This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2905522, IEEE Transactions on Vehicular Technology

DeQoS Attack: Degrading Quality of Service in VANETs and its Mitigation

Anjia Yang, *Member, IEEE,* Jian Weng*, *Member, IEEE,* Nan Cheng, *Member, IEEE,* Jianbing Ni, *Member, IEEE,* Xiaodong Lin, *Fellow, IEEE,* and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—In this paper, we introduce a degradation-of-QoS (DeQoS) attack against vehicular ad hoc networks (VANETs). Through DeQoS, the attacker can relay the authentication exchanges between roadside units (RSUs) and faraway vehicles to establish connections but will not relay the service afterwards, which wastes the limited connection resources of RSUs. With enough number of dummy connections, RSUs' resources could run out such that they can no longer provide services for legitimate vehicles. Since the mobility of vehicles is highly related to the success probability of the attacker, we model the arrival and departure of vehicles into an $M/M/N$-queue system and show how the attacker can adaptively choose different attack strategies to perform the attack in distinct traffic environments. A series of simulations are conducted to verify the practicality of the attack using MatLab. The experimental results demonstrate that the attacker can easily find exploitable vehicles and launch the DeQoS attack with an overwhelming probability (e.g., more than 0.98). As DeQoS exploits the weakness of lacking physical proximity authentication, only employing existing application-layer defense protocols in VANETs such as cryptography-based protocols cannot prevent this attack. Therefore, we design a new cross-layer relay-resistant authentication protocol by leveraging the distance-bounding technique. Security analysis is given to show that the defense mechanism can effectively mitigate DeQoS.**

***Keywords*—VANETs, attacks, authentication, distance-bounding.**

I. Introduction

Vehicular ad hoc networks (VANETs) [1], [2] have drawn enormous attention from both academia and industry since it was first introduced in early 2000s. For simplicity, a VANET consists of mobile vehicles equipped with onboard units that allow the vehicles to communicate, and fixed infrastructure called roadside units (RSUs) that are sparsely deployed in critical locations. According to the dedicated short-range communication (DSRC) standard, vehicles can exchange information with other vehicles in vehicle-to-vehicle (V2V) communication mode and RSUs in vehicle-to-infrastructure (V2I) communication mode to avoid crashes, alleviate traffic congestion and improve driving environment. Typical applications of VANETs include traffic information systems that broadcast up-to-minute message alerts to surrounded vehicles, and on-the-road services that drivers and passengers can enjoy such as the Internet access. All these applications can provide significant benefits on developing intelligent transportation systems, making our life more convenient and safe.

Despite the great advantages of VANETs, there are still quite a few gaps needed to be filled before the practical deployment. One of the serious issues is the security and privacy for practical VANETs [1], [3]–[5]. In safety-related applications such as crashes prevention, vehicles take actions based on the messages received from other vehicles or RSUs. Interception and modification of messages by evil attackers could result in fatal consequences. To ensure message authenticity and integrity, a natural way is to make authentication on the messages before transmission. Indeed, various authentication proposals [6]–[16] have been introduced since last decade, some of which can achieve batch verification and perform very efficiently, and some others address the privacy issue as well.

Although extensive theoretical work on designing secure and privacy-preserving authentication protocols for VANETs has been done recently, the question of whether these solutions could capture all the practical attacks remains to be answered. Indeed, due to the characteristics of wireless communication channels (e.g., susceptible to eavesdropping and interference), an attacker can launch potential attacks against VANETs with some physical contexts. Considering the application that an RSU provides infortainment services especially for some band-consuming services like watching videos to vehicles that are inside its communication range, authentication and access control decisions are usually made by the verifier (RSU) based on the credentials provided by the prover (vehicle). Namely, if the prover successfully completes a secure cryptographic authentication protocol with the verifier, it is assumed that the prover is present within the communication range of the verifier. Nevertheless, judging the participant proximity by the communication range of a system can be circumvented by a simple man-in-the-middle attack where an attacker holding proxy devices relays the messages sent by the protocol participants over a larger distance. More precisely, a malicious attacker sitting in the RSU's communication range can trick the RSU and outside vehicles that are actually far away

* Corresponding author (E-mail: cryptjweng@gmail.com)

Anjia Yang and Jian Weng are with the College of Informatin Science and Technology / College of Cyber security, National Joint Engineering Research Center of Network Security Detection and Protection Technology, and Guangdong Key Laboratory of Data Security and Privacy Preserving, Jinan University, Guangzhou, 510632, China; Anjia Yang is also with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

Nan Cheng, Jianbing Ni and Xuemin (Sherman) Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

Xiaodong Lin is with the School of Computer Science, University of Guelph, Guelph, Ontario, Canada, N1G 2W1

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2905522, IEEE Transactions on Vehicular Technology

from the RSU to establish connections by relay attacks. The attacker plays as a prover (vehicle) with the RSU (verifier) and plays as the RSU with an outside vehicle, relaying the credential messages sent between the real RSU and vehicle for the purpose of authentication. Since the outside vehicle is valid, it should be correctly authenticated by the RSU and thus a connection will be established if the protocol runs normally. After relaying resources-accessing requests from the outside vehicle to the RSU, however, the attacker will not relay the resources to the vehicle anymore. This dummy connection takes up the transmission channel and the RSU's service capability, both of which are limited, and thus degrades the quality of service (QoS) for the legitimate vehicles that are inside the RSU's communication range. Even worse, the exploited outside vehicle has to wait for its resources that may never arrive. If enough number of outside vehicles are exploited, the RSU's resources could be used up. It seems like a distributed denial-of-service (DoS) attack in the sense that the outside vehicles are exploited to flood the RSU with large number of band-consuming resources-accessing requests. Compared with conventional denial-of-service attacks such as jamming attack which deliberately interferences the wireless medium with attempt of disabling legal users to access network resources, the new attack is more difficult to detect and prevent since neither the RSU nor the outside vehicles realize the existence of the attacker. Therefore, the demonstrated attack could be more severe.

This kind of distance fraud attacks caused by simply relaying techniques have been shown to be practical and effective against actual systems. For example, Francillon *et al.* [17] demonstrated relay attacks on passive keyless entry and start systems in modern cars, where the attacker can enter and start a car by relaying messages transmitted between the car and the smart key; Roland *et al.* [18] described a software-based relay attack on the mobile contactless payment application Google Wallet. Unfortunately, it is very challenging to address this problem from a pure cryptographic protocol design perspective since any conventional challenge-response authentication protocol could be relayed.

An intuitive way to eliminate the distance fraud attacks is verifying physical proximity between the RSU and vehicles. GPS (Global Positioning System) data could be integrated into the message to achieve proximity authentication, but the availability of GPS in urban environments filled up with tunnels and high buildings could be reduced significantly. Moreover, it is well-known that GPS is subject to spoofing attacks [19], [20] and thus the authenticity of the data sources cannot be guaranteed. A promising approach is distance-bounding protocols which utilize the round-trip time of multiple cryptographic challenge-response pairs to determine an upper bound on the physical distance between a verifier and a prover. Since the notion is proposed by Brands and Chaum [21], it has been an active research area to construct secure and efficient distance-bounding protocols [22]–[24], which is also one of the critical techniques employed in our proposed protocol. In this paper, we reexamine the security issues of VANETs taking physical contexts of vehicular communications into consideration and aim to provide a more secure environment for intelligent transportation systems. The details of the contributions are as follows:

1) We demonstrate a new attack named DeQoS which can degrade the quality of service in VANETs communications.
2) We make a thorough analysis of the attacker's chance to launch DeQoS which indicates the practicality of the attack. In particular, we model the arrival and departure of vehicles into an $M/M/N$-queue system and thus convert the probability that the attacker can launch an attack to the probability of there existing at least one vehicle in the attack area. We show that the attacker can adaptively choose different attack strategies according to distinct environments in order to maximize the chance to start an attack.
3) We simulate the probability that an attacker can launch DeQoS in different scenarios with MatLab. Simulated results verify the theoretical analysis and show that the presented attack is practical and easy to launch. Specifically, with a good attack strategy, an attacker can launch a DeQoS attack with an overwhelming probability (e.g., more than 0.98).
4) We propose a cross-layer authentication protocol that can prevent the demonstrated DeQoS attack by leveraging distance-bounding techniques. Since Yang *et al.* [24] have formalized a general framework for designing distance-bounding protocols, we follow their framework to build a specific distance-bounding construction which is a part of the proposed protocol. In addition, since distance-bounding process requires a special transmission channel, we adopt time division multiple access (TDMA) protocol in the data link layer and elaborate how to design a secure distance-bounding based solution that can authenticate both the identity and the physical proximity of vehicles.

