8-2017

On the Security of Information Dissemination in the Internet-of-Vehicles

Danda B. Rawat
Howard University

Moses Garuba
Howard University

Lei Chen
Georgia Southern University, lchen@georgiasouthern.edu

Qing Yang
Montana State University-Bozeman

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 09/09 pp437–445
Volume 22, Number 4, August 2017

On the Security of Information Dissemination in the Internet-of-Vehicles

Danda B. Rawat*, Moses Garuba, Lei Chen, and Qing Yang

Abstract: Internet of Vehicles (IoV) is regarded as an emerging paradigm for connected vehicles to exchange their information with other vehicles using vehicle-to-vehicle (V2V) communications by forming a vehicular ad hoc networks (VANETs), with roadside units using vehicle-to-roadside (V2R) communications. IoV offers several benefits such as road safety, traffic efficiency, and infotainment by forwarding up-to-date traffic information about upcoming traffic. For instance, IoV is regarded as a technology that could help reduce the number of deaths caused by road accidents, and reduce fuel costs and travel time on the road. Vehicles could rapidly learn about the road condition and promptly respond and notify drivers for making informed decisions. However, malicious users in IoV may mislead the whole communications and create chaos on the road. Data falsification attack is one of the main security issues in IoV where vehicles rely on information received from other peers/vehicles. In this paper, we present data falsification attack detection using hashes for enhancing network security and performance by adapting contention window size to forward accurate information to the neighboring vehicles in a timely manner (to improve throughput while reducing end-to-end delay). We also present clustering approach to reduce travel time in case of traffic congestion. Performance of the proposed approach is evaluated using numerical results obtained from simulations. We found that the proposed adaptive approach prevents IoV from data falsification attacks and provides higher throughput with lower delay.

Key words: Internet of Vehicles (IoV); VANET security; IoV security; VANET; data falsification attacks

1 Introduction

The data released by the National Highway Traffic Safety Administration (NHTSA) in 2014 show a total number of 32 675 fatal crashes in the United States. It can also be found in the same set of data that 2.3 million injuries from vehicle accidents were reported in the same year[1]. In addition to lives and injuries, two other major losses on road are time and cost of fuel, which are typical in cities and metropolitan areas where commuters suffer from great amount of time loss due to traffic congestion and road conditions during peak time for their weekday commuting. A study released in 2015 by the Texas A&M Transportation Institute indicates that annually the U.S. suffers a loss of $140 million due to time and fuel wasted in traffic congestion, and on average each commuter spends an extra 42 hours and wastes 19 gallons of fuel caused by traffic and road conditions[2]. These problems could be reduced or minimized by implementing communications in IoV for exchanging traffic information. Specifically, IoV is

• Danda B. Rawat and Moses Garuba are with the Department of Electrical Engineering & Computer Science at Howard University, Washington, DC, USA. E-mail: db.rawat@ieee.org, mgaruba@howard.edu.
• Lei Chen is with the Department of Information Technology, Georgia Southern University, Statesboro, GA 30458, USA. E-mail: lchen@georgiasouthern.edu.
• Qing Yang is with Department of Computer Science at Montana State University, Bozeman, MT, USA. E-mail: qing.yang@montana.edu.
* To whom correspondence should be addressed.
Manuscript received: 2016-11-26; revised: 2017-01-06; accepted: 2017-01-10

meant to be primarily for improving road safety, traffic efficiency, and infotainment applications on the road where vehicles transmit and receive critical roadway and traffic updates based on their current travel route and information received from surrounding vehicles and roadside units.

To support vehicular communications using V2V and V2R, there is a Dedicated Short Range Communication (DSRC) enabled IEEE 802.11p technology that allows On Board Units (OBUs) exchange information using vehicular networks in IoV. In IoV, private information of owners/drivers/renters is directly linked to vehicles. Security and privacy-aware communications are essential components to protect IoV and concerned authorities. Falsified data transmitted over the VANET can be detrimental to lives of drivers and passengers. In this paper, we investigate data manipulation attack in IoV for enhancing overall throughput and reducing end-to-end delay during information dissemination.

Related work: Recent related works include cryptographic hash chains to authenticate IoV users[3,4], trust-based security to protect vehicular network[4,5], location-based vehicular security[4,6,7], security through third party authentication[8], security through signature-based authentication[9], security using cryptographic technique[10], and enhancing VANET performance/throughput[4,11–15]. Other approaches for vehicular network security have been surveyed in Ref. [16] (for further details about different security approaches, please refer to Refs. [4, 16] and references therein). None of these existing techniques consider mitigating data manipulating attacks to enhance overall throughput while reducing overall end-to-end delay.

