Reading Out Scheme for Digitally Signed Random Network Coded Communication on VANET

TOMOKI MATSUKAWA[†1] TAISUKE YAMAMOTO[†1] YOUJI FUKUTA[†2]
MASANORI HIROTOMO[†3] MASAMI MOHRI[†4] YOSHIAKI SHIRAISHI[†5]

Random network coded communication is vulnerable to possible malicious pollution attacks on wireless and ad-hoc network. Homomorphic signature scheme is well known as countermeasure against the pollution attack for random network coded communication. This paper focuses on digitally signed random network coded communications on vehicular ad-hoc network (VANET). In high vehicle density situations, if a node broadcasts packets, all nodes receive the same packets within the reachable range of sender. If the nodes store the received packets and read out them from the head or the tail of the buffer in the same order by First-in First-out (FIFO) or Last-in First-out (LIFO), the node reads out packets including same generation number and encoding vector as neighbors. Then, the linear independence is lost and rank of encoding matrix decreases. In this paper, we propose a reading out scheme to suppress diminution of *rank* of encoding matrix for improving throughput of digitally signed random network coded communications on VANET. The proposed scheme prevents a node re-encoding same packets with neighbor nodes and suppresses diminution of *rank* of encoding matrix. We confirmed that the throughput of the communication using the proposed scheme is higher than that using FIFO or LIFO from the simulation results.

1. Introduction

In 2008, about 37,000 people died in motor vehicle traffic crashes in the United States, and about 40 percent of the crash accidents were intersection related crashes [1,2]. A field of Intelligent Transport System (ITS) provides some traffic information to prevent the crash accident on vehicular ad-hoc network (VANET). ITS has some applications which assist driving. For example, the assistance system at intersections provides drivers an image of dead angle area and information of probe [3] on VANET [4-9]. In such ITS applications, data source sent must be timely provided with integrity, since it influences an action of vehicles indirectly. Movement of nodes and the electromagnetic interference cause packet-loss on VANET. A requirement of VANET is to efficiently transmit data by reducing the influence of packet-loss, so that drivers can smoothly get information.

Automatic repeat request (ARQ) and coding schemes are well known as countermeasures against packet-loss in the network. In order to recover lost data, ARQ requires feedback from receiver node to the source node. End-to-end feedback is not practical for broadcast because of feedback message explosions. The feedback message explosions disturb other traffic and retransmission data. Coding techniques is suited to VANET because they can recover lost data without end-to-end feedback. There are two coding schemes for packet-loss robustness. One is forward error correction (FEC) and the other is network coding (NC) [10,11]. The references [12-14] have presented methods for the content distribution using erasure codes (EC) [15-17], which are one of FEC, on VANET. However, in using EC, the nodes take long time to collect the packets to decode data which source node sent because nodes transmit a lot of duplicate packets for the content distribution [18]. NC has an advantage of the content distribution since NC reduce duplicate packets [19,20]. The references [19-21] have presented methods for the content distribution using random network coding (RNC) [22,23], which are one of NC, on VANET. However, network coded communication may face potential security threats due to open multi-hop communications and re-encoding process at intermediate forwarders. The pollution attack is originated from any malicious behaviors of un-trusted forwarders or adversaries, such as injecting polluted data, modifying and replaying the disseminated data, which could be fatal to the whole networks. If an invalid data is mixed by a forwarder, the output data of the forwarder will be contaminated and receiver node fails to decode an original data. Towards secure network coded communications, it is prerequisite to achieve efficient data integrity. There are the homomorphic signature schemes [24-28] as countermeasure against the pollution attack.

In [24], a source node divides data of a generation number into m fragments and constructs an encoded data by combining linearly m fragments and an encoding vector randomly generated by the source node. After encoding process, the source node generates a signature of an encoded data by a signing key and includes an encoded data, its signature and a generation number in the sending packet. Intermediate node verifies the signature of the received data by a verification key. If the received data is the invalid data, intermediate node discards it. Intermediate node linearly combines received data and an encoding vector randomly generated by intermediate node. Next, Intermediate node linearly combines signatures of received data and an encoding vector. After including re-encoded data and combined signature in packet, transmit it. Receiver node computes the *rank* of encoding matrix which is composed of encoding vector after verifying the signature of received data. The *rank* is the number of linearly independent packet. When rank is m, receiver node decodes m fragments from m encoded data.

This paper focuses on digitally signed random network coded communications on VANET. In high vehicle density situations,

†1 Nagoya Institute of Technology
†2 Aichi University of Education
†3 Saga University
†4 Gifu University
†5 Kobe University

if a node broadcasts packet, many one-hop nodes receive the same packets. If the nodes stores the received packet and read out them from the head or the tail of the buffer in the same order by First-In First-out (FIFO) or Last-in First-out (LIFO), the one-hop nodes read out packet including same generation number and encoding vector. The linearly independence of received encoding vectors decreases and the *rank* of encoding matrix decreases by re-encoding packets including same generation number and encoding vector as neighbors at intermediate nodes.

In this paper, we propose a reading out scheme to suppress diminution of *rank* of encoding matrix for improving throughput for VANET using digitally signed random network coded communications. The proposed scheme can suppress that some nodes re-encode same packet and transmit by uniformly reading out packets from buffer so as to maintain the linearly independence of received encoding vectors. We confirm that the throughput of communication using the proposed scheme is higher than that using FIFO or LIFO from the simulation results. This paper is organized as follows.

