Proof-of-relevance: Filtering false data via authentic consensus in Vehicle Ad-hoc Networks

Conference Paper · May 2008

DOI: 10.1109/INFOCOM.2008.4544650 · Source: IEEE Xplore

5 authors, including:

Zhen Cao
China Mobile Research Institute
15 PUBLICATIONS **100** CITATIONS
SEE PROFILE

Jiejun Kong
University of Florida
71 PUBLICATIONS **2,919** CITATIONS
SEE PROFILE

Zhong Chen
Peking University
180 PUBLICATIONS **642** CITATIONS
SEE PROFILE

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2008 proceedings.

Proof-of-Relevance: Filtering False Data via Authentic Consensus in Vehicle Ad-hoc Networks

Zhen Cao*, Jiejun Kong†, Uichin Lee†, Mario Gerla†, Zhong Chen*
*School of Electronics Engineering and Computer Science, Peking University, Beijing 100871
{caozhen, chen}@infosec.pku.edu.cn
†Department of Computer Science, University of California, Los Angeles, CA 90024
{jkong, uclee, gerla}@cs.ucla.edu

***Abstract*—Emerging applications in Vehicle Ad hoc Networks (VANETs) not only open tremendous business opportunities and navigation benefits; they also pose formidable research challenges in security provisioning. A critical security threat to VANETs is false data injection, i.e., an attacker disseminates false information to disrupt the behavior of the other drivers. Information driven operations of vehicular networks make false data injection a very effective attack. As the first line of defense, this paper presents the notion of Proof-of-Relevance (PoR), which consists in proving that the event reporter is authentically relevant to the event it has reported. The PoR is accomplished by collecting authentic consensus on the event from witness vehicles in a cooperative way. Event reports from attackers who fail to provide this PoR are disregarded, making the network immune to bogus data. Performance evaluation and security analysis demonstrate the efficiency and security of the proposed scheme.**

I. Introduction

Vehicle Ad-hoc Networks (VANETs) are emerging as a brand new family of envisioned distributed services that will make safety and navigation related applications on vehicles very attractive and readily available. On the one hand, safety related applications such as collision avoidance, cooperative driving and road hazard notification can save lives. In fact, alerts from these applications enable the drivers to react to dangerous conditions such as accidents or bad road conditions, hence reducing the chance of an accident. On the other hand, traffic congestion optimization, payment services and advertisement dissemination strike a good balance between traveling convenience (for the drivers) and potential profit gains for the service providers. These applications not only open tremendous opportunities for the drivers and manufacturers, but also raise formidable research challenges.

One of these challenges is security. It is crucial to make sure that the life critical navigation information in these applications cannot be forged or modified by an attacker. To address the security challenges, various mechanisms in vehicular networks have recently been proposed with emphasis on security design challenges [1], overall architectures [2] and certificate revocations [3]. However, our key observation is that these applications in vehicular networks are especially vulnerable to false data injection attacks where misbehaving vehicles inject bogus information into the network to affect the behaviors of the other drivers for their selfish objectives. In fact, the information dependency of vehicular applications makes this false data injection a very effective attack. For example, in traffic congestion optimization, honest drivers may be misled and driven to congested areas by falsely injected information, while the attacker vehicle can enjoy less traffic on his/her own path. More catastrophically in some safety applications, the drivers may be misled into potential accidents.

A. Our Contributions

The goal of this paper is to investigate techniques to protect the driver against this false data injection attack. First, this paper proposes the notion of Proof-of-Relevance (PoR) as the first step to defend against false data injection in VANETs. Proof-of-Relevance is designed to prove that the vehicle is authentically relevant to the event it has reported. This general notion of PoR can be implemented in various ways. In particular, PoR can be achieved via authentic consensus, constituted by the vehicles collecting digital endorsements from other witnesses in the detecting area. After collecting a number of endorsements to reach a verifiable consensus, vehicles disseminate the information along their routes to notify other drivers. On receiving the information, vehicles can accept and respond only after they have verified all the signatures in the event report. In this way, PoR keeps the network immune to bogus data. Second, it should be noticed that an efficient and secure signature collection protocol is a key component to reach such an authentic consensus. In this work, we borrow the idea of Growth Code [4] to design an efficient and secure signature collection protocol. Finally, we analyze the security of the proposed scheme and use simulation to demonstrate its effectiveness and efficiency.

