Journal of Computers Vol. 28, No. 3, 2017, pp. 108-119
doi:10.3966/199115592017062803009

New Anatomy of Reliable Communication in a Vehicular Ad Hoc Network

Shu-Ching Wang[1], Shun-Sheng Wang[2,*], and Kuo-Qin Yan[3,*]

[1] Department of Information Management, Chaoyang University of Technology
Taichung 409, Taiwan, ROC
scwang@cyut.edu.tw

[2] Department of Industrial Engineering and Management, Chaoyang University of Technology
Taichung 409, Taiwan, ROC
sswang@cyut.edu.tw

[3] Department of Business Administration, Chaoyang University of Technology
Taichung 409, Taiwan, ROC
kqyan@cyut.edu.tw

Received 30 April 2016; Revised 24 May 2016; Accepted 06 December 2016

Abstract. Recent advances in hardware, software and communication technologies are enabling the design and implementation of a wide range of different types of networks that are being deployed in various environments. One such network that has been widely employed in automobile technology, allowing vehicles within this network to communicate effectively with each another, is the Vehicular Ad-Hoc Network (VANET). VANETs are classified as a mobile ad hoc network, with the potential for improving road safety and providing travelers with better service. Therefore, it is important that VANETs are applied with reliable communication. However, the problem of reaching consensus in the distributed system is one of the most important issues in designing a reliable communication network. Reaching consensus on a same value in a distributed system is required; even if certain components in the distributed system fail, the protocol is necessary so that system can still operate correctly. In this study, the identity-based cryptosystem (IDCrypto) is used to satisfy such reliability-related objectives when a message is transmitted. The consensus problem is revisited with the assumption of transmission medium failure via malicious faults in the VANET. The proposed protocol, Reliable Communication Protocol (RCP) of VANET, allows all fault-free nodes to reach reliable consensus with minimal rounds of message exchanges, and tolerates the maximal number of allowable components in the VANET.

Keywords: distributed consensus problem, fault tolerant, identity-based cryptosystem, vehicular ad-hoc network

1 Introduction

Vehicular ad hoc networks (VANETs) have been widely employed in automobile technology, allowing vehicles within these networks to communicate effectively with each another [16]. VANETs are an emerging type of network which facilitates communication between vehicles on the road, improving driving safety. The basic idea is to allow arbitrary vehicles to broadcast ad hoc messages (e.g. regarding traffic accidents) to other vehicles; however, this raises security and privacy concerns [20]. Messages should first be verified as reliable and the real identity of vehicles should not be revealed, yet remain traceable by an authorized party.

[*] Corresponding Author

VANETs are also known as vehicular sensor networks by which driving safety is enhanced through inter-vehicle communications or communications with roadside infrastructure [8]. They are therefore an important element of Intelligent Transportation Systems (ITSs). In a typical VANET, each vehicle is assumed to have an on-board unit (OBU), while stationary roadside units (RSUs) are installed along the roads. A trusted authority (TA), and perhaps some other application servers, are also installed in the backend. The OBUs and RSUs communicate using the Dedicated Short Range Communications (DSRC) protocol over a wireless channel [8]. The basic application of a VANET is to allow arbitrary vehicles to broadcast safety messages to other vehicles and nearby RSUs. Other vehicles may adjust their travel routes based on information received, and RSUs may instruct a traffic control center to adjust traffic lights in order to avoid possible traffic congestion.

VANETs consist of vehicles and roadside equipment that are able to communicate with each other by wireless and multi-hop communication [13]. VANETs are prone to interference and propagation issues, as well as different types of attacks and intrusions that can harm ITS services [11]. These networks characteristically have highly mobile nodes, rapid and significant network topology changes, as well as wireless links subject to interference and fading due to multipath propagation [3]. The absence of central entities increases the complexity of security management operations, in particular access control, node authentication and cryptographic key distribution, resulting in vulnerability to misbehaving (malicious or selfish) nodes in the network, posing nontrivial challenges to security design. In a VANET, the network is assumed to be reliable and synchronous [4]. Reaching consensus on a same value in a VANET is imperative; even if certain components in the distributed system failed (inner damage or outer intruder); the protocols are required so that the system can still be executed correctly. Therefore, the identity-based cryptosystem (IDCrypto) is used to satisfy such reliability-related objectives when a message is transmitted [20].

To achieve high reliability in a VANET, a mechanism that allows a set of nodes to reach a common safety agreement, even in the presence of faulty nodes, is needed. Such an agreement problem was first introduced by Pease *et al.* in 1980 [14], and the problem has since been called the Byzantine Agreement (BA) problem [10]. The BA problem is one of the most fundamental problems in seeking to reach an agreement value in a distributed system [10]. In the classical BA problem, several troops from the same military force are surrounding an enemy city, where each general leads his own troops. The generals can only communicate with each other through messengers. To conquer the enemy city, the generals must reach a common agreement on whether or not to launch a united attack at dawn. It is very important that all the loyal generals should decide on the same agreement, since an attack called by only a small number of the generals would result in a failed assault. The original BA problem is assumed as follows [10]:

(1) There are n nodes in a synchronous distributed system, where n is a constant and $n \geq 4$.

(2) Each node can communicate with all other nodes through a reliable fully connected network.

(3) One or more of the nodes might fail, so a faulty node may transmit incorrect message(s) to other nodes.

(4) After message exchanges, all healthy nodes should reach a common agreement, if and only if the number of faulty nodes t is less than one-third of the total number of nodes in the network, or $t \leq (n\text{-}1)/3$.