The remainder of this paper is organized as follows. Section II describes the related work, while Section III introduces the preliminaries that will be used in subsequent sections. In Section IV the system and security models are defined, and the security objectives are listed as well. In Section V, we demonstrate the new attack and make a thorough analysis of the success probability. A distance-bounding based defense protocol is presented in Section VI and the security analysis of the protocol is also given in the same section. Section VII evaluates the demonstrated attack in terms of practicability and effectiveness. Finally, the conclusion is shown in Section VIII.

II. Related Work

Among various security attacks in VANETs [3], DoS attack is most related to our demonstrated DeQoS attack. In a DoS attack, an attacker floods the network by jamming invalid messages in order to make the resources and services unavailable to the users. Signature-based authentication schemes can alleviate this problem by rejecting those invalid messages. However, the attackers can still broadcast a large number of forged signatures. The heavy computation of verifying excessive signatures may exhaust the verifier's computational resources and thus lead to computation-based DoS attacks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2905522, IEEE Transactions on Vehicular Technology

He *et al.* [7] proposed to add a pre-authentication process before verifying the signatures by combining a one-way hash chain and a group rekeying scheme. Compared with signature verification, one-way hash function is more computationally efficient and thus can lessen the impacts of computation-based DoS attacks. Another promising approach is lightweight broadcast authentication that employs symmetric cryptographic algorithms. For example, Lin *et al.* [25] proposed a timed efficient and secure vehicular communications that is based on the TESLA algorithm [26]. The verifier only needs to perform some symmetric MAC functions to authenticate the source of the messages. The TESLA based authentication scheme inherits a limitation, i.e., suffers from memory-based DoS attacks. To address this issue, Lyu *et al.* [27] proposed a prediction-based authentication protocol which only stores shortened re-keyed MACs of signatures.

There are also some non-cryptographic solutions to deal with the DoS attacks in VANETs. Verma *et al.* [28] proposed to check the similar IP addresses of beacon messages. Malla and Sahu [29] proposed a DoS-resistant method basing on a redundancy elimination method that included rate decreasing algorithm and state transition mechanism. However, neither these cryptography-based nor non-cryptographic solutions can prevent DeQoS, since the attacker does not care the content of transmitted messages or bother to modify or delete the messages but instead just simply relay all the messages sent between authentic vehicles and RSUs.

To defend against DeQoS, it is indispensable to verify the physical proximity between the RSU and vehicles. The most related work is location verification for VANETs [30]–[35], which is achieved with mainly two approaches. The first one verifies the position claims of a node based on its reliable neighbor positions obtained with GPS technique. In particular, each node broadcasts its current position calculated with GPS data so that all its neighbors can build up a table of neighboring nodes including the positions. Leinmüller *et al.* [30] proposed a position cheating detection mechanism in geographic routing protocols for VANETs, where multiple sensors are equipped in each vehicle and each sensor is associated with a weight value according to its reliability and known performance. Observations of multiple weighted sensors are accumulated to estimate the trustworthiness of the position claims of a node. Ren *et al.* [33] proposed a location verification scheme through distributed message exchange from two directional antennas. Each node collects information from both its front and behind neighbors with two antennas, based on which it calculates the relative position with the neighbors. Malicious nodes will be detected if the relative positions are suspect. Abumansoor *et al.* [34] proposed to utilize cooperative neighboring vehicles to ensure nonline-of-sight location verification for VANETs. All of the above methods rely on GPS technique. However, GPS signals are easily disturbed or blocked by obstacles such as buildings which may result in inaccuracy and even unavailability in some complex environments like urban and tunnels. Even worse, GPS signals can be easily spoofed so that the calculated position could be totally inaccurate.

An alternative approach to verifying the location for VANETs is based on measuring physical parameters such as time of arrival, angle of arrival and the received signal strength. Yan *et al.* [31] proposed to verify a vehicle's position claim by using radars that can measure the physical parameters like the relative velocity and angle to the target object. However, this solution always requires line of sight between two vehicles, which may not be the case in reality. Yan *et al.* [35] presented a location verification system for VANETs in the setting of Rician fading channels. They investigated how to achieve the best performance of detecting whether a claimed location given by a vehicle is legitimate. Nevertheless, a malicious vehicle can easily circumvent this detection by amplifying its signal or deploying a relay device nearby the RSU. Song *et al.* [32] combined distance bounding, plausibility checks and ellipse-based location estimation to verify a vehicle's position claim with the cooperation of a neighbor. However, the assisting neighbor's position has an impact on the computation's results. Singelee *et al.* [36] discussed how to verify a location claim of a node with distance bounding protocols. More precisely, the node is required to execute distance bounding protocols with three verifiers each of which can determine an upper bound on the distance to the node. Combining the three bounds from the corresponding verifiers can thus estimate the location of the node to a limited area. Although our proposed defense scheme also employs distance bounding protocols as the foundation technique, we observe that it is not necessary for an RSU to calculate the exact location of a vehicle but knowing that the vehicle is within a certain distance (saying the communication range) suffices to prevent DeQoS.

III. Preliminary

In this section, we describe the preliminary knowledge about distance-bounding protocols that will be employed as a one of the foundations in the proposed protocol.

Distance-bounding protocols were introduced by Brands and Chaum [21] as an efficient countermeasure against relay attacks in wireless communication systems. Intuitively, they are real-time challenge-response authentication protocols that aim to verify both the credentials and the proximity of an entity at the same time. The basic idea of proximity verification is to compute an upper bound on the physical distance between the verifier and the prover according to the round-trip time of cryptographic challenge-response pairs given that the propagation speed of the radio signal is approximate to the speed of light. Let v be the propagation speed of the signal, d the upper bound on the distance between the verifier and the prover, t_m the measured round-trip time, t_p the one-way propagation time and t_d the prover's processing delay, then we have $d = c \cdot (t_m - t_d)/2$ with $t_m = 2 \cdot t_p + t_d$. The fact of d being proportional to t_m indicates that if t_m is less than a given bound then so is d.

A typical distance-bounding protocol consists of three phases: an initialization phase, a distance bounding phase and a verification phase. The initialization and verification phases are not time critical and thus during these two phases the verifier and the prover can transmit messages over conventional channels and perform conventional cryptographic operations. The distance bounding phase is time critical requiring a special

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2905522, IEEE Transactions on Vehicular Technology

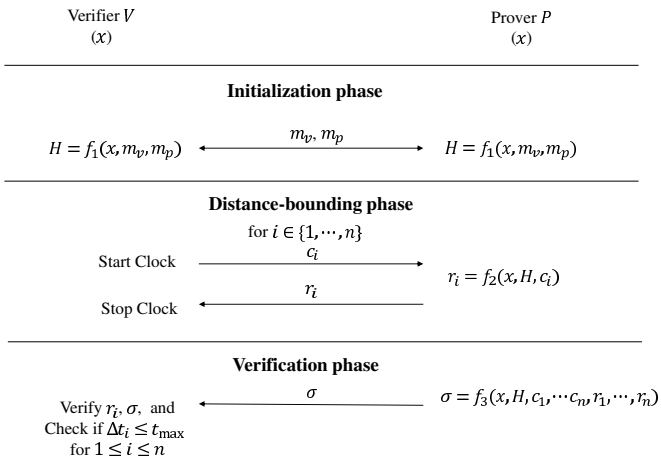


Fig. 1: A general register-based distance-bounding protocol.

