized out of which two vehicle nodes are associated with $VN2VN$ communication and the remaining vehicle node is associated with $VN2BS$ communication. Let us assume in β-ring structure, the number of vehicles that are assigned arbitrary node numbers, i.e., VN_1,VN_2, VN_3,...,$VN_{|N_\beta|}$. In DS th data collection process, VN_{k3} is involved for $VN2BS$ communication at different time-slots numbers t. Also, at the particular time-slot number for DS th data collection process, $VN2VN$ communication is involved in which VN_{k3} sends data to VN_{k4}, where k3, k4, and k5 are arbitrary node numbers in a β-ring.

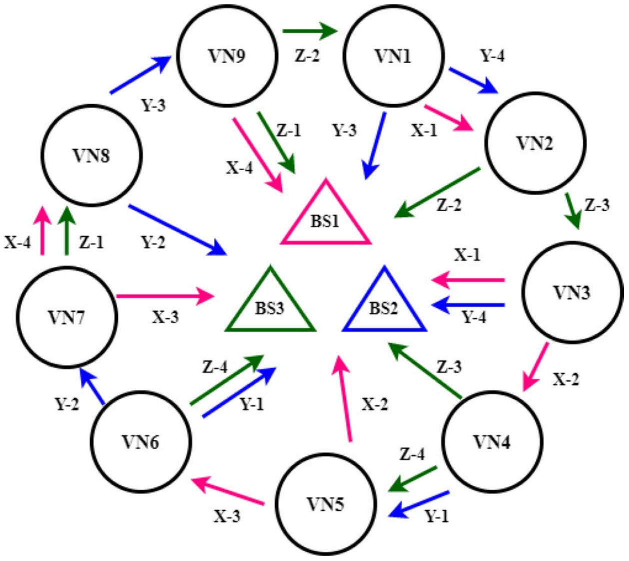


Fig. 3 Vehicle communication and data collection in the network having VN_β=9 and DS=3 (X,Y,Z). Arrows are showing flow of different data streams

$$k3 = (1 + mod(3(DS - 1) + 2(t - 1), |VN_\beta|)), \tag{10}$$

$$k4 = (1 + mod(3(DS - 1) + 2(t - 1) + 1, |VN_\beta|)), \tag{11}$$

$$k5 = (1 + mod(3(DS - 1) + 2(t - 1) + 2, |VN_\beta|)). \tag{12}$$

The complete process of formation of a β-ring is shown in Algorithm 2.

Algorithm 2 $\beta - rings$

```
Procedure:1. Enter the number of vehicle nodes $VN_\beta$.
2. Enter the number of data streams $DS$.
3. Calculate $w_{max}$.
4. If $w_{max} = 3$
5. Calculate T1 and T2 using equations (4) and (6).
6. To find which two vehicle nodes are participating in $VN2VN$ communication and which remaining vehicle node in $VN2BS$ communication
    6.1. Calculate k3, k4, and k5 using equations (10), (11), and (12).
END
```

Consider a case of β-ring structure in which total number of vehicles that are involved for communication are 9 and data streams are 3, i.e., $VN_\beta = 9$, and $DS = 3$. Therefore,

$$w_{max} = \left\lfloor \frac{|VN_\beta|}{DS} \right\rfloor = 3$$

The total time taken is calculated using equations (4) and (6). Hence,

$$T = T1 + T2 = 4 + 1 = 5.$$

The above Fig. 3 describes the $VN2VN$ communication, and $VN2BS$ communication in which circles are used to represent the vehicles, triangles represents the base stations, and arrows represents the flow of different data streams.

4.3 Multiple-rings

In this section, we have considered the the value of w_{max} is greater than 3 therefore, the multiple α-rings and β-rings of distinct sizes are formed for data collection among vehicles.

4.3.1 When w_{max} is an even number ($w_{max} \geq 4$)

In this scenario, where w_{max} is an even number then the total number of α-rings can be calculated as per following:

$$VN_\alpha = \frac{w_{max}}{2}.$$

Firstly, $2DS$ vehicle nodes are allotted with an α-ring. Then the remaining $|VN| - VN_\alpha(2DS)$ vehicle nodes are allotted with an α-ring or a β-ring. For the given time-slot T1, the number of vehicle nodes utilized by data streams are $2VN_\alpha = w_{max}$, and the remaining vehicle nodes i.e. $|VN| - T1w_{max}$ communicate in T2 time-slot.

4.3.2 When w_{max} is an odd number ($w_{max} \geq 5$)

In this scenario, where w_{max} is an odd number one β-ring along with some α-rings are formed. The total number of α -rings can be calculated using the following:

$$VN_\alpha = \frac{w_{max} - 3}{2}.$$

Firstly, a β-ring is allotted with $3DS$ vehicle nodes and α -ring is allotted with $2DS$ vehicle nodes. The remaining $|VN| - 3DS_{BS} - VN_\alpha(2DS_{BS})$ vehicle nodes are allotted to β-ring. It is because the overall duration for data collection in β-ring is less in comparison to α-ring. For T1 time-slot, the maximum communication is done between $VN2VN$ with β-ring size limited upto 2T1+1. This process ensures the collection of data from w_{max} vehicles in T1 time-slot. If any vehicle is remaining then the data collection is done in T2 time-slot.

5 Security analysis

In this section, we have analyzed the security of the network against various possible attacks.

5.1 Data transmission process

During information transmission, the vehicle node (VN_i) transmits the vehicle identity (ID_{VN_i}), and data stream (DS) at time-slot (T_{VN_i}) to the vehicle node (VN_j) for $VN2VN$ communication. Once the communication has been done among the vehicle nodes, the node that receives the data at the last, transmits the data to the base station first. Some basic operations used for transmission are bit-wise XOR operation ($\oplus$), concatenation operation (||), and single hash function (h(.)). The complete data transmission process is shown in Algorithm 3.