Our contributions: We propose to use adaptive contention window to enhance network throughput in case of data falsification attacks in the network and hash chain to validate messages to mitigate data-falsification attacks. We further investigate a clustering algorithm for vehicular networks in IoV for reducing waiting/congestion time in case of traffic jams where vehicles make announcements about their candidacy for cluster head. The cluster head is chosen based on geolocation, trust level, and the number of neighbors that the vehicle has during the polling process. Cluster head is responsible for making decision about when to communicate with other clusters and when to reduce the contention window where needed. Because of hashing bits (say b_h), there will be communication overhead but it is negligible compared to the benefit it offers and reduction in delay because of adjustment of the contention window. Note that b_h is very very small compared to the size of the message S_P (i.e., $S_P << b_h$) and thus the overhead ratio $\frac{b_h}{S_P}$ will be very small.

Paper organization: The remainder of this paper is organized as follows. Section 2 presents the system model. Section 3 presents the proposed solution with formal analysis. Numerical results obtained from Monte Carlo simulation are presented in Section 4. Finally conclusions are presented in Section 5.

2 System Model

A typical system model for IoV considered in this paper is depicted in Fig. 1 where both V2V and V2R communications are used to forward traffic information. We consider that when there are only a few vehicles, Road Side Units (RSUs) help to reach out the vehicles. When there are enough vehicles for V2V communications, they communicate directly using single hop or multi-hop communications. Furthermore, in case of high vehicle density, V2V is sufficient to relay the information in IoV. However, in case of sparse vehicular network, there might not be sufficient vehicles for relaying the information, thus V2R and R2V communications are needed.

In IoV, we assume that a source vehicle sends information with its hash value. Each vehicle that receives the information calculates a hash value locally based on the received message. This locally computed hash value is compared against the hash value sent by the source vehicle. In single hop or multi-hop communications for IoV, when a vehicle finds any discrepancies in hash values, it stops forwarding the compromised information to other vehicles. In this case, information has to be re-transmitted by the source vehicle. To compensate this delay introduced by the retransmission, we proposed contention window reduction for vehicles so that waiting for channel

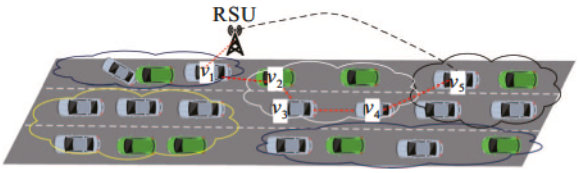


Fig. 1 Internet of Vehicles with a source vehicle (v_1), relay nodes/vehicles (v_2, v_3, and v_4), road-side-unit and a destination v_5 where vehicle v_1 and vehicle v_5 are not reachable using single hop and thus they rely on multi-hop communications.

access opportunities for message transmission could be reduced.

Note that two vehicles, or vehicles and roadside units are assumed to be within the communication range if their communication ranges are overlapped, that is

$$R_{\min} < D_{i,j}(t) \leqslant R_i \tag{1}$$

and the probability of two nodes being within the communication range is expressed as

$$\Pr(\text{CR}) = \Pr\{R_{\min} < D_{i,j}(t) \leqslant R_i\} \tag{2}$$

where $R_{\min}$ is the minimum separation distance between two nodes (two vehicles or vehicle and RSU) in IoV, R_i is the maximum transmission range that is allowed in vehicular communications (for instance, 1000 meters in IEEE 802.11p DSRC enabled VANET).

Note that the RSU is treated as a stationary vehicle/node with zero speed ($v = 0$). When there are enough vehicles present in the network, the relaying vehicle forwards both the data and its hash to all vehicles within its range including the RSU.

3 Proposed Approach

3.1 Clustering in IoV and drive-time saving through detouring

Congested traffic results in a sudden decrease of drivable path-ways for vehicles on the road. In order to accurately and promptly exchange information among vehicles and save time and costs, we postulate and examine the probability of drivers being able and willing to take a detour from their original route when the projected time for passing through the traffic via the original route is greater than that of the detour. As the number of surrounding vehicles increases, the expected time to be spent by the drivers for slowly moving and/or completely stopping will be gradually increased. Thus based on the location of vehicles and location of exits on the road, vehicles on the road can be divided into multiple groups or clusters. Such as Groups A, B, and C in Fig. 2, based on how close they are approaching to an event or incident on the road and how close to the highway exists. In this scenario, Group A is the front group and is closest to the incident and is expected to experience the least of travel time among all groups, while Group C at the end of the growing queue is expected to see longer travel time through the traffic ahead. However, Group A has no choice but wait until the wrecked cars are removed. Groups B and C have choices to take exits as shown in Fig. 2. If vehicles in Group B take exits, by the time vehicles of Group C get

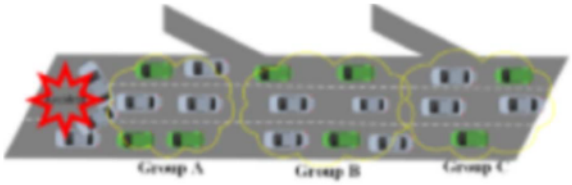


Fig. 2 Clustering in Internet of Vehicles based on how close they are approaching to an event or incident on the road and how close to the highway exists.

to the location of Group B, the road could possibly be cleared.