channel and response function. In 2005, Hancke and Kuhn [37] presented a register-based distance-bounding protocol which has been the foundation of subsequent protocol constructions due to its high efficiency compared with Brands and Chaum's scheme. Our proposed defense scheme is also a register-based distance-bounding protocol. Following Yang *et al.*'s definition [24], we introduce the general structure of a register-based distance bounding protocol as shown in Figure 1:

a) Initialization Phase: In this phase, the verifier V and the prover P may exchange some messages such as random nonces, and pre-generate all the materials required during the distance-bounding phase, such as the response registers by $H = f_1(x, m_v, m_p)$ where f_1 is usually a secure keyed hash function, x is the shared secret key between V and P, m_V and m_P are the exchanged messages. This can avoid cryptographic operations performed in the time critical distance-bounding phase so that the processing delay t_d is minimized to reduce the affect on calculating the distance.

b) Distance-Bounding Phase: It is a time-critical phase composed of n rounds with the same structure. For each round, V sends a challenge c_i (e.g., a random bit) to P and starts the clock. P will compute the response r_i according to a function f_2. Once receiving r_i, V stops the clock immediately and records the time difference Δt_i between sending out c_i and receiving r_i.

c) Verification Phase: In this phase, V verifies the correctness of all the received responses and checks whether all the recorded round-trip time is smaller than a given bound t_{max} that denotes the maximum round-trip time between P and V. If all the conditions are satisfied, the verifier justifies that the prover is physically nearby and authenticated. Optionally, V can also require P to generate an additional message σ (e.g., a MAC or a signature on all the interactive messages) in order to increase the security level of the protocol.

IV. System Model, Security Model, and Security Objectives

In this section, the system and security models are formalized. The security objectives are identified as well.

A. System Model

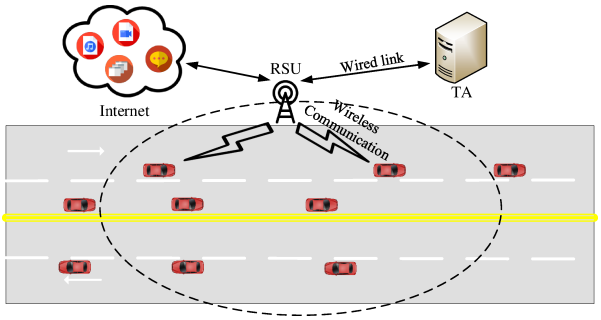


Fig. 2: The system model.

As shown in Figure 2, we consider a typical VANET composed of a trusted authority (TA), a number of vehicles and RSUs. RSUs are connected with Internet in order to provide infortainment services, while interacting with vehicles through wireless communication techniques adhering to IEEE 802.11p standard.

1) TA: it is a trusted party responsible for the registration of RSUs and vehicles, specifically, generating system parameters and distributing secret keys to members (RSUs and vehicles). TA is assumed to have sufficient computation and storage capability such that no adversary can compromise it.
2) RSU: as the infrastructure of a VANET, it communicates with vehicles to provide services like disseminating information. In particular, each RSU deals with resource-accessing requests from vehicles that are inside its communication range, then acts as a proxy to search from the Internet and send the corresponding resources to them. Due to the limited band of wireless communication channel allocated to VANETs, each RSU can only serve for a limited number of vehicles within a specific period.
3) vehicle: each vehicle is equipped with on-board units (OBUs) that are used to communicate with RSUs and other vehicles. Drivers or passengers can enjoy infortainment services through communications between OBUs and RSUs.

B. Security Threats

In this section, we give the security assumptions which describe the capabilities of all the system entities and the attacker and also describe the security threats of the system which can be exploited by the attacker to launch the proposed attack.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2905522, IEEE Transactions on Vehicular Technology

The TA is trusted and cannot be compromised by any attacker. RSUs are semi-honest, i.e., following the protocol but maybe curious about the sensitive information of vehicles. Vehicles could be malicious in the sense that they may claim to be closer to RSUs in order to enjoy the services and this kind of attackers are denoted as *inside* attackers. An *outside* attacker is an entity who is not an authentic member in the VANET system and holds a transceiver that helps it to eavesdrop, inject, send and even modify messages transmitted in the network in order to harm the infrastructure of VANETs. In this paper, only the outside attacker is considered. It can launch the distance fraud attack by utilizing a well-known man-in-the-middle attack as the tool, aiming to shorten the distance between the verifier and the prover.

C. Security Objectives

VANETs suffer from various security and privacy challenges which have been extensively investigated by researchers. In this paper, however, we mainly concentrate on the distance fraud attacks that will be demonstrated in the following section. The security objective of this paper is to resist the DeQoS attack. More precisely, the following two requirements should be guaranteed.

1) *Entity Authentication.* The authenticity of vehicles RSUs should be guaranteed before a connection is established. Authenticating vehicles ensures that only authentic vehicles can enjoy the RSU's services, while authenticating RSUs can prevent the attacker from impersonating RSUs.
2) *Proximity Authentication.* The distance between vehicles and the RSU should be within a given bound. This is to defend the relay attack.

V. Proposed Attack: DeQoS

A. Description of DeQoS

Due to the constrained channel resources, each RSU can only serve for a limited number of vehicles within a specific period in order to ensure the quality of service. It is therefore natural for RSU to authenticate vehicles before starting the service. However, in this section, we elaborate a general attack DeQoS which can bypass existing authentication protocols and significantly degrades the quality of service in VANETs.

As shown in Figure 3, we consider the scenario that consists of a main road and three streets. An RSU is deployed at the intersection of the second street and the main road with the communication range S_R, while the attacker stays somewhere inside S_R and has the communication range S_A. Note that the attacker holds a wireless transceiver which could be very powerful and thus may have better demodulation capacity than the RSU, allowing it to have a larger communication range. Let the intersection area of S_R and S_A be denoted as S_I, then we have $S_I = S_A \cap S_R$. The following describes how the attacker launches a DeQoS attack.

1) The attacker intercepts the "hello" message broadcast by the RSU and relays it to vehicles that are inside $(S_A - S_I)$, namely the vehicles that are inside S_A but not inside S_I.

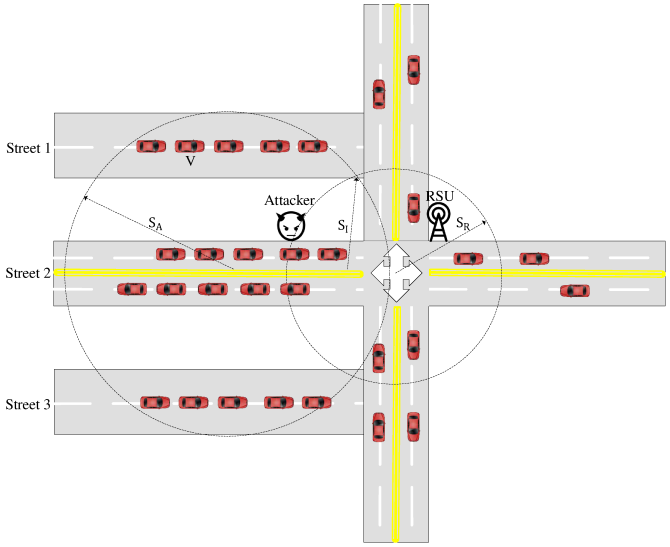


Fig. 3: The demonstrated attack model.
S_A/S_R: the communication range of the attacker/RSU.
S_I: the intersection area of S_A and S_R.

