Wireless Personal Communications (2007) 43:141–156
DOI 10.1007/s11277-006-9235-2

Cooperation Enhancement for Message Transmission in VANETs

ZHOU WANG and CHUNXIAO CHIGAN

Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI 49931, USA
E-mail: cchigan@mtu.edu

Abstract. As one special case of the Mobile Ad Hoc Networks (MANET), vehicular ad-hoc networking (VANET) is featured by its high mobility and constantly changing topology. In VANET, nodes can work properly only if the participating vehicles cooperate with each other during communications. However, as a distributed network, individual vehicles might be non-cooperative for their own benefits. In order to prevent non-cooperative vehicles from tampering packet relaying in the network, we propose a cooperation enhancement mechanism using "*Neighborhood WatchDog*" to generate "*Trust Token*" based on the first-hand observation. Therefore, trust relationships and packet-acceptance decisions of the receiving nodes are based on the instant observation and the token-proved relaying behavior of the benign neighboring vehicles. With the inherit mapping between the *Electronic ID* of one vehicle and its public key, keys can be distributed on-the-fly. As a network layer solution, the cooperation enhancement mechanism proposed in this paper is built on the top of our previous proposed Media Access Control (MAC) protocol: Relative Position Based-MAC (RPB-MAC).

Keywords: VANET, WatchDog, trust token, E_ID, public key, digital signature.

1. Introduction

Consider an urban area with hundreds of thousands of vehicles. Drivers and passengers are interested in information relevant to their trips and the traffic conditions a short distance ahead. All these information is important for drivers to optimize their travels, to alleviate traffic congestion, to avoid wasteful driving and to prevent driving accidents.

In the future, vehicles equipped with communication capabilities can enable inter-vehicle communication (IVC) to promote coordinated safety driving [2]. By then, vehicles will serve as network nodes in the vehicular ad hoc networks (VANET). Indeed, VANET is an instantiation of mobile ad hoc network (MANET), lacking a fixed infrastructure and relying on ordinary nodes to perform basic network functions such as packet routing and network management. However, VANET behaves fundamentally different from the traditional MANET, in that it is characterized for high mobility and rapidly changing network topology, with limited temporal and functional redundancy. Therefore, it poses special challenges and high demands for cooperation among individual vehicles to contribute to the network performance.

Previously, we proposed a Media Access Control (MAC) protocol for VANET, *Relative Position Based-MAC (RPB-MAC)* [4], which provides dedicated communication channels among neighboring vehicles. In this paper, we introduce a trust model: *WatchDog-Trust Token (WD-TT)*, which is built on top of the RPB-MAC for cooperation enhancement among vehicles during packet disseminations. Our goal is to detect and prevent misbehaving nodes from altering packets during transmission and to guarantee the authentic packet delivery in VANET. In

the proposed scheme, packets are forwarded hop-by-hop. *Trust evaluations* are given instantly based on the first-hand observations of the upstream node, and *packet-acceptance decisions* are made according to the *trust evaluation*. *Digital signature* is used to protect packet integrity. Based on the inherit mapping between Electronic ID and the vehicle's public key, no priori key distribution is required and the keys can be distributed on-the-fly.

The rest of this paper is organized as follows. Section 2 presents the related work and Section 3 gives a detailed description of the proposed approach. In-depth discussions are provided in Section 4. Section 5 depicts the performance evaluation of our proposed approach. Conclusions and discussions are provided in Section 6.

2. Related Work

As a distributed and unbounded system, VANET can function properly only if the participating vehicles cooperate well in transmitting and forwarding packets among each other. On the other hand, packets transmission in VANET relies on potentially untrustworthy nodes since individual nodes may act maliciously by fabricating, dropping or altering data packets for their own benefits, and data packets dissemination may be subject to corruption during transmission. Therefore, cooperative communication among nodes is vital for the packet delivery in VANET.

To date, a rich family of mechanisms that detects and prevents uncooperative behaviors has been proposed in the literature [3, 5, 7–9, 11]. Most of these solutions rely on the *historical reputation records* which require temporal or functional network redundancy to enforce cooperative communication in the traditional MANET. In those mechanisms, each node is ranked with a reputation based on its serving behavior observed by other nodes in the same neighborhood. A node's reputation can be learned by other nodes farther away from the neighborhood. A node with bad reputation is then refused service by other nodes, and hence isolated from the network. However, few studies have investigated the cooperation issue in VANET wherein the extremely high mobility and limited connectivity redundancy impose new research challenges to enforce cooperation among nodes.

Vehicle Ad-Hoc Reputation System (VARS) [5] makes use of direct and indirect trust as well as opinion piggyback to enable confident decisions on event packets. Opinions are appended for packet forwarding. In [9], authors developed a reputation system in mobile networks. The study in [11] proposes a pairwise-evaluating buddy system. Researches reported in [3, 7, 8] apply the *WatchDog* mechanism to overhear the forwarding behaviors of the downstream neighboring nodes within the transmission range to detect uncooperative behaviors. In addition, various policies are adopted in the baseline *WatchDog* mechanism to punish the misbehaving nodes. However, solutions in [3, 7, 8] depend on the long-term reputation maintenance while mechanism in [5] involves accumulating reputation evaluation over time. Such relatively "static" reputation maintenance scheme is not suitable for the highly dynamic VANETs where nodes may interact with the same node only once (with short duration) in the life time. In addition, the solution proposed in [9] requires human interaction while solution in [11] requires good connectivity to establish buddies. Therefore, these solutions are inherently not applicable to the highly distributed and dynamic VANETs.