B. Related Work

Although lots of studies are dedicated to false data filtering in wireless sensor networks [5] [6], they are not applicable to VANETs because they are designed for static sensor networks and those en-route filtering schemes require the use of probabilistic symmetric keys which are hard to pre-distribute and maintain among mobile vehicles with high speed. Several security mechanisms [7] [8] [9] [10] in VANETs have been proposed which are aware of malicious detection and hence are relevant to this paper. The schemes proposed in [7] try to address that a given message indeed originates

978-1-4244-2219-7/08/$25.00 ©2008 IEEE.

from a legitimate vehicle driving on the same lane ahead of the recipient's current location (called Area of Relevance). Messages from vehicles out of the AOR are discarded, but they are not aware of bogus data originating from inside of the AOR. Raya et.al [8] introduce the Misbehavior Detection System to enable the neighbors of a faulty node to detect its deviation from normal behaviors, but it only detects the attackers who enlarge the distance between the event and the victim in their event reports. In [9], a node searches for possible explanations for the collected data and only accepts the data that is consistent with its network model, but there is no further validation to justify this general model. Ostermaier et.al [10] develop four decision making schemes based on voting to evaluate the plausibility of received hazard messages, however their schemes are highly vulnerable to Sybil attacks because of the lack of cryptographical protections. Our Proof-of-Relevance scheme differentiates the aforementioned work in that it provides data authenticity from the source, i.e., if a node fails to prove that it is relevant to the reported event by providing endorsements from the other witnessing vehicles, its report will be discarded.

II. Proof-of-Relevance: Defence against False Data Injection

In this section, we first lay out the assumptions and an overview of the Proof-of-Relevance scheme, and then describe the three procedures including report generation, signature collection and report verification. Then the applicability of the proposed scheme is analyzed in the context of the danger warning application in VANETs. Finally we analyze the security of the scheme.

A. Assumptions

We make the following assumptions: (1) We assume each vehicle possesses an Elliptic Curve Cryptography (ECC) public/private key pair K_V^+ / K_V^- and a certificate $Cert_V$ issued by a trusted authority (which has a public key K_{CA}^+ trusted by all vehicles). (2) Vehicles are not likely to be compromised by attackers, partially because they are physically protected by the driver and partially because of some Tamper Proof Device [2] may exist on vehicles in the near future. (3) Without loss of generality, we assume the property of honest majority, which means a good majority of nodes in vehicular networks are benign and honest. (4) For attackers, we assume they have valid public/private key pairs so that they can generate and sign messages with their valid credentials, which means we are concerned with misbehaving nodes equipped with valid credentials. As assumed in [10], attackers may collude but they do not have out-of-band channels to conceal their colluding activities.

B. Overview

We introduce the notion of Proof-of-Relevance (PoR), which is designed to prove that the vehicle is authentically relevant to the event it has reported. This general notion of PoR can be implemented in various ways. In particular, we propose a PoR based on authentic consensus, which is generated by vehicles collecting digital endorsements from the other witnesses. In this PoR scheme, the event report is considered to reach a verifiable consensus if it has carried enough digital endorsements. The PoR scheme based on authentic consensus includes three phrases of report generation, signature collection and report verification, which are described as below.

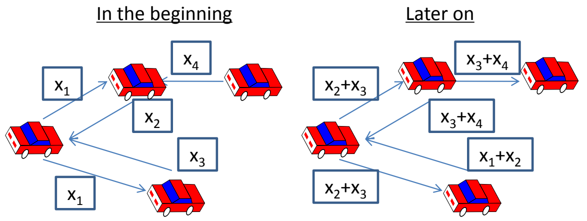

Fig. 1. Signature Collection using Growth Code

C. Report Generation

Once a vehicle detects some event, it generates an event report of the following format $E = \{L_E, D, t\}$, where L_E is the location of the event, D is the event type and t is the event time. The witness vehicle signs and broadcasts the message, so that the message of vehicle V_i with the signature looks like this: $M = E, Cert_{V_i}, Sign(K_{V_i}^-, E)$, where $Sign()$ is the signature algorithm (ECDSA is used in this paper). Since the proposed proof of relevance scheme requires at least T signatures to compose a valid report, the detecting node should try to collect signed messages with respect to the same event broadcasted by the other witnesses. Signature collection protocol is described in the next subsection.