The solutions define a protocol for BA, which can reach agreement by using the minimal number of rounds for message exchanges to obtain the maximum number of components with allowable faulty capability. The problem of BA is to enable all fault-free nodes to reach agreement underlying an n-nodes distributed system. The ***source node*** chooses an initial value to start with, and communicates to all other nodes by exchanging messages. The nodes can reach an agreement if following conditions are satisfied [10]:

(Agreement): All fault-free nodes agree on a common value.

(Validity): If the ***source node*** is fault-free, then all fault-free nodes shall agree on the initial value the source node sent.

A closely related sub-problem of BA, the consensus problem, has been extensively studied [5] as well. The solutions of consensus problem are defined as protocols, which achieve a consensus and aim to use the minimum number of rounds of message exchanges to achieve the maximum amount of allowable faulty capability. In this study, our concern is achieving a solution to the consensus problem, i.e. making fault-free nodes in an n-node cluster-based VANET to reach consensus. ***Every node*** chooses an initial value to start with, and communicates with the others by exchanging messages. A group of nodes achieves a consensus if it satisfies the following conditions [10]:

(Agreement): All fault-free nodes agree on a common value.
(Validity): If the initial value of ***each*** fault-free node n_i is v_i then all of the fault-free nodes shall agree on the value v_i.

In a consensus problem, many cases are based on the assumption of node failure in a fail-safe network [5]. Based on this assumption, a transmission medium fault is treated as a node fault, whatever the correctness of an innocent node, so an innocent node does not involve consensus. However, the definition of a consensus problem requires all fault-free nodes to reach a consensus.

In the cluster-based VANET, numerous nodes are interconnected. Achieving consensus on a same value in a distributed system; even if certain components in distributed system fail, the protocols are required so that systems can still operate correctly. However, in this study, the consensus problem is revisited with the assumption of transmission medium failure due to malicious faults in the VANET. The proposed protocol, *Reliable Communication Protocol* (RCP) of VANET, can make all fault-free nodes reach consensus with minimal rounds of message exchanges, and tolerate the maximal number of allowable faulty components

The remainder of this paper is arranged as follows: Section 2 illustrates the topology of VANET, the failure types and the security technology. Section 3 illustrates the concept of the *Reliable Communication Protocol* (RCP) of VANET. An example of RCP executed is given in Section 4. The correctness and complexity of the proposed protocol is explained in Section 5. Finally, conclusions are presented in Section 6.

2 Literature Review

The design and development of the trustworthy consensus protocol has several requirements that must be considered. Therefore, the topology of VANET, the failure types and the security technology will be discussed in this section.

2.1 The Topology of VANET

VANET architecture spans various hardware and software components. Two primary types of devices used in VANETs are On Board Units (OBUs) and Road Side Units (RSUs). OBUs are mounted on vehicles, and RSUs are deployed along roadsides as infrastructure. Accordingly, the two major types of communication in VANETs are Vehicle to Vehicle (V2V), where vehicles communicate directly with each other, and Vehicle to Infrastructure (V2I), where vehicles communicate with nearby infrastructure [12].

In a VANET, a node can be a vehicle with a radio system operating in the DSRC channels, or a node can be a unit of roadside equipment that communicates with mobile ad hoc vehicular nodes. Such roadside units serve as gateways, providing access to infrastructure for mobile nodes. This paper refers to the radio system on vehicular nodes as OBUs, and to fixed roadside units as RSUs. An example of a four-node VANET is shown in Fig. 1.

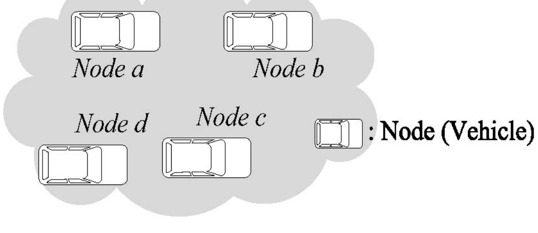


Fig. 1. An example of VANET

The main components of the ad hoc part of a VANET are vehicles equipped with sensors: the OBU and the Trusted Platform Module (TPM). On the other hand, the infrastructure component consists of the manufacturers, Trusted Third Party (TTP), legal authorities and service providers. In the infrastructure component, the RSU serves as a bridge between the infrastructure environment and the MANET environment. The components and communication mode of a VANET are shown in Fig. 2 [12].

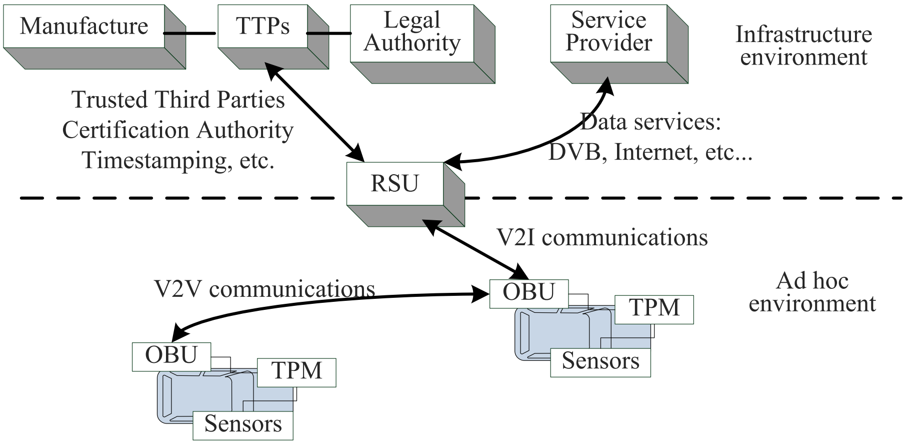


Fig. 2. The components and communication model of VANET [12]