Different from these existing works relying on the historical record of node behaviors, we propose a dynamic WatchDog *Trust-Token* (WD-TT) mechanism which relies on the instant performance of each VANET node. Instead of using traditional *historical reputation record*

concept, only run-time relaying behavior is required for instant reputation evaluation, which will later be used for packet acceptance decision. In addition, our mechanism requires no information update, which thus engages negligible performance degradation (e.g., transmission delay, etc.). Therefore, it well suits the highly dynamic VANET with limited connectivity redundancy.

3. Main Mechanism

3.1. General View

In our previous work [4], we proposed an innovative Relative Position Based MAC (RPB-MAC) protocol (Figure 1) for VANET. By combining the dedicated directional antenna and the dedicated communication channel further associated to the Relative Position, an essentially *contention-free* MAC for VANET is realized. Therefore, it guarantees high throughput and minimal cost of control packet exchanging, and adapts quickly to the highly mobile and constantly changing VANET topology.

In this paper, we propose a cooperative packet forwarding schemes built upon RPB-MAC protocol. With the support of RPB-MAC protocol, we consider the misbehavior of packet dropping/modification is only caused by intentional node misbehavior, and assume the packet dropping/modification due to accidental collision or poor physical layer channel condition has been taken care of. Nodes are defined as *well behaved* or *reliable* if they coordinate in the communication and forward packets faithfully and instantly, while those nodes refusing to cooperate are referred as *misbehaved* and assigned a bad reputation. Three kinds of misbehaviors are defined here (listed in Table 1). *Silent nodes* refer to the nodes that neither send *Hello* packets nor relay packets for others. They keep quiet all the time and never join VANET communications. *Selfish nodes* use the network but do not cooperatively forward packet for others to save their own resource. *Malicious nodes*, however, actively launch attack on packet authenticity and integrity during the communication.

If all the downstream nodes cooperatively relay packet for others, VANET can function properly. However, if the intermediate relaying nodes behave maliciously, security issues will arise. In this paper, we mainly target at how to detect *malicious nodes* during packet transmission. We propose a new mechanism to prevent the modified packets from being propagated

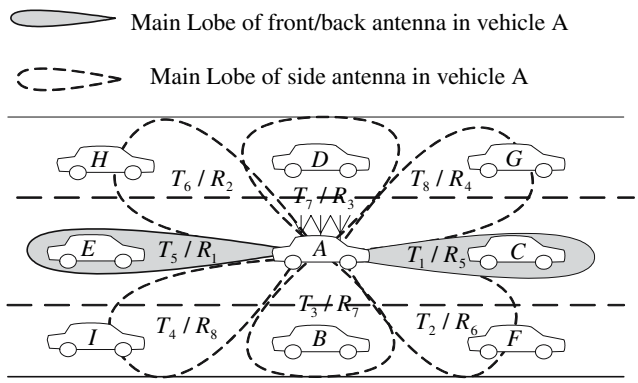


Figure 1. General view of RPB-MAC protocol.

Table 1. Three kinds of misbehaviors

	Sending "Hello" packets	Relaying packets for others	Maintain packets integrity while relaying
Silent node	×	×	×
Selfish node	√	×	×
Malicious node	√	√	×

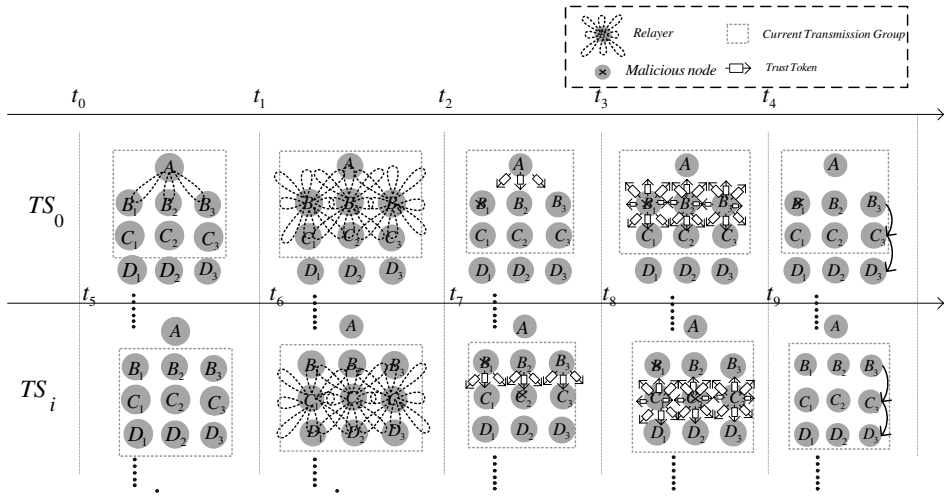
so as to guarantee the integrity of data packets propagated within such a highly dynamic network. Our solution is a local mechanism, wherein each node sends *Hello* packet periodically to maintain local connectivity. When an emergent event is detected, the detecting node will initiate a packet transmission session and to have its downstream nodes relaying the information packet hop-by-hop. While relaying packets to its downstream node, the current relayer's forwarding behavior will be overheard by its upstream node which will evaluate whether this relayer node is acting faithfully. Here, the upstream monitor node is referred as a *WatchDog* [8]. The evaluation results are included in a special packet called *"Trust Token"* that helps downstream nodes judge whether the data packet it received is reliable or not. Only those data packets authentically forwarded will be accepted, others will be dropped.