D. Signature Collection using Growth Code

Signature collection is a key procedure in our Proof-of-Relevance scheme. Vehicles detecting the event will participate in the signature collection protocol on the same event until they collect more than T signatures. Since simply broadcasting the signed messages will result into many duplicate transmissions which waste much time and network resource, in this study we consider how to design an efficient signature collection protocol so that more detecting vehicles can collect enough signatures with fewer transmissions.

Growth Code [4] is a kind of erasure code whose degree grows with time initially proposed to enhance data persistence in sensor networks. We borrow the idea of Growth Code to promote the efficiency of the signature collection protocol. There are several advantages of Growth Code that we can take in designing our signature collection protocol. First, by encoding codewords with growing degrees, Growth Code provides a high probability of decoding at the receiving node, hence making each transmission more valuable. Fig.1 depicts the working of signature collection using growth codes. Initially vehicles send and receive low degree codewords which are able to be decoded immediately. Later on, they send and receive codewords with higher degrees which are more valuable than lower degree codewords in recovering more symbols. Second, since Growth Code can be decoded with good opportunities, the receiver can check the newly decoded symbol [1] by verifying the correctness of the signature. In this way, growth codes are resistent to pollution attacks [11] (i.e., injection of large portion of corrupted codewords to suppress successful decoding) which are virulent to common network coding schemes especially random linear codes.

Using growth codes, each node starts from sending the original symbols and decides when to switch to codewords of a higher degree. Suppose $K_1, K_2, \ldots, K_N$ denote the transition points where a node should increase the degree of codewords sent out, e.g., K_1 denotes when having decoded more than K_1 symbols, a node should switch to sending codewords of degree two by randomly choosing two symbols from its set of decoded symbols.

The basic idea of deciding the transition points is: when codewords with a higher degree provide a higher probability of successful decoding, a node should switch to this higher degree. We can arrive at the following lemma to determine K_i. (We prove it in the Appendix)

Lemma 1: If a node has recovered more that $K_i = \frac{iN-1}{i+1}$ symbols, it should switch to sending codewords with degree $i+1$. N is the number of nodes in the detecting area.

Alg.1 describes the signature collection algorithm using growth codes. When receiving the codeword x_i, the node decodes it and stores the newly decoded symbol s_i if it is valid per the signature verification algorithm (Line 2-6), and otherwise drops the codeword (Line 7-9). The node determines the degree of codewords sent out through the computation in Line 10-12 per Lemma.1.

Alg 1 : Signature Collection using Growth Code

```
 1: Receive codeword $x_i$ from neighborhors
 2: if $x_i$ can be decoded right now then
 3:     Decode $x_i$ and get the new symbol $s_i = \{E_i, Cert_i, Sig_i\}$;
 4:     Verify the certification $Cert_i$ and the signature $Sig_i$;
 5:     Drop the packet if verification fails.
 6:     Store the new symbol $s_i$ into decoded set X;
 7: else
 8:     //$x_i$ is duplicate or undecodable right now
 9:     Drop the codeword $x_i$ as unusable;
10: // Determine the best degree $d$ of the codewords to be sent;
11: while ( $\|X\| \geq K_d$ and $d < N$) do
12:     $d$++
13: XORing $d$ symbols randomly chosen from set $X$;
14: Send out the codeword;
```

Finally, after collecting T signed messages, the vehicle could generate the final report as below. (Note as well: since different reports are not accurately the same with respect to the time and location, $E_{i_1}, \ldots, E_{i_T}$ cannot be combined although they are all about the same event type.)

$$Report = \{E_{i_1}, Cert_{i_1}, Sig_{i_1}, \ldots, E_{i_T}, Cert_{i_T}, Sig_{i_T}\} \quad (1)$$

After collecting enough endorsements for the event, the detecting nodes can broadcast their final reports to notify the other vehicles on their ways. Since detecting nodes may travel in different directions, the scheme that each detecting node acts as an event reporter will help diffuse the information far and wide.

The choice of the parameter T is a trade-off between detection power and overhead. Here we present two example criteria for the choice of T. The first one is based on the importance of the report. If the report is a safety alert regarding to braking or accelerating, a larger T is required. If the report is a traffic alert, a smaller threshold value is enough. Also, the regular inspection of the authority may help to determine the network status. The authority agency could provide information on how to determine the threshold based on their investigation of the network status.

E. Report Verification and Decision

When a node receives a report, it first examines whether there are enough signatures in the report. Reports with less than T signatures will be discarded. If there are T signatures, the node goes on to validate each signature in the report using the corresponding public key. If any of the T signatures is incorrect, the packet will be discarded. If all the T signatures are checked as valid, the vehicle will accept the message and react according to the event type.

F. Applicability

The Proof-of-Relevance scheme, which is a general solution to defend against false data attacks in mobile networks, can be applied to various applications in VANETs. We will analyze the applicability of our PoR scheme in the danger warning application. Danger warning is an important and useful application of VANETs [10], which consists in vehicles exchanging road condition, hazard and accident information to enhance the safety driving in a predictable way. Security is a big concern in this application. It is especially vulnerable to false data injection attacks in that false warning messages can disturb the behavior of benign drivers. Conventional security mechanisms like authentication and encryption cannot prevent this attack because they cannot deal with false data injection attackers equipped with valid credentials.

Proof-of-Relevance can prevent false data injection attacks in the danger warning system by providing the data authenticity via the authentic consensus. When detecting an event and before sending the warning message, the vehicle will spend some time collecting digital endorsements from the other witness vehicles on the same event. After collecting enough signatures, the vehicle will generate the final warning message with the authentic consensus to alert the other vehicles in the network. The vehicles receiving the warning message will verify the authentic consensus and accept it only if verification succeeds. In this way the Proof-of-Relevance via authentic consensus makes the network immune to false data injection attacks.

[1] In our scenario, each symbol is in the form of a signed message denoted as $M = E, Cert_{V_i}, Sign(K^-_{V_i}, E)$, and each codeword is the XOR of d symbols, while d denotes the degree of the codeword

Although we have assumed the property of honest majority, this does not rule out the possibility of colluding attacks where more than T attackers collude to generate a false report. In the danger warning system, there are two mechanisms introduced to prevent colluding attacks. The first one is to introduce a "revocation report." Since the colluders must participate in the signature collection (we assume the non-existence of out-of-band channel), once a legitimate node detects some colluders are exchanging signatures about a fake event (different from its own observation), it generates a revocation report of the event to counter the fake report. The second mechanism is called "delayed decision", which means the receivers will not respond to one warning message immediately but delay their decisions until they are approaching a specific "decision area." (i.e., in close proximity to the event's location). During the delay, the receiver will continue to collect the authentic consensus. If and only if it has received more warning messages than revocation messages, it will accept and react to the warning message, and otherwise disregard it. Because of the property of honest majority, averagely the recipient will receive more revocation reports than fake reports, hence resistant to this attack. This method is quite effective to defend against colluding as shown in our simulation result in the next section.

G. Security Analysis

The security of the proposed PoR scheme can be reviewed as the probability of the event reporter being an attacker given its report has been endorsed by T peers, i.e., the posterior probability $P(A \mid O_1, \ldots, O_T)$, where A means the reporter is an attacker and O_i denotes the fact that the *i*-th signature in the report is valid. Using Bayesian formula, we can easily obtain the following lemma. (We prove it in the Appendix)

Lemma 2: $P(A \mid O_1, \ldots, O_T) = \frac{1}{1+2^{KT} \cdot \frac{P(\overline{A})}{P(A)}} < 2^{-KT}$, where K denotes the key strength of the signature scheme.

Lemma.2 indicates that the failure probability of our PoR scheme is negligible with respect to the key strength of the signature scheme. Besides, the PoR based on authentic consensus is immune to Sybil attacks where the nodes claim to have multiple identities, because Sybil nodes are unable to forge the authentic consensus without private keys even if they can claim to have multiple identities. We also prevent the PoR scheme from colluding attacks via the delayed decision and revocation report as introduced in Sec. II-F.

III. Simulation Evaluation

We base our simulation on a random topology generated by a VANET mobility generator [12] in an $1000 \times 1000 m^2$ area. In our simulation, we have considered two different scenarios for the signature collection protocol. The first one is the dense scenario with many vehicles as detectors, for example in traffic jams. The second one is the sparse scenario with much fewer detectors, such as a road hazard happening in the early morning. Without loss of generality, we have simulated 144 nodes and 12 nodes in these two scenarios respectively. In the simulation, each vehicle has a 300 meters broadcast range and broadcasts a packet every 0.1 second. We summarize our evaluation results as below.

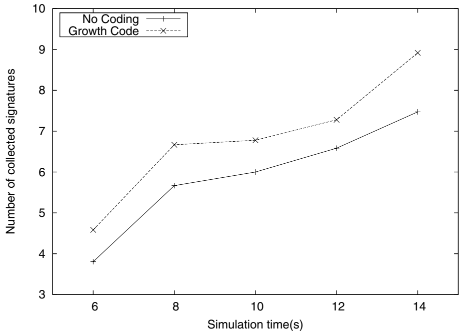

Fig. 2. Average number of collected signatures v.s. Simulation time in the sparse scenario

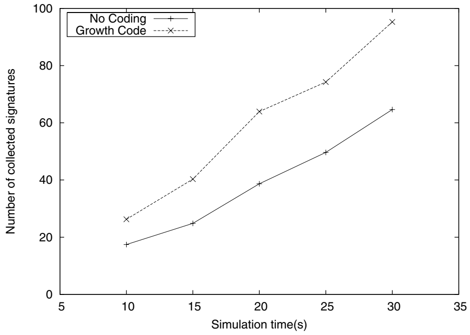

Fig. 3. Average number of collected signatures v.s. Simulation time in the dense scenario

Efficiency of signature collection. Our signature collection protocol outperforms simple flooding protocol. Fig.2 and Fig.3 depict the average number of signatures collected versus the elapsed time in our simulation in sparse and dense scenarios respectively, which demonstrates around 10% and 50% enhancements respectively. Fig.4 and Fig.5 indicate the average number of collected signatures versus the average number of codewords in sparse and dense scenarios respectively, in which we can see the signature collection using growth codes could help the vehicles collect more signatures with fewer transmissions.

Comparison with existing schemes. In SEF [5] and IHA [6] , only one elected Center-of-Stimulus (CoS) is responsible for collecting the Message Authentication Codes (MAC) from the neighborhood. If only the CoS is responsible for report collection, the event report will not propagate in the network as quickly as our Proof-of-Relevance scheme. Fig.6 depicts the percentage of nodes that have been notified in the network versus the simulation time. Compared with false data filtering schemes SEF and IHA in sensor networks, our PoR scheme is able to make more drivers aware of the danger. We also simulate the PoR scheme in the danger warning system compared with voting based schemes in [10]. Fig.7 depicts the percentage of false decisions versus the percentage of attackers in the network (we only find one false decision when 40% of

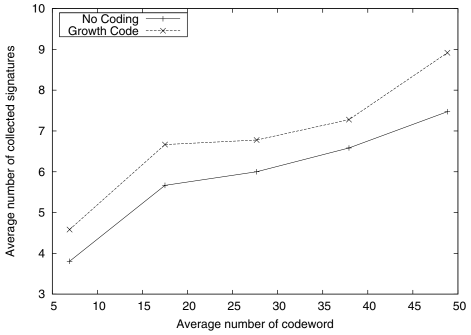

Fig. 4. Average umber of collected signatures v.s. Average number of codewords sent in the sparse scenario

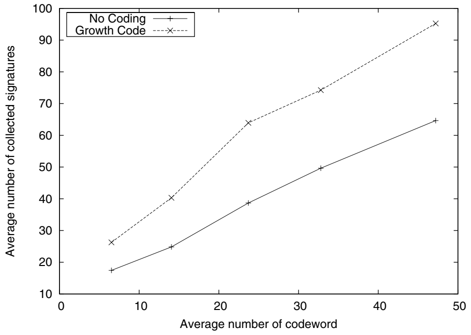

Fig. 5. Average umber of collected signatures v.s. Average number of codewords sent in the dense scenario

nodes are attackers), which shows our scheme is resistant to colluding attacks and also even better than the most effective case in ODS's scheme [10].

Overhead. The packet overhead mainly comes from the list of signatures. In this study, we choose Elliptic Curve Digital Signature Algorithm (ECDSA) since it is one of the most acceptable signature schemes in VANETs per the analysis in [13]. For the 20-byte signature and the 84-byte ECDSA signed certificate and the report with l bytes, each codeword sums up to $(104+l)$ bytes. Per Equation.1, the length of the final report is $(l+104)T$ bytes, which will not cause much burden on the protocol for the small T.

IV. Conclusion

This paper proposes the notion of Proof-of-Relevance to defend against false data injection attacks in VANETs. PoR is achieved via authentic consensus, in which each event detector collects a number of signatures from the other witnessing nodes and generates the final report with the authentic consensus to notify the other drivers. This PoR via authentic consensus represents the first step towards building resilient vehicular networks that can filter bogus data intentionally injected by misbehaving nodes. Our plan for the next step includes evaluation of our scheme in realistic applications of vehicular networks and use of formal specifications to analyze its security.

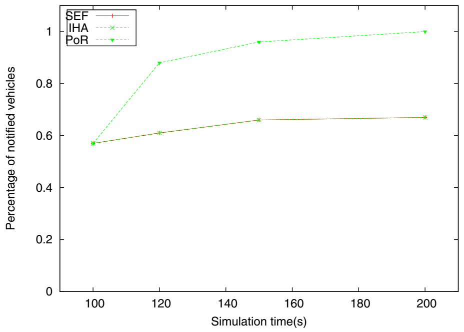

Fig. 6. Comparison with SEF and IHA

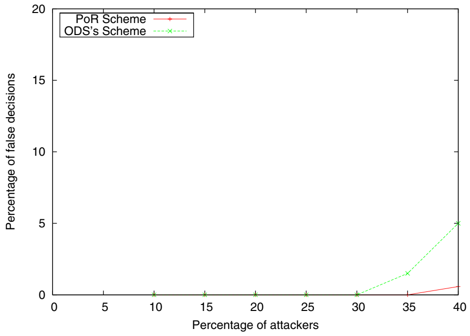

Fig. 7. Comparison with ODS's scheme

V. Acknowledgement

This work is partially supported by the National Natural Science Foundation of China under Grant No. 60773163. We thank the anonymous reviewers for their valuable comments.

References

[1] Bryan Parno and Adrian Perrig, "Challenges in securing vehicular networks," in *Proceedings of ACM Hotnet*, 2005.

[2] Maxim Raya and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, pp. 39–68, 2007.

[3] Ashwin Rao, Ashish Sangwan, Arzad Kherani, Anitha Varghese, Bhargav Bellur, and Rajeev Shorey, "Secure v2v communication with certificate revocations," in *Proceedings of IEEE Workshop on MObile Networking for Vehicular Environments (MOVE'07)*, 2007.

[4] Abhinav Kamra, Jon Feldman, Vishal Misra, and Dan Rubenstein, "Growth codes: Maximizing sensor network data persistence," in *Proceedings of ACM Sigcomm*, Pisa, Italy, September 2006.

[5] Fan Ye, Haiyun Luo, Songwu Lu, and Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," in *Proceedings of Infocom*, Hongkong, March 2004.

[6] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data injection in sensor networks," in *Proceedings of IEEE Symposium on Security and Privacy*, 2004.

[7] Ahren Studer, Mark Luk, and Adrian Perrig, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs," in *Proceedings of 3rd International Conference on Security and Privacy in Communication Networks (SecureComm'07)*, Sept. 2007.

[8] Maxim Raya, P. Papadimitratos, Imad Aad, Daniel Jungels, and J.P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *To appear in IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, 2007.

[9] Philippe Golle, Dan Greene, and Jessica Staddon, "Detecting and correcting malicious data in vanets," in *Proceedings of ACM Workshop on VANET*, October 2004.

[10] Benedikt Ostermaier, Florian Dotzer, and Markus Strassberger, “Enhancing the security of local dangerwarnings in vanets - a simulative analysis of voting schemes,” in *Proceedings of IEEE International Conference on Availability, Reliability and Security (ARES’07)*, 2007.

[11] Zhen Yu, Yawen Wei, Bhuvaneswari Ramkumar, and Yong Guan, “An efficient signature-based scheme for securing network coding against pollution attacks,” in *Proceedings of IEEE INFOCOM 2006*, USA, April 2008.

[12] “Vanetmobisim,” http://vanet.eurecom.fr/.

[13] Maxim Raya and Jean-Pierre Hubaux, “The security of vehicular ad hoc networks,” in *Proceedings of the ACM Workshop on Security in Adhoc and Sensor Networks (SASN’05)*, 2005.

Appendix

We present the proofs of Lemma.1 and Lemma.2 here.

Proof of Lemma.1. Let $\rho_{r,d}$ represent the probability of successfully decoding a codeword with degree *d* when a node has already recovered *r* symbols. The number of ways of choosing a degree d codeword such that the component symbols are distinct and are spread uniformly randomly is $\binom{N}{d}$. There are r recovered symbols and $N - r$ unrecovered symbols. For a degree d codeword, the number of ways of choosing 1 component from the $N - r$ unrecovered symbols is $N - r$. Similarly, the number of ways of choosing $d - 1$ components from the set of r recovered symbols is $\binom{r}{d-1}$. Hence, the probability that for a degree *d* codeword, $d - 1$ components are from the set of *r* recovered symbols and 1 from the set of $N - r$ unrecovered symbols is $\rho_{r,d} = \frac{\binom{r}{d-1}(N-r)}{\binom{N}{d}}$.

The basic idea of deciding the transition points is: when codewords with a higher degree provide a higher probability of a successful decoding, a node should switch to this higher degree. Namely, if $\rho_{r,i} < \rho_{r,i+1}$, a node should switch to sending codewords of degree $i + 1$.

$$\begin{aligned} \rho_{r,i} &< \rho_{r,i+1} \\ \Leftrightarrow \frac{\binom{r}{i-1}(N-r)}{\binom{N}{i}} &< \frac{\binom{r}{i}(N-r)}{\binom{N}{i+1}} \\ \Leftrightarrow \frac{N-i}{i+1} &< \frac{r-i+1}{i} \\ \Leftrightarrow r &> \frac{iN-1}{i+1} \end{aligned}$$

That’s to say, if a node has recovered more that $\frac{iN-1}{i+1}$ symbols, it should switch to sending codewords of degree $i+1$ because they are able to be decoded with a higher probability. □

Proof of Lemma.2. In the following deduction, the two hidden variables for $P(O_1, \ldots, O_T)$ are $h_1 = A$ and $h_2 = \overline{A}$, denoting attacker and non-attacker. Since we have assumed that an attacker has no way of compromising the public key cryptography other than brute force, the probability of an attacker fabricating a signature is 2^{-K} independently. Note as well here we do not analyze the possibility of colluding attacks.

$$\begin{aligned} P(A \mid O_1, \ldots, O_T) &= \frac{P(A, O_1, \ldots, O_T)}{P(O_1, \ldots, O_T)} \\ &= \frac{P(O_1, \ldots, O_T \mid A)P(A)}{\sum_{i=1}^{2} P(O_1, \ldots, O_T \mid h_i)P(h_i)} \\ &= \frac{2^{-KT}P(A)}{2^{-KT} \cdot P(A) + P(\overline{A})} \\ &= \frac{1}{1 + 2^{KT} \cdot \frac{P(\overline{A})}{P(A)}} \end{aligned} \qquad (2)$$

Let $\alpha = \frac{P(\overline{A})}{P(A)}$. From the assumption of honest majority, we know that $\alpha > 1$, so we have

$$\begin{aligned} P(A \mid O_1, \ldots, O_T) &= \frac{1}{1 + 2^{KT} \cdot \frac{P(\overline{A})}{P(A)}} \\ &< \frac{1}{1 + 2^{KT}} < 2^{-KT} \end{aligned}$$

For ECDSA algorithm with 20-byte key, $K = 160$. So from Lemma.2, we can see that $P(A \mid O_1, \ldots, O_T)$ should be very small ($< 2^{-160T}$), which demonstrates the effectiveness of the proposed proof of relevance scheme.□