A mobile VANET differs from a fully connected network or broadcast network in that the nodes in a mobile environment have high mobility. These nodes may enter or leave the network at any time. How nodes reach agreement in the VANET is critical to network reliability. However, network technology continues to grow very rapidly, and applications in mobile VANETs have reached astonishing achievements in the last year. It is thus very important to solve the BA problem in mobile VANETs. Thus, this research will focus on the VANET, and propose a protocol that will allow all the network's fault-free nodes to reach agreement. The definitions and assumptions used in mobile VANETs are listed as follows:

1. Nodes have mobility in a VANET. Thus, each node can enter the network or leave the network at any time.
2. If a node moves away from the network or enters the same network later, the protocol will treat this node as a new participator.
3. Each node is cognizant of the total number of nodes in the VANET at any time.

The VANET environment contains numerous challenges for communication, many of which can be addressed by a clustered network [7]. As highlighted in [21], VANETs suffer from high mobility and high node-density, which lead to channel congestion and the hidden terminal problem. VANETs have a highly-mobile environment with a rapidly changing network topology. Clustering the vehicles into groups of similar mobility will reduce the relative mobility between communicating neighbor nodes, and simplify routing. VANETs demand a high frequency of broadcast messages to keep the surrounding vehicles updated on position and safety information. These broadcasts lead to the "broadcast storm problem" [17], which describes the resulting congestion in the network. Both [1, 17] recommend a clustered topology to effectively alleviate this congestion. In addition, both delay-sensitive (e.g. safety messages) and delay-tolerant (e.g. road/weather information) data will need to be transmitted, necessitating Quality-of-Service (QoS) requirements. Clustering the network will aid in supporting these QoS requirements, as shown in [9].

Currently, the cluster VANET is a more practical kind of VANET. Multiple nodes in a cluster of the VANET cooperate to achieve some objectives [15]. A cluster-based VANET consists of a set of loosely or tightly connected nodes that work together so that, in many respects, they can be viewed as a single system. The cluster-based VANET is shown in Fig. 3.

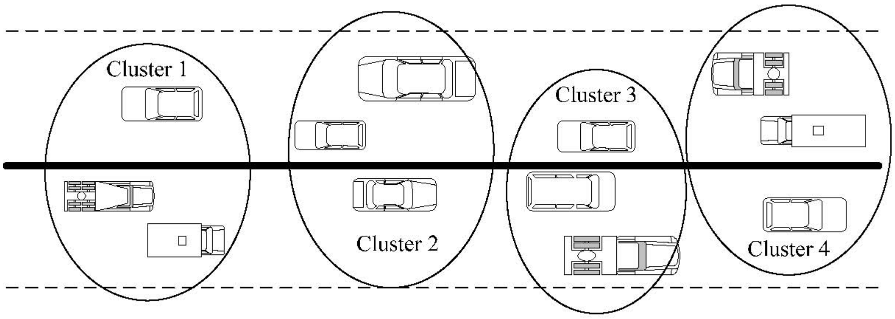


Fig. 3. Cluster-based VANET [15]

2.2 Failure types

The symptoms of a faulty component can be classified into two categories. They can be either dormant faults (include crashes and omissions) or malicious faults [2].

Dormant faults include both crashes and omissions. A crash fault happens when a component is broken, while an omission fault takes place when a component fails to transmit or receive a message on time or at all. In the synchronous system, each fault-free processor can detect the components with dormant faults if the protocol appropriately encodes a message before transmission by using the Manchester code [2].

In case of a malicious fault (also called a Byzantine fault or an arbitrary fault), the behavior of the faulty component is unpredictable and arbitrary. For example, the behavior of a faulty component with the malicious, may lie, lose, or mangle messages. Therefore, this is the most damaging failure type and causes the worst problem. Therefore, a malicious fault is the most damaging failure type, and causes the most serious problems. However, if malicious faults can be addressed, then the other fault types can surely be solved [6]. In this study, malicious faults are investigated, and the means by which fault-free nodes may reach consensus in the VANET are explored.

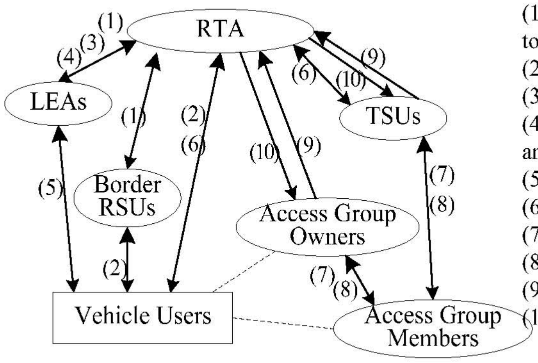
2.3 Safety technology

Safety in VANETs is of special concern because human lives are constantly at stake, whereas in traditional networks the major security concerns include confidentiality, integrity and availability, none of which are primarily involved in protecting lives. It is therefore crucial that, in a VANET, it is impossible for an attacker to modify or delete vital information [19]. VANET security also includes the ability to determine driver responsibility, while maintaining driver privacy. Information about vehicles and their drivers must be exchanged securely and, more importantly, rapidly, since message delays may result in catastrophic consequences, such as vehicle collisions.