Algorithm 3 Data Transmission Process

```
1. $VN_i$ inputs $ID_{VN_i}$, $DS$ and $T_{VN_i}$
2. Calculate E = h( $key_i \oplus ID_{VN_i}$)
3. $VN_i$ calculates:
      i.$D1 = h(ID_{VN_i} \oplus key_i^{'})$
      ii.$D2 = h(D1 \| T_{VN_i})$
      iii. $D3 = D2 \oplus T_{VN_i} \oplus DS$
      iv. $D4 = h(DS \| T_{VN_i} \| ID_{VN_i})$
4. $VN_j$ authenticates:
      i. $D2^{'} = h(E \| T_{VN_i})$
      ii. $DS^{'} = D3 \oplus D2^{'} \oplus T_{VN_i}$
      iii. $D4^{'} = h(DS^{'} \| T_{VN_i} \| ID_{VN_i})$
4. If $D4^{'} = D4$ then, data is received without any modifications
5. Else Attack has been occurred
```

5.2 Integrity of network structure

In this section, we have discussed about the integrity of network structure which integrates LSMB protocol with concurrent data collection trees.

Theorem 1 *The proposed network structure is guarded against attacks that breach the integrity using single hash function.*

Proof To verify the exactness of the information that is being transferred, the network should adhere to the integrity constraint for information transmission. In the proposed network, VN_i transmits ID_{VN_i} and DS at T_{VN_i} to the VN_j for $VN2VN$ communication, i.e., $\{ID_{VN_i}, DS, T_{VN_i}\}$ over the channel. If an attacker tries to alter the information, then a single hash function has been used to maintain the integrity of the communicated information. At the receiver end, vehicle node VN_j computes $D2'$, DS and $D4'$. After the computation, VN_j verifies DS by comparing $D4'$ and $D4$. In case $D4'$ = $D4$, then DS is not altered and is the original data sent by VN_i. If $D4' \not\equiv D4$, then VN_j interprets that the received data is altered and hence neglects it. Hence by this receiver vehicle node comes to know about the exactness of the transferred data. Therefore, the proposed network maintains the integrity in case of attacks.

Algorithm 4 When vehicle node becomes faulty

```
Procedure:1. If vehicle node does not certify its neighbouring vehicle node within particular time-slot then acknowledgement packet is sent again.
2. Further if the acknowledgement is not obtained within that particular time-slot, then there are high chances that the vehicle node is faulty.
3. Calculate $w_{max} = \left\lfloor \frac{|VN|-VN'}{DS} \right\rfloor$, where $VN'$ is the number of vehicle nodes that becomes faulty.
4. Determine the new values for T1 and T2.
5. Network structure is reconstructed using new values of k1, k2, k3, k4 and k5 for $VN2VN$ and $VN2BS$ communication..
```

6 Enhancing fault tolerance using concurrent data collection trees

During $VN2VN$ and $VN2BS$ communication, if any fault occurs then the network can be re-constructed again using α-rings and β-rings of concurrent data collection trees. In this section, we have provided the three different scenarios in which fault can occur and also provided the way for reconstruction of network to recover from fault.

6.1 When vehicle nodes (VN) become faulty

In this scenario, when an acknowledgement is not obtained in a specified time period then there is a possibility that the vehicle node has become faulty. To depict this scenario, we have considered the case of 200 vehicle nodes and ten base stations out of which 50 vehicles nodes are faulty. Firstly, the value of w_{max} has been calculated by using Algorithm 4 and new values of T1 and T2 are determined. For $VN2VN$ and $VN2BS$ communication, reconstruction of the network structure takes place by calculating the new values of arbitrary node numbers k1, k2, k3, k4 and k5 .

In Fig. 4, a new network structure has been constructed using Algorithm 4. In case of α-rings, if any fault takes place in the initial time-slots then there are less chances of data failure as the whole network structure can be constructed again which is shown in Fig. 5a–c. These figures represents the visual representation of reconstructed network when the fault occurs at time-slots T = 1, T = 2, and T = 3 respectively. Similarly, the network can be reconstructed for the remaining time-slots. The network starts functioning properly after the reconstruction. Table 1 shows the values of the parameters k1, k2, k3, k4 and k5 for the network structures before and after the vehicle node failure at different time-slots. In case of β-rings, if any fault takes place then the data failure chances in contrast to α-rings, are high as some vehicle nodes have already sent their data to the base station.

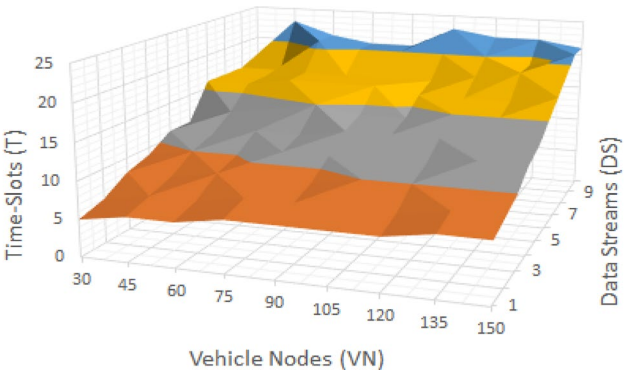


Fig. 4 Network structure with $VN = 200$ and $DS = 10$ where, 50 vehicles nodes become faulty