In section II, we focus the related works about the countermeasure against the packet loss and the pollution attack. In section III, we focus the VANET model using digitally signed random network coded communication. In section IV, we propose the reading out scheme from buffer. In section V, we compare the performance of the proposed scheme with FIFO and LIFO. In section VI, we conclude this paper.

2. Related Work

Packet-loss occurs by the link disconnection when network topology dynamically changes in VANET. The packet-loss decreases throughput. The packet-loss robustness is important in contents distribution.

There are two coding schemes for packet-loss robustness. One is FEC and the other is NC. The references [12-14] have presented methods for VANET using EC [15-17] which are one of FEC. Unlike the traditional forwarding approach like EC [15-17] which requires duplicating every input data, NC [10,11] allows each intermediate node to encode packets. Therefore, each output data sent to neighbor nodes can be linear combination of input data received from other nodes. In practical network coding techniques like RNC, packet tagging and buffering allow the encoding and decoding process to proceed in a distributed manner, even if asynchronous packets arrive and depart in arbitrarily varying rate, delay, and loss. Thus, network coding is well suited for dynamic network scenarios.

Random network coded communication may face potential security threats due to open multi-hop communications and the packet re-encoding at intermediate forwarders. Since RNC involves mixing of packet inside the network, nodes are influenced by pollution attacks. Pollution attack is originated from any malicious behaviors of untrusted forwarders or adversaries, such as injecting polluted data, modifying and replaying the disseminated data, which could be fatal to the whole networks. Although this may also occur in a traditional

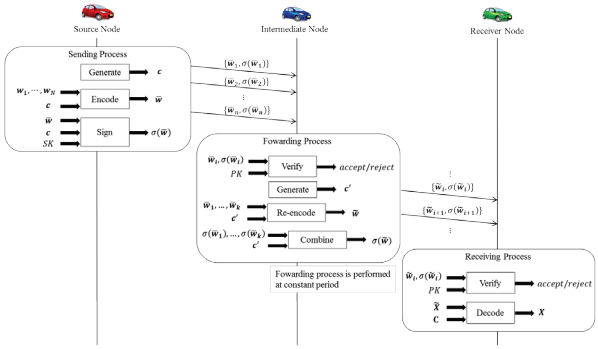


Figure 1 The model of digitally signed random network coded communication on VANET

network system without network coding, its effect is far more serious with network coding. If an invalid data is mixed by a forwarder, the output data of the forwarder will be contaminated. Such polluted data should be detected and filtered as early as possible, since they may spread to all downstream nodes by re-encoding invalid data [25].

There are symmetric key solutions and public-key solutions as countermeasures against pollution attack. While symmetric key solutions are computationally more efficient than public-key ones, they suffer from significant limitations. Symmetric key require an extra secure channel, suffer from extra transmission overhead [24].

The public-key based solutions can be classified in two groups. One is based on homomorphic hashing and other is based on homomorphic signatures. Homomorphic hashing based scheme is often more efficient in terms of computation but requires transmission of long signatures with each packet or the pre-distribution of per-generation information to other nodes. Homomorphic signatures, on the other hand, are somewhat more expensive computationally but do not require pre-distribution or the appending of long signatures to each packet [24]. We note that in this paper we assume homomorphic signature schemes proposed in [28] as the countermeasure against pollution attack.

3. The Model of Digitally Signed Random Network Coded Communication on VANET

The model of digitally signed random network coded communication on VANET consists of source node, intermediate node and receiver node as shown in Fig.1. Each node broadcasts packets and shares the original data sent by the source node. We assume that coding process, signing process and verifying process are based on the process of [28]. In [28], the source node generates a signature of each coded data using a secret private key *SK*, and the signature is transmitted with encoded data. Upon receiving the encoded data along with the signature, nodes verify the encoded data with the given security information using the public key ***PK*** that is made available via broadcast. Nodes only store the verified encoded data in the buffer, and read out them for further mixing. In the homomorphic scheme proposed in [28], the security parameters are described as follows: the source node has a public key

$\boldsymbol{PK} = (N, e, g_1, \ldots, g_m)$, where N is a product of two large safe primes, e is the public RSA exponent chosen as a prime, and $g_1, \ldots, g_m$ are random generators of the cyclic subgroup G of quadratic residues modulo N. In addition, a private signing key SK is defined such that $ed = 1 \bmod \varphi(N)$ $(d \leq \varphi(N))$ where the $h_i = H(i, fid)$ $(i = 1, \ldots, m)$. fid is the generation number of data. Next, we define the process of source node, intermediate node and receiver node as follows.

[Process of Source Node]

An original data $\boldsymbol{X}$ is divided into the m block data $\boldsymbol{x_1}, \ldots, \boldsymbol{x_m}$. Each block is also divided into n symbols. Each symbol is represented by an element of the finite field $GF(2^8)$. Next, the source node constructs fragment $\boldsymbol{w_i} = [\boldsymbol{e_i}, \boldsymbol{x_i}]$ $(i = 1,2, \ldots, m)$. $\boldsymbol{e_i}$ is the $\boldsymbol{i}$ th unit vector. Process for each fragment to downstream nodes is executed as follows.

Step.1. Generate an encoding vector $\boldsymbol{c} = [c_1, \ldots, c_m]$, randomly.

