IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 7, 2020, accepted August 13, 2020, date of publication August 18, 2020, date of current version October 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3017557

Context-Aware Quantification for VANET Security: A Markov Chain-Based Scheme

JIAN WANG, HONGYANG CHEN, AND ZEMIN SUN
[1]College of Computer Science and Technology, Jilin University, Changchun 130012, China
[2]Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun 130012, China

Corresponding author: Zemin Sun (laurasun166@gmail.com)

This work was supported in part by the National Nature Science Foundation under Grant 61572229, Grant 6171101066, Grant 61872158, and Grant 61806083; in part by the Jilin Provincial Science and Technology Development Foundation under Grant 20170204074GX, Grant 20180201068GX, and Grant 20190103051JH; and in part by the Jilin Provincial International Cooperation Foundation under Grant 20180414015GH.

ABSTRACT Recently, the quantification of VANET security has drawn significant attention due to the lack of standard computational metrics. The salient features of VANET, such as highly dynamic connections, sensitive information sharing, and unreliable fading channels, make the security quantification challenging. Accurate measurement for VANET security depends on the sufficient understanding of ''context'', or making sense of the states, environment, or situation. This article proposes a context-aware security quantification scheme for VANET based on the Markov chain. Firstly, a Homogeneous Continuous-Time Markov Chain (HCTMC)-based security state model is designed for VANET. The value of each state of the HCTMC is determined with a value function that incorporates the security strength of transmitted data, dynamic and randomness of the vehicular channel, and transmission delay of the current situated environment of VANETs. Finally, the state transition matrix is derived based on the Homogeneous Discrete-Time Markov Chain (HDTMC) and Homogeneous Poisson Process (HPP). Simulation results show that the security quantification method enables the VANET's system to adopt context-aware defense strategies according to the situated environment.

INDEX TERMS Security quantification, VANET, Markov chain, state transition.

I. INTRODUCTION

Vehicular Ad Hoc Network (VANET), as a prominent form of Mobile Ad Hoc Network (MANET), plays an essential role in the future Intelligent Traffic System (ITS) by providing a wide range of applications to improve road safety and driving comfort. It is a distributed self-organizing network built up by high-speed vehicles [1], and is consisted of three parts: Trusted authorities (TA), Road Side Unit (RSU), and On Board Unit (OBU) [2]. TA can be regarded as an authority center that provides RSUs and OBUs with a variety of security services such as registration, identity authentication, and certificate management. Furthermore, RSUs are deployed at alongside the road to transmit the information collected from OBUs to TA. Besides,each vehicle is equipped with an OBU that enables it to communicate with other vehicles or RSUs through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructures (V2I) modes, respectively. Consequently, VANETs facilitate the real-time exchanges of information on traffic conditions, further provide the prediction of the current environment, and make drivers more aware of driving situations, and take early measures against anomalies [3].

Despite these advantages, VANET is facing various challenges, particularly in the aspect of security. VANET is distinct from other types of MANETs in terms of highly dynamic topology, open-access wireless environment, and the salient features of propagation channels such as time-varying, fading, and path loss, which makes vehicles more vulnerable to various attacks. An attacker may impersonate a legitimate transmitter vehicle, and the messages may be eavesdropped, forged, or replayed by an adversary. VANET must provide adequate security mechanisms to protect against the attacks because the transmitted messages are closely related to driving security.

Most of the recent studies focus on the security mechanisms design, such as authentication, confidentiality, integrity, or privacy [4]. The quantification for VANET

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Arshad.

security is a prerequisite for vehicles to adopt right defense strategies but remains a challenging issue. Although several works propose quantitative security metrics by designing attacker or threat models [5], [6], they enforce predefined policies in advance. These methods are static and lack the flexibility of protecting against various attacks. The vehicle can only respond to specific attacks but is not capable of behaving adaptively to the potential threats. As a consequence, an accurate quantification should be context aware to understand the surrounding environment.