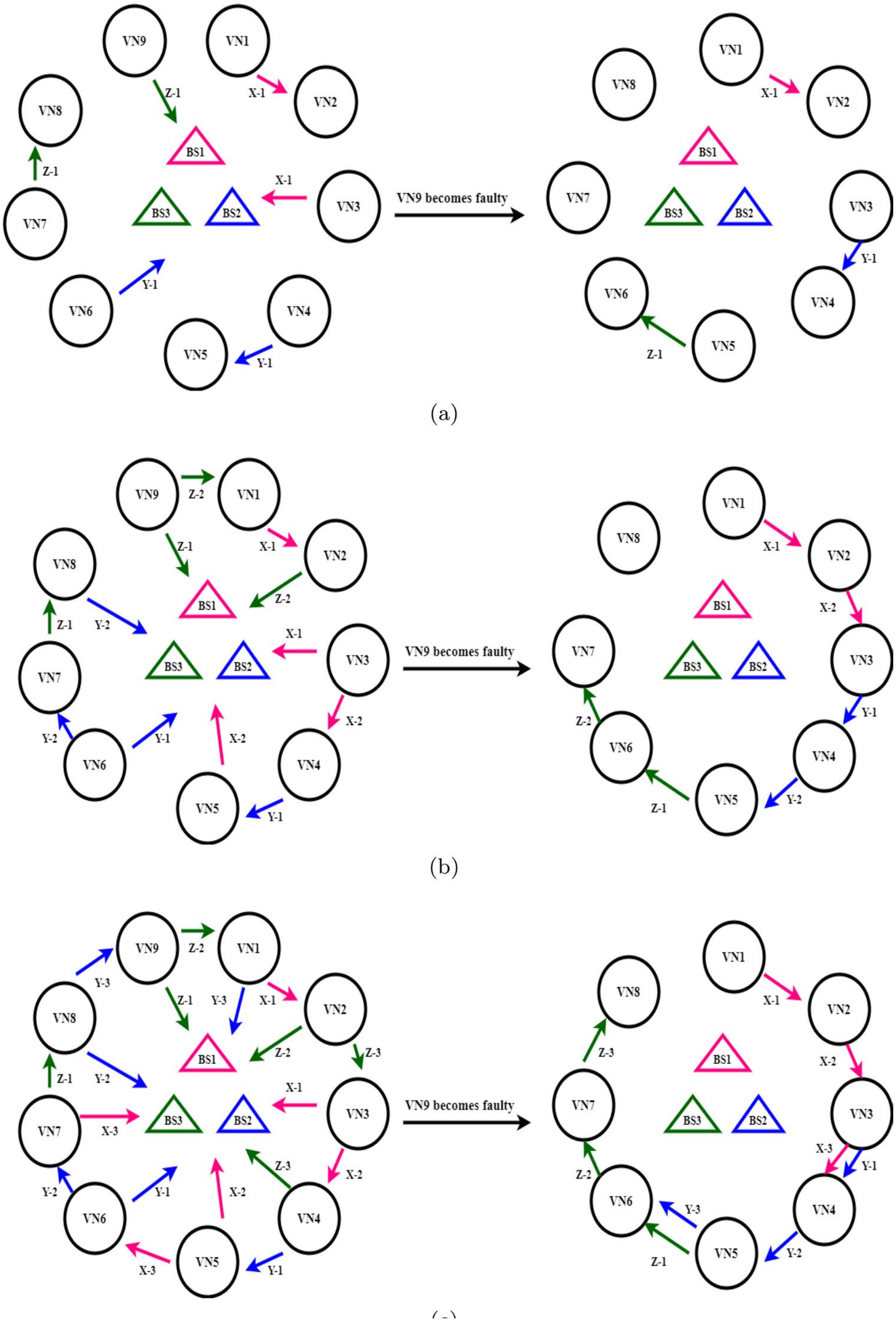
6.2 When base stations (BS) become faulty

In this scenario, when an acknowledgement is not obtained in a specified time period then there are chances that the base station has become faulty. To discuss this scenario we have considered the case of 200 vehicle nodes and ten base stations, out of which 4 base stations are faulty. Initially, the value of w_{max} has been calculated using Algorithm 5 and the new values of T1 and T2 are determined. For $VN2VN$ and $VN2BS$ communication, reconstruction of the network structure takes place by calculating the new values for k1, k2, k3, k4 and k5. In Fig. 6, a new network structure has been constructed using Algorithm 5. In case of α-rings if any fault takes place before last time-slot then any kind of data that might have lost can be recovered completely as the data gathering vehicle nodes contain all the data of a vehicle nodes. If fault occurs at the intermediate time-slot values, then the complete network structure need to be reconstructed. Figure 7a–c depicts the visual representation of network reconstruction for vehicle node failure in first three time-slots. Similarly, the network can be reconstructed for the remaining time-slots. Table 2 shows the values of the parameters k1, k2, k3, k4 and k5 for the network structures before and after the base station failure at different time-slots.

Algorithm 5 When the Base Station becomes faulty

```
Procedure:1. If the base station does not certify the vehicle node within particular time-slot then acknowledgement packet is sent again.
2. Further if the acknowledgement is not obtained within that particular time-slot, then there are high chances that the base station is faulty.
3. Calculate $w_{max} = \left\lfloor \frac{|VN|}{DS - BS'} \right\rfloor$, where $BS'$ is the number of base stations that becomes faulty.
4. Determine the new values of T1 and T2.
5. Network structure is reconstructed using new values of k1, k2, k3, k4 and k5 for $VN2VN$ and $VN2BS$ communication..
```

Fig. 5 Reconstructed network when vehicle node becomes faulty **a** T = 1, **b** T =2, **c** T = 3



(a)

(b)