Step.2. Encode $\boldsymbol{w_i}$ to data $\bar{\boldsymbol{w}}$ by the encoding vector $\boldsymbol{c}$.

$$\bar{\boldsymbol{w}} = \sum_{i=1}^{m} c_i \boldsymbol{w_i}$$

Step.3. Generate a signature $\sigma(\bar{\boldsymbol{w}})$ of the encoded data $\bar{\boldsymbol{w}}$ by the signing key SK and the encoding vector $\boldsymbol{c}$.

$$\sigma(\bar{\boldsymbol{w}}) = \left(\prod_{i=1}^{m} h_i^{c_i} \prod_{j=1}^{n} g_j^{x_{i,j}} \right)^{SK} \bmod N$$

Step.4. Packetize the encoded data $\bar{\boldsymbol{w}}$ and the signature $\sigma(\bar{\boldsymbol{w}})$, then broadcast the packet.

[Process of Intermediate Node]

An intermediate node buffers a received packet per each generation number in the order they have arrived. Then, the node read out by FIFO (Fig.2) or LIFO (Fig.3) as follows.

Step.1. Read out k packets from the head (FIFO) or the tail (LIFO) of the buffer of the generation number and discard the remained packet. The k packets include the encoded data $\bar{\boldsymbol{w}}_1, \ldots, \bar{\boldsymbol{w}}_k$ and the signatures $\sigma(\bar{\boldsymbol{w}}_1), \ldots, \sigma(\bar{\boldsymbol{w}}_k)$ $(k \leqq m)$.

Step.2. Verify the signature $\sigma(\bar{\boldsymbol{w}}_i)$ by the verification key $\boldsymbol{PK}$ and the encoded data $\bar{\boldsymbol{w}}_i = [\boldsymbol{c_i}, \bar{\boldsymbol{x}}_i]$. Discard the packet which is not accepted at the verification.

$$accept/reject \leftarrow \sigma(\bar{\boldsymbol{w}}_i)^e \stackrel{?}{=} \prod_{i=1}^{m} h_i^{c_i} \prod_{j=1}^{n} g_j^{\bar{x}_{i,j}} \bmod N$$

Step.3. Generate the encoding vector $\boldsymbol{c'} = [\tilde{c}_1, \cdots, \tilde{c}_k]$, randomly.

Step.4. Re-encode the received data $\bar{\boldsymbol{w}}_1, \ldots, \bar{\boldsymbol{w}}_k$ to an re-encoded data $\tilde{\boldsymbol{w}}$ by the encoding vector $\boldsymbol{c'}$.

$$\tilde{\boldsymbol{w}} = \sum_{i=1}^{k} \tilde{c}_i \bar{\boldsymbol{w}}_i$$

Step.5. Generate the signature $\sigma(\tilde{\boldsymbol{w}})$ by the signatures $\sigma(\bar{\boldsymbol{w}}_1), \ldots, \sigma(\bar{\boldsymbol{w}}_k)$ and the encoding vector $\boldsymbol{c'}$.

$$\sigma(\tilde{\boldsymbol{w}}) = \prod_{i=1}^{k} \sigma(\bar{\boldsymbol{w}}_i)^{\tilde{c}_i} \bmod N$$

Step.6. Packetize the re-encoded data $\tilde{\boldsymbol{w}}$ and the signature $\sigma(\tilde{\boldsymbol{w}})$, then broadcast the packet.

[Process of Receiver Node]

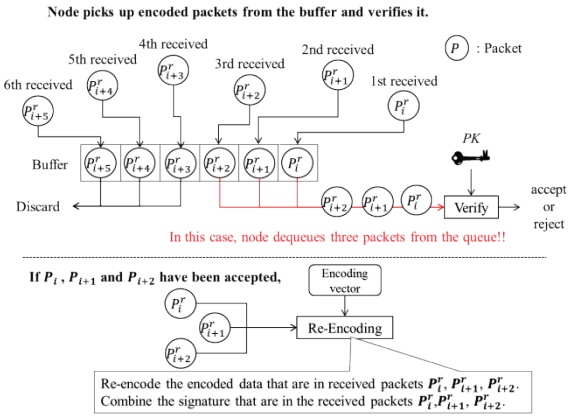


Figure 2 The forwarding process using FIFO on digitally signed random network coded communication on VANET

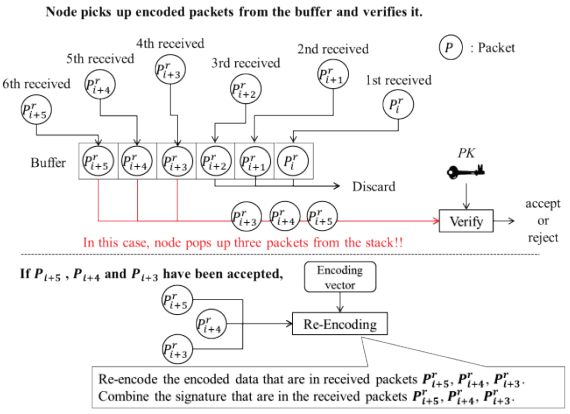


Figure 3 The forwarding process using LIFO on digitally signed random network coded communication on VANET

A receiver node buffers a received packet per each generation number in the order they have arrived.