Based on the above modeling, we present the traffic scenario as an "inchworm"[17,18]. During traffic peak time, and in the event or incident such as sports events and traffic accidents, the queue of vehicles can be observed as multiple groups A, B, C, D, etc. The number of vehicles in a group can be random, unless constraints exist, e.g., same queue divided into more groups may potentially increase the amount of communication in the IoV. In Fig. 2, at the instant of stopped traffic (e.g., around vehicle Group A), there will be a ripple motion causing all vehicles in Groups A through C to slow down, leading to the happening of the "inch worm" effect. Consequently each forthcoming vehicle group will have to slow down and all groups have to wait until they slowly move and pass the root cause point of the traffic. It can be assumed that Group A will be close enough to the incident that any amount of detour time will not be beneficial to them, while groups behind Group A will be increasingly beneficial by detouring as farther away from the start of the queue. In the case that some drivers in any groups decide to reroute and take the detour (when such detouring exists), all vehicles behind them will have a more open route while vehicles ahead of them will still be moving through the obstruction in the case when rerouting is not worthwhile for these vehicles. By enforcing rerouting as soon as changes to the queue occur, it is expected that all recent incoming traffic will only slightly be or not be slowed down at all by the event. Here we give an example scenario to further explain how making decision of detouring may affect the overall travel time. Suppose the travel time for vehicles in Groups B and C extends to 30 minutes due to the congestion, while the detour only takes 20 minutes. In this case it is possible some of the drivers may decide to take the detour but the others may not. In the scenario that most would take the detour, the traffic ahead of a new Group D may see an update with reduced travel time, e.g., from 45 to 60

minutes down to 20 to 30 minutes. As in Fig. 2, where Group B takes the detour and frees up the traffic in the main pathway where the accident happened, Group C will expect reduced travel time due to the detour of vehicles ahead of that group.

Performance Evaluation: We have considered two simulation scenarios: (1) one similar to the one given in Fig. 2 where enough vehicles were present to form vehicular clusters/groups and there were two exits for two groups (Group B and Group C) of vehicles. However, there was no option to reroute for vehicles in Group A. (2) The other scenario had enough vehicles to form groups (Groups A, B, and C) but no group had an option to take exits. Figure 3 shows the variation of estimated delay time to reach a given destination for a typical scenario with and without an alternative route for vehicle clusters B and C considered in our analysis where there is an accident in front of the cluster/Group A. For Group A, there is no alternative route, thus the waiting time or delay is same for both cases. However, for Group B and Group C, there are alternative routes, thus the delays to reach to a given destination (or waiting times) for these vehicles are smaller when there is alternative route than that of when there is no alternative route.

The information dissemination in IoV should happen as quickly as possible and as securely as possible. We propose hash-based detection of false data injection attack and a process of reducing contention window to compensate the delay introduced by the false data detection process. Hashing and contention window adaptation approach is discussed in the following section.

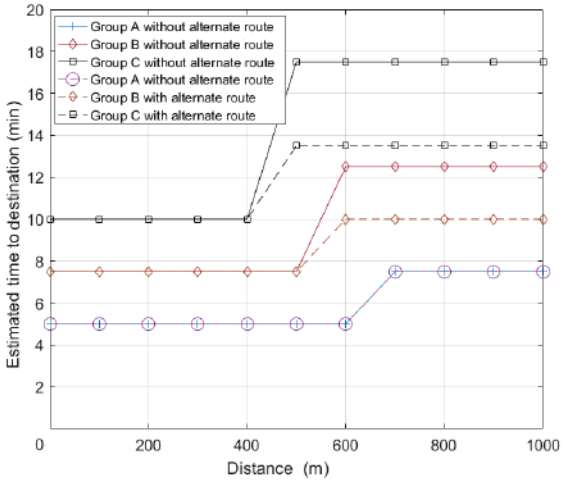


Fig. 3 Variation of estimated delay time to reach the destination for a typical scenario with and without an alternative route for vehicle clusters B and C.