2) Upon receiving the broadcast hello message, these vehicles think they are entering the service range of an RSU. Suppose a vehicle V on Street 1 hopes to connect with the RSU for enjoying services. V will transmit its credentials generated with certain cryptographic algorithm.
3) The attacker receives and relays V's credentials to the RSU.
4) The RSU verifies V with the credentials. Once passed, it will send a confirmation message to V which is again relayed by the attacker, since actually the RSU and V cannot hear from each other without the relay of the attacker. By far, the connection between the RSU and V is established.
5) V sends a request, for example, watching a video.
6) The attacker relays the request to the RSU.
7) The RSU queries for related video resources from other database servers and then sends the video data to V.
8) However, the attacker stops relaying the video data to V, making this service suspended.
9) The attacker repeats step 1-8 with other vehicles inside $S_A - S_I$.

Note that wireless local area networks applies CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) protocol for carrier transmission adhering to the IEEE 802.11 standard, which means at any time only one party is allowed to send messages while others keep silent to avoid transmission collision. Therefore, each party including the RSU maintains a message queue cached with packets that will be sent later. In the above attack, the RSU transmits the video data and waits for an acknowledgment message from V. However, since the attacker does not relay the video data which thus cannot be received by V, V has to keep waiting. Even worse, the attacker can repeatedly establish more dummy connections

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2905522, IEEE Transactions on Vehicular Technology

between the RSU and other vehicles. Sending the resources (especially for the large volume of video data) to vehicles significantly takes up the transmission channel and the RSU's service capability which are both limited. Thus, the resources are wasted, and meanwhile those exploited vehicles have to wait for their services that never turn out. This significantly reduces the quality of service for the legitimate vehicles that are inside the RSU's communication range and should have been able to enjoy the services. If the attacker exploits enough number of outsider vehicles, he could "use up" the RSU's resources which are essentially wasted. In that sense, the RSU is broken down and totally out of service.

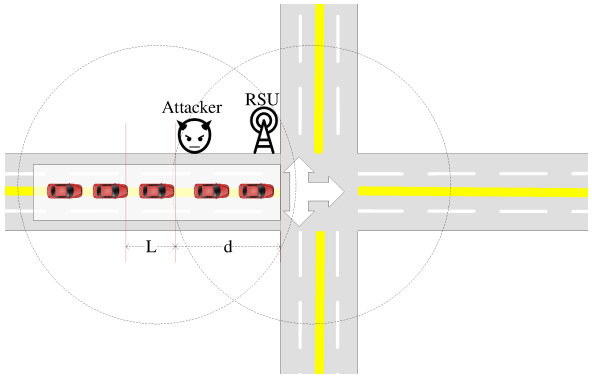


Fig. 4: Modeling a simple attack case with queue theory

B. Analysis of the Success Probability

Figure 4 shows the modeling of a simple case of the attack, where an RSU is installed at the crossroads and an attacker sits close to the RSU. For more complex scenarios with regard to multiple streets, the analysis is similar. Suppose the left and right dashed circles are the communication ranges of the attacker and the RSU, respectively. Let d be the length of the road locating at the intersection of the attacker and the RSU's communication ranges, and L be the length of a vehicle plus the headway distance. We assume that all the vehicles are willing to enjoy the services from the RSU, i.e., all the vehicles are potential victims that could be attacked by the attacker as long as they enter the attack area $S_A - S_I$. This means that the attacker can succeed once the number of vehicles inside $S_A - S_I$ is not zero. The success probability of the attacker is defined to be the chance that the attacker can launch DeQoS attacks, which essentially becomes the probability of the event that there is at least one vehicle inside $S_A - S_I$.

We assume that the arrival of vehicles follows Poisson process with the average arrival rate λ and the average departure rate μ, respectively. We consider a multi-channel queuing model $M/M/N$-queue. Let $\rho = \lambda/\mu$, then ρ/N is the traffic intensity. Let $\Pr(X = k)$ be the probability that the system contains k vehicles. Then, we have

$$\Pr(X=0) = \frac{1}{\sum_{k=0}^{N-1} \frac{\rho^k}{k!} + \frac{\rho^N}{N!(1-\rho/N)}}, \tag{1}$$

$$\Pr(X=k) = \begin{cases} \Pr(X=0) \cdot \frac{\rho^k}{k!}, & if\ 0 < k < N. \\ \Pr(X=0) \cdot \frac{\rho^k}{N!N^{k-N}}, & if\ k \geq N. \end{cases} \tag{2}$$

As discussed above, the attacker can succeed if there exists at least one vehicle inside $S_A - S_I$. Therefore, the attacker has chance to launch attacks if there are more than $\lfloor d/L \rfloor$ vehicles inside the queue, where $\lfloor d/L \rfloor$ is the number of vehicles in the queue that is located inside S_I. Note that vehicles inside S_I can directly communicate with the RSU and thus are excluded from the victims. In addition, vehicles that are being served (i.e., leaving through different lanes) in the queuing system are not counted into the candidates of exploited vehicles either, since it is more practical in sense that the intersection areas of crossroads are usually covered by the RSU as well. Let $\Pr_{adv}$ be the probability that the attacker can launch a DeQoS attack. We have

$$\begin{aligned} \Pr_{adv} =& \Pr(X > N + \lfloor d/L \rfloor) \\ =& 1 - \Pr(X \leq N + \lfloor d/L \rfloor) \\ =& 1 - \sum_{k=0}^{N+\lfloor d/L \rfloor} \Pr(X=k). \end{aligned} \tag{3}$$

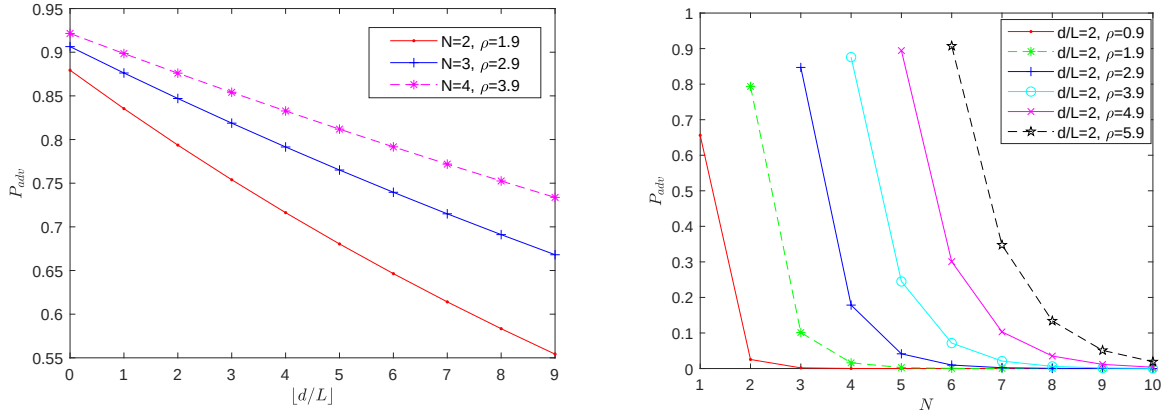
Combining Equation 1, 2 and 3, we can obtain

$$\Pr_{adv} = 1 - \frac{1 + \sum_{k=1}^{N-1} \frac{\rho^k}{k!} + \sum_{k=N}^{N+\lfloor d/L \rfloor} \frac{\rho^k}{N!N^{k-N}}}{\sum_{k=0}^{N-1} \frac{\rho^k}{k!} + \frac{\rho^N}{N!(1-\rho/N)}}. \tag{4}$$

According to Equation 4, the attacker's success probability $\Pr_{adv}$ is related to three factors: $\lfloor d/L \rfloor$ (the number of vehicles inside the intersection area), N (could be the number of forks at the crossroads or the number of lanes in the road), and ρ (note that ρ/N is the traffic intensity). We now explore the impact of these factors on $\Pr_{adv}$, which provides a guide to the attacker for launching the attack with optimal advantages. As shown in Figure 5, we consider the impact of each factor with fixing another two.