Step.1. Read out m packets from the buffer of the generation number. The m packets include the encoded data $\tilde{\boldsymbol{w}}_1, \ldots, \tilde{\boldsymbol{w}}_m$ and the signatures $\sigma(\tilde{\boldsymbol{w}}_1), \ldots, \sigma(\tilde{\boldsymbol{w}}_m)$.

Step.2. Verify the signature $\sigma(\tilde{\boldsymbol{w}}_i)$ by the verification key $\boldsymbol{PK}$ and the encoded data $\tilde{\boldsymbol{w}}_i$. Discard the packet which is not accepted at the verification.

Step.3. Construct $\tilde{\boldsymbol{X}} = [\tilde{\boldsymbol{x}}_1, \tilde{\boldsymbol{x}}_2, \ldots, \tilde{\boldsymbol{x}}_m]$ and $\boldsymbol{C} = (\boldsymbol{c_1}, \boldsymbol{c_2}, \ldots, \boldsymbol{c_m})^T$ from the received data $\tilde{\boldsymbol{w}}_i = [\boldsymbol{c_i}, \tilde{\boldsymbol{x}}_i]$ $(i = 1,2, \ldots, m)$. If the $rank$ of $\tilde{\boldsymbol{X}}$ is m, decode it to the original data $\boldsymbol{X} = \boldsymbol{C^{-1}}\tilde{\boldsymbol{X}}$.

4. Proposed Scheme

In random network coded communications, if a node broadcasts packets, all nodes receive the same packets within the reachable range of sender. Then the packets including a generation number and an encoding vector reach some neighbor nodes at same time. If the nodes store received packet and read out packets from the head or the tail of the buffer in the order by FIFO or LIFO, the node reads out the packet including same generation number and encoding vector with neighbors. The

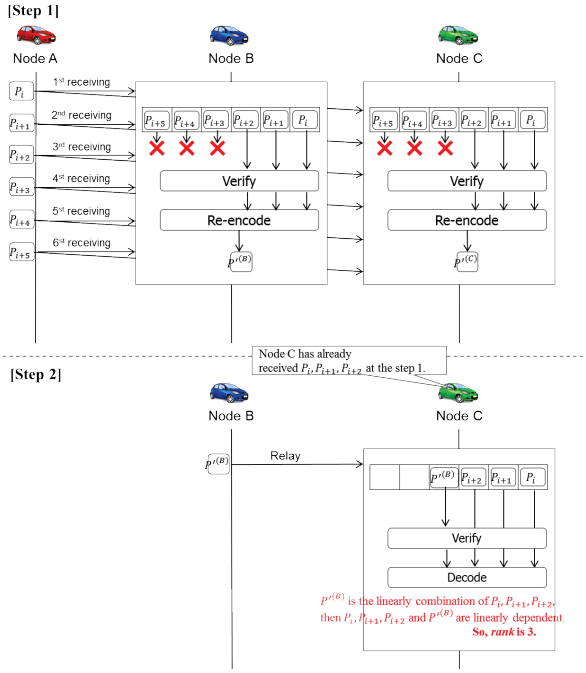


Figure 4 High vehicle density situation using FIFO

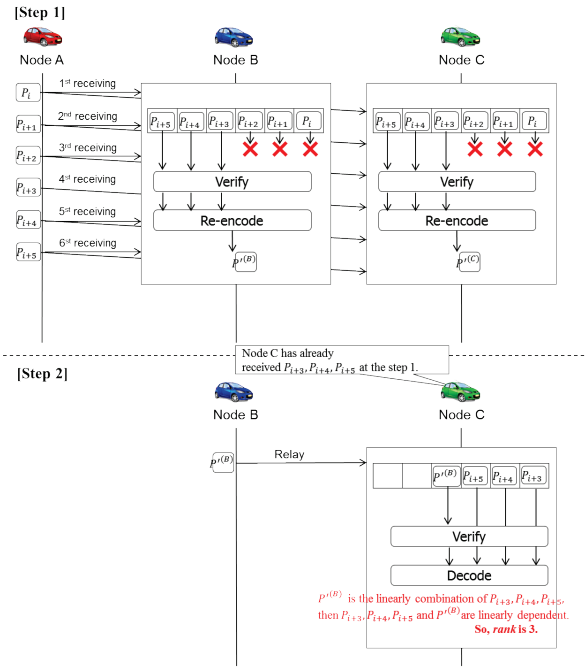


Figure 5 High vehicle density situation using LIFO

linearly independence of received encoding vectors decreases and *rank* of encoding matrix decreases because the intermediate node re-encode the same packet as the packet which receiver node has received.

Fig.4 shows that a node buffering received packet in the buffer by FIFO. In Fig.4, node A broadcasts packets $P_i, P_{i+1}, \dots, P_{i+m}$ including the encoded data and the signature obtained in Step 1. Nodes B and C verify and re-encode packets P_i, P_{i+1} which are stored in the head of the buffer. Next, node B broadcasts the re-encoded packet P' which is linearly computed from P_i, P_{i+1} and node C receives it in Step 2. However, P' is the linearly dependent packet for node C since node C already has received P_i, P_{i+1}. Then, the *rank* does not increase. When the node stores and reads out packet by LIFO, the *rank* does not increase as same as FIFO (Fig.5).

Some nodes re-encode the same packet as the packet which receiver node already has received, then, the receiver node receives linearly dependent packets and the *rank* of encoding matrix does not increase.