Unlike the conventional MANET cooperation mechanisms which use historical reputation records as the index for node's reliability, our solution only depends on nodes' instantaneous behaviors. Therefore, the decision about whether to accept or to drop the packet is made based on the instant behavior of the forwarding node. The nature of our mechanism assures that, if a relayer refuses to cooperate, its malicious behavior will be detected by the upstream WatchDog and reported to the downstream nodes so that the modified packet would not propagate in VANET. As a result, the misbehaved nodes would not benefit from being malicious.

3.2. Detailed Design

In this section, we present the detailed design of our proposed cooperation enhancement mechanism for VANETs. We assume that the origin node is trust worthy and any information packets sent by the orgin node is authentic. It is also assumed that a global clock is maintained among all the vehicles for synchronization purpose. In our mechanism, three types of protocol nodes, *predecessor, relayer and successor*, are defined. *Relayer (Rel)* refers to the node responsible for relaying packets. *Predecessor (pre)* is the one-hop upstream node of the Relayer serving as the WatchDog. *Successor (suc)* is the one-hop downstream node of the Relayers responsible for making decisions whether to accept packets or not. Both predecessor and successor are within the wireless transmission range of relayer. Each node maintains a *packet buffer*, wherein data packets are stored for a period of time: *timeout*, while waiting for corresponding token packets. After processing the data packet associated with the token packet, successors will only accept those valid packets and further forward them.

The general view of our cooperation enhancement mechanism is illustrated in Figure 2. TS_0 is the initiating session and TS_i is one typical transmission sessions. At TS_0, the initiator detects one emergent event and initiates one packet transmission. The packet will be passed on hop-by-hop during each transmission session (TS_i). Each TS_i includes four phases: Packet



	Packet Relay	Behavior Evaluation	Trust Token Relay	Packet Acceptance
Predecessor		uses Algorithm 1 to evaluate the behavior of the relayers ; generate Trust Token;	Pass the Trust Token to relayers.	
Relayer	add their own *E_ID* with the packet and broadcast data packet to all directions;		pass the token to the downstream successors	
Successor	store packets in the packet buffer for a period of time			decide whether to accept or drop the packet using Algorithm 2

Figure 2. General view of packet flow.

Relaying (PR : t1–t2 for TS_0 and t6–t7 for TS_i); Behavior Evaluation (BE : t2–t3 for TS_0 and t7–t8 for TS_i); Token Relay (TR: t3–t4 for TS_0 and t8–t9 for TS_i) and Packet Acceptance (PA: t4 for TS_0 and t9 for TS_i). During *Packet Relay* phases, relayer node relays the packet to all eight dedicated directions, while predecessor triggers its WatchDog to monitor relayer's behavior. At *Behavior Evaluation* phase, the predecessor generates "Trust Token" using Algorithm 1. At *Token Relay* phase, the token packet will be relayed by relay. Before receiving the token packet, successor stores packet in packet buffer for a "timeout" period. During *Packet Acceptance* period, the successor makes the decision on whether to accept or drop the packet based on the evaluation results contained in token packet. After that, vehicles change their roles using algorithm 3 to prepare for the next transmission session. The general view of our cooperation enhancement mechanism is illustrated in Figure 2. The flow chart of one transmission session is shown in Figure 3, and the main algorithms are illustrated in Figure 4. The details of each TS are explained in Appendix B.

3.3. Case Study

In this section, two specific scenarios are discussed to verify our proposed cooperation enhancement mechanism: One is in the ideal case in which every vehicle is cooperative and no misbehavior occurs, while the other is where some malicious nodes involved.

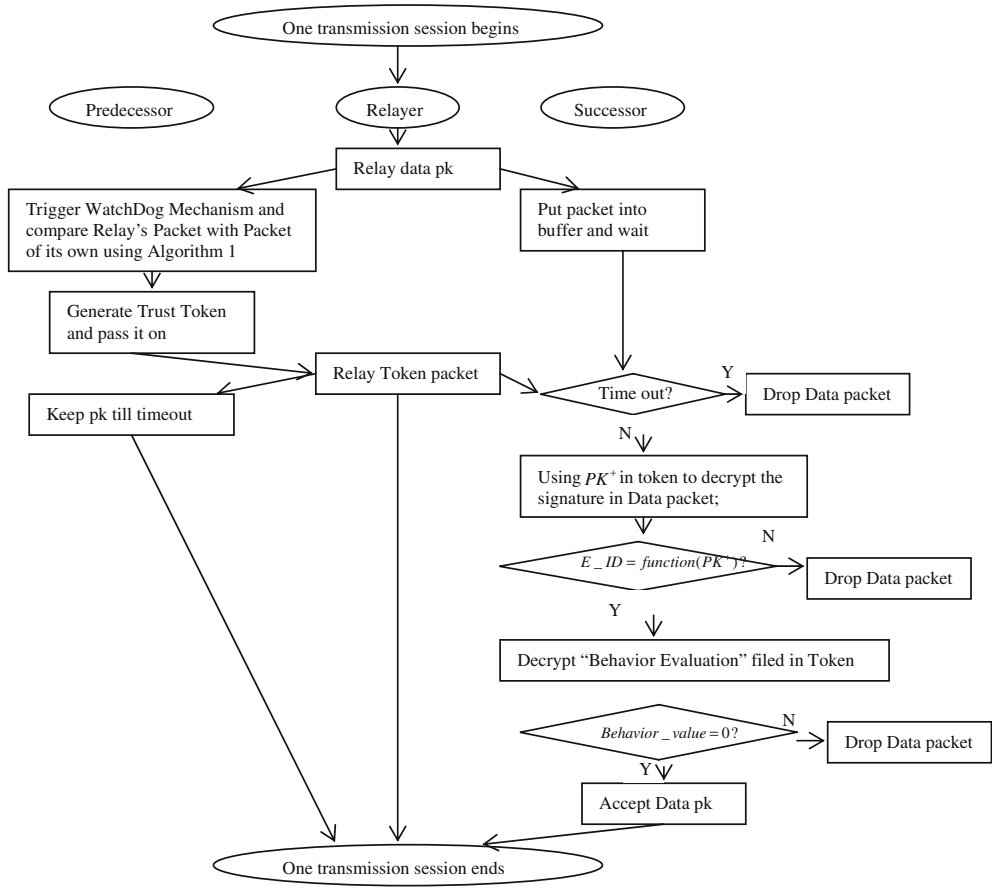


Figure 3. Flow chart of one entire transmission session.