We first look into the factor $\lfloor d/L \rfloor$, with fixed (N, ρ) pairs of $(2, 1.9), (3, 2.9), (4, 3.9)$ and thus the corresponding traffic intensities $\rho/N = 0.95, 0.967, 0.975$, respectively. Figure 5(a) shows the success probability of the attack with different values of $\lfloor d/L \rfloor$. It is observed that the bigger $\lfloor d/L \rfloor$, the smaller $\Pr_{adv}$. Intuitively, this means that if there are more vehicles in the intersection area, the attacker has less victims to exploit. Thus, the attacker should stay as far away from the RSU as possible to increase its attack advantages but he should at least be able to be heard by the RSU. In practice, the attacker could stay at the edge of the RSU's communication

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2905522, IEEE Transactions on Vehicular Technology



(a) The impact of d/L

(b) The impact of N and ρ

Fig. 5: The attacker's success probability in different scenarios. Three factors $\lfloor d/L \rfloor$, N and ρ impact the attacker's success probability. We discuss the relationship between the attacker's success probability and the three factors separately.

range.

In terms of the factors N and ρ, we show their impacts on $\Pr_{adv}$ in Figure 5(b). The case is a little subtle, since the traffic intensity ρ/N should belong to $[0, 1]$ while we consider ρ and N separately. It is thus not hard to understand that when we consider the factor of N with a given ρ where $\rho \in [0, x]$, the curve starts from the point $N = x$. Otherwise, the traffic intensity ρ/N could be larger than 1 which makes the traffic system not steady. According to Figure 5(b), given a fixed N, the bigger ρ, the bigger $\Pr_{adv}$. A bigger $\rho = \lambda/\mu$ means a heavier road traffic, which provides the attacker more vehicles to exploit. This indicates that the attacker should choose a road with heavy traffic (imagine a congestion case) to launch the attack. On the other hand, given a fixed ρ, the bigger N, the smaller $\Pr_{adv}$. This is obvious since a bigger N means there are more forks in the crossroads or more lanes in the road, which reduces the queue length and thus the attacker has less vehicles to exploit. This reminds the attacker that he should choose roads with less lanes or less forks at a crossroads to launch the attack. In practice, though, $N = 3$ is a very common case, for example, a crossroads with three forks.

According to the above analysis, the attacker can adaptively choose his strategy to launch the attack in consistence with the environment he is in. Ideally, he would choose a one-way road with a heavy traffic and stay at the edge of the RSU to maximize his chance to launch attacks. For example, if there is no vehicle inside the intersection area (i.e. $\lfloor d/L \rfloor = 0$), $N = 1$, and $\rho = 0.99$, then the probability $P_{adv} = 0.9801$.

VI. Proposed Defense Scheme

A. Establishing a Communication Channel

The main medium access control (MAC) protocols in the data link layer designed for VANETs include carrier-sense multiple access with collision avoidance (CSMA/CA) and time division multiple access (TDMA). Unfortunately, CSMA/CA protocol does not support the deployment of distance bounding. The reason is that the distance-bounding phase is interactive and time-critical, where the prover is required to send the response to the verifier immediately once upon having received the challenge in order to minimize the delay. However, in CSMA/CA, both RSU and vehicles have to contend for transmission chance from the same channel, while at the same time, only one party is allowed to send packages. Suppose an RSU and a vehicle are going to run a distance bounding protocol and more specifically suppose they have already finished the slow phase and will do the n-rounds distance-bounding phase, then the RSU sends a challenge and starts its clock. It is impossible to guarantee that the vehicle can send the response in time since it could be standing in the queue for transmitting information to avoid potential collision. The waiting time is not deterministic and cannot be measured in advance. As a consequence, the round-trip time of the challenge/response propagating cannot be derived accurately from the recorded time, which fails the distance bounding.

To avoid this problem, we adopt TDMA to our proposed scheme. In particular, TDMA runs in a time slotted structure, namely, a virtual frame including a set of time slots with the same time period (e.g. 1ms). Each node is allocated at least one time slot in each frame when the node can send information with no collision. As shown in Figure 6, according to DSRC, the VANET communication channel consists of a control channel c_0 and m service channels $c_1, c_2, \cdots, c_m$. The control channel c_0 is utilized to transmit high priority short applications like periodic safety messages and control information which indicates the time slot on a designated channel that the node can access. The service channels allow transmission of specific application messages where the node can determine the contents themselves. For example, vehicles can exchange their resources with each other through these

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2905522, IEEE Transactions on Vehicular Technology

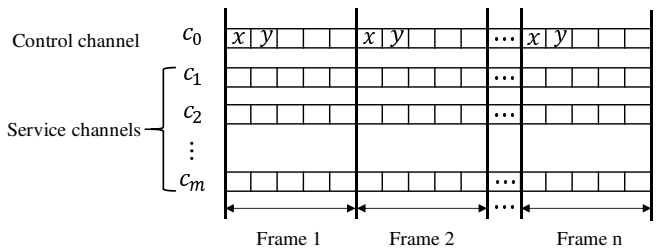


Fig. 6: Time slotted structure of TDMA based MAC protocol for VANETs

service channels.

It will be ideal if a time-critical interactive protocol such as the distance bounding can be finished within one time slot, in which case there will be no waiting time for the verifier and the prover before sending out their information and thus the round-trip time of messages can be measured more precisely. As TDMA-based MAC is widely used in VANETs such as [38], based on their protocols, we propose to establish a communication channel for running distance bounding protocols with two steps.

1) First, the verifier and the prover can make an agreement on selecting an available service channel at an available time slot through the control channel. More precisely, the verifier claims an available time slot t_{i_j} selected from the set of accessible time slots which is determined with the same way as [38] on a service channel c_i and announces an information on the control channel c_0 indicating that it hopes to communicate with the prover with the specified time slot and service channel, where $i \in [1, m]$, $j \in [1, M]$, M is the number of time slots on channel c_i.
2) Upon receiving the announcement, the prover determines whether to accept the claimed service from the verifier. Once the channel c_i and time slot t_{i_j} are determined, the verifier and the prover can first run the proposed distance-bounding based protocol to for authentication purpose, and then exchange information within the left time.

B. Description of the Protocol

In this section, we describe the details of our proposed protocol. For simplicity, we consider the communication between one RSU R and one vehicle V. Intuitively, it is comprised of an authenticated key establishment (AKE) and a distance-bounding procedure. We employ Schnorr signature [39] as the foundation of the key establishment, while the distance-bounding phase is designed based on Yang *et al.*'s framework [24]. In addition, we consider a noisy environment for the distance-bounding channel. Therefore, a noisy tolerant technique is employed. Finally, in the distance-bounding phase, the processing delay of the vehicle is assumed to be fixed and known to the RSU so that it can be eliminated from the measured round-trip time of messages. With this assumption, the distance between the RSU and the vehicle is able to be

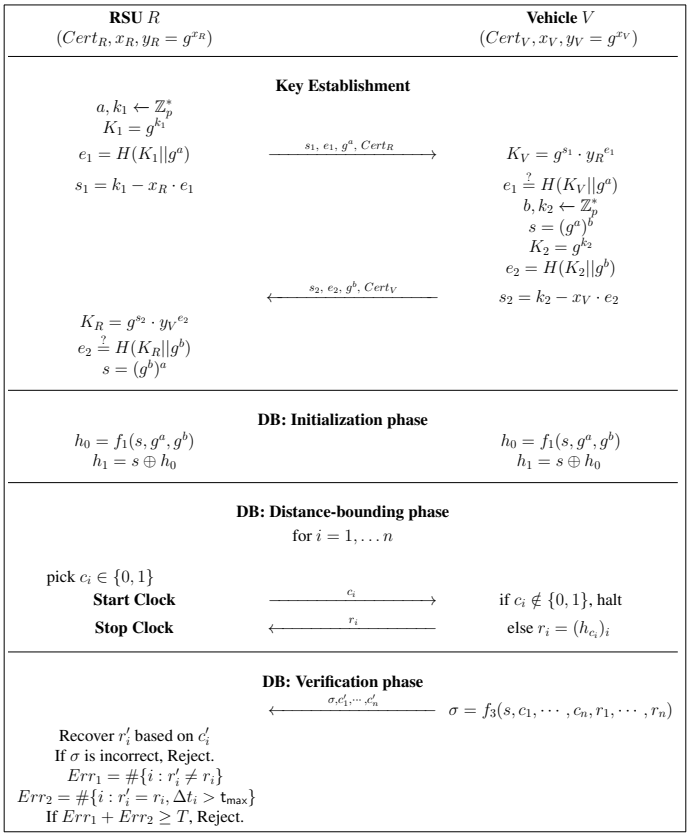


Fig. 7: The proposed defense scheme.

estimated from the message round-trip time and the speed of light. The whole protocol can be elaborated as follows.