The deployment of a comprehensive security system for VANETs is very challenging in practice. A safety breach of a VANET is often critical and hazardous. Moreover, vehicular networks are highly dynamic, with frequent and instantaneous arrivals and departures of vehicles, as well as short connection durations. In addition to its dynamic nature and high mobility, the use of wireless media also makes VANETs vulnerable to attacks that exploit the open and broadcast nature of wireless communication. VANETs are exposed to various threats and attacks [19]. Since the vehicle itself is a sufficient source of electricity, OBUs are not subject to the bottleneck of limited battery life faced by other mobile devices, such as smart phones and wearable devices.

An identity-based security system for VANETs, proposed by Sun et al., can effectively solve the conflict between privacy and traceability [20]. The system uses a pseudonym-based scheme to preserve user privacy. It employs a threshold signature-based scheme to enable traceability for law enforcement. The integral part of the system is the privacy-preserving defense scheme that leverages the authentication threshold. Any extra authentication beyond the threshold will indicate misbehavior, and result in revocation of the user's credentials. In addition, the scheme employs a dynamic accumulator for the authentication threshold, which places further restrictions beyond the threshold on other communicating users. This is particularly attractive to service providers since they can achieve more efficient services.

Fig. 4 depicts the entities and their interactions in the identity-based cryptosystem [20]. The arrows indicate the direction of packet flow or physical communications. The details of the message exchanges of each arrow are numbered and explained on the right-hand side. It is worth noting that vehicle users are further divided into members and access group owners, because only group owners can access the RSUs. The identity-based cryptosystem facilitates efficient communication and storage schemes. Through security and efficiency analysis, the system is shown to satisfy the security objectives, including preserving user privacy, enabling traceability and nonframeability, with desirable efficiencies.



(1) Pre-established trust relationship (RTA assigns key pairs to border RSUs and LEAs)
(2) Pseudonym generation and authentication
(3) Threshold signature
(4) Tracing law violators (LEAs request RTA to lookup PLT and return the results
(5) Legal actions
(6) Membership registration
(7) Access group setup and revoking
(8) Threshold authentication
(9) Tracing misbehaving vehicle users
(10) Revocation/recovery

Fig. 4. Interactions of the identity-based cryptosystem [20]

Since the proposed identity-based cryptosystem proposed by Sun et al. does not require certificates for authentication [20], it is used in this study when a message is transmitted. In this study, a VANET whose nodes are fallible during the BA execution is considered. In this scenario, nodes may be considered faulty due to interference from some noise or a hijacker, and result in exchanged messages that can exhibit arbitrary behavior. However, the proposed RCP is used to address the consensus problem with malicious faulty transmission media in a VANET. When all nodes reach consensus, the fault-tolerance capacity is enhanced, even if there are faults between the nodes.

In this study, we consider a distributed system whose nodes are reliable during the consensus execution in a cluster-based VANET; the transmission media may be faulty due to interference from some noise or a hijacker and result in the exchanged message exhibiting arbitrary behavior. A protocol to achieve consensus in an unreliable communication environment has been proposed before. The proposed protocol can tolerate $\lceil c/2 \rceil$-1 faulty transmission media where c is the connectivity of the network [20]. When all nodes reach consensus in a cluster-based VANET, the fault-tolerance capacity is enhanced due to each node being able to transmit its messages directly, even with a transmission medium fault.

3 The Proposed Protocol

This study proposes a new protocol, called *Reliable Communication Protocol* (RCP), to solve the consensus problem due to faulty transmission media which may send wrong messages, in order to influence the system to achieve consensus in a cluster-based VANET. The assumptions and parameters of this network topology are shown below.

- Each node in the network can be identified uniquely.
- All messages are signed by IDCrypto; nodes cannot falsely a message signed by other nodes.
- Let n_i be a node, n is the total number of nodes and N being the set of all nodes in the cluster-based VANET.
- Let C_j be a cluster and C be the total number of clusters in the cluster-based VANET, where $1 \leq j \leq C$ and $C \geq 4$.
- TM$_{ij}$ is the transmission medium between cluster C_i and C_j.

- IT$_{ij}$ is the set of transmission media between cluster C_i and C_j. If the number of faulty transmission media in IT$_{ij}$ is greater or equal to half of the set, then the IT$_{ij}$ is a faulty IT; otherwise, it is a fault-free IT.
- Let f_{IT} be the number of faulty ITs in all clusters.
- Let c be the connectivity of a cluster-based VANET, and $c \geq 2f_{IT}+1$.
- Let v_{ki} denoted as the value stored in the k-th row and i-th column of a matrix.

The proposed protocol RCP consists of two phases: the message exchange phase and decision-making phase. Moreover, RCP only needs two rounds of message exchange to solve the consensus problem. In the message exchange phase, each fault-free node communicates with other nodes and itself via radio waves via an identity-based cryptosystem (IDCrypto). Finally, the decision-making phase will reach consensus among the nodes. The progression steps of node n_i executed RCP are shown in Fig. 5.

In the first round of the message exchange phase, each node n_i multicasts its initial value v_i through transmission media by IDCrypto, and then receives the initial value of other nodes by IDCrypto as well. In the second round, each node n_i acts as the sender, sending the vector received in the first round by IDCrypto, and constructs a matrix, called the MAT_i, $1 \leq i \leq n$. The concept of the constructed MAT is shown in Fig. 5. Fig. 5(a) is an example of a 4-cluster VANET. Figs. 5(b) and 5(c) are examples of MAT constructed by RCP.