3.3.1. Protocol execution when no misbehavior exists

In this scenario, all the nodes behave well. Thus the behavior evaluations in Trust Token are all TRUE which guarantee that the packets are faithfully and correctly transmitted. As a result, the successors accept the packets.

3.3.2. Protocol execution when misbehavior is detected

In this case, some relayers are not cooperative. Thus the behavior evaluations related to them in Trust Token are FALSE. The successors will therefore drop the packet from these relayers.

3.4. Main Algorithms

There are three algorithms involved in our proposed cooperation enhancement mechanism, as shown in Figure 4.

- *Algorithm. 1* is for WatchDog to evaluate the behavior of current relayers. By comparing whether the packet received from the relayer matches with the one it sent out, the predecessor can judge whether the downstream node has faithfully forwarded the packet or not. If the result matches, it concludes the node to be benign and set its trust value to TRUE.

Algorithm 1: Trust Evaluation

Define: *Plain-text message in the predecessor's packet:* Msg_{PRE}

Plain-text message in the relayer's packet: Msg_{REL}

Trust value of one relayer: $Trust_{REL}$

Begin *Trust Evaluation*:

if ($Msg_{PRE} == Msg_{REL}$) $Trust_{REL} = TRUE$;

else $Trust_{REL} = FALSE$;

End

Algorithm 2: Packet Acceptance Decision

Define: *Packet stored in the successor's buffer:* Msg_{PRE}

Packet decision: $Packet_{Dec}$

Begin *Packet Acceptance Decision*:

if ($PK^{+}_{PRE} = function\ (E\_ID_{PRE})$ && $E\_ID_{PRE} \neq E\_ID_{REL}$

begin

token packet is valid;

if ($Trust_{REL} = TRUE$)

$Packet_{Dec} = Accept$;

else $Packet_{Dec} = DROP$;

end

else

token packet is invalid;

$Packet_{Dec} = DROP$;

End

Algorithm 3: Role Shift

Role in current transmission session	Role in next transmission session
Predecessor	No longer involved
Relayer	Predecessor
Successor	Relayer
Downstream node of successor	successor

Figure 4. Main algorithms.

Otherwise, it concludes the node to be malicious and set its trust value to FALSE. The trust value will be included in the trust token packet.

- *Algorithm 2* is for successors to decide whether to accept one packet or not. First, the successors will check whether the mapping function between E_ID and PK^{+} matches. If they match, the successor will further decrypt the behavior evaluation fields in the trust token packet and check the trust value of each relayer.
- *Algorithm 3* is performed after the successor accepts or rejects the packets. At the next packet transmission session, previous relayer will become the predecessor, previous successor will become the relayer, previous predecessor will not participate in the communication, and the downstream node of previous successor will become the successor.

3.5. Packet Format

Besides the hello packet, two kinds of special packets are involved here. One is the data packet, which reports the data information (e.g., associate with emergency situation). The other is the token packet containing the trust value of the current data packet, containing the trust value of the current packet relayer evaluated by the predecessor. The token packet is used by the successor to evaluate the validity of one data packet. Only those packets forwarded by the trustworthy relayers can propagate in the network.

The format of data and token packet are shown in Figure 5, and the details about each packet are described in Appendix A.

Flag illustrate the packet type: whether it is a data packet (flag = 1), or a token packet (flag = 2), or a token packet (flag = 2).

Data Packet

flag	*Plain Text*	Initiator's signature: $(E\_ID_{ini}, Timestamp_{ini}, Message\_ID_{ini})_{PK^{-}_{ini}}$	Predecessor's signature: $(E\_ID_{pre}, Timestamp_{pre})_{PK^{-}_{pre}}$	E_ID_{rel}	$(E\_ID_{rel}, Timestamp_{rel})_{PK^{-}_{rel}}$

Token Packet

flag	*Behavior Evaluation :* $(E\_ID_{rel_i}, Behavior_{rel_i}...)_{PK^{-}_{pre_i}}$	PK^{+}_{ini}	$PK^{+}_{pre_i}$	$E\_ID_{rel_i}$	$(E\_ID_{rel}, Timestamp_{rel})_{PK^{-}_{rel}}$

Figure 5. Packet format.