Compared with the traditional MANET, it is challenging to measure the security level in VANET, where the network is highly dynamic, the link is time-varying, and the scenario random (e.g., urban and suburban). Therefore, this article focus on designing the quantitative security model with context-awareness and environment-adaption by considering the salient features of VANET. Firstly, regarding the environment, the Nakagami multi-pathcand fading of the vehicular network. Furthermore, from the perspective of the vehicle user's inherent characteristics, the transmission delay is incorporated into the security metric to express the vehicle's Quality of Service (QoS) requirement, i.e., time-sensitivity. Besides, regarding the various types of attackers, the attacker's capability is considered in the process of security quantification. At last, the Homogeneous Continuous-Time Markov Chain (HCTMC) and Homogeneous Discrete-Time Markov Chain (HDTMC) are employed to analyze the security state transition under different VANET environment. In conclusion, this article proposes a context-aware method for security quantification based on HCTMC and HDTMC. This scheme enables vehicles to adopt strategies in the dynamic VANET environment adaptively. The main contributions can be concluded as:

- A context aware and environment adaptive security quantification scheme for VANET based on the Markov chain is proposed.
- An HCTMC-based security state model is designed by incorporating the dynamic and randomness of the vehicular channel, along with the QoS consideration.
- The matrix of state transition is derived based on the HDTMC and Homogeneous Poisson Process (HPP).

The remainder of this article is organized as follows. Section II overviews the related work in recent years. Section III introduces the system models in detail. Section IV shows the extensive simulation results and numerical analysis. Finally, we give the conclusion in Section V.

II. RELATED WORK

VANET has been extensively studied and is gradually becoming a research hotspot in the 5G era. Hasrouny *et al.* [4] presented an extensive overview of VANET security challenges and existing solutions in a comprehensive manner. Rehman *et al.* [7] evaluates the impact of speed differences among vehicles over the performance of two widely adopted classes of messaging schemes in VANETs, namely the furthest distance and link quality based schemes. El-Sayed *et al.* [8] proposed a new entity centric trust framework using decision tree classification and artificial neural networks.This model uses multifaceted role and distance based metrics like Euclidean distance to estimate the trust. Arif *et al.* [9] used the HABE encryption method to provide central security and offers secure and reliable communication. The proposed framework can address major VANETs problems by delivering Vehicle to Infrastructure (V2I) and V2V communications. Therefore, with the in-depth study of VANET by more and more domestic and foreign research scholars, the importance of VANET's safety has emerged.

Regarding the security of VANET, Mihai *et al.* [10] provides a comprehensive classification of related state-of-the-art approaches following three key directions: 1) privacy, 2) authentication and 3) message integrity within VANETs. Discussions, challenges and open issues faced by the current and next generation of vehicular networks are also provided. El-Rewini *et al.* [11] proposed a three-layer framework (sensing, communication and control), through which automotive security threats can be better understood and provides the state-of-the-art review on attacks and threats relevant to the communication layer and presents countermeasures. In [12], a location-based secure preset group is proposed to create a communication network where both local security and global security can be achieved dynamically. Wagan *et al.* [13] presented a hardware based security framework that uses both standard asymmetric PKI and symmetric cryptography for faster and secure safety message exchange. Szczypiorski *et al.* [14] improved on Wagan's security framework by addressing problems related to traffic efficiency and public transport operations. It provides a tool to monitor and secure routing protocols, as well as to detect and remove untrusted nodes in the network. Siddiqui and Khaliq [15] proposed a security analysis method based on authentication attacks: classifying attacks based on security requirements and pointing out security vulnerabilities about unique threats. Chen *et al.* [16] classified the received information based on the routing protocol information and analyzed the security threats for different types of information content.

In terms of security quantification, to obtain the risk value in real-time, Wei *et al.* [17] designed a hidden Markov to quantify network security risks and assess threats in real-time. Zhang [18] used the big data fuzzy mean clustering algorithm to cluster and evaluate the statistical characteristic information data of network intrusion. By extracting the security status of cyber risks, the high-level spectrum characteristics of big data were quantitatively analyzed, and the quantitative assessment of the security status of cyber risks and the detection of network intrusions were achieved. Griffin *et al.* [19] proposed a semi-Markov processes (SMP) to model the transition between the security states of abstract software systems to analyze the security of software systems. Almasizadeh and Azgomi [20] presented a suitable method to quantify security: stochastic modeling technology, which treats the intrusion process as a series of basic attack phases

and strictly analyzes the interaction between the attacker and the system at each phase. Quantify security by modeling complex attack processes and assessing the required security measures. Rahman *et al.* [21] constructed a vehicle-to-vehicle task offloading framework that allows vehicles to utilize computation resources available at nearby vehicles. To overcome mobility issues, we implement Context-aware opportunistic offloading schemes based on speed, direction, and locality of vehicles.

Although the safety of VANET has attracted the attention of researchers, few people have been able to evaluate VANET from a quantitative perspective. Most of them use external devices or strengthen the VANET from the perspective of an attacker, or conduct quantitative security research on other system networks. This article focuses on quantifying VANET security using a context awareness-based computational model.

III. METHOD

The quantitative security model and the state transition model are introduced in this section. The HCTMC state model is presented firstly corresponding to each security state of VANET. Then, the quantitative security level of VANET is modeled based on the HCTMC. Finally, we derive the matrix of HCTMC state transition, according to which the VANET can adjust the security defense strategy adaptively according to the situated context.

A. HCTMC STATE MODEL

In this section, an HCTMC state model is used to describe the security states of VANET, as shown in Fig.1. Assume there are seven security level of VANET, i.e., security state, vulnerable state, attacked state, degenerate state, failed state, positive state, and negative state [22]. The HCTMC model is divided into seven states accordingly, where the process starts from the current state and moves successively from one state to another. Furthermore, the security level of each state is quantified as the value of each HCTMC state, which is formulated according to the information security and communication delay in the situated environment.

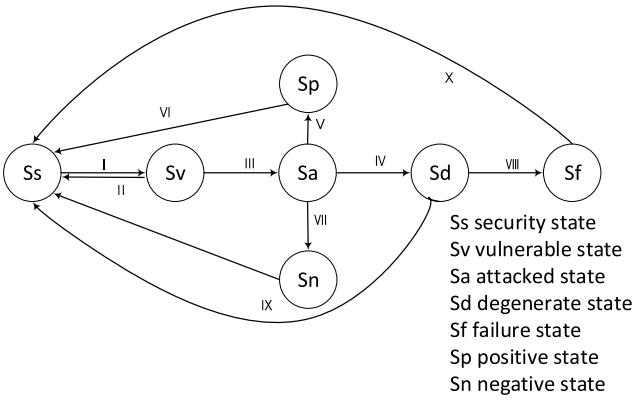

FIGURE 1. HCTMC Model [22].

The state transition model in Fig.1 is described as follows. (I) When the system's protection measures are failed (e.g., authentication failure, system upgrade vulnerability, encryption failure, and access control invalid), the system will transfer from a security state to a vulnerable state. Conversely, if the system is capable of protecting against attacks, it will stay in a security state. (II) If an attacker is detected, the vehicular system will immediately take protective measures to eliminate the threat. In this case, the vehicular system transfers from a vulnerable state to a security state. The system in this state periodically monitors the status of the communication and takes appropriate measures against the potential threats. (III) If the system fails to detect an attacker's behaviors in a vulnerable state, it will enter the attacked state. In the attacked state, the system aims to minimize the damage caused by the attacker. At the same time, the system will follow the principle of priority to reply to a security state. (IV) If the strategies adopted by the system fails to resist the attacks, the system will move into a degenerate state. (V) The system transfers from an attacked state in a positive state when the threats are successfully detected and resisted. (VI) The system in a positive state will gradually enter the self-healing phase and move into a safe state. (VII) The system in an attacked state without sufficient protection strategies will moves into the passive state. (VIII) The system situated in a degenerate state will eventually move into a failed state due to the lack of sufficient protective measures. (IX) (X) (XI) The system can be restored from failed, degenerate, or negative state to the initial state by external manual intervention, which helps it upgrade for future security considerations.