Finally, the decision-making phase will reach consensus among the nodes. The pseudo-code of the RCP is shown in Fig. 6. In the RCP protocol, MAT_i is the matrix set up at node n_i for i = 1 to$n$. However, the RCP protocol can be presented with the following primitives:

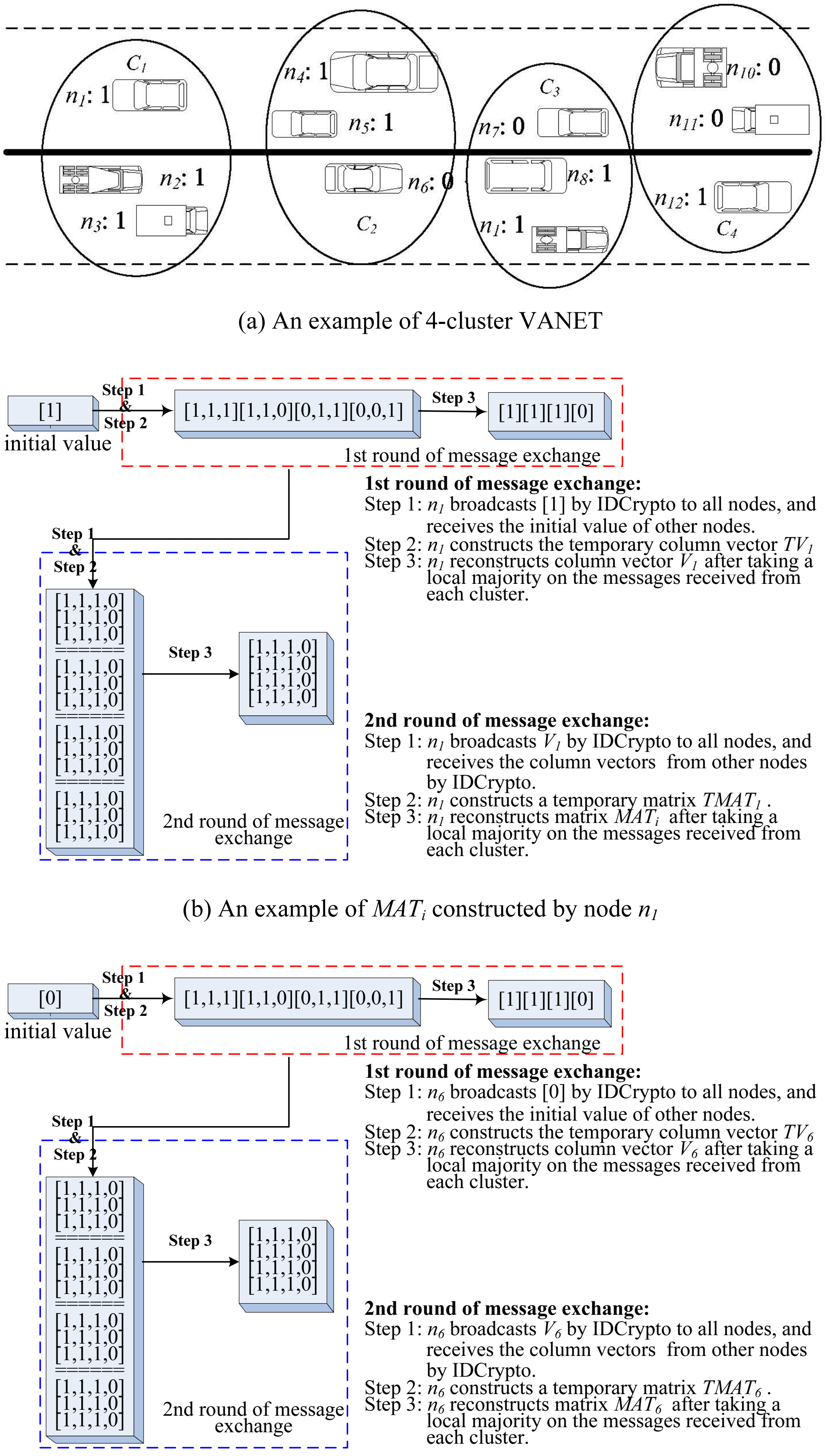
- CrtV(n_i, v_i): creates the initial vector of node n_i, and sets the initial value of vector = [v_i].
- CrySend(m_i, n_j): sends the message m_i to node n_j by IDCrypto.
- CryRcv(m_j, n_j): receives the message m_j from node n_j by IDCrypto.
- ConTS(n_i, TS_i): according to the structure of the received messages, it constructs a temporary message structure TS_i.
- RConS(n_i, S_i): reconstructs a message structure S_i after taking a local majority on the messages received from each cluster.
- MAJ(n_i, k):takes the majority value (Maj_k) of the k-th row of MAT_i for $1 \leq k \leq n$.
- DEC(n_i): takes the decision value.

4 Example of RCP Executed

Subsequently, a detailed example of executing the RCP protocol is based on the cluster-based VANET. However, Fig. 5(a) is a 4-cluster VANET in which IT$_{1,10}$, IT$_{2,11}$, IT$_{3,6}$, IT$_{3,12}$, IT$_{4,8}$ and IT$_{9,12}$ fail.