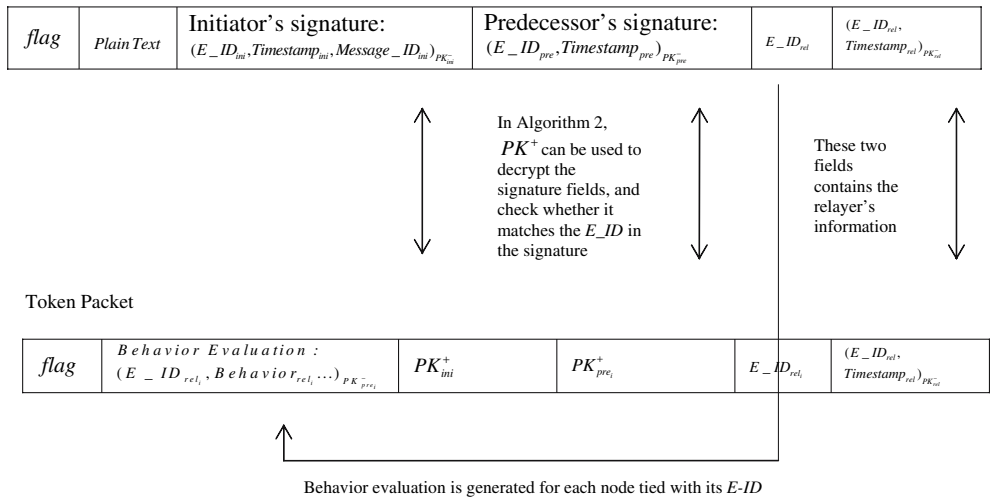


Figure 6. Relationship between data packet and token packet.

In the data packet, *Plain Text* field describes the event, i.e. what happens or what has been detected. *The initiator's signature* field is the constant field within the data packet, indicating who initiates the current transmission session, when it is initiated and what is the packet number. *The predecessor's signature* field indicates who relays the packet and when the current packet is relayed.

In Token packet, PK_{ini}^+ and PK_{pre}^+ fields tie to the initiator's signature and the predecessor's signature fields in the data packet respectively. PK_i^+ is valid only if it matches the corresponding E_ID_i: $(PK_i^+ = \text{function}(E\_ID_i))$. Relayers also append their E_ID_{REL} and digital signatures $(PK_{\text{REL}}^+ = \text{function}(E\_ID_{\text{REL}}))$ with the token packet while relaying. The *Behavior Evaluation* field contains the trust level of the relayer's behavior. To keep consistency of the packet format, relayers also append their E_ID_{REL} and digital signatures $(E\_ID_{\text{rel}}, \text{Timestamp}_{\text{rel}})_{PK_{\text{rel}}^-}$ with the token packet while relaying.

When relaying a packet, each relayer will append its E_ID_{REL} and digital signatures $(E\_ID_{\text{rel}}, \text{Timestamp}_{\text{rel}})_{PK_{\text{rel}}^-}$ with that data packet. E_ID_{rel} is for trust evaluation purpose. The predecessors (WatchDogs) observe the instant behavior of the relayers and include its evaluation results with those E_ID_{REL}s in the *Behavior Evaluation* field of the token packet. The relationship between the two packets is shown in Figure 6.

4. Discussion

In this session, we discuss the details on key management, and the protections of data /token packets.

4.1. Key Management

With the moderate resource constraints, VANETs can partially apply public-key cryptography primitives to implement security services. While lacking the online servers, the efficient key distribution mechanism has to be developed for secure VANET applications.

In [10], the authors suggested that during VANET communications, each vehicle has to store the following cryptographic information: an *electronic identity* (E_ID^*) and *a pair of*

public cryptography key (PK^+/PK^-). E_ID is unique to each vehicle thus one vehicle cannot claim to be the other vehicle. In the security implementation of the WD_TT solution, we propose to derive the public key pair PK^+/PK^- from the corresponding unique E_ID by one particular mapping function: $PK^+ = \text{function}(E\_ID)$. With such mapping function between the E_ID and the public key pair, each vehicle could derive others' public keys through their E_IDs during communications. This is essentially a dynamic key distribution approach.

*E_ID is referred as an Electronic License Plate (ELP) if issued by the government, or alternatively an Electronic Chassis Number (ECN) if issued by the vehicle manufacturer [6].

4.2. Packet Authentication/Protection

The Following sections discuss how to protect the data packet and the token packet during communication.

4.2.1. Data packet authentication

Due to the broadcast nature of the wireless communication, while receiving the relayer's forwarded data packet (the packet sent by the predecessor to be forwarded by relayer), the predecessor can serve as a *WatchDog*, checking the authenticity of the packet forwarded by the relayer, and comparing it with the original packet. *WatchDog* is basically a monitoring mechanism wherein the predecessor node maintains a buffer of the recently sent packets and overhears the transmissions of its downstream relayer node. Based on its observation, the predecessor assigns the trust evaluation of the current relayer been monitored. Only if the relayer' is cooperative can it be grant a Token with a "TRUE" value as its owned trust evaluation. Otherwise, the Token singed by the predecessor will have a "FALSE" value. Based on the trust value, the successor of the packet is able to decide whether to accept the data packet (trust value == TRUE) or to drop it (trust value == FALSE).

4.2.2. Token packet protection

To make it illegal for the relayer node to modify the Token packet, we need to protect the Token packet from being modified by the uncooperative relayer nodes. In our implementation mechanism, this problem is solved by two unique features embedded in our proposed solution and its implementation mechanism described above:

- *Feature 1*: The Data packet and the Token packet cannot be sent by the same node during the same Transmission Session (TS). He Data packet is from the relayer node with the E_ID_{REL} appended, while the Token packet is from the predecessor node with the E_ID_{PRE} appended.
- *Feature 2*: each PK^+/PK^- public key pair is corresponding to one particular E_ID associated with the mapping function.

Based on feature 1, if the relayer generates a new Token packet appending the predecessor's E_ID, it cannot correctly encrypt the plain message since it has no idea about the predecessor's private key PK^-. On the other hand, if the relayer generates a new Token packet applying its own public key pair PK^+/PK^-, it has to append its E_ID according to feature 2. This will, however, certainly result in confliction with feature 1, since the relayer and the predecessor

happen to be the same node. Therefore, there is no way for the relayer to generate a new token packet and satisfy the 2 features at the same time.