In this paper, we propose reading out scheme for suppressing the *rank* reduction of encoding matrix in order to improve the throughput of digitally signed random network coded communication on VANET. The proposed scheme can suppress that some intermediate nodes re-encode the same packet as the packet which receiver node has received since nodes read out the packet uniformly from the buffer as shown in Fig.6. Then the linearly independent of received encoding vectors will increase, and the node can receive linearly independent packet as shown in Fig.7. Next, we present the process of source node, intermediate node and receiver node in the proposed scheme as follows.

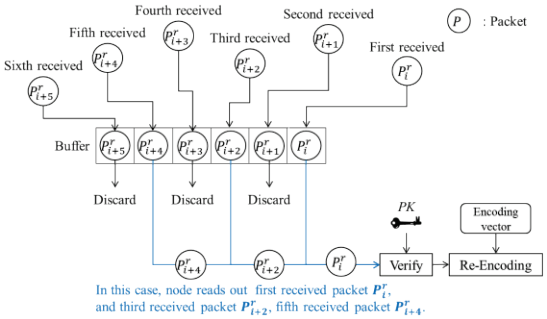


Figure 6 The proposed scheme

[Process of Source Node]

An original data $\boldsymbol{X}$ is divided into the m block data $\boldsymbol{x_1}, \dots, \boldsymbol{x_m}$. Each block is also divided into n symbols. Each symbol is represented by an element of the finite field $\mathrm{GF}(2^8)$. Next, source node constructs fragment $\boldsymbol{w_i} = [\boldsymbol{e_i}, \boldsymbol{x_i}]$ $(i = 1,2, \dots, m)$. $\boldsymbol{e_i}$ is $\boldsymbol{i}$ *th* unit vector. Process for each fragment to downstream nodes is as follows.

Step.1. Generate an encoding vector $\boldsymbol{c} = [c_1, \dots, c_m]$, randomly.

Step.2. Encode $\boldsymbol{w_i}$ to data $\bar{\boldsymbol{w}}$ by the encoding vector $\boldsymbol{c}$.

Step.3. Generate a signature $\sigma(\bar{\boldsymbol{w}})$ of the encoded data $\bar{\boldsymbol{w}}$ by signing key *SK* and the encoding vector $\boldsymbol{c}$.

Step.4. Packetize the encoded data $\bar{\boldsymbol{w}}$ and the signature $\sigma(\bar{\boldsymbol{w}})$, then broadcast the packet.

[Process of Intermediate Node]

An intermediate node buffers a received packet per each generation number in the order they have arrived.

Step.1. Output k $(k \leqq m)$ integers $a_1, a_2, \dots, a_k$ from the uniformly function. $(a_1 \neq a_2 \neq, \dots, \neq a_k)$

$$Uniformity(k) \rightarrow a_1, \dots, a_k, \qquad (a_1, \dots, a_k \in k)$$

Step.2. Read out a_ith received packet from the buffer and

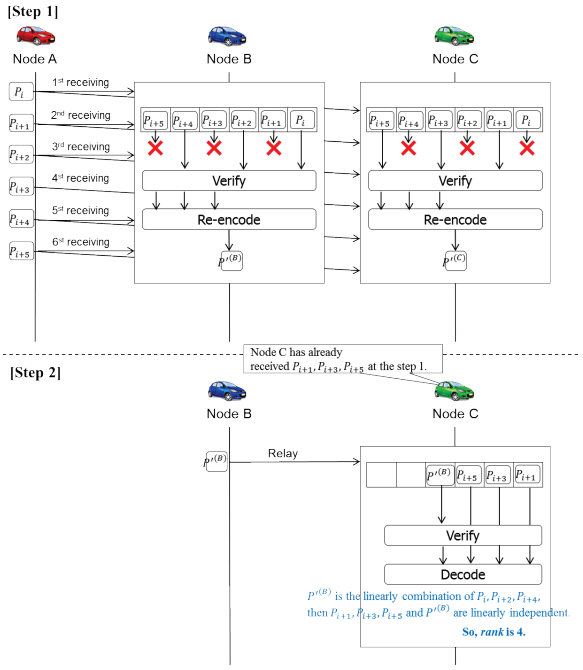


Figure 7 High vehicle density situation using the proposed scheme

discard the packet which is not read out ($i = 1, \dots, k$). The k packets include the encoded data $\bar{\boldsymbol{w}}_1, \dots, \bar{\boldsymbol{w}}_k$ and the signatures $\sigma(\bar{\boldsymbol{w}}_1), \dots, \sigma(\bar{\boldsymbol{w}}_k)$.

Step.3. Generate the encoding vector $\boldsymbol{c}' = [\tilde{c}_1, \cdots, \tilde{c}_k]$, randomly.

Step.4. Re-encode the received data $\bar{\boldsymbol{w}}_1, \dots, \bar{\boldsymbol{w}}_k$ to an re-encoded data $\tilde{\boldsymbol{w}}$ by the encoding vector $\boldsymbol{c}'$.

Step.5. Generate the signature $\sigma(\tilde{\boldsymbol{w}})$ by the signatures $\sigma(\bar{\boldsymbol{w}}_1), \dots, \sigma(\bar{\boldsymbol{w}}_k)$ and the encoding vector $\boldsymbol{c}'$.

Step.6. Packetize the re-encoded data $\tilde{\boldsymbol{w}}$ and the signature $\sigma(\tilde{\boldsymbol{w}})$, then broadcast the packet.