In the first round of message exchange, each node n_i multicasts its initial value v_i through transmission media by IDCrypto to all other nodes, where $1 \leq i \leq n$, and receives the initial value of other nodes by IDCrypto. Each node uses the received message to construct vector TV_i, as shown in Fig. 7(a). Then, each node reconstructs column vector V_i after taking a local majority on the messages received from each cluster, as shown in Fig. 7(b).

In the second round of message exchange, each node multicasts its vector V_i and receives the column vectors from other nodes by IDCrypto. Each node constructs MAT_i after taking a local majority on the messages received from each cluster, as shown in Fig. 7(c). Finally, the decision-making phase takes the majority value of MAT_i to construct the matrix MAJ_i, as shown in Fig. 7(d), and achieves the common value by DEC_i.



(a) An example of 4-cluster VANET

1st round of message exchange:

Step 1: n_1 broadcasts [1] by IDCrypto to all nodes, and receives the initial value of other nodes.

Step 2: n_1 constructs the temporary column vector TV_1

Step 3: n_1 reconstructs column vector V_1 after taking a local majority on the messages received from each cluster.

2nd round of message exchange:

Step 1: n_1 broadcasts V_1 by IDCrypto to all nodes, and receives the column vectors from other nodes by IDCrypto.

Step 2: n_1 constructs a temporary matrix $TMAT_1$.

Step 3: n_1 reconstructs matrix MAT_i after taking a local majority on the messages received from each cluster.

(b) An example of MAT_i constructed by node n_1

1st round of message exchange:

Step 1: n_6 broadcasts [0] by IDCrypto to all nodes, and receives the initial value of other nodes.

Step 2: n_6 constructs the temporary column vector TV_6

Step 3: n_6 reconstructs column vector V_6 after taking a local majority on the messages received from each cluster.

2nd round of message exchange:

Step 1: n_6 broadcasts V_6 by IDCrypto to all nodes, and receives the column vectors from other nodes by IDCrypto.

Step 2: n_6 constructs a temporary matrix $TMAT_6$.

Step 3: n_6 reconstructs matrix MAT_6 after taking a local majority on the messages received from each cluster.

(c) An example of MAT_i constructed by node n_6

Fig. 5. The progression steps of executed RCP

```
Protocol: Reliable Communication Protocol (RCP) /* for each node $n_i$, where $v_i$ is the initial value of $n_i$ */
/* Initialization */
CrtV($n_i$, $v_i$);                 /* create the initial vector of node $n_i$ */
/* Message Exchange Phase */
for $n_i, n_j \in N$ do
  for $x$=1 to 2 do                 /* round 1 and 2 */
    CrySend($m_i$, $n_j$);          /* $n_i$ sends the message of $n_i$ to $n_j$ by IDCrypto */
    CryRcv($m_j$, $n_j$);           /* $n_i$ receives the message of $n_j$ by IDCrypto */
    ConTS($n_i$, $TS_i$);           /* construct the temporary message structure $TV_i$ or $TMAT_i$ */
    RConS($n_i$, $S_i$);            /* reconstruct the message structure $V_i$ or $MAT_i$ after taking
                                       a local majority on the messages received from each cluster */
  end
/* Decision Making Phase */
  MAJ($n_i$, $k$);                  /* $k$ is the row of $MAT_i$ for $1 \le k \le n$ */
  for $k$=1 to $n$ do
    if ($\exists Maj_k = \neg v_i$) then
      DEC($n_i$)=$\phi$;
    if ($\exists Maj_k$ =?) and ($v_{ki}=v_i$) then   /* $v_{ki}$ is the value stored in the $k$-th row and $i$-th column of a matrix */
      DEC($n_i$)=$\phi$;            /* $\phi$ is a default value */
    else
      DEC($n_i$)= $v_i$;
  end
end
```

Fig. 6. The RCP protocol

5 The Correctness and Complexity of the RCP Protocol

In this section, the correctness and complexity will be proven. The first subsection will prove the correctness of the RCP, and the complexity will be proven in the next subsection. The following lemmas and theorems are used to prove the correctness and complexity of the RCP. It can tolerate $\lceil c/2 \rceil$-1 faulty transmission media where c is the connectivity of VANET. Furthermore, it only requires 2 rounds of message exchanges to enable all fault-free nodes to reach consensus.

5.1 The Correctness of the RCP Protocol

The lemmas and theorems are used to prove the correctness of the RCP.

Lemma 1. Let the initial value of sender node n_i be v_i. By using IDCrypto, the destination cluster's nodes can receive the value v_i from the sender node n_i if $f_{IT} <= \lceil c/2 \rceil$ -1, where f_{IT} is the number of faulty ITs in all clusters and c is the connectivity of a cluster-based VANET.

Proof. By using IDCrypto, the sender node can transmit its value to the destination cluster's nodes through TM_{xy} cluster-disjoint paths. According to the assumption of $f_{IT} <= \lceil c/2 \rceil$ -1, the nodes in the destination cluster, in the worst case, can get the TM_{xy} values from the sender node. We can take the local majority and normal majority on these TM_{xy} values and let each of the nodes in the destination cluster get the value v_s.

Lemma 2. The decision value DEC(n_i) = majority value.

Proof. Lemma 2 is proven by the definition of the consensus problem.

Theorem 1. Protocol RCP is valid.

Proof. According to Lemmas 1 and 2, the validity of RCP is confirmed.

Theorem 2. Protocol RCP can make each fault-free node agrees on a common consensus.