1) System Set Up: The trusted authority TA chooses a Schnorr group G with a prime order p and a generator g, a cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$, and its own private and public key pairs (SK_{TA}, PK_{TA}). The parameters g, p, H and TA's public key PK_{TA} are published. TA also issues certificates $Cert_R, Cert_V$ to R and V, respectively. Specifically, when R registers in the system, it randomly selects a private key $x_R \leftarrow \mathbb{Z}_p^*$, computes the corresponding public key $y_R = g^{x_R}$, and sends its identity and public key to TA which will generate a certificate $Cert_R = (ID_R, y_R, g, p, Sig_{SK_{TA}}(ID_R, y_R, g, p))$ for R, where $Sig_{SK_{TA}}(ID_R, y_R, g, p)$ is the signature signed by TA's private signing key SK_{TA} with any secure signature algorithm. Similarly, V selects its private key x_V, computes the corresponding public key y_V and registers to TA to obtain its certificate $Cert_V = (ID_V, y_V, g, p, Sig_{SK_{TA}}(ID_V, y_V, g, p))$.

2) Key Establishment: This phase allows R and V to generate a shared session key s that will be used for the following distance-bounding procedure and future communications. It can be done with the following steps.

1) R selects two random elements a, k_1 in $\mathbb{Z}_p^*$ and computes $K_1 = g^{k_1}$ which will be used by V to authenticate R. Meanwhile, R also generates the signature (e_1, s_1) with

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2905522, IEEE Transactions on Vehicular Technology

$e_1 = H(K_1||g^a)$ and $s_1 = k_1 - x_R \cdot e_1$.

2) R sends the signature together with g^a and $Cert_R$ to V.
3) Upon receiving the messages, V first verifies the signature before establishing the shared key. In particular, it computes $K_V = g^{s_1} \cdot y_R^{e_1}$ and checks the following equation:

$$e_1 \stackrel{?}{=} H(K_V||g^a) \tag{5}$$

where y_R is extracted from $Cert_R$. If Equation 5 holds, V selects random elements $b, k_2 \leftarrow \mathbb{Z}_p^*$ and it generates the shared key $s = (g^a)^b$; otherwise, it will exit from the protocol.
4) V calculates the signature (e_2, s_2) and transmits $s_2, e_2, g^b, Cert_V$ to R.
5) R computes $K_R = g^{s_2} \cdot y_V^{e_2}$ and compares whether e_2 is equivalent to $H(K_R||g^b)$. If yes, it generates the shared key $s = (g^b)^a$; otherwise, it exits from the protocol.

By far, the shared key has been established as $s = (g^a)^b = (g^b)^a = g^{ab}$.

3) Distance Bounding: Once the session key s is created, R and V can start the distance-bounding protocol immediately which consists of three phases.

a) DB:Initialization phase: In this phase, both R and V calculate two registers $h_0 = f_1(s, g^a, g^b)$ and $h_1 = s \oplus h_0$, where f_1 is a pseudorandom function with output length of p. This phase is actually merged with the key establishment phase in sense that g^a and g^b are used as random nonces to ensure the freshness of register.

b) DB:Distance-bounding phase: This phase consists of n rounds. In each round, R sends a random challenge $c_i \in \{0, 1\}$ to V, and starts its clock. Once receiving c_i, V responds $(h_{c_i})_i$ to R who will stop the clock and record the round-trip time Δt_i as long as receiving r_i.

c) DB:Verification phase: In this phase, V computes a final message σ that takes input of s and all previous challenges/responses with a pseudorandom function f_3 with output length of n. Then V sends σ and its received challenges $c_1', \cdots, c_n'$ to R. R recovers r_i' from h_0/h_1 and c_i', based on which R computes the value of σ. If σ is not correct, R will reject V and exit from the protocol. Otherwise, R calculates the number of faulty responses Err_1 from V and the number of positions Err_2 where the response is correct but $\Delta t_i > t_{max}$, where t_{max} is a pre-defined threshold. If $Err_1 + Err_2 \geq T$, then R rejects V and exits, where T is a given threshold.

Correctness of Equation 5. To verify the signature sent from R, V computes $H(K_V||g^a)$ and compares its value with e_1. Note that

$$\begin{aligned} H(K_V||g^a) &= H(g^{s_1} \cdot y_R^{e_1}||g^a) \\ &= H(g^{(k_1 - x_R \cdot e_1)} \cdot (g^{x_R})^{e_1}||g^a) \\ &= H(K_1||g^a) \\ &= e_1. \end{aligned}$$

Therefore, as long as Equation 5 holds, R is authenticated by V. Similarly, V can be authenticated by R through verification of V's signature.

C. Security Analysis

In this section, we analyze the security of the proposed defense protocol. According to the security goals, we will show that our protocol can achieve both entity authentication and proximity authentication.

1) Entity Authentication: The entity authentication is ensured by the authenticated key establishment procedure. In particular, R sends its certificate $Cert_R$ which includes its public key y_R verified by the trusted TA. The signature (e_1, s_1) together with y_R allow V to verify the authenticity of R. It is the same for R to verify V. The security of the key establishment holds as long as the Schnorr's signature scheme is secure. Therefore, with this method, both R and V can be convinced that they are communicating with each other.

2) Proximity Authentication: The proximity authentication is achieved by the distance-bounding procedure which utilizes the round-trip time of radio signals to measure the distance. Note that no attacker can accelerate the velocity of the radio signal since it is approximate to the speed of light. The attacker in DeQoS stands between an RSU (e.g., R) and a vehicle (e.g., V) that is outside the communication range of R. Therefore, in order to trick R to connect a dummy connection with V, the attacker has to shorten the distance between R and V, i.e., returning all of the correct responses that should be given by V to R within t_{max}. The only thing that the attacker can do is sending a guessed response r_i^* calculated by itself to R before it receives the actual response r_i from V in each distance-bounding round.

We first consider the scenario of a noiseless environment. If the attacker follows the protocol and guesses all the responses itself, then the best strategy is to return a random bit as the response, which results in the success probability of $\frac{1}{2}$ for each round and thus $(\frac{1}{2})^n$ as the overall success probability. However, a smart attacker could launch a *pre-ask strategy* where it queries V with its own chosen challenge c_i^* to obtain the corresponding response r_i^* from V before the actual distance-bounding phase between R and V happens. Then in the actual distance-bounding phase, the attacker alone plays with R trying to pass the protocol with the previously collected messages. With probability of $\frac{1}{2}$, R's challenge c_i is equivalent to the attacker's pre-asked challenge (i.e., $c_i = c_i^*$) and thus the attacker can reply the correct response r_i^* which should equal r_i. Otherwise, if $c_i \neq c_i^*$, the attacker returns a random bit as the response. Thus, the success probability that the attacker can return a correct response for each round is $\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$. Since different rounds of distance-bounding phases are independent, the probability that the attacker can return correct answers to all of R's challenges is $(\frac{3}{4})^n$. As to the noisy environment, the protocol can tolerate T errors which thus leaves the attacker T positions where it does not bother to guess. In this case, the attacker's success probability becomes $(\frac{3}{4})^{n-T}$.