5. Performance Evaluation

The overhead of the cryptographic security solution, such as the transmission delay, power consumption, would greatly degrade the system performance. VANET is not subject to severe power restraints since its nodes are energy-rich. However, the simulation results in [1] show that, only 50–60% of a vehicle's neighbors could receive a broadcast message within the tolerable latency, and an upper bound on the processing time overhead $T_{\text{overhead}}(\text{Packet})$ has to be conforming to VANET application requirements. Interested readers please refer Dedicated Short Range Communication (DSRC) [13] for details.

In our mechanism, the time overhead $T_{\text{overhead}}(\text{Packet})$ for each packet includes the duration of generating one packet ($T_{\text{generate}}(\text{Packet})$) which includes the time for packet encryption and digital signature generation, packet transmission time ($T_{\text{transmit}}(\text{Packet})$), and the time for the successor to make decision on whether to accept or drop the data packet ($T_{\text{accept}}(\text{Packet})$). Thus the total time overhead can be calculated as:

$$T_{\text{overhead}}(\text{Packet}) = T_{\text{generate}}\ (\text{Packet}) + T_{\text{transmit}}(\text{Packet}) + T_{\text{accept}}\ (\text{Packet}) \tag{1}$$

There are two kinds of packets used in this mechanism: the data packet and the token packet. They may have different time duration for packet generation, transmission and acceptance. Here, we use the worst case to calculate the upper bound of processing time overhead ($T_{\text{overhead}}(\text{total})$) to evaluate our WD_TT mechanisms:

$$\begin{aligned} &T_{\text{overhead}}(\text{total}) = T_{\text{overhead}}(\text{Data}) + T_{\text{overhead}}(\text{token}) \\ &\leq 2^{*} T_{\text{overhead}}(\text{Packet}) = 2^{*}\{T_{\text{generate}}(\text{Packet}) + T_{\text{transmit}}\ (\text{Packet}) + T_{\text{accept}}(\text{Packet})\}. \end{aligned} \tag{2}$$

Based on this equation, both the size of key/signature/certificate and the execution speeds of the signature generation/verification operation have to be taken into consideration when evaluating the algorithm efficiency.

According to DSRC [13], the safety-related packets should be sent within 100 ms. Thus, the upper bound $T_{\text{overhead}}(\text{Packet})$ should be within this range. Given the minimal data rates in DSRC (6 Mbps) and the typical data rate for safety message (12 Mbps) [11], the process overhead of three public key cryptosystems (PKCS), RSA, ECC (Elliptic Curve Cryptography) and NTRU, are listed in Table 2 [12].

Herein, it can be concluded that the transmission overheads introduced in terms of delay are all within the acceptable scale of VANET applications. Moreover, ECC and NTRU outperform RSA, in that they have smaller key size and faster signing/verification speed. In terms of compactness, ECC is better than NTRU. On the other hand, NTRU is much faster than ECC and consumes less overhead in all.

Table 2. Size and Transmission overhead of three public key cryptosystems

PKCS	Transmission overhead (ms)			
	T_{sign}(ms)	T_{relay}(Sig)(ms)	T_{Verify}(Sig)(ms)	T_{oh}(ms)[a]
RSA	43	8	0.6	102.6
ECC	3.255	7.617	0.019	21.7163
NTRU	1.587	1.488	0.131	6.2810

[a]According to (1), $T_{\text{oh}}(pk) \leq 2^*(T_{\text{sign}}(pk) + T_{\text{relay}}(pk) + T_{\text{verfication}}(pk)$.

6. Conclusion and Future Work

Vehicular Ad Hoc Network (VANET) demands cooperative communication among peer nodes under the operation environment of high mobility, rapidly changing topology and low connectivity redundancy. In this paper, we proposed a dynamic Watch-Dog *Trust-Token* (WD-TT) mechanism to instantly evaluate nodes' packet transmission behaviors based on the first-hand observation. The Trust Token is used to pass the trust evaluation to the downstream successors which can decide whether to accept or drop the packet. With the inherit mapping between the ELP and the public key, digital signature can be used for packet integrity protection. Our proposed mechanism detects and prevents misbehaving nodes from modifying the packet during transmission and guarantees the trustworthiness of packets passing on in VANET.

Our solution is a passive detect-and-react mechanism, which relies on a special MAC protocol: RPB_MAC. Focusing mainly on detecting malicious uncooperative nodes, it prevents packets containing false information from further propagation into the larger scope of the network while maintaining core network performance. However, it lacks incentive to encourage nodes behaving well in the first place, since it neither punishes malicious nodes, nor it rewards well-behaved nodes. On the other hand, the dependence of the WD-TT mechanism to the RPB-MAC protocol limits the deployment of such a mechanism. Indeed, the ultimate solution for cooperation enforcement in VANET should be suitable for the generic lower-layer protocol. In addition, it should be capable of not only passive detect-and-react to the uncooperative nodes, but also have nodes fully motivated for cooperative packet transmission actively. These will be our future research thrusts.

Appendix A. Packet Format

A.1. Data Packet

	Description	Function
Flag	Whether this packet is • Data packet • A token packet	Illustrate packet type
Plain text	Packet contents	report event information

	Description	Function
$(E\_ID_{\text{ini}}, Timestamp_{\text{ini}}, Message_{\text{ini}}\_ID)_{PK^{-}_{\text{ini}}}$	Initiator's digital signature	• Who initiate the packet • When the packet has been initiated • "Tie" with the trust token
$(E\_ID_{\text{pre}}, Timestamp_{\text{pre}})_{PK^{-}_{\text{pre}}}$	Predecessor's digital signature	• Who send the packet to the relayer • When the packet been sent to the relayer • "Tie" with the trust token
E_ID_{Rel}	E_ID of the current relayer	• Who relay the packet • This field is used for trust evaluation
$(E\_ID_{\text{Rel}}, Timestamp_{\text{Rel}})_{PK^{-}_{\text{rel}}}$	Relayer's digital signature	• Who relay the packet • This field is used for trust evaluation

A.2. Token Packet

	Description	Function
Flag	Whether this packet is a: • Data packet • A token packet	Illustrate packet type
$(E\_ID_{\text{Rel}_i}, Behavior_{\text{Rel}_i}; E\_ID_{\text{Rel}_j}, Behavior_{\text{Rel}_j}; ...)_{PK^{-}_{\text{pre}}}$	Behavior evaluation given by the predecessor, using *Algorithm 1*	Each evaluation is corresponding to certain relayer based on theE_ID_{Rel} field of each relaying packet
PK^{+}_{ini}	Public key of the initiator	Corresponding to $(E\_ID_{\text{ini}}, \text{Timestamp}_{\text{ini}})_{PK^{-}_{\text{ini}}}$ field in data packet: PK^{+}_{ini}= function(E_ID_{ini})
PK^{+}_{pre}	private key of the Predecessor	Corresponding to $(E\_ID_{\text{pre}}, \text{Timestamp}_{\text{pre}})_{PK^{-}_{\text{pre}}}$ field in data packet: PK^{+}_{PRE}= function(E_ID_{PRE})
E_ID_{Rel}	E_ID of the current relayer	• Who relay the packet

	Description	Function
$(E\_ID_{\text{Rel}}, \text{Timestamp}_{\text{Rel}})_{PK_{\text{rel}}^-}$	Relayer's digital signature	• This field is used for trust evaluation • Who relay the packet • This field is used for trust evaluation

Appendix B. WD-TT Working Process and Time Sequence

B.1. Transmission Session 0: (Initiator acts as the Predecessor)

t_0 : Initiator (A) detects the emergent event and sends data packet to its immediate followers $B_1B_2B_3$:

Flag	Plain Text	$(E\_ID_A, \text{Timestamp}_A, \text{Message}_{A\_ID})_{\text{PK}_A^-}$	$(E\_ID_A, \text{Timestamp}_A)_{\text{PK}_A^-}$	E_ID_A

$B_1B_2B_3$ become the current relayers.

They modify the packet, replacing E_ID_A with their own E_ID_B

Flag	Plain Text	$(E\_ID_A, \text{Timestamp}_A, \text{Message}_{A\_ID})_{\text{PK}_A^-}$	$(E\_ID_A, \text{Timestamp}_A)_{\text{PK}_A^-}$	E_ID_B

t_1 : $B_1B_2B_3$ relay data packet to all the directions at the same time.
t_2 : Both the Predecessor A and those successors $C_1C_2C_3$ get the packet. A will do "Behavior Evaluation" while $C_1C_2C_3$ put the packet into their packet buffer, waiting for a certain period of time without performing any actions.
A compares the packets (excluded the E_ID field) sent by $B_1B_2B_3$, using *Algorithm 1*.This can be called "*Evaluation by first-hand observation*".
t_3 : A sends the "Trust Token" to $B_1B_2B_3$:

Flag	$(E\_ID_{B_1}, \text{Behavior}_{B_1};$ $E\_ID_{B_2}, \text{Behavior}_{B_2};$ $E\_ID_{B_3}, \text{Behavior}_{B_3})_{PK_A^-}$	PK_A^+	PK_A^+	E_ID_A

$B_1B_2B_3$ modify the "Trust Token" packet by appending their own E_ID

Flag	$(E\_ID_{B_1}, \text{Behavior}_{B_1};$ $E\_ID_{B_2}, \text{Behavior}_{B_2};$ $E\_ID_{B_3}, \text{Behavior}_{B_3})_{PK_A^-}$	PK_A^+	PK_A^+	E_ID_B

$B_1B_2B_3$ relaying the "Trust Token" packet to all the directions at the same time, appending their E-ID and Timestamp:

Flag	$(E\_ID_{B_1}, \text{Behavior}_{B_1};$ $E\_ID_{B_2}, \text{Behavior}_{B_2};$ $E\_ID_{B_3}, \text{Behavior}_{B_3})_{PK_A^-}$	PK_A^+	PK_A^+	E_ID_B	$(E\_ID_B, \text{Timestamp}_B)_{PK_B^-}$

t_4: $C_1C_2C_3$ get the "Trust Token" packet, using *Algorithm 2.*

(1) With thePK_A^+, they can decrypt the behavior evaluation part to see which car behaves well and which car behaves badly.
(2) $C_1C_2C_3$will only take those packets from good nodes (indicated by the $E_ID$field). Others which are sent by bad nodes will be dropped.