3.2 Hashing and delay

As discussed in the system model, each vehicle computes hash values based on the received information and compares the calculated hash value with the hash value transmitted by the source vehicle (as in Fig. 4). By comparing these two hash values, each vehicle can detect data falsifying attacks if there was any tempering in the message.

Hashing is one of the effective methods for securing vehicular communication in IoV as it is computationally less complex and easier to implement for highly dynamic IoV environment. In Fig. 1, source vehicle v_1 sends data packets M to destination (vehicle v_5), either through direct transmission if the node is present within its transmission range or through a multiple hop using relay nodes $(1, 2, ..., i, ..., N)$ or directly through the RSU if present within its range. The message M and its hash value is transmitted. At each node, data packet takes the time Δ_i, i.e.,

$$\Delta_i = (\delta_i + \mathrm{CW}_i + \varphi_i)(1 - \Pr(\mathrm{CR})) \qquad (3)$$

where Δ_i time comprises of processing time δ_i for hash calculation, contention window CW time for channel access, and the wait time φ_i for which a node waits to receive the data from another relay path. When the hash of the message M is sent over to the $(i+1)$ node, computed hash value is compared with the transmitted hash value from the source node. With using hash chains the tampered data will have a completely different hash whereas an un-tampered packet will have the exact same hash value as the hash sent by the

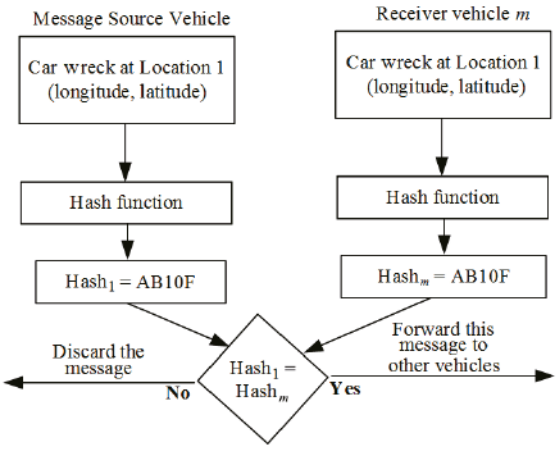


Fig. 4 Hash values computed by the message source vehicle (which is transmitted with the message) and by the m-th vehicle are compared to decide whether the message should be forwarded or not in IoV. Note that the message in IoV should be delivered to all vehicles but it should be validated for its legitimacy.

source vehicle. So using this kind of authentication, false messages can be easily differentiated by the hash message relayed across the network. Prior to data transmission the source node checks if the destination node is within communication ranges, if not, it looks for relay nodes or RSU within its transmission range. If the nodes are within each others' transmitting range, time period for which the nodes would remain within range is calculated based on relative velocity (V_{rel}) and their Transmission Range (TR) as

$$T = \frac{\text{TR}}{V_{\text{rel}}} \tag{4}$$

To completely transmit the S_{P} size of the information, following condition should be satisfied.

$$\frac{\text{TR}}{V_{\text{rel}}} \geqslant \frac{S_{\text{P}}}{B} + \Delta_i \tag{5}$$

where S_{P} is the size of the data being transmitted with data rate B (bps) in IoV.

3.3 Adaptation of contention window size

In IoV, each vehicle computes hash value upon receiving data and compares the locally computed hash value with the hash value transmitted by the source. If these hash values do not match, that is, hash (M at node 1) $\neq$ hash (M at node m) say at node m, then the m-th node will recognize that the message sent by the previous node is malicious. When data packets are tampered from an attack in a relay path, the node will look for the same untempered data packet from another relay path or from RSU. This will add a certain amount of delay in data transmission. To compensate this delay, reducing the contention window times of the nodes present after m-th node (or all nodes in the cluster where the m-th node is located) will help reduce the delay in the network. The adaptation of contention window size is carried out as

$$\text{CW}_{m+1} = \begin{cases} \dfrac{\text{CW}_{m+1}}{2}, & \text{if } h_m \neq h_1; \\ \text{CW}_{m+1}, & \text{if } h_m = h_1 \end{cases} \tag{6}$$

where the hash $h_m = \text{hash}(M)$ at node m and hash $h_1 = \text{hash}(M)$ at source node $i = 1$ and when malicious attacker is present then node i is denoted as $m = i$. Note that if there is no any malicious user present along the relay path, nodes would communicate without any reduction in the CW sizes.