B. OBJECTIVE FUNCTION

In this section, the VANET's security level of each current state is formulated as the objective function T by considering the effect of security operation on the communication delay. Therefore, T can be modeled by integrating the expected security strength S_e and the delay D and can be expressed as:

$$T = \alpha \cdot S_e + \beta \cdot D_e \tag{1}$$

A large value of T indicates that VANETs are in a relatively safe network environment, where the system operates effectively. On the contrary, the system with a small value of T strives to transfer into a secure state actively. Furthermore, the value range of T is divided into seven sub-ranges corresponding to the seven states of the HCTMC model. α and β are the weights of security and delay metrics, respectively, which depend on the system's requirements for security and delay of communication. The sum of α and β is 1; both of the weights are given as 0.5 by default.

$$\alpha + \beta = 1 \tag{2}$$

1) SECURITY STRENGTH

The communications among legitimate vehicles could be exposed into the threats of attackers due to the openness

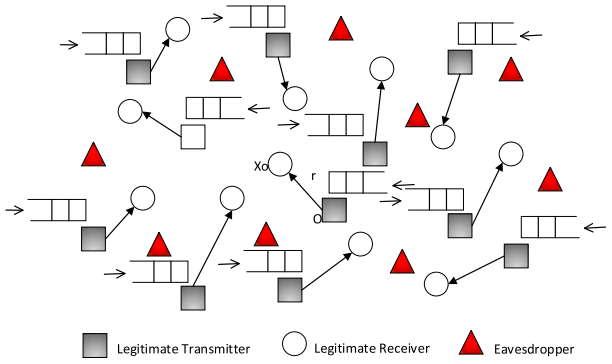

FIGURE 2. Receivers, senders, and attackers in the network topology [27].

and dynamic of wireless channels, as shown in Fig.2. The security strength of the information is quantified according to the amount of computation required by an attacker to crack the messages [23]. Ideally, a computationally secure encryption system makes it impossible for an attacker to crack with exhaustive search. Therefore, the security level of the transmitted messages depends on the attacker's strength to break the cipher.

We assume the transmitted frame is encrypted using block encryption where a transmitted frame is split into several data blocks that are encrypted separately. The " vulnerability" of an encrypted data block with length N can be expressed as the probability of being cracked by attackers:

$$\phi = p_r\left(\sigma = N\right), \tag{3}$$

where σ denotes the strength of an attacker. An adversary node with the strength σ can crack any encrypted data with length less than or equal to N in limited time, i.e., $p_r\left(\sigma = N\right) = p_r(\sigma \geq N)$. The Linear Adversary Strength Model [24] is used to model an attacker's strength as a uniform distribution: $\frac{1}{N_{max}-N_{min}}$, where N_{max} and N_{min} are the upper-bound and lower-bound of the data length. Assuming that the data length varies in the range $[0, N_f]$ (i.e., $N_{min} = 0, N_{max} = N_f$), the vulnerability can be further expressed as:

$$\phi = p_r(\sigma \geq N) = \frac{N_f - N}{N_{max} - N_{min}} = \frac{N_f - N}{N_f - 0} = \frac{N_f - N}{N_f}, \tag{4}$$

where N_f denotes the size of data frame. Furthermore, the security level of a frame depends on the number of attackers who can crack the encrypted block (assuming that all attacks have the same attack capability). Therefore, the security level of a data frame facing n_e attackers can be given as:

$$S_e = (1-\phi)^{n_e} = (\frac{N}{N_f})^{n_e} \tag{5}$$

The derivation of n_e will be introduced in detail. The average communication transmission range [23] of the transmitter can be expressed as:

$$\bar{r} = \left(\frac{p_t K}{m\Upsilon_0 W}\right)^{\frac{1}{\beta}} \left(\frac{1}{\beta}\right) \sum_{l=0}^{m-1} \frac{\Gamma\left(1+\frac{1}{\beta}\right)}{l!}, \tag{6}$$

where μ (vehicles/m^2) denotes the total vehicle density, ρ (vehicles/vehicle) is the eavesdropping node density, p_t is the transmission power, β is the path loss coefficient, m is the fading coefficient of the Nakagami channel, and γ_0 is the threshold of the carrier-to-noise ratio (CNR). K is a constant related to the path loss model and is expressed as:

$$K = \frac{G_t G_r C^2}{4\pi f_c}, \tag{7}$$

where G_t,G_r represents the gain of the transmitting and receiving antennas, C is the speed of light, and f_c is the carrier frequency. W denotes the total input noise power of a legitimate receiver and can be expressed as:

$$W = BT_0AF, \tag{8}$$

where B is Boltzmann constant, T_0 is the noise temperature of the receiving system, A is the channel bandwidth, and F is the noise figure. Substituting (7) and (8) into (6), $\bar{r}$ can be expressed as:

$$\bar{r} = \left(\frac{p_t G_t G_r C^2}{m\Upsilon_0 \left(4\pi f_c\right) BT_0AF}\right)^{\frac{1}{\beta}} \left(\frac{1}{\beta}\right) \sum_{l=0}^{m-1} \frac{\Gamma\left(1+\frac{1}{\beta}\right)}{l!} \tag{9}$$