B.2. TRANSMISSION SESSION I:

t_5: $C_1C_2C_3$become the relayers, while $B_1B_2B_3$ become the predecessors and $D_1D_2D_3$ become the successors.
Now the relayers hold the data packets and the Trust Token packets (*shown in figure 5*).
t_6: $C_1C_2C_3$ start relaying packet. Now the packet format is:

Flag	Plain Text	$(E\_ID_A, \text{Timestamp}_A \cdot$ $\text{Message}_A\_ID)_{PK_A^-}$	$(E\_ID_B, \text{Timestamp}_B)_{PK_B^-}$	$E\_ID_{C_i}$

Both the Predecessors $B_1B_2B_3$ and successors $D_1D_2D_3$ get the packet $B_1B_2B_3$ will do "Behavior Evaluation" while $D_1D_2D_3$ put the packet into their packet buffer, waiting for a certain period of time without performing any actions.
$B_1B_2B_3$ compares the packets (excluded the E_ID field) sent by $C_1C_2C_3$, using *Algorithm 1.* This can be called "*Evaluation by first-hand observation*".
t_7: $B_1B_2B_3$ send "Trust Token" to $C_1C_2C_3$. $C_1C_2C_3$ will only take the evaluation from good nodes in $B_1B_2B_3$(judged by their E_ID)

Flag	$(E\_ID_{C_1}, \text{Behavior}_{C_1};$ $E\_ID_{C_2}, \text{Behavior}_{C_2};$ $E\_ID_{C_3}, \text{Behavior}_{C_3})_{PK_{B_i}^-(i=1,2,3)}$	PK_A^+	$PK_{B_i}^+$	$E\_ID_{B_i}$

$C_1C_2C_3$ modify the "Trust Token" packet by appending their own E_ID:

Flag	$(E\_ID_{C_1}, \text{Behavior}_{C_1};$ $E\_ID_{C_2}, \text{Behavior}_{C_2};$ $E\_ID_{C_3}, \text{Behavior}_{C_3})_{PK_{B_i}^-(i=1,2,3)}$	PK_A^+	$PK_{B_i}^+$	$E\_ID_{C_i}$

Flag	$(E\_ID_{C_1}, \text{Behavior}_{C_1};$ $E\_ID_{C_2}, \text{Behavior}_{C_2};$ $E\_ID_{C_3}, \text{Behavior}_{C_3})_{PK^-_{B_i}(i=1,2,3)}$	PK^+_A	$PK^+_{B_i}$	$E\_ID_{C_i}$	$(E\_ID_{C_i},$ $\text{Timestamp}_{C_i})_{PK^-_{C_i}(i=1,2,3)}$

t_8: $C_1C_2C_3$ relay the "Trust Token" packet to all the directions at the same time, appending their E-ID and Timestamp:

t_9: $D_1D_2D_3$ get the "Trust Token" packet, using *Algorithm 2*.

(1) With the $PK^+_{B_i}$, they can decrypt the behavior evaluation part to see which car behaves well and which car behaves badly.

(2) $D_1D_2D_3$ will only take those packets from good nodes (indicated by the $E - ID$ field). Others which are sent by bad nodes will be dropped.

B.3. Transmission Session $i+1, i+2, i+3, i+4$:

All the following sessions can be done similarly to *Transmission Session 1*. The only difference is the role of each vehicle is changing.

References

1. J. Blum and A. Eskabdaruab, "The threat of intelligent collision", *IT Professional*, Vol. 6, pp. 24–29, Jan.–Feb. 2004.
2. J. Blum, A. Eskandarian, and L. Hoffman, "Challenges of Intervehicle ad hoc networks", *IEEE Transportation Systems*, Vol. 5, pp. 347–351, Dec. 2004.
3. S. Buchegger and J. Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes-fairness in dynamic ad-hoc networks", in *Proc. of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing* (MoBiHOC), June 2002.
4. C. Chigan and V. Oberoi, and J. Li, "RPBMACn: A relative position based collision-free MAC nucleus for vehicular ad hoc networks". IEEE Globecom 2006, Nov. 2006.
5. F. Dotzer, L. Fischer, and P. Magiera, "VARS: A Vehilce Ad-hoc network Reputation System", sixth *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks* (WoWMoM'05), pp. 454–456, 2005.
6. J. Hubaus, S. Capkun, and J. Luo, "The security and privacy of smart vehicles", *IEEE Security and Privacy Magazine*, Vol2(3), pp. 49–55, May–June 2004.
7. P. Michiardi and R. Molva, "Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks", IFIP-Communication and Multimedia Security Conference, Sept. 2002.
8. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in *Proc. of ACM MobiCom*, 2000.
9. S. Moloney and P. Ginzboorg. "Security for interactions in pervasive networks", in *Proc. of first European Workshop on Security in Ad-Hoc and Sensor networks*, Aug. 2004.
10. M. Raya and J. Hubaus, "The security of vehicular networks", EPFL Tech. Rep. IC/2005/009, March 2005.
11. S. Tahnrich and P.Oreiter, "The buddy system: A distributed reputation system based on social structure", Tech. Rep. 2004-1, Universität Karlsruhe, Faculty of Informatics, March 2004.
12. http://www.scramdisk.clara.net/pgpfaq.html#SubKeysize
13. CAMP Vehicle Safety Communications Consortium, "Vehicle Safety Communications Project: Task 3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC", National Highway Traffic Safety Administration, U.S. Department of Transportation, Washington, DC, 2005.

Zhou Wang received her BS in Radio Engineering Department from Southeast University, Nanjing, China, in 2004. She is currently a MS candidate in electrical engineering at Michigan Technological University. Her research interests are in the areas of security provisioning for Vehicular Ad Hoc Networking (VANET).

Chunxiao (Tricia) Chigan is presently an Assistant Professor of Electrical and Computer Engineering at Michigan Tech, Houghton, MI. Her research interests include information assurance for network systems, dependable computing and communication systems, cross-layer network design, wireless ad hoc and sensor networks, wireless network security, adaptive network protocol design for cognitive radio systems, and network resource allocation and management. Dr. Chigan received the MS and Ph.D. degrees in electrical engineering from the State University of New York, Stony Brook, in 2000 and 2002, respectively.