In the process of sending data packets through N relay nodes, we define the probability for a data packet M at the i-th node to hop to the $(i+1)$-th node as

$$P_{xy} = P[M \text{ is accurate at } (i+1) | M \text{ was accurate at } i] \tag{7}$$

Using P_{xy}, the probability to successfully transmit data from the source-to-destination is calculated using Markov chain 1-step state transition probability as

$$P(N) = \sum_{i=1}^{N} P(i) P_{xy} \tag{8}$$

where $P(i)$ is the probability that the data is at the i-th node at a given time. The resulting probability $P(N)$ is the probability that data M will reach its destination node without any discrepancies. However, when an attacker is present in the relay path, the transmitted message will have to be stopped from transmission. The probability that message would be transmitted with modification because of an attacker can be defined as

$$P(\text{A}) = 1 - P(N) \tag{9}$$

Note that the paper does not consider data loss due to interference, shadowing, fading, etc., which is out of the scope of the work. When an attacker is detected through hashing process, the data is dropped from further propagation in the VANET.

3.4 Throughput and delay analysis

The total time spent for the data packet in the network is denoted by T_{a} when the m-th node to be a malicious, that is,

$$T_{\text{a}} = \sum_{i=1}^{m} (\delta_i + \text{CW}_i + \varphi_i)(1 - \text{Pr}_i(\text{CR})) = \sum_{i=1}^{m} \Delta_i, \quad m \in \{1, 2, ..., N\} \tag{10}$$

If the attacker at the m-th node is detected, the contention window of the $(m+1)$-th node CW_{m+1} is reduced to half of its original size. This node waits for legitimate packet from another route or node. The time spent at each node for a data packet until it reaches the destination from $(m+1)$-th node is expressed as

$$T_{\text{b}} = \sum_{i=m+1}^{N} (\delta_i' + \text{CW}_i' + \varphi_i')(\text{Pr}_i(\text{CR})) = \sum_{i=m+1}^{N} \Delta_i' \tag{11}$$

The throughput is computed through the computation specified in Ref. [11]. However, we have modified the equation to accommodate the presence of malicious users and also incorporate the contention window wait times into the equation. Based on these parameters, end-to-end throughput θ of the network is computed as

$$\theta = \frac{P(N)[T_{\text{a}} + T_{\text{b}}]}{[P(N)T_{\text{a}} + P(\text{A})T_{\text{b}}]} \tag{12}$$

Then the network delay is calculated as

$$d = [T_{i,i+1}](N+1) + T_{\text{a}} + P(\text{A})T_{\text{b}} \tag{13}$$

where $T_{i,i+1}$ is the propagation time for the message between two consecutive nodes i and $i+1$.

4 Performance Evaluation and Discussion

To corroborate our analysis presented in the previous section, we have performed Monte Carlo simulations where source and destination vehicles are not reachable directly using single hop and there are multiple relay paths using multi-hop communications (in dense network scenario) and/or roadside unit communications (in sparse network scenario). Each vehicle is assumed to be equipped with DSRC/WAVE enabled 802.11p computing and communication devices. Speeds of the vehicles were assumed to be between 25 mph and 70 mph that covers the most city and highway speed limits. For simulation setup, we have considered three scenarios: (1) without any data falsification or manipulation attacks, (2) with data falsification attack along the relay path where attack was detected and CW size was adapted, and (3) with data falsification attack where attack was detected and CW size was not adapted (kept fixed).

First, we have plotted the variation of expected normalized throughput vs. the connectivity probability (for source and destination vehicles) as shown in Fig. 5. When the probability of connectivity increases, the throughput increases for IoV as shown in Fig. 5. Furthermore, we observed that the throughput is lower in case of attacks where vehicles had to wait longer to transmit accurate information. When attack was detected, the given vehicle dropped the packet and waited for an accurate copy of the message from another path or another node/vehicle and then forwarded the accurate copy of the message but with lower contention window size for channel opportunities. When contention window was adapted, throughput was higher than the case without adaptation of contention window as in Fig. 5. Note that for the data manipulation/falsification attacks, intermediate vehicle(s) changed the message to mislead the vehicular communications.

We have also plotted the variation of expected end-to-end delay vs. the probability of connectivity (for source and destination vehicles) as shown in Fig. 6 for three different scenarios. We observed that the end-to-end delay is decreasing with increasing probability of connectivity as shown in Fig. 6.

The end-to-end delay is the highest in case of attack when contention window was not adapted after attack. The delay is lower in the case of contention window adaptation than that of fix contention window as shown in Fig. 6. Note that, as expected, the end-to-end delay is the least in case of no data falsification attack in the network as shown in Fig. 6.