Therefore, the number of eavesdroppers can be roughly estimated as:

$$\begin{aligned} n_e &= \pi \bar{r}^2 \mu\rho \\ &= \pi \left(\left(\frac{p_t G_t G_r C^2}{m\Upsilon_0 \left(4\pi f_c\right) BT_0AF}\right)^{\frac{1}{\beta}} \left(\frac{1}{\beta}\right) \sum_{l=0}^{m-1} \frac{\Gamma\left(1+\frac{1}{\beta}\right)}{l!}\right)^2 \mu\rho \end{aligned} \tag{10}$$

2) DELAY

In this subsection, the delay metric D is constructed using the random geometry and queuing theory, which are the primary and extensively used methodological framework for analyzing network delay. Firstly, service rate of the queue can be given as:

$$p_q = p\left(1 - p_{cf}\right), \tag{11}$$

where p is the transmission probability, and p_{cf} denotes the connection failure probability in each time slot. The activation probability of a legitimate link q is expressed as:

$$q = \frac{\xi}{\left(1 - p_{cf}\right)}, \tag{12}$$

where the probability of a packet arriving in each time slot is ξ

The queuing system at a legitimate transmitter is a Geo / G / 1 queue, or a discrete-time single-server retry queue [25], [26]. In the Geo / G / 1 queue, the probability of a packet

arriving in each time slot is ξ, the probability of successful transmission is $p\left(1-p_{cf}\right)$, and the service time of the data packet is a geometric distribution. According to [25], the average delay of the Geo / G / 1 queue D_e can be given as:

$$D_e = \begin{cases} \dfrac{\xi}{p\left(1-p_{cf}\right)-\xi}, & \text{if } p(1-p_{cf}) > \xi \\ \infty, & \text{if } p(1-p_{cf}) < \xi \end{cases} \tag{13}$$

From the above discussion, we can get the average delay in a dynamic scenario by the following formula. Assuming that all interfering transmitters are activated with the same probability q, the connection failure probability [27] can be expressed as:

$$p_{cf} = min\left\{1 + \frac{\xi\lambda_I \pi r_0^2 \theta_t^{\delta} C(\delta)}{W\left(-\xi\lambda_I \pi r_0^2 \theta_t^{\delta} C(\delta)\right)}, 1-\xi\right\} \tag{14}$$

Substituting (14) into (13), the average delay can be presented as:

$$D_e = \frac{1-\frac{1}{\xi}}{1+\frac{p\lambda_I \pi r_0^2 \theta_t^{\delta} C(\delta)}{W\left(-\xi\lambda_I \pi r_0^2 \theta_t^{\delta} C(\delta)\right)}} \tag{15}$$

According to the definition of Lambert-W function, $W(z) \sim x$ if $z \to 0$. Therefore, the expression of D in (15) can be simplified as (16)) if $\lambda_I r_0^2 \theta_t^{\delta} C(\delta) \to 0$.

$$\begin{aligned} D_e &\simeq \frac{1-\frac{1}{\xi}}{1+\frac{p\lambda_I \pi r_0^2 \theta_t^{\delta} C(\delta)}{-\xi\lambda_I \pi r_0^2 \theta_t^{\delta} C(\delta)}} \\ &\simeq \frac{1-\frac{1}{\xi}}{1-\frac{p}{\xi}} \\ &\simeq \frac{\xi-1}{\xi-p} \end{aligned} \tag{16}$$

It can be concluded that the expression of delay D can be approximated as the simplified form in (16) if one of the following conditions is satisfied: $\lambda_I \to 0$, $r_0 \to 0$, or $\theta_t \to 0$.