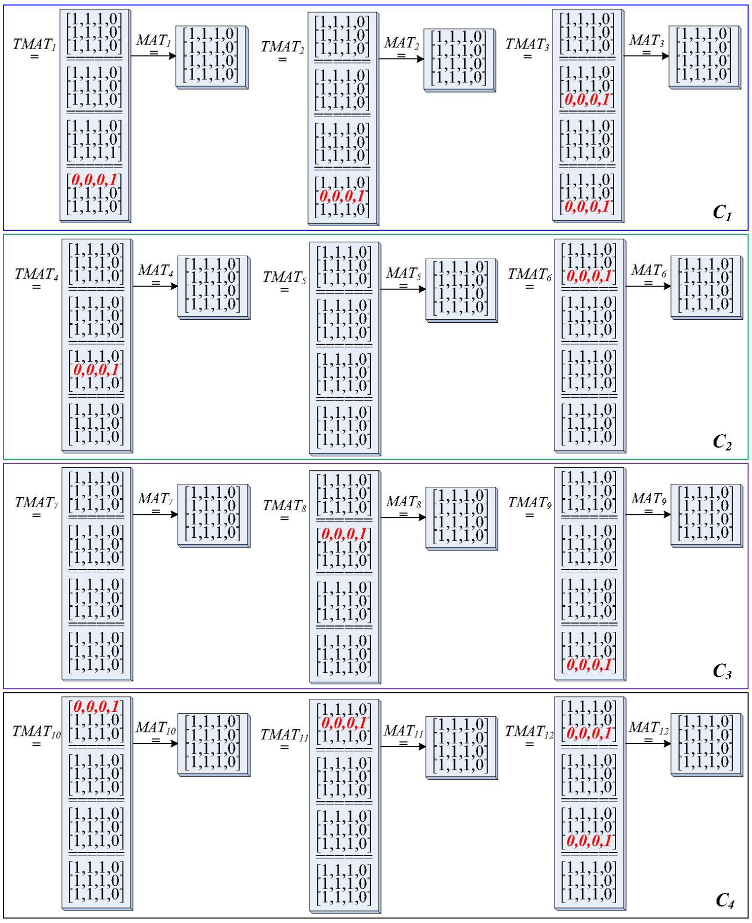
Proof. If a node agrees on value Z (where Z = v_i= v_s, and $1 \le i \le n$ by Lemma 2), all nodes should agree on value Z.

	C_1			C_2			C_3			C_4		
	n_1	n_2	n_3	n_4	n_5	n_6	n_7	n_8	n_9	n_{10}	n_{11}	n_{12}
TV_1	1	1	1	1	1	0	0	1	1	***1***	0	1
TV_2	1	1	1	1	1	0	0	1	1	0	***1***	1
TV_3	1	1	1	1	1	***1***	0	1	1	0	0	***0***
TV_4	1	1	1	1	1	0	0	***0***	1	0	0	1
TV_5	1	1	1	1	1	0	0	1	1	0	0	1
TV_6	1	1	***0***	1	1	0	0	1	1	0	0	1
TV_7	1	1	1	1	1	0	0	1	1	0	0	1
TV_8	1	1	1	***0***	1	0	0	1	1	0	0	1
TV_9	1	1	1	1	1	0	0	1	1	0	0	***0***
TV_{10}	***0***	1	1	1	1	0	0	1	1	0	0	1
TV_{11}	1	***0***	1	1	1	0	0	1	1	0	0	1
TV_{12}	1	1	***0***	1	1	0	0	1	***0***	0	0	1

(a) The temporary column vector TV_i of each node n_i

	C_1	C_2	C_3	C_4
V_1	1	1	1	1
V_2	1	1	1	1
V_3	1	1	1	0
V_4	1	1	0	0
V_5	1	1	1	0
V_6	1	1	1	0
V_7	1	1	1	0
V_8	1	1	1	0
V_9	1	1	1	0
V_{10}	1	1	1	0
V_{11}	1	1	1	0
V_{12}	1	1	0	0

(b) The column vector V_i of each node n_i



(c) The MAT_i after the 2nd round message exchange

MAJ of MAT_i = for i = 1 to 12 $\begin{array}{|c|}\hline 1\\\hline 1\\\hline 1\\\hline 1\\\hline\end{array}$ DEC(n_i)=1

(d) The common value DEC of node n_i

Fig. 7. An example of RCP executed

5.2 The Complexity of the RCP protocol

The complexity of the RCP is evaluated in terms of 1) the number of rounds of message exchanges, and 2) the number of allowable faulty components. Theorems 3 and 4 below will show that the optimal solution is reached.

Theorem 3: One round of message exchange cannot solve the consensus problem.

Proof: Message exchange is necessary. A node cannot derive whether or not a disagreeable value exists in other nodes without message exchanging. Therefore, the consensus problem cannot be implemented. In addition, one round of message exchange is not enough to solve the consensus problem. If node n_i of C_x is connected with node n_m of C_y by faulty transmission medium, node n_i may not know the initial value in node n_m by using only one round of message exchanges. Hence, it is possible to reach a consensus by using one round of message exchanges.

Theorem 4: The total number of allowable faulty transmission media by RCP is optimal.

Proof. According to relevant studies, we may obtain a protocol which can tolerate the transmission media faults in a system provided that $\lceil c/2 \rceil$-1 faulty transmission media, where c is the network connectivity. However, the results are not appropriate for the cluster-based VANET.To cope with cluster-based VANET, the total number of faulty ITs in whole network is $f_{IT}=\lceil c/2 \rceil-1$.

6 Conclusions

VANETs are classified as an application of MANET with the potential for improving road safety and providing service to travelers [18]. Recently VANETs have emerged to turn the attention of researchers in the field of wireless and mobile communications; they differ from MANET by their architecture, challenges, characteristics and applications.

The consensus problem is a fundamental problem in the distributed environment [6]. The problem has been studied by various kinds of network models in the past [11]. According to previous studies, the network topology plays an important role in this problem [11]. Traditionally, complex networks have been studied in a branch of mathematics known as graph theory. However, the network topology developed in recent years shows a mobile feature such that the previous protocols cannot adapt to it.

Therefore, in this study, the consensus problem in cluster-based VANETwas revisited. The reliable consensus problem was redefined by the RCP protocol within the IDCrypto in a cluster-based VANET. The proposed protocol ensures that all nodes in the network can reach a common value to cope with the influences of the faulty transmission media by using the minimum number of message exchanges, while tolerating the maximum number of faulty components at any time.

That is, the RCP has the following features:

- The RCP can solve the consensus problem in a cluster-based VANET.
- The RCP allows the design of reliable communication using the identity-based cryptosystem (IDCrypto).
- The RCP can solve the consensus problem by the minimum number of rounds of message exchanges (*2* rounds of message exchanges).
- The RCP increases the fault tolerance capability by allowing for malicious faulty transmission media.

References

[1] K.H. Chang, Wireless communications for vehicular safety, IEEE Wireless Communications 22(1)(2015) 6-7.

[2] W. Chen, Computer Networks: Principles, Technologies and Protocols for Network Design, Elsevier, Brazil, 2015.

[3] A. Dixit, S. Singh, K. Gupta, Comparative study of P-AODV and improved AODV in VANET, International Journal of Advance Research in Computer Science and Management Studies 3(1)(2015) 270-275.

[4] M. Fathian, A.R. Jafarian-Moghaddam, New clustering algorithms for vehicular ad-hoc network in a highway communication environment, Wireless Networks 21(8)(2015) 2765-2780.

[5] M. Fischer, The consensus problem in unreliable distributed systems (a brief survey), Lecture Notes Computer Science 158(2002) 127-140.

[6] M. Fischer, N. Lynch, A lower bound for the assure interactive consistency, Information Processing Letters 14(4)(1982) 183-186.

[7] B. Hassanabadi, C. Shea, L. Zhang, S. Valaee, Clustering in vehicular ad hoc networks using affinity propagation, Ad Hoc Networks 13(2014) 535-548.

[8] Y.L. Hsieh, K. Wang, Dynamic overlay multicast for live multimedia streaming in urban VANETs, Computer Networks 56(2012) 3609-3628.

[9] C. Jayakumar, C. Chellappan, Quality of service in associativity based mobility-adaptive K-clustering in mobile ad-hoc networks, International Journal of The Computer, the Internet and Management 14(1)(2006) 61-80.

[10] L. Lamport, R. Shostak, M. Pease, The byzantine heneral problem, ACM Transactions on Programming Language and Systems 4(3)(1982) 382-401.

[11] J. Liu, J. Wan, Q. Wang, P. Deng, K. Zhou, Y. Qiao, A survey on position-based routing for vehicular ad hoc networks, Telecommunication Systems 62(1)(2016) 15-30.

[12] M.N. Mejri, J. BenOthman, M. Hamdi, Survey on VANET security challenges and possible cryptographic solutions, Vehicular Communications 1(2)(2014) 53-66.

[13] S.A. Muhammad, Q. Amir, A.K. Kishwer, Information delivery improvement for safety applications in VANET by minimizing Rayleigh and Rician fading effect, Vehicular Ad-hoc Networks for Smart Cities, the series Advances in Intelligent Systems and Computing 306(2014) 85-92.

[14] M. Pease, R. Shostak, L. Lamport, Reaching agreement in the presence of faults, Journal of the ACM 27(2)(1980) 228-234.

[15] B. Ramakrishnan, R.S. Rajesh, R.S. Shaji, Analysis of routing protocols for highway model without using roadside unit and cluster, International Journal of Scientific & Engineering Research 2(1)(2011) 5-13.

[16] D.B. Rawat, S. Reddy, N. Sharma, S. Shetty, Cloud-assisted dynamic spectrum access for VANET in transportation cyber-physical systems, in: Proc. 2014 IEEE International Conference on Performance Computing and Communications, 2014.

[17] P. Ruiz, P. Bouvry, Survey on broadcast algorithms for mobile ad hoc networks, ACM Computing Surveys 48(1)(2015) 1-8.

[18] A.S. Saif, M.A. Moath, A.B. AliH, Z. Hussien, A comprehensive survey on vehicular ad hoc network, Journal of Network and Computer Applications 37(2014) 380-392.

[19] I.A. Sumra, H. Hasbullah, J.A. Manan, VANET security research and development ecosystem, in: Proc. the National Postgraduate Conference, 2011.

[20] J. Sun, C. Zhang, Y. Zhang, Y. Fang, An identity based security system for user privacy in vehicular ad hoc networks, IEEE Transactions on Parallel and Distributed Systems 21(9)(2010) 1227-1239.

[21] F. Wang, Big challenges of vehicle communication and application, in: Proc. 2015 IEEE 4th Asia-Pacific Conference on Antennas and Propagation (APCAP), 2015.