Table 1 Change in the value of parameters when vehicle node becomes faulty

Time-slot	Network before fault			Reconstructed network	
	w_{max}=3 (β-ring) DS = 3 VN = 9			w_{max} = 2 (α-ring) DS = 3 VN = 8	
	k3	k4	k5	k1	k2
T1	(1,4,7)	(2,5,8)	(3,6,9)	(1,3,5)	(2,4,6)
T2	(3,6,9)	(4,7,1)	(2,5,8)	(2,4,6)	(3,5,7)
T3	(5,8,2)	(6,9,3)	(4,7,1)	(3,5,7)	(4,6,8)

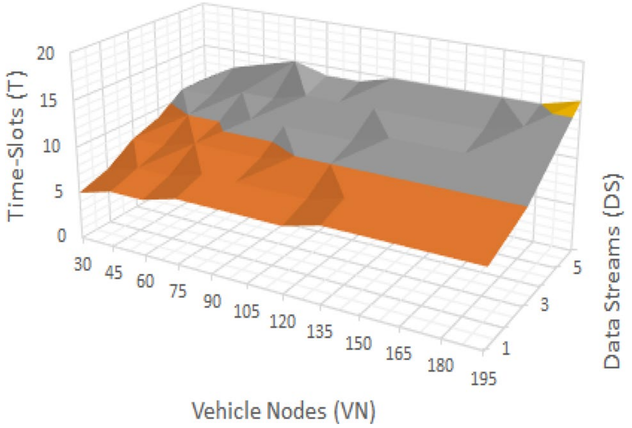


Fig. 6 Network structure with VN = 200 and DS = 10 where, 4 base stations become faulty

In case of β-rings, if any fault occurs then the data failure rate is high in comparison to α-rings. It is because, as some vehicle nodes have already sent their data to the base station and when a data gathering vehicle nodes tries to recover data during failure then that data is not recovered fully.

6.3 When vehicle nodes (VN) and base stations (BS) both become faulty

When vehicle node and base station both fail to send/receive the acknowledgement within a specified period of time then there are chances that both the vehicle node and the base station are faulty. To depict this scenario, we have considered the case of 200 vehicle nodes, and 10 base stations out of which 50 vehicle nodes and 4 base stations are faulty. Firstly, the value of w_{max} has been calculated using Algorithm 6 and the new values for T1 and T2 are determined. For $VN2VN$ and $VN2BS$ communication, reconstruction of the network structure takes place by calculating new values for k1, k2, k3, k4 and k5.

Algorithm 6 When both vehicle node and Base Station becomes faulty

Procedure:1. If the vehicle node or base station does not certify the vehicle node or its neighbouring vehicle node within particular time-slot then acknowledgement packet is sent again.

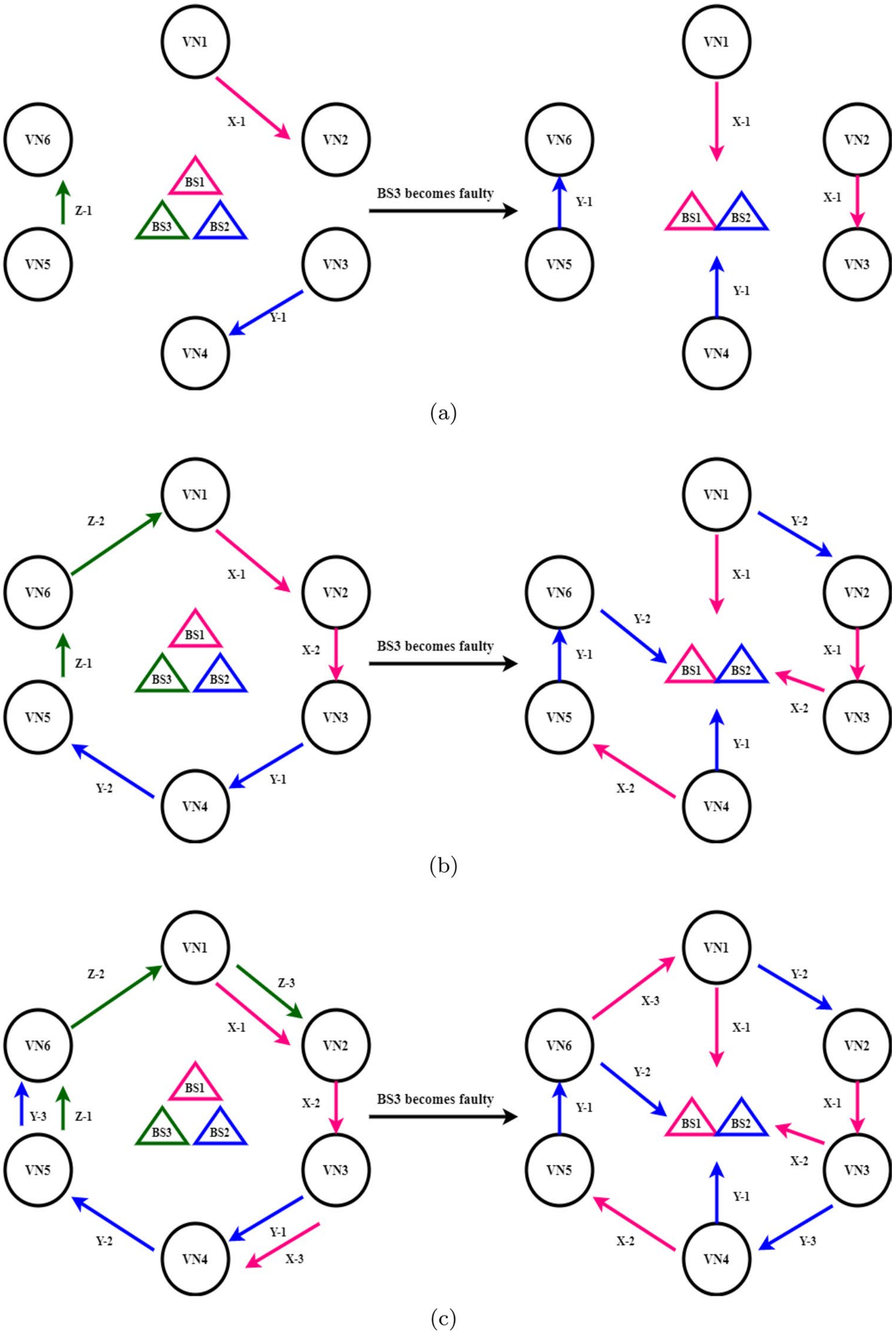
2. Further if the acknowledgement is not obtained within that particular time-slot, then there are high chances that the vehicle node or the base station is faulty.

3. Calculate $w_{max} = \left\lfloor \frac{|VN| - VN'}{DS - BS'} \right\rfloor$, where VN' is the number of vehicle nodes that becomes faulty and BS' is the number of base stations that becomes faulty.

4. Determine the new values for T1 and T2.

5. Network structure is reconstructed using new values of k1, k2, k3, k4 and k5 for $VN2VN$ and $VN2BS$ communication..

Fig. 7 Reconstructed network when base station becomes faulty **a** T = 1, **b** T = 2, **c** T = 3



In Fig. 8, a new network structure has been constructed using Algorithm 6. Here, α-rings and β-rings behave the same as they did in case of vehicle nodes are faulty, and base stations are faulty. The visual representation of the reconstructed network is shown in Fig. 9a–c. Table 3 shows the values of the parameters k1 and k2 for the network structures before and after the vehicle node and base station failure at different time-slots.

7 Performance analysis

In this section, we have analyzed the performance of data collection process in terms of time-delay. The minimization in time-delay is observed when compared with the existing schemes.

Theorem 2 *In the proposed network |N| with vehicle nodes VN and data streams DS, the total time required in collecting the data is less when compared with DADCNS* (*Cheng et al.* 2011).

Table 2 Change in the value of parameters when base station becomes faulty

Time-slot	Network before fault		Reconstructed Network		
	w_{max}=2 (α-ring) DS=3 VN=6		w_{max}=3 (β-ring) DS=2 VN=6		
	k1	k2	k3	k4	k5
T1	(1,3,5)	(2,4,6)	(1,4)	(2,5)	(3,6)
T2	(2,4,6)	(3,5,1)	(3,6)	(4,1)	(5,2)
T3	(3,5,1)	(4,6,6)	(ϕ)	(6,3)	(1,4)

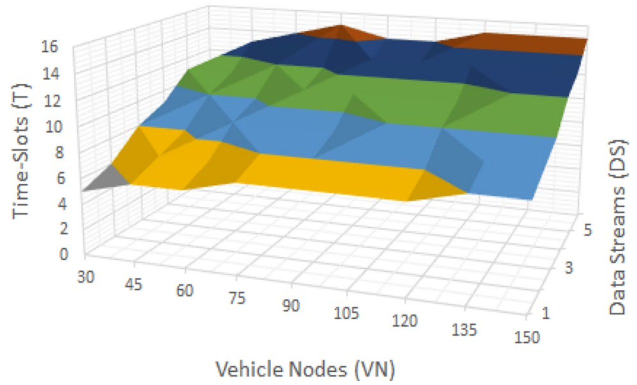


Fig. 8 Network structure with $VN = 200$ and $DS = 10$ where, 50 vehicle nodes and 4 base stations become faulty

Proof T_{PN} and T_{TN} are denoting total time required by proposed network and DADCNS respectively.

- **Case A** When $DS = 1$ and $|VN| = w_{max}$

$$\begin{aligned} T_{PN} &= \left\lfloor \frac{2|VN| - w_{max}}{w_{max}} + 1 \right\rfloor \\ &\quad + \left\lfloor log_2\left(|VN| - T1\left\lceil \frac{w_{max}}{2} \right\rceil\right) \right\rfloor + 1 \\ &= 1 + \left\lfloor log_2\left(|VN| - \left\lceil \frac{|VN|}{2} \right\rceil\right) \right\rfloor + 1 \\ &\le 1 + \left\lfloor log_2\left(|VN| - \frac{|VN|}{2}\right) \right\rfloor + 1 \\ &= \lfloor log_2(|VN|) \rfloor + 1 \\ &= T_{TN} \end{aligned}$$

- **Case B** When $DS \geq 2$ and w_{max} is *odd*

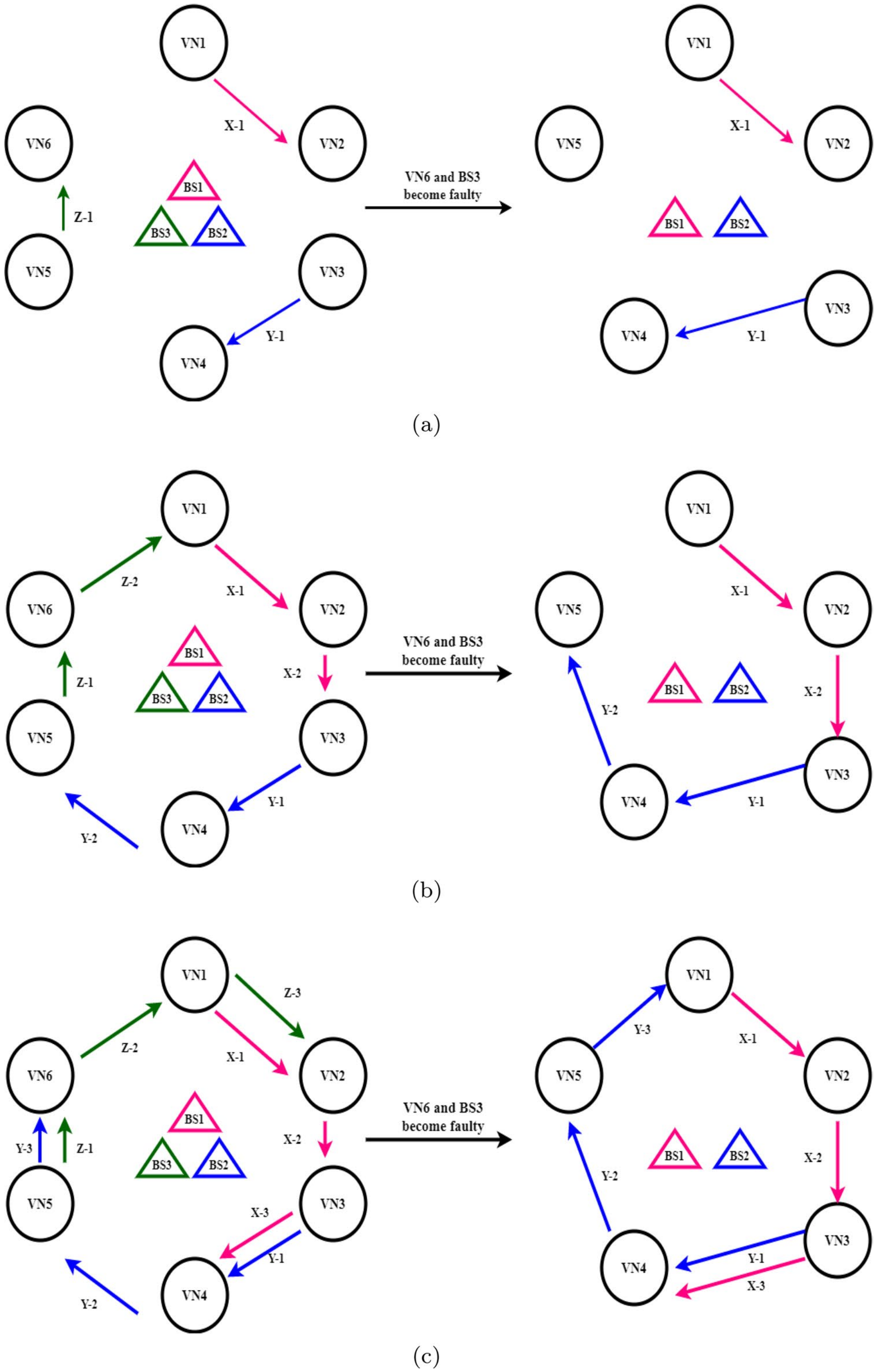
$$\begin{aligned} T_{PN} &= \left\lfloor \frac{2|VN| - w_{max}}{(w_{max} + 1)} + 1 \right\rfloor \\ &\quad + \left\lfloor log_2\left(|VN| - T1\left\lceil \frac{w_{max} + 1}{2} \right\rceil\right) \right\rfloor + 1 \\ &\le \left\lfloor \frac{2|VN| - w_{max}}{(w_{max} + 1)} + 1 \right\rfloor + \left\lfloor log_2\left(\frac{|VN|}{2}\right) \right\rfloor + 1 \\ &\le \left\lfloor \frac{2|VN| - w_{max}}{w_{max}} + 1 \right\rfloor + \left\lfloor log_2\left(\frac{|VN|}{2}\right) \right\rfloor + 1 \\ &= \left\lfloor \frac{2|VN|}{w_{max}} \right\rfloor + \left\lfloor log_2\left(\frac{|VN|}{2}\right) \right\rfloor \\ &\le 2\left\lfloor \frac{|VN|}{w_{max}} \right\rfloor + 1 + \left\lfloor log_2\left(\frac{|VN|}{2}\right) \right\rfloor \\ &= 2DS + \lfloor log_2(|VN|) \rfloor \\ &\le DS + DS\lfloor log_2(|VN|) \rfloor = T_{TN} \end{aligned}$$

- **Case C** When $DS \geq 2$ and w_{max} is *even*

$$\begin{aligned} T_{PN} &= \left\lfloor \frac{2|VN| - w_{max}}{w_{max}} + 1 \right\rfloor \\ &\quad + \left\lfloor log_2\left(|VN| - T1\frac{w_{max}}{2}\right) \right\rfloor + 1 \\ &\le \left\lfloor \frac{2|VN|}{w_{max}} \right\rfloor + \left\lfloor log_2\left(\frac{|VN|}{2}\right) \right\rfloor \\ &\le 2\left\lfloor \frac{|VN|}{w_{max}} \right\rfloor + 1 + \left\lfloor log_2\left(\frac{|VN|}{2}\right) \right\rfloor \\ &= 2DS + \lfloor log_2(|VN|) \rfloor \\ &\le DS + DS\lfloor log_2(|VN|) \rfloor = T_{TN} \end{aligned}$$

Here, from Cases A–C we can analyze that the the total time required in collection of data is less in comparison to DADCNS. Hence, we can say that *Theorem* 2 is proved.

Fig. 9 Reconstructed network when both vehicle node and base station become faulty at **a** T = 1, **b** T =2, **c** T = 3



(a)

(b)

(c)

8 Results

The performance of the proposed network structure is analysed by using various simulations for the various scenarios. Here, we have considered T as the total time required for the overall process of data gathering, DS as the data streams, BS as base stations and VN as the vehicle nodes. These vehicle nodes authenticate and transfer their data among themselves securely by using LIAU, LSMB protocol, and concurrent data collection trees. The proposed scheme is capable of handling integrity attacks: replay, man-in-the-middle, modification and impersonation attack. Also we have compared this scheme with the existing schemes on the basis of these attacks. In Table 4, Y represents successful handling of the attack and N represents failure to do so. To estimate the performance and effectiveness of the proposed network, we have considered the different number of vehicle nodes and data streams. Once the number of vehicle nodes that are participating in the communication are known, then the time required is reduced or minimized using α-rings and β-rings. This network structure is also compared with the existing delay-aware data collection network structure (DADCNS) (Cheng et al. 2011). This can be seen that the proposed network structure takes less time for data collection from the vehicle nodes and is also capable of handling faults of various vehicle nodes and base stations failure. These results are shown in subsequent figures. In Fig. 10a we have considered 200 vehicle nodes and 10 data streams. Using these values, we have calculated the total time required for collecting the data using proposed scheme. In Fig. 10b we have considered 200 vehicle nodes and 10 data streams. Using these values, we have calculated the total time required for collecting the data using DADCNS.

From Fig. 10a, b, it can be clearly seen that in DADCNS the time increases linearly with $|VN|$ and DS whereas in the proposed network, there is no monotonous increase in time with respect to $|VN|$ and DS. This is because in the proposed network the value of w_{max} varies when $|VN|$ or DS changes. This in turn varies the number of α-rings and β -rings. Numerically, it can be observed that the proposed network has a 37.72% reduction in time delay when compared with DADCNS.

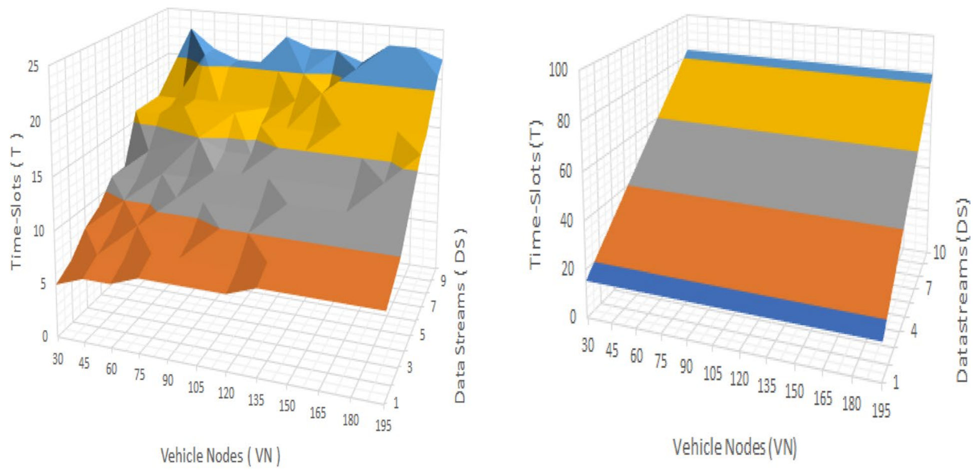
We have also considered other existing data acquisition networks namely extended content-centric network (ECCN) Niari et al. (2018) and vehicular named data networking (VNDN) Wang and Li (2019). We compared the schemes with the proposed network on the basis of time required for data collection considering similar parameters. After the comparison it was observed that there was a reduction of

Table 3 Change in the value of parameters when both vehicle node and base station become faulty

Time-slot	Network before fault		Reconstructed Network	
	w_{max}=2 (α-ring) DS=3 VN=6		w_{max}=2 (α-ring) DS=2 VN=5	
	k1	k2	k1	k2
T1	(1,3,5)	(2,4,6)	(7,1,3)	(8,2,8)
T2	(2,4,6)	(3,5,1)	(2,4)	(3,5)
T3	(3,5,1)	(4,6,2)	(3,5)	(4,1)

Table 4 Security attacks handled by different schemes

Schemes	Replay	Man-in-the-middle	Modification	Impersonation
Lim and Tuladhar (2019)	N	Y	N	N
Xu et al. (2019)	Y	N	Y	Y
Tan et al. (2018)	Y	N	N	Y
Vijayakumar et al. (2016)	N	N	Y	Y
Wang et al. (2016)	N	N	Y	N
Timpner et al. (2013)	Y	N	Y	N
Torrent-Moreno et al. (2009)	N	N	N	N
Proposed	Y	Y	Y	Y



(a)

(b)

Fig. 10 Comparative time duration analysis with $VN = 200$ and $DS = 10$ **a** proposed scheme and **b** DADCNS

time delay by 25.9% and 15% with respect to ECCN and VNDN respectively. Furthermore, neither of the data acquisition networks mentioned above are capable of handling faults. Additionally, the proposed network is capable of handling various integrity attacks which makes the communication secure. This gives the proposed network a great advantage over these data acquisition networks.

9 Conclusion

In vehicular network, the communication among vehicle nodes should be secure and fast when a large number of vehicles are involved in the network. Therefore, we have proposed a framework for secure vehicle-to-vehicle communication that implements the LIAU scheme and LSMB protocol along with concurrent data collection trees. Obtained results show that the proposed structure is capable of handling integrity attacks such as replay, man-in-the-middle, modification and impersonation attacks. Furthermore, the use of α-rings and β-rings using concurrent data collection trees have minimized the total time required for data collection by 37.72%, 25.9%, and 15% when compared with the scheme DADCNS, ECCN, and VNDN respectively. Moreover, the proposed network is fault tolerant as it can reconstruct the network in case of any vehicle node or base station failure.

Availability of data and material The data used to support the findings of this study are available from the corresponding author upon request.

Compliance with ethical standards

Conflicts of interest Authors have no Conflict of Interest.

Code Availability All the codes are written in original and available with authors.