Next, we simulated three scenarios (without any data falsification attacks, with data falsification attack in the middle of relay chain where attack was detected and CW size was adapted, and with data falsification attack in the middle of relay chain where attack was detected and CW size was not adapted) and have plotted the variation of average throughput vs. the simulation time as shown in Fig. 7. We observed that the throughput is increasing with the time as shown in Fig. 7 when there is no data manipulation or falsification attack in the network. The throughput is higher when attack was detected and CW size was adapted than that of fixed CW size as shown in Fig. 7. Furthermore, the throughput is the highest when there is no attack in the

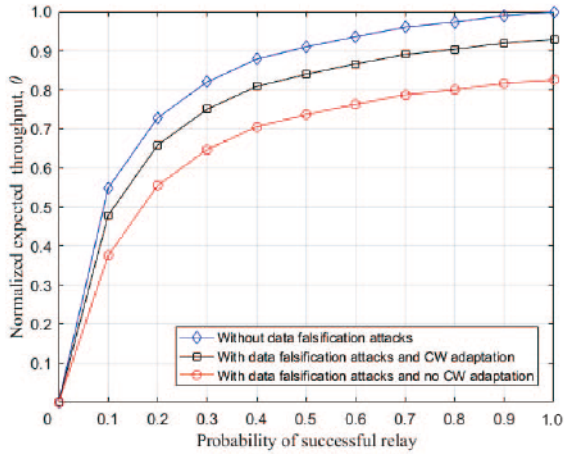


Fig. 5 Variation of normalized throughput vs. the connectivity probability Pr(CR).

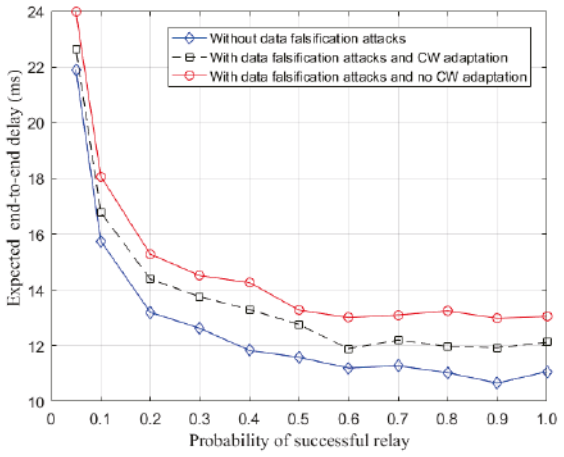


Fig. 6 Expected end-to-end delay vs. the connectivity probability Pr(CR).

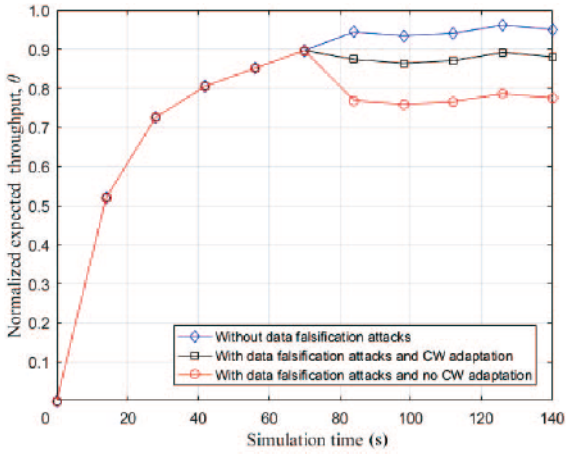


Fig. 7 Variation of normalized throughput vs. the simulation time after an attack around halfway.

network as shown in Fig. 7.

For all these three scenarios, we have plotted the expected end-to-end delay as shown in Fig. 8. We found that the delay is highest when data falsification attack is detected but CW size was not adapted and the delay is the lowest when there is no attack in the IoV. When data falsification attack was detected and CW size was adapted, the end-to-end delay gets reduced as shown in Fig. 8.

It can be concluded from above results and analysis that the adaptation of contention window size when attack is detected can help compensate/reduce the delay (introduced by the data falsification attack) while increasing the throughput in the vehicular network.

5 Conclusion

In this paper, we have presented data falsification attack detection using hashes for improving network security and enhancing the overall performance by adapting contention window size while forwarding accurate information to the neighboring vehicles in a timely manner (to improve throughput while reducing end-to-end delay). We have also presented clustering approach to reduce travel delay time in case of traffic congestion. Performance evaluation is done by using numerical results obtained from Monte Carlo simulations. We observed that the contention window adaptation once data manipulation attack is detected results in lower delay and higher throughput than that of fixed contention window size. Furthermore, when accurate information is transmitted to vehicles, they could make informed decision to reduce their waiting time when alternative routes are available.