Nevertheless, the attacker still needs to return the correct final message σ to R as well. Without the secret session key s, the success probability of the attacker generating the correct σ is $(\frac{1}{2})^{l_f}$ if f is a secure pseudorandom function that is indistinguishable with a random string, where l_f is the length

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2905522, IEEE Transactions on Vehicular Technology

of the output of f. As a consequence, the attacker's overall success probability becomes $\min\{(\frac{1}{2})^{l_f}, (\frac{3}{4})^{n-T}\}$. In practice, n is supposed to be less than 160. Therefore, if we deploy the pseudorandom function with 256-bits outputs, then the attacker's success probability is $(\frac{1}{2})^{256}$ which is negligible. This means the attacker has no way to break the proximity authentication of the protocol.

VII. Evaluations

In this section, we evaluate the demonstrated DeQoS attack in case of different scenarios in order to verify the practicability of the attack. As to the defense scheme, due to the limitation of there having not been tools for simulating distance-bounding protocols, we leave it in the future work. We implement the attack with Matlab R2017b on a laptop with 2.8 GHz Intel(R) Core(TM) i7-7700HQ CPU and 16 GB RAM. A series of traffic simulations with a number of roads and vehicles are conducted under different scenarios.

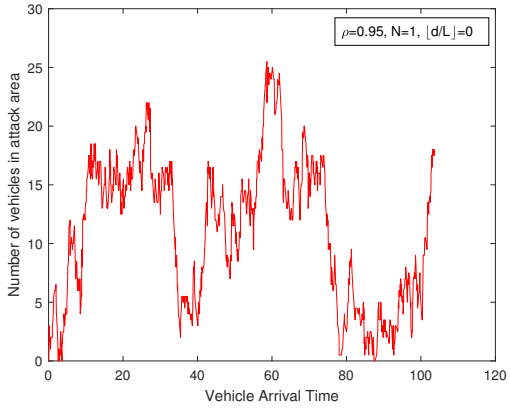
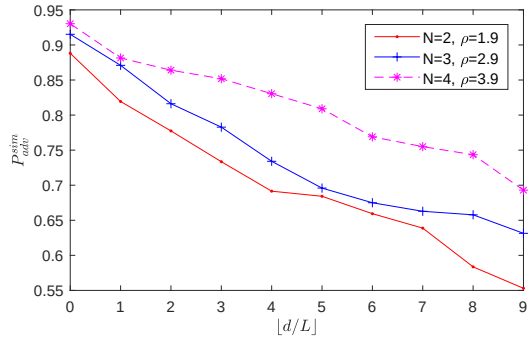


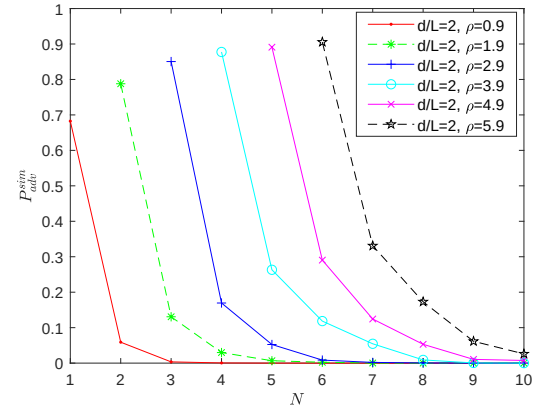
Fig. 8: Number of vehicles in attack area at specific vehicle arrival times

Figure 8 shows the number of vehicles in attack area at any specific vehicle arrival time. In this experiment, we consider the $M/M/1$-queue model (considering a one-way road in practice) with the utilization rate (i.e., traffic intensity) of $\rho/1 = 0.95$, and there is no vehicle locating in the intersection area of the attack and RSUs communication ranges (i.e., $\lfloor d/L \rfloor = 0$). The number of vehicles arriving and then leaving the system is 1000. The mean arrival time is 0.1 min, i.e., 10 arrivals per minute. The mean service time is 0.095. We can see from the figure that in majority of time there are vehicles standing in the attack area, which provides opportunities for the attacker to launch attacks.

In the second experiment, we simulate more complex traffics, in particular, an $M/M/N$-queue with different utilization rates, different server rates and different number of vehicles in the intersection area. The number of vehicles in the system is 1000, the number of vehicles inside the intersection area of RSU and attacker's communication ranges $\lfloor d/L \rfloor$ is not more than 9; for the $M/M/N$-queue parameters,



(a) The impact of d/L



(b) The impact of N and ρ

Fig. 9: Simulated results of the attacker's success probability in different scenarios.

the value of N varies from 1 to 10 (it is reasonable to set the maximum value of N to be 10 since it is really rare to have ten-or-more-way intersections in practical traffic roads), a series of $\rho = \{0.9, 1.9, 2.9, 3.9, 4.9, 5.9\}$ are considered and thus the corresponding queue system utilization rates ρ/N are $\{0.9/1, 1.9/2, 2.9/3, 3.9/4, 4.9/5, 5.9/6\} = \{0.9, 0.95, 0.967, 0.975, 0.98, 0.9833\}$. Figure 9 shows the simulated results of the attacker's success probability P_{adv}^{sim} under different environments, in contrast with the theoretical results in Figure 5. Figure 9(a) demonstrates the relationship of P_{adv}^{sim} and $\lfloor d/L \rfloor$, while Figure 9(b) shows the impacts of N and ρ on P_{adv}^{sim}. Both figures indicate that the experiment results verify the correctness of the theoretical analysis. Namely, the bigger the $\lfloor d/L \rfloor$, the smaller the P_{adv}^{sim}; given a fixed N and $\lfloor d/L \rfloor$, the bigger ρ, the bigger P_{adv}^{sim}; given a fixed ρ and $\lfloor d/L \rfloor$, the bigger N, the smaller P_{adv}^{sim}.

VIII. Conclusions

In this paper, we have investigated the security issues of VANETs communications and introduced a new attack which can utilize physical contexts as the attack tool to impact the quality of service. The attacker's success probability was

comprehensively discussed by converting it to the probability that there exists at least one client in the queue in an $M/M/N$-queue system. To demonstrate the practicability of the attack, we implemented it with Matlab and the simulated results verified the theoretical analysis. Furthermore, we have proposed a new cross-layer authentication protocol combining an authenticated key exchange process and a distance-bounding process and analyzed its effectiveness to prevent DeQoS. In the future work, we will implement the distance-bounding based defense mechanism to explore its practicability.

ACKNOWLEDGMENT

Jian Weng was partially supported by National Key R&D Plan of China (Grant Nos. 2017YFB0802203, 2018YFB1003701), National Natural Science Foundation of China (Grant Nos. 61825203, U1736203, 61732021), Guangdong Provincial Special Funds for Applied Technology Research and Development and Transformation of Important Scientific and Technological Achieve (Grant Nos. 2016B010124009 and 2017B010124002). Anjia Yang was partially supported by National Natural Science Foundation of China (Grant No. 61702222), China Postdoctoral Science Foundation (Grant No. 2017M612842), Postdoctoral Foundation of Jinan University. Xiaodong Lin and Xuemin (Sherman) Shen were partially supported by NSERC of Canada.

REFERENCES

[1] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8–15, 2006.

[2] N. Cheng, F. Lyu, J. Chen, W. Xu, H. Zhou, S. Zhang, and X. Shen, "Big data driven vehicular networks," *IEEE Network*, vol. 32, no. 6, pp. 160–167, 2018.

[3] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[4] C. Huang, R. Lu, and K.-K. R. Choo, "Vehicular fog computing: Architecture, use case, and security and forensic challenges," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 105–111, 2017.

[5] J. Weng, J. Weng, Y. Zhang, W. Luo, and W. Lan, "Benbi: Scalable and dynamic access control on the northbound interface of sdn-based vanet," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 822–831, 2019.

[6] A. Wasef and X. Shen, "Emap: Expedite message authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 78–89, 2013.

[7] L. He and W. T. Zhu, "Mitigating dos attacks against signature-based authentication in vanets," in *2012 IEEE International Conference on Computer Science and Automation Engineering*, vol. 3, 2012, pp. 261–265.