[Process of Receiver Node]

A receiver node buffers a received packet per each generation number in the order they have arrived.

Step.1. Read out m packets from the buffer of a generation number. The m packets include encoded data $\tilde{\boldsymbol{w}}_1, \dots, \tilde{\boldsymbol{w}}_m$ and the signatures $\sigma(\tilde{\boldsymbol{w}}_1), \dots, \sigma(\tilde{\boldsymbol{w}}_m)$.

Step.2. Verify the signature $\sigma(\tilde{\boldsymbol{w}}_i)$ by verification key $\boldsymbol{PK}$ and the encoded data $\tilde{\boldsymbol{w}}_i$. Discard the packet which is not accepted at the verification.

Step.3. Construct $\tilde{\boldsymbol{X}} = [\tilde{\boldsymbol{x}}_1, \tilde{\boldsymbol{x}}_2, \dots, \tilde{\boldsymbol{x}}_m]$ and $\boldsymbol{C} = (\boldsymbol{c}_1, \boldsymbol{c}_2, \dots, \boldsymbol{c}_m)^T$ from received data $\tilde{\boldsymbol{w}}_i = [\boldsymbol{c}_i, \tilde{\boldsymbol{x}}_i]$ $(i = 1,2, \dots, m)$. If the *rank* of $\tilde{\boldsymbol{X}}$ is m, decode it to the original data $\boldsymbol{X} = \boldsymbol{C}^{-1}\tilde{\boldsymbol{X}}$.

5. Performance Evaluation

We evaluate the performance of the proposed scheme, FIFO and LIFO. In this evaluation, the coding process of [21] is applied to the simulation model. In this section, first we show

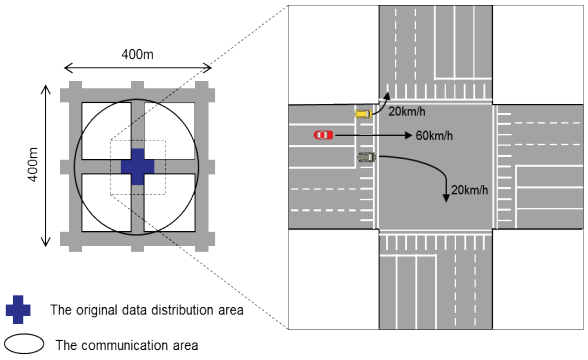


Figure 8 Simulation field

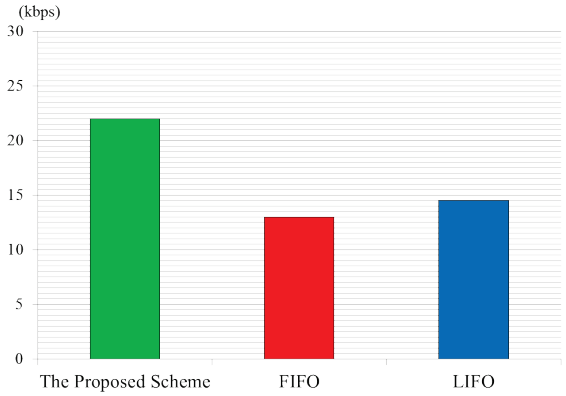
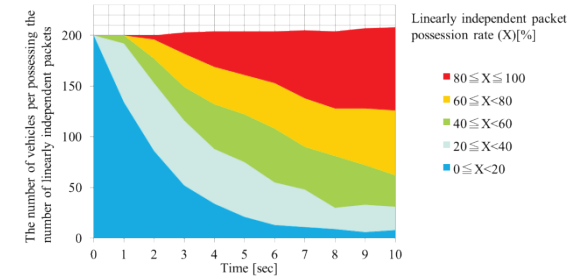


Figure 9 The average throughput

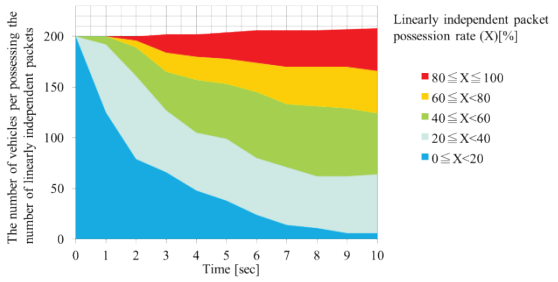
the average throughput of digitally signed random network coded communication on VANET using the proposed scheme, FIFO and LIFO. Then, we compare the number of nodes of each linearly independent packet possession rate. The linearly independent packet denotes the packet which can be used to decode. We conduct the simulation model using OMNeT++4.0 netwok simulator [29] and MiXiM1.1 wireless framework [30]. In this simulation model, nodes transmit the data with point-to-multipoint broadcast on VANET. In the simulation field, is each road has three lanes in opposing direction as shown in Fig. 8, and 200 nodes run through the intersection. Some vehicles go straight at 60 km/h, the legal speed of Japan, and the others turn right/left at 20 km/h. The headway of going straight node is 40 m, and the headway of turning node is 20m.

The simulation parameters are the followings: MAC protocol is IEEE802.11b. Network bandwidth is 11 Mbps and then transmission power is 10 mW [31]. Source node generates an original data and assigns a generation number to each data of size 10 KB. A fragment size is 1 KB, so receiver node must get 10 linearly independent packets to decode an original data of a generation number. Source node transmits the packet at a constant bit-rate 80 kbps. The finite field is $\mathrm{GF}(2^8)$.

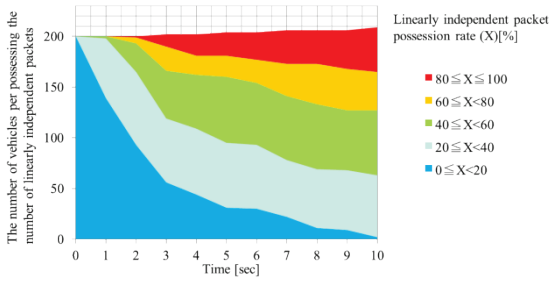
We regard the node entering the original data distribution area as source node. Other nodes are intermediate/receiver nodes. The area for generating the original data is within the radius of 50 m from the center of intersection. The role of source node, intermediate node and receiver node follow the process shown in Section 4. The source node's role or the both of intermediate node's role and receiver node's role is assigned to each node before the simulation starts. The intermediate/receiver nodes read out 3 packets from the buffer and verify them after 200 second since they have received the first packet. Signature verification cost is 100 ms. The generating signature cost, the encoding/re-encoding cost and decoding cost are 10 ms respectively. All nodes will stop communicating when they go to



(a) The proposed scheme



(b) FIFO



(c) LIFO

Figure 10 The number of vehicles per linearly independent packet possession rate

the outside of the communication area. The communication area denotes the area which is within the radius of 200 m from the center of intersection.

We evaluate the average throughput T and the number of nodes of each linearly independent packet possession rate. The two evaluation criteria are calculated from the followings.

[*The average throughput*]

The average throughput T is the average of the amount of decoded data per a second in the node i.

$$T = \frac{\sum_{i \in V} M_i}{t \times |V|}$$

where t is an elapsed time after source node began to send packet, V is the set of nodes, and M_i is the size of decoded data.

[*The linearly independent packet possession rate*]

We count the number of nodes for the linearly independent packet possession rate 0-20%, 20-40%, 40-60%, 60-80% and 80-100% respectively. The linearly independent packet possession rate R is calculated as follows.

$$R = \frac{\sum_{i \in r} D^i}{S}$$

where r is a generation number, D^i is the number of the linearly independent packet of a generation number i, and S is the number of the sending packet of source node. We plot the result of the number of nodes of the linearly independent packet possession rate R of every second.

Fig.9 shows the average throughput which denotes the average size of the decoded data per second at 10 second after source node began to send packets. From Fig.9, the average throughput of the proposed scheme is higher than others by approximately 8-10 kbps. Since the number of received linearly independent packets of the proposed scheme is larger than others, the nodes in the proposed scheme can decode data in a shorter time than the scheme using FIFO or LIFO.

Fig.10 shows the number of vehicles of each the linearly independent packet possession rate at 10 second after source node began to send packets. In the case of comparison of the number of nodes in possession rate more than 60 %, the number of nodes of the proposed scheme is larger than that of FIFO and LIFO. The possession rate about 70 % of nodes is less than 60 % in FIFO and LIFO schemes. The proposed scheme can increase the number of vehicles of high possession rate.

Consequently, the proposed scheme can improve the average throughput of digitally signed random network coded communication on VANET since the proposed scheme increases the number of nodes of high possession rate of the linearly independent packets.

6. Conclusion

We have mentioned about reading out scheme that node reads out received packet from buffer of digitally signed random network coded communication on VANET. If node uses FIFO or LIFO as reading out scheme in high vehicle density situations, the *rank* of encoding matrix decreases since node re-encodes same packet as neighbor nodes. In this paper, we proposed the scheme that nodes read out uniformly packet from buffer to suppress diminution of *rank*.

We compare the average throughput and the number of nodes of each linearly independent packet possession rate of communications using the proposed scheme, FIFO or LIFO. As the results, the performance of the proposed scheme is greater than communication by FIFO or LIFO. The average throughput of the proposed scheme is higher than that of others. Also, the number of nodes of high possession rate of the linearly independent packets of the proposed scheme is more than that of others. This result indicates that the proposed scheme increases nodes receiving data which source node sent per unit time. Thus, the proposed scheme is better than FIFO and LIFO as reading out scheme from buffer for digitally signed random network coded communication on VANET.

Reference

1) National Highway Traffic Safety Administration: TRAFFIC SAFETY FACTS Research Note, (2013).

2) National Highway Traffic Safety Administration: Crash Factors in Intersection-Related Crashes: *An On-Scene Perspective*, (2010).

3) Nakamura, N., Kida, K., Fujiyama, K., and Imai, T.,: High-Speed Probe Information Collection/Analysis Using Data Stream Processing Platform, *NEC Technical Journal*, Vol.3, No.1, (2008).

4) Park, J.-S., Lee, U., Oh, Y.S., Gerla, M., and Lun, D.,: Emergency related video streaming in VANET using network coding, *in Proc. of the 3rd international workshop on Vehicular adhoc networks*, pp.102-103, (2006).

5) Sakai, H., Koyamaishi, M., and Toyota, K.,: Experiment of Safety Drive in an Intersection by Visual Assistances based on HIR System, *IEEE Intelligent Vehicles Symposium*, (2003).