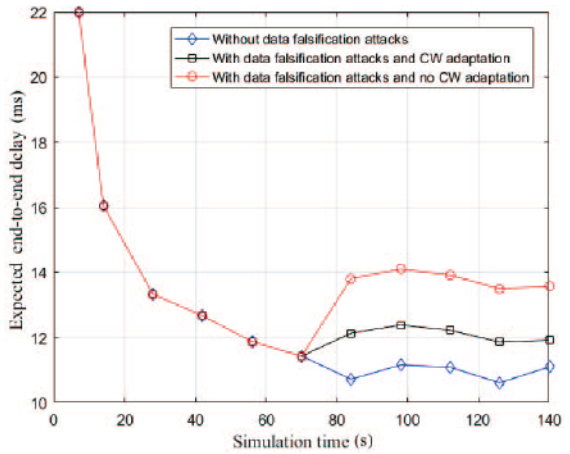


Fig. 8 Variation of expected end-to-end delay vs. the simulation time after an attack around halfway.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation (NSF) under grants CNS-1650831, CNS-1552109, CNS-1405670, and CNS-1658972. However, any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NSF.

References

[1] NHTSA, *Traffic Safety Facts*, 1st ed. NHTSAs National Center for Statistics and Analysis, Washington, DC, USA, 2015.

[2] D. Schrank, B. Eisele, T. Lomax, and J. Bak, 2015 urban mobility scorecard, Texas A&M Transportation Institute and the Texas A&M University System, 2015.

[3] A. Dvir, L. Buttyan, and T. V. Thong, SDTP+: Securing a distributed transport protocol for wsns using merkle trees and hash chains, in *2013 IEEE International Conference on Communications (ICC)*, 2013, pp. 2073–2078.

[4] D. B. Rawat and C. Bajracharya, *Vehicular Cyber Physical Systems: Adaptive Connectivity and Security*. Springer, 2016.

[5] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, Trust on the security of wireless vehicular ad-hoc networking, *Ad Hoc & Sensor Wireless Networks*, vol. 24, nos. 3&4, pp. 283–305, 2015.

[6] G. Yan, W. Yang, J. Lin, and D. B. Rawat, Cross-layer location information security in vehicular networks, *Journal of Next Generation Information Technology*, vol. 3, no. 2, pp. 37–56, 2012.

[7] G. Yan, D. B. Rawat, and B. B. Bista, Towards secure vehicular clouds, in *Complex, Intelligent and Software Intensive Systems (CISIS), 2012 Sixth International Conference on*, 2012, pp. 370–375.

[8] N. Vighnesh, N. Kavita, S. R. Urs, and S. Sampalli, A novel sender authentication scheme based on hash chain for vehicular Ad-Hoc networks, in *2011 IEEE Symposium*

on Wireless Technology and Applications (ISWTA), 2011, pp. 96–101.

[9] L. He and W. T. Zhu, Mitigating DoS attacks against signaturebased authentication in VANETs, in *2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, 2012, pp. 261–265.

[10] L. Zhu, F. R. Yu, B. Ning, and T. Tang, Joint security and QoS provisioning in cooperative vehicular ad hoc networks, in *2013 IEEE International Conference on Communications (ICC)*, 2013, pp. 1594–1598.

[11] J. Zheng and Q. Wu, Performance modeling and analysis of the IEEE 802.11 p EDCA mechanism for VANET, *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2673–2687, 2015.

[12] D. B. Rawat, D. C. Popescu, G. Yan, and S. Olariu, Enhancing VANET performance by joint adaptation of transmission power and contention window size, *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 9, pp. 1528–1535, 2011.

[13] D. B. Rawat, S. Reddy, N. Sharma, B. B. Bista, and S. Shetty, Cloud-assisted GPS-driven dynamic spectrum access in cognitive radio vehicular networks for transportation cyber physical systems, in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, 2015, pp. 1942–1947.

[14] D. B. Rawat, B. B. Bista, and G. Yan, CoR-VANETs: Game theoretic approach for channel and rate selection in cognitive radio VANETs, in *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on*, 2012, pp. 94–99.

[15] D. B. Rawat, B. Bista, and G. Yan, Securing vehicular Ad-hoc networks from data falsification attacks, in *IEEE TENCON 2016*, 2016.

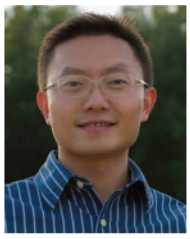
[16] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, Recent advances in vanet security: A survey, in *Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd.*, 2015, pp. 1–7.

[17] M. Schliwa, Kinesin: Walking or limping? *Nature Cell Biology*, vol. 5, no. 12, pp. 1043–1044, 2003.

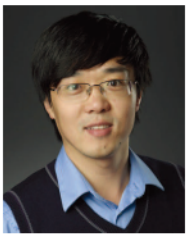
[18] I. J. Cushman, D. B. Rawat, L. Chen, and Q. Yang, Performance evaluation of vehicular ad hoc networks for rapid response traffic information delivery, in *International Conference on Wireless Algorithms, Systems, and Applications*, 2016, pp. 571–579.

Danda B. Rawat is an associate professor in the Department of Electrical Engineering & Computer Science at Howard University, Washington, DC, USA. Prior to Howard University, he was with the College of Engineering & Information Technology of Georgia Southern University, Statesboro, GA, as a faculty member. Dr. Rawat's research focuses on wireless communication networks, cyber security, cyber physical systems, Internet of Things, big data analytics, wireless virtualization, software-defined networks, smart grid systems, wireless sensor networks, and vehicular/wireless ad-hoc networks. Dr. Rawat is the recipient of NSF Faculty Early Career Development (CAREER) Award. He has been serving as an Editor/Guest Editor for over 15 international journals. He serves as an IEEE INFOCOM 2018 TPC Vice Chair (Information Systems), served as a Web-Chair for IEEE INFOCOM 2016 and 2017, as a Student Travel Grant Co-chair of IEEE INFOCOM 2015, Track Chair for IEEE CCNC 2016, 2017 and 2018, Track Chair for Communications Network and Protocols of IEEE AINA 2015, and so on. He served as a program chair, general chair, and session chair for numerous international conferences and workshops, and served as a technical program committee (TPC) member for several international conferences including IEEE INFOCOM, IEEE GLOBECOM, IEEE CCNC, IEEE GreenCom, IEEE AINA, IEEE ICC, IEEE WCNC and IEEE VTC conferences. He is the recipient of Outstanding Research Faculty Award (Award for Excellence in Scholarly Activity) 2015, Allen E. Paulson College of Engineering and Technology, GSU among others. He is the Founder and Director of the Cyber-security and Wireless Networking Innovations (CWiNs) Research Lab. He received the PhD degree in electrical and computer engineering from Old Dominion University, Norfolk, Virginia, USA, in 2010. Dr. Rawat is a senior member of IEEE and member of ACM and ASEE. He served as a Vice Chair of the Executive Committee of the IEEE Savannah Section and Webmaster for the section from 2013 to 2017.

Moses Garuba is a professor of computer science at Howard University, Washington, DC, USA. He received the PhD degree in computer science and information from University of London in 2000, master degree in computer science from Howard University in 2000, master degree of science in information technology from University of London in 1993, and bachelor of science from University of London in 1992. His research interests include multilevel database security, secure transaction processing, quantum cryptography, integrity of digital evidence, electronic privacy law, and e-commerce. He has authored numerous research articles and has received many awards from the National Science Foundation, Department of Defense and the Defense Advanced Research Projects Agency. He is an editor of the Journal of Information Technology Impact, an associate editor and program committee member of the International Conference on Information Technology: Next Generations, a member of the IEEE-USA Working Group on Bioterrorism, and co-founder of the International Federation For Information Processing (IFIP) Working Group 9.6 IT Misuse and the Law.



Lei Chen is an associate professor in the Department of Information Technology at Georgia Southern University. He received the BEng degree in computer science and applications from Nanjing University of Technology, China, in 2000, and PhD degree in computer science and software engineering from Auburn University, USA, in 2007. He joined Georgia Southern University in 2015, before when he served in the Department of Computer Science at Sam Houston State University as an assistant professor and later tenured associate professor for 8 years. He also served as the Graduate Coordinator for all three master programs offered by the department at SHSU. Dr. Chen's research interests focus on network, information, cloud, and Big Data security, digital forensics, and mobile, hand-held and wireless security. His extended research reaches the areas of computer networking, multimedia networking, network routing, and artificial intelligence. He started research as a graduate research assistant for 5 years at Auburn University and worked as Vodafone Research Fellow during his PhD study. He has authored or co-authored more than 90 peer-reviewed scholarly works, including journal papers, book chapters, and conference proceeding papers. His edited book *Wireless Network Security*: *Theories and Practices*, published by Springer (U.S.) and Higher Education Press (HEP), was released in May 2013. He has secured both internal and external funding to support his research, with support from U.S. federal funding sources such as the National Security Agency.



Qing Yang is a RightNow Technologies Assistant Professor in the Gianforte School of Computing at Montana State University. He received the PhD degree in computer science from Auburn University in 2011. His research interests include online social network, trust assessment, vehicular networks, and the Internet of Things. He has published more than 50 papers in prestigious journals and conferences such as IEEE Transactions on Dependable and Secure Computing, IEEE INFOCOM and IEEE CNS.