[8] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[9] A. Yang, X. Tan, J. Baek, and D. S. Wong, "A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification," *IEEE Transactions on Services Computing*, vol. 10, no. 2, pp. 165–175, 2017.

[10] H. J. Jo, I. S. Kim, and D. H. Lee, "Reliable cooperative authentication for vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 4, pp. 1065–1079, 2018.

[11] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "Healthdep: An efficient and secure deduplication scheme for cloud-assisted ehealth systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4101–4112, 2018.

[12] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 289–299, 2014.

[13] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.

[14] S. Tzeng, S. Horng, T. Li, X. Wang, P. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in vanets," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235–3248, 2017.

[15] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6504–6517, 2018.

[16] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J. Liu, Y. Xiang, and R. Deng, "Crowdbc: A blockchain-based decentralized framework for crowdsourcing," *IEEE Transactions on Parallel and Distributed Systems*, 2018.

[17] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proceedings of the Network and Distributed System Security Symposium*, 2011.

[18] M. Roland, J. Langer, and J. Scharinger, "Applying relay attacks to google wallet," in *2013 5th International Workshop on Near Field Communication*, 2013, pp. 1–6.

[19] K. Zeng, S. Liu, Y. Shu, and D. Wang, "All your gps are belong to us: Towards stealthy manipulation of road navigation systems," in *27th USENIX Security*. USENIX Association, 2018, pp. 1527–1544.

[20] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*. New York, NY, USA: ACM, 2011, pp. 75–86.

[21] S. Brands and D. Chaum, "Distance-bounding protocols (extended abstract)," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques-EUROCRYPT*. Springer-Verlag, 1993, pp. 344–359.

[22] A. Yang, Y. Zhuang, and D. S. Wong, "An efficient single-slow-phase mutually authenticated RFID distance bounding protocol with tag privacy," in *International Conference on Information and Communications Security*, ser. LNCS, vol. 7618. Springer, 2012, pp. 285–292.

[23] H. Kılınç and S. Vaudenay, "Efficient public-key distance bounding protocol," in *Advances in Cryptology – ASIACRYPT*. Springer Berlin Heidelberg, 2016, pp. 873–901.

[24] A. Yang, E. Pagnin, A. Mitrokotsa, G. P. Hancke, and D. S. Wong, "Two-hop distance-bounding protocols: Keep your friends close," *IEEE Transactions on Mobile Computing*, vol. 17, no. 7, pp. 1723–1736, 2018.

[25] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "Tsvc: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4987–4998, 2008.

[26] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," *RSA Cryptobytes*, vol. 5, no. 2, pp. 2–13, 2002.

[27] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "Pba: Prediction-based authentication for vehicle-to-vehicle communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 71–83, 2016.

[28] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of dos attacks in vanet," *Wireless Personal Communications*, vol. 73, no. 1, pp. 95–126, 2013.

[29] A. M. Malla and R. K. Sahu, "Security attacks with an effective

solution for dos attacks in vanet," *International Journal of Computer Applications*, vol. 66, no. 22, pp. 45–49, 2013.

[30] T. Leinmuller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 16–21, 2006.

[31] G. Yan, G. Choudhary, M. C. Weigle, and S. Olariu, "Providing vanet security through active position detection," in *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*. New York, NY, USA: ACM, 2007, pp. 73–74.

[32] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Secure location verification for vehicular ad-hoc networks," in *IEEE Global Telecommunications Conference*, 2008, pp. 1–5.

[33] Z. Ren, W. Li, and Q. Yang, "Location verification for vanets routing," in *2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2009, pp. 141–146.

[34] O. Abumansoor and A. Boukerche, "A secure cooperative approach for nonline-of-sight location verification in vanet," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 275–285, 2012.

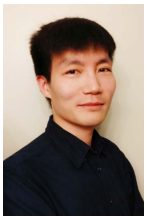
[35] S. Yan, R. Malaney, I. Nevat, and G. W. Peters, "Location verification systems for vanets in rician fading channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp. 5652–5664, 2016.

[36] D. Singelée and B. Preneel, "Location verification using secure distance bounding protocols," in *IEEE 2nd International Conference on Mobile Adhoc and Sensor Systems*, 2005.

[37] G. P. Hancke and M. G. Kuhn, "An RFID Distance Bounding Protocol," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, ser. SECURECOMM '05. IEEE Computer Society, 2005, pp. 67–73.

[38] H. A. Omar, W. Zhuang, and L. Li, "Vemac: A tdma-based mac protocol for reliable broadcast in vanets," *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1724–1736, 2013.

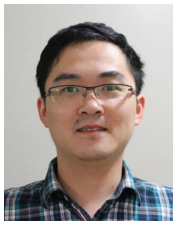
[39] C. P. Schnorr, "Efficient identification and signatures for smart cards," in *Advances in Cryptology – CRYPTO*, G. Brassard, Ed. New York, NY: Springer New York, 1990, pp. 239–252.



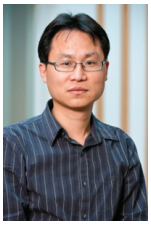
Anjia Yang received the Ph.D. degree from the City University of Hong Kong in 2015. He is currently a postdoctoral researcher in Jinan University, Guangzhou, and a visiting scholar at the University of Waterloo, Canada. His research interests include VANETs security, IoT security, applied cryptography, blockchain security and cloud computing.

Jian Weng received the Ph.D. degree in computer science and engineering from Shanghai Jiao Tong University, in 2008. From 2008 to 2010, he held a post-doctoral position with the School of Information Systems, Singapore Management University. He is currently a Professor and the Dean with the College of Information Science and Technology, Jinan University. His research interests include public key cryptography, cloud security, blockchain, etc. He has published over 100 papers in cryptography and security conferences and journals, such as CRYPTO, EUROCRYPT, ASIACRYPT, TCC, PKC, TPAMI, TIFS, and TDSC. He served as a PC co-chairs or PC member for more than 30 international conferences. He also serves as associate editor of IEEE Transactions on Vehicular Technology.

Nan Cheng Nan Cheng (S'12,M'16) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo. He is currently working as a joint Post-doctoral fellow with the Department of Electrical and Computer Engineering, University of Toronto and the Department of Electrical and Computer Engineering, University of Waterloo. His research interests include performance analysis, MAC, opportunistic communication for vehicular networks, unmanned aerial vehicles, and application of AI for wireless networks.



Jianbing Ni (M'18) received the Ph.D. degree in Electrical and Computer Engineering from University of Waterloo, Waterloo, Canada, in 2018. He is currently a postdoctoral fellow at the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada. His research interests are applied cryptography and network security, with current focus on cloud computing, smart grid, mobile crowdsensing and Internet of Things.



Xiaodong Lin (M'09-SM'12-F'17) received the PhD degree in Information Engineering from Beijing University of Posts and Telecommunications, China, and the PhD degree (with Outstanding Achievement in Graduate Studies Award) in Electrical and Computer Engineering from the University of Waterloo, Canada. He is currently an associate professor in the School of Computer Science at the University of Guelph, Canada. His research interests include computer and network security, privacy protection, applied cryptography, computer forensics, and software security. He is a Fellow of the IEEE.

Xuemin (Sherman) Shen (M'97-SM'02-F'09) received Ph.D. degree from Rutgers University, New Jersey (USA) in electrical engineering, 1990. Dr. Shen is a University Professor, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.

Dr. Shen is the Editor-in-Chief for IEEE Internet of Thing Journal and the vice president on publications of IEEE Communications Society. He received the Joseph LoCicero Award in 2015, the Education Award in 2017, the Harold Sobol Award in 2018, and the James Evans Avant Garde Award in 2018 from the IEEE Communications Society. He has also received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, 2010, 2014, and 2018 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada. Dr. Shen served as the Technical Program Committee Chair/Co-Chair for IEEE Globecom' 16, IEEE Infocom'14, IEEE VTC'10 Fall, the Symposia Chair for IEEE ICC'10, the Tutorial Chair for IEEE VTC'11 Spring, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking.