Trustworthy Data Communication in VANET

Sabah Suhail, Shashi Raj Pandey, *Choong Seon Hong
Department of Computer Engineering,
Kyung Hee University,
Yongin, 446-701 Korea
Email: sabah,shashiraj,cshong@khu.ac.kr

M. Ali Lodhi
Department of Computer Science,
COMSATS Institute of Information and Technology,
Sahiwal, Pakistan
Email: alilodhi30@googlemail.com

***Abstract*—Vehicular ad hoc networks (VANETs) rely heavily on node-to-node communication to provide services including road safety and vehicle security. The data being communicated by the nodes is crucial for correct decision-making. However, due to ease of information access, a malicious adversary may forge the data. Therefore, assuring high data trustworthiness is important. Data provenance plays a key role in evaluating the trustworthiness of data. In this paper, we have presented a provenance-based scheme to ensure the integrity of data in VANET. The scheme works by embedding provenance information as an identity of participating vehicles and path traversed by the packet. We have evaluated the performance of the proposed scheme in terms of energy consumption and delay.**

Keywords—provenance, trustworthiness, VANET

I. Introduction

Vehicular ad hoc networks (VANETs) refer to a set of smart vehicles used on the road that provide communication services among vehicles and roadside equipment (Road Side Unit-RSU) based on wireless Local Area Network (LAN) technologies [1]. The message exchange among communicating vehicles leads to various advantages including conveying the emergency message (accidents, road warnings), traffic management, automated toll payment, location-based services (tracking nearby restaurants, fuel stations) and infotainment [2].

However, the communication among vehicles may raise the question about *how vehicles can ensure that the data does not tamper with its way and the message being communicated is reliable*. For instance, if we consider a military surveillance system where vehicles communicate with each other in order to update the information, for instance, tracking of surplus or other resources. The vehicles propagate the supplies information to the other vehicles or to the RSU infrastructure and make decisions accordingly, for instance, military supply and logistics. To address such issues, it is important to keep track of the messages along with the identity of the vehicles participating in communication through *Provenance*. Provenance is a metadata describing the complete lineage of data and processes chain [4]–[6]. Provenance being beneficial in auditing, debugging, performance evaluation, result reproducibility, forensics investigation and quality assessment have been extensively used in various domains including databases, scientific work-flows, distributed systems, and networks [7]. The rationale behind using provenance-aware framework for VANET is to enable the communicating entries (vehicles and RSU) to ensure the trustworthiness of data.

The main contribution of this paper is to devise a provenance-aware trustworthy data model for VANET that is capable of identifying integrity of messages based on hash-based provenance meta-data.

The paper is organized as follows. Section 2 discusses the system model and Section 3 explains the working of the proposed methodology. Section 4 shows simulation results. Finally, Section V concludes the paper with future work.

II. System Model

A. Network Model

The network is modeled as a graph $G(V, E)$ where V= $\{v_i \mid 1 \leq i \leq |V|\}$ represents a set of vehicles participating in the network, and E represents a set of edges, containing an element $\{e_{i,j} : i \neq j\}$ for each pair of vehicles v_i and v_j that are either communicating with each other (V2V) or vehicle v communicating with RSU $\mathcal{R}$ (V2I). The RSU assign each vehicle a vehicle id $\mathcal{V}_{\mathcal{ID}}$ and a secret key K_s.

B. Data Model

The data packet d_p consist of three fields including sequence number S, data d, provenance information $\mathcal{P}$.

C. Provenance Model

The provenance data consist of information about traversed path T_{path} by data packet d_p and identity of participating vehicles V_ω. The provenance data $\mathcal{P}$ can be defined as:

$$\mathcal{P}_{\mathcal{D}} = V_\omega + T_{path} \tag{1}$$

III. Provenance Scheme for VANET

Scenario:

Consider a war zone where assigned vehicles $\mathcal{V}$ at different locations $\mathcal{L}$ have to disseminate pivotal information $\mathcal{P}$ about surrounding events, food supplies, and other resources. Each vehicle v_i residing in a particular location l_i forward the information either to its neighboring vehicle node or to the RSU $\mathcal{R}$. The Information collected by RSU is being verified and convey to the headquarters who make critical decisions and execute their strategies accordingly. The vehicles may also verify the information if required.

*Dr. CS Hong is the corresponding author.

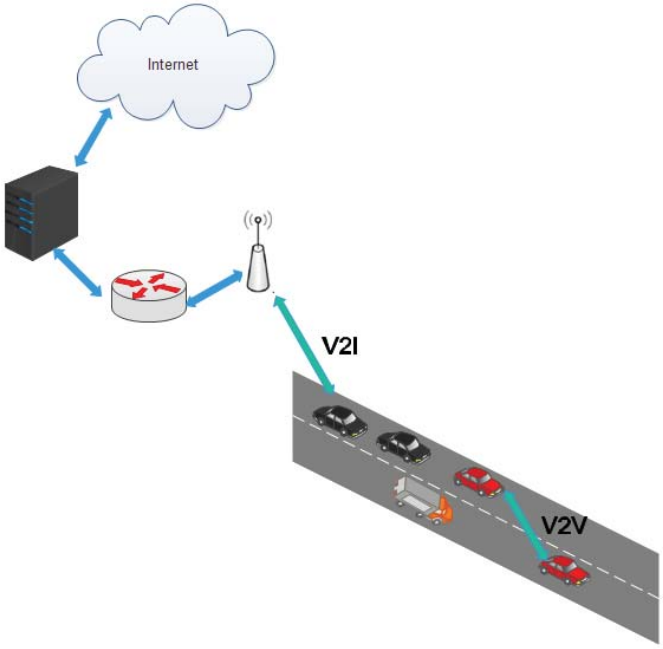

Fig. 1. VANET architecture

A. Provenance Embedding

In order to embed the provenance data $\mathcal{P}$ in d_p, the source vehicle v_s compute the hash of its id $\mathcal{H}(\mathcal{V}_{\mathcal{ID}})$ and forward it to the neighboring vehicle node v_n. The receiving node attaches the hash of its own node ID to the $\mathcal{P}$ and forwards the d_p to other neighboring vehicles or RSU.

$$P_{data} = \mathcal{H}(CUR_{VID})||\mathcal{H}(PRE_{VID}) \quad (2)$$

Thus, the v_n can either forward it to subsequent neighboring node or verify the message as discussed in Case I of Section III-B until the message arrives at destination D.

B. Provenance Verification

Case I: : Verification by $\mathcal{V}$
Consider a scenario in which a vehicle v has to take a decision by accumulating information from any one v_n vehicle or more than one vehicles v_{n+m}. Under such circumstances, the vehicle has to verify the trustworthiness of provenance data to ensure precise decision making.

Case II: : Verification by $\mathcal{R}$
Each vehicle v_i forward data d including the provenance data $\mathcal{P}$ to its neighboring vehicles until it reaches the RSU $\mathcal{R}$. The $\mathcal{R}$ verifies the p_{data} containing the identity of vehicle and packet path traversed.

IV. Simulation

We run our experiments on Cooja [8]-a Contiki based simulator. For our simulations, we use Tmote sky as things. A Tmote sky has a CCC2420 transceiver and 48kB of ROM. We have run simulations for 10 minutes. Fig.3 and 4 report the results after an interval of 1 minute that is required to converge the topology. All simulations are run 5 times and average results are presented.

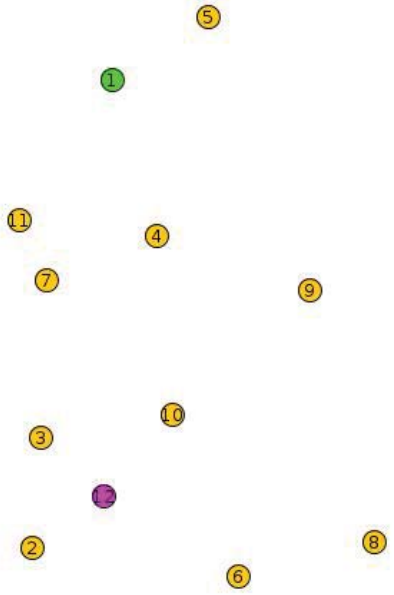

Fig. 2. Network Configurations

To evaluate the working of the proposed scheme for VANET, we consider 10 source nodes (from node 2 to node 11) where node 1 is sink node. To demonstrate the trustworthiness of the proposed scheme, we consider a malicious node $\mathcal{V}_{\mathcal{M}}$ (res presented as node 12). 6→12→10→4→1 (see fig.2). Node 12 may intent to perform any attack in the hope to forge or modify data, for example, data tampering by injecting false messages or fabricating messages [9], [10]. When the packet along with provenance data arrives at sink node 1, it verifies the packet path as discussed in section III-B.

A. Delay

One of the important requirement of VANETs applications is related to the nodes ability to transmit messages within an acceptable time constraint [11]. To justify this feature we have evaluated the scheme in terms of delay. We compute the delay between data packet sent (P_S) and received (P_R) with and without provenance hash scheme.

$$Delay = P_R - P_S \quad (3)$$

The results in fig 3 shows that delay caused at the cost of data integrity is negligibly small.

B. Energy Consumption

Energy consumption is also an important issue in VANET. Therefore, we measure energy consumption with and without provenance hash scheme. We have used the nominal values of the Tmote sky [12]. To compute the energy, we have followed

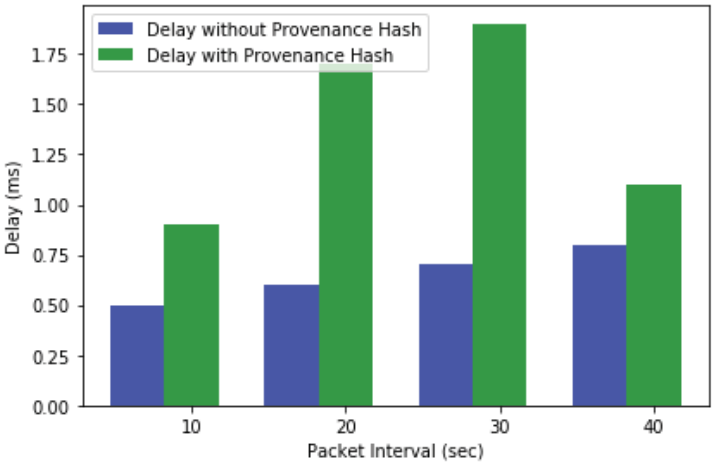

Fig. 3. Comparison of Delay between without hash provenance and with hash provenance

equation [13]

$$Energy(mJ) = (Tx * 19.5mA + Rx * 21.8mA + CPU * 1.8mA + LPM * 0.0545) * 3V/4096 * 8 \quad (4)$$

where as Tx and Rx represent the values for transmitter and receiver respectively.
The results in fig 4 shows that the energy consumed after applying hash provenance is not much as compared to without hash provenance.

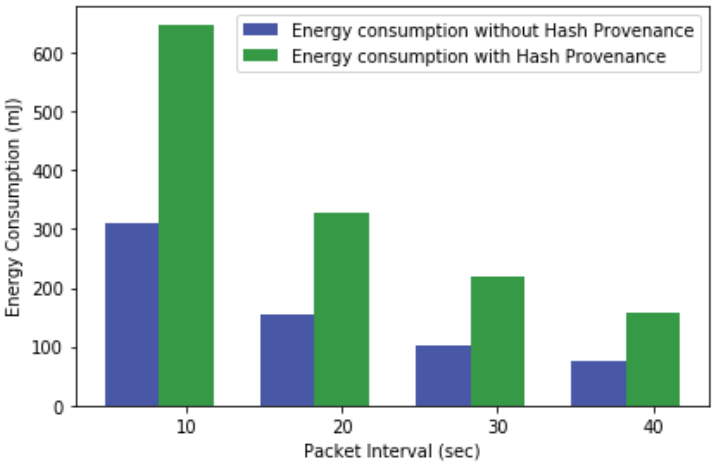

Fig. 4. Comparison of Energy Consumption between without hash provenance and with hash provenance

V. Conclusion

In this paper, we have presented a provenance-based scheme to ensure the trustworthiness of data in VANET. The scheme works by embedding provenance information as an identity of participating vehicles and path traversed by the packet. We have evaluated the performance of the proposed scheme in terms of energy consumption. In future, we would like to incorporate other requirements of provenance in addition to data integrity.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2015-0-00274, Development of Smart Mediator for Mashup Service and Information Sharing among ICBMS Platform).

This work was supported by the Industrial Core Technology Development Program(10049079, Development of Mining core technology exploiting personal big data) funded by the Ministry of Trade, Industry and Energy (MOTIE, Korea).

References

[1] Engoulou, R.G., Bellache, M., Pierre, S. and Quintero, A., 2014. *"VANET security surveys"*. Computer Communications, 44, pp.1-13.

[2] Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A. and Hassan, A., 2012.

[3] "Vehicular ad hoc networks (VANETS): status, results, and challenges". Telecommunication Systems, 50(4), pp.217-241.

[4] Suhail, Sabah, and Choong Seon Hong. *"A Secure Provenance-Aware Model for Internet of Things"*. (2016): 1154-1156.

[5] Sabah Suhail, Choong Seon Hong, Abid Khan et al. *Introducing Secure Provenance in IoT: Requirements and Challenges*. The Int. Workshop on Secure Internet of Things) SIOT 2016), held in Conjunction with ESORICS 2016.

[6] Sabah Suhail, Choong Seon Hong, M. Ali Lodhi, Faheem Zafar, Abid Khan and Faisal Bashir *"Data Trustworthiness in IoT"* 2018 International Conference on Information Networking (ICOIN) (in-press)

[7] Zafar, F., Khan, A., Suhail, S., Ahmed, I., Hameed, K., Khan, H.M., Jabeen, F. and Anjum, A., *"Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes"*. Journal of Network and Computer Applications, 94, pp.50-68.

[8] Osterlind, Fredrik, et al. *"Cross-level sensor network simulation with cooja"*. Local computer networks, proceedings 2006 31st IEEE conference on. IEEE, 2006.

[9] Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A. and Hassan, A., 2012. *"Vehicular ad hoc networks (VANETS): status, results, and challenges"*. Telecommunication Systems, 50(4), pp.217-241.

[10] Sumra, I.A., Hasbullah, H.B. and AbManan, J.L.B., 2015. *"Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey"*. In Vehicular Ad-Hoc Networks for Smart Cities (pp. 51-61). Springer, Singapore.

[11] X. Yang, L. Liu, N.H. Vaidya, F. Zhao, *"A vehicle-to-vehicle communication protocol for cooperative collision warning"*. The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004, pp. 114123.

[12] Tmote Sky Datasheet http://www.sentilla.com/pdf/eol/tmote-skydatasheet. pdf.

[13] Raza, Shahid, Linus Wallgren, and Thiemo Voigt. *"SVELTE: Real-time intrusion detection in the Internet of Things"*. Ad hoc networks 11.8 (2013): 2661-2674.