6) Nakanishi, T., Yendo, T., Fujii, T., and Tanimoto, M.,: Right Turn Assistance System at Intersections by Vehicle-Infrastructure

Cooperation, *IEEE Intelligent Vehicles Symposium*, (2006).
7) Sakai, H., Toyota, K., Fujii, T., Kimoto, T., and Tanimoto, M.,: Visual assistance to right turn in an intersection by Using HIR (Human-Oriented Information Restructuring) System, *IEEE Intelligent Vehicles Symposium*, (2002).
8) Morioka, Y., Sota, T., and Nakagawa, M.,: An Anti-CarCollision System Using GPS and 5.8 GHz Inter-Vehicle Communication at an Off-Sight Intersection, *IEEE Vehicular Technology Conference*, (2000).
9) Miller, R., Huang, Q.,: An Adaptive Peer-to-Peer Collision Warning System, *IEEE Vehicular Technology Conference*, (2002).
10) Ahlswede, R., Cai, N., Li, R.S.-Y. and Yeung, W.R.,: Network Information Flow, *IEEE Transactions on Information Theory*, vol.46, no.4, pp.1204-1216, (2000).
11) Li, R.S.-Y., Yeung, W.R., and Cai, N.,: Linear Network Coding, *IEEE Transactions on Information Theory*, vol.49, no.2, pp.371-381, (2003).
12) Abdullah, F.N., Doufexi, A., and Piechocki, J.R.,: Car-to-Car Safety Broadcast with Interference using Raptor Codes, *IEEE Vehicular Technology Conference*, pp.1-5, (2011).
13) Palma, V., Mammi, E., Vegni, M.A., and Neri, A.,: A Fountain Codes-based Data Dissemination Technique in Vehicular Ad-hoc Networks, *International Conference on ITS Telecommunications*, pp.750-755, (2011).
14) Liu, W., Yang, Y., and Zhu, M.,: Research on inter Hospital and Ambulance Data Transmission using LT-Coding over VANET, *International Conference on Complex Medical Engineering*, pp.119-123, (2013).
15) Shokrollahi, A.,: Raptor Codes, *IEEE Transactions on Information Theory*, vol.52, no.6, pp.2551-2567, (2006).
16) MacKay, C.J.D.,: Fountain Codes, *IEE Proceedings on Communications*, vol. 152, no. 6, pp. 1062-1068, (2005).
17) Luby, M.,: LT Codes, *IEEE Symposium on Foundations of Computer Science*, pp. 271-280, (2002).
18) Zhou, Y., Zhang, L., and Liu, Y.,: An Approach of Eliminating Duplicate Associates in Fountain Codes, *International Conference on Wireless Communications*, pp. 1-4, (2009).
19) Li, M., Yang, Z., and Lou, W.,: CodeOn: Cooperative Popular Content Distribution for Vehicular Networks using Symbol Level Network Coding, *IEEE Journal on Selected Areas in Communications*, vol.29 no.1, pp.223-235, (2011).
20) Yang, Z., Li, M., and Lou, W.,: CodePlay: Live multimedia streaming in VANETs using symbol-level network coding, *Proceedings of the 18th IEEE International Conference on Network Protocols*, pp.223-232, (2010).
21) Lee, U., Park, J., Yeh, J., Pau, G., and Gerla, M.,: Code torrent: Content distribution using network coding in vanet, *Proceedings of the 1st International Workshop on Decentralized Resource Sharing Mobile Computing. Networking*, pp. 1-5, (2006).
22) Chou, A.P., Wu, Y., and Jain, K.,: Practical network coding, *Proceeding of the 41st Annual Allerton Conference on Communication, Control, and Computing*, (2003).
23) Ho, T., Médard, M., Koetter, R., Karger, R.D., Effros, M., Shi, J., and Leong, B.,: A Random Linear Network Coding Approach to Multicast, *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413-4430, (2006).
24) Lee, S.-H., Gerla, M., Krawczyk, H., Lee, K.-W., and Quaglia, A.E.,: Performance Evaluation of Secure Network Coding using Homomorphic Signature, *International Symposium on Network Coding*, pp.1-6, (2011).
25) Jiang, Y., Zhu, H., Shi, M., Shen, X., and Lin, C.,: An efficient dynamic-identity based signature scheme for secure network coding, *Computer Networks*, vol.54, pp.28-40, (2010).
26) Charles, D., Jain, K., and Lauter, K.,: Signatures for Network Coding, *Information Sciences and Systems*, pp.857-863, (2006).
27) Yu, Z., Wei, Y., Ramkumar, B., and Guan, Y.,: An efficient signature-based scheme for securing network coding against pollution attacks, *in Proc. of IEEE INFOCOM*, pp.1409-1417, (2008).
28) Gennaro, R., Katz, J., Krawczyk, H., and Rabin, T.,: Secure Network Coding Over the Integers, *International Conference on Practice and Theory in Public Key Cryptography*, pp.142-160, (2010).
29) OMNeT++, available form <http://www.omnetpp.org/>, (accessed 2014-02-07).
30) MiXiM, available from <http://sourceforge.net/projects/-mixim/ >, (accessed 2014-02-07).
31) ITS Info-communications Forum of Japan: Experimental Guideline for Vehicle Communications System using 700 MHz-Band ITS FORUM RC-006 Version 1.0, (online), available from <http://www.itsforum.gr.jp/Public/J7Database/p35/ITSFORUMRC006engV1_0.pdf>, (accessed 2014-02-07).