References

Ahmad SA, Hajisami A, Krishnan H, Ahmed-Zaid F, Moradi-Pari E (2019) V2V system congestion control validation and performance. IEEE Trans Veh Technol. https://doi.org/10.1109/TVT.2019.2893042

Boban M, Barros J, Tonguz OK (2014) Geometry-based vehicle-to-vehicle channel modeling for large-scale simulation. IEEE Trans Veh Technol. https://doi.org/10.1109/TVT.2014.2317803. arxiv:1305.0124

Cheng CT, Tse CK, Lau FC (2011) A delay-aware data collection network structure for wireless sensor networks. IEEE Sens J. https://doi.org/10.1109/JSEN.2010.2063020

Cheng CT, Ganganath N, Fok KY (2017) Concurrent data collection trees for IoT applications. IEEE Trans Ind Inf. https://doi.org/10.1109/TII.2016.2610139

Chinnasamy A, Sivakumar B, Selvakumari P, Suresh A (2019) Minimum connected dominating set based RSU allocation for smartCloud vehicles in VANET. Cluster Comput. https://doi.org/10.1007/s10586-018-1760-8

Dey KC, Rayamajhi A, Chowdhury M, Bhavsar P, Martin J (2016) Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–performance evaluation. Transp Res Part C Emerg Technol. https://doi.org/10.1016/j.trc.2016.03.008

Dharminder D, Mishra D (2020) Lcppa: lattice-based conditional privacy preserving authentication in vehicular communication. Trans Emerg Telecommun Technol 31(2):e3810. https://doi.org/10.1002/ett.3810

Dharminder D, Rana S, Kundu N, Mishra D (2020) Construction of lightweight authentication scheme for network applicants using smart cards. Sādhanā 45(1):1–14. https://doi.org/10.1007/s12046-019-1254-2

He R, Molisch AF, Tufvesson F, Zhong Z, Ai B, Zhang T (2014) Vehicle-to-vehicle propagation models with large vehicle obstructions. IEEE Trans Intell Transp Syst. https://doi.org/10.1109/TITS.2014.2311514

Huang X, Xu C, Wang P, Liu H (2018) LNSC: a security model for electric vehicle and charging pile management based on blockchain ecosystem. IEEE Access. https://doi.org/10.1109/ACCESS.2018.2812176

Kuai M, Hong X, Yu Q (2019) Delay-tolerant forwarding strategy for named data networking in vehicular environment. Int J Ad Hoc Ubiquitous Comput 31(1):1–12. https://doi.org/10.1504/IJAHUC.2019.099634

Li J, Lu H, Guizani M (2015) ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Trans Parallel Distrib Syst. https://doi.org/10.1109/TPDS.2014.2308215

Lim K, Tuladhar KM (2019) LIDAR: Lidar information based dynamic V2V authentication for roadside infrastructure-less vehicular networks. In: 2019 16th IEEE annual consumer communications & networking conference (CCNC). IEEE, pp 1–6. https://doi.org/10.1109/CCNC.2019.8651684

Limbasiya T, Das D (2020) Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication. IEEE Syst J. https://doi.org/10.1109/JSYST.2019.2932807

Mishra D, Kumar V, Dharminder D, Rana S (2020) Sfvcc: Chaotic map-based security framework for vehicular cloud computing. IET Intell Transp Syst 14(4):241–249. https://doi.org/10.1049/iet-its.2019.0250

Mohanakrishnan U, Ramakrishnan B (2020) MCTRP: an energy efficient tree routing protocol for vehicular ad hoc network using genetic whale optimization algorithm. Wirel Pers Commun. https://doi.org/10.1007/s11277-019-06720-4

Niari AK, Berangi R, Fathy M (2018) Eccn: an extended ccn architecture to improve data access in vehicular content-centric network. J Supercomput 74(1):205–221. https://doi.org/10.1007/s11227-017-2126-3

Omar HA, Zhuang W, Li L (2013) VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs. IEEE Trans Mobile Comput. https://doi.org/10.1109/TMC.2012.142

Tan H, Gui Z, Chung I (2018) A secure and efficient certificateless authentication scheme with unsupervised anomaly detection in VANETs. IEEE Access. https://doi.org/10.1109/ACCESS.2018.2883426

Timpner J, Schürmann D, Wolf L (2013) Secure smartphone-based registration and key deployment for vehicle-to-cloud communications. Proc ACM Conf Comput Commun Secur. https://doi.org/10.1145/2517968.2517970

Torrent-Moreno M, Mittag J, Santi P, Hartenstein H (2009) Vehicle-to-vehicle communication: fair transmit power control for safety-critical information. IEEE Trans Veh Technol. https://doi.org/10.1109/TVT.2009.2017545

Vijayakumar P, Azees M, Kannan A, Deborah LJ (2016) Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Trans Intell Transp Syst. https://doi.org/10.1109/TITS.2015.2492981

Wang F, Xu Y, Zhang H, Zhang Y, Zhu L (2016) 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. IEEE Trans Veh Technol. https://doi.org/10.1109/TVT.2015.2402166

Wang X, Li Y (2019) Vehicular named data networking framework. IEEE Trans Intell Transp Syst. https://doi.org/10.1109/TITS.2019.2945784

Xu H, Zeng M, Hu W, Wang J (2019) Authentication-based vehicle-to-vehicle secure communication for VANETs. Mobile Inf Syst 2019:9. https://doi.org/10.1155/2019/7016460

Yasser A, Zorkany M, Abdel Kader N (2017) VANET routing protocol for V2V implementation: A suitable solution for developing countries. Cogent Eng. https://doi.org/10.1080/23311916.2017.1362802

Zhang R, Cheng X, Yang L, Shen X, Jiao B (2015) A novel centralized TDMA-based scheduling protocol for vehicular networks. IEEE Trans Intell Transp Syst. https://doi.org/10.1109/TITS.2014.2335746