C. STATE TRANSITION

In this section, we mainly introduce the state transition between VANET states. The transition probabilities among states are calculated using HDTMC and Poisson processes that provide a theoretical basis for the security mechanisms of VANET. Vehicles can take appropriate protective strategies according to the current state so that to enter the secure state. The state transition matrix $\delta(t)$ at time t can be given as:

$$\delta(t) = \sum_{n=0}^{\infty} \delta(0) P^n \cdot e^{-\lambda_t} \frac{(\lambda_t)^n}{n!}, \tag{17}$$

where $\delta(0)$ is the initial state probability vector of HDTMC, λ_t denotes the strength of the Poisson process, and P is the transition probability matrix.

As shown in Fig.3, the HDTMC model includes seven states and eleven transition routes, each of which is triggered by a trigger event. This article models each trigger event as

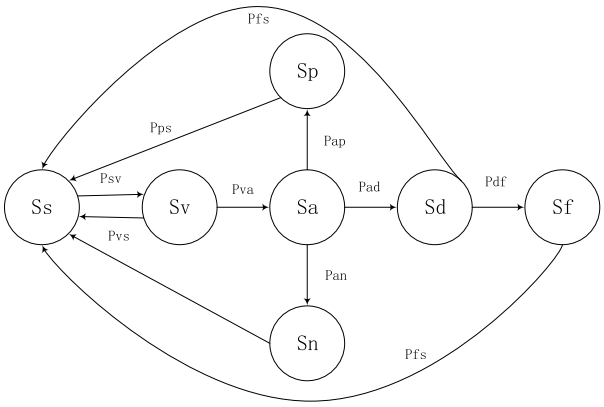

FIGURE 3. HDTMC State transition model.

a Poisson process with rate $\lambda^{(ij)} = \{\lambda_u^{(ij)}, \lambda_d^{(ij)}\}$, where $\lambda_u^{(ij)}$ and $\lambda_d^{(ij)}$ denote upward transition and downward transition, respectively. Specifically, the transition of HDTMC follows the Poisson process with the rate of $\lambda_u^{(ij)}$ so that to transform to a more secure state when the VANET environment is sensed secure. On the contrary, it follows a downward transition with Poisson parameter $\lambda_d^{(ij)}$ when the communication is exposed to threats. $\lambda_u^{(ij)}$ and $\lambda_d^{(ij)}$ are expressed as:

$$\lambda_u{}^{(ij)} = k^{(ij)} \cdot e^{T}, \tag{18}$$

$$\lambda_d{}^{(ij)} = k^{(ij)} \cdot e^{-T}, \tag{19}$$

where the parameter $k^{(ij)}$ denotes the strength of each $\lambda^{(ij)}$ [22]. The total rate of the Poisson process in the HDTMC model can be expressed as the sum of trigger event's rates:

$$\Lambda = \sum_{m=1}^{M} \lambda_{u/d}{}^{(ij)}, \tag{20}$$

where M is the number of trigger events or transition routes (e.g., $M = 11$ for Fig. 3).

The sum of transition probability can be expressed as:

$$P = \sum_{i,j \epsilon I} P^{(i,j)}, \tag{21}$$

where $I = \{Ss, Sp, Sv, Sa, Sn, Sd, Sf\}$ is the set of states in HDTMC. $P^{(i,j)}$ denotes the matrix of transition probability that transform from state i to j, which is given as:

$$P^{(i,j)} = \frac{Q^{(i,j)}}{\lambda_{u/d}{}^{(ij)}} + E. \tag{22}$$

Obviously, the following equations are satisfied for $\forall i, j \in I$, $i \neq j$: $p_{ij} = \frac{q_{ij}}{\lambda} \geq 0$, $p_{ii} = 1 + \frac{q_{ii}}{\lambda} \geq 0$, and $\sum_{j\in I} p_{ij} = 1 + \sum_{j\in I} p_{ij} = 1 + \frac{q_{ii}}{\lambda} + \sum_{j\in I, j\neq i} \frac{q_{ij}}{\lambda} = 1$.

From this, we find the transition probability matrix P to the transition rate matrix Q.

$$Q = \begin{bmatrix} -q_{sv} & q_{sv} & 0 & 0 & 0 & 0 & 0 \\ q_{vs} & -(q_{vs}+q_{va}) & q_{va} & 0 & 0 & 0 & 0 \\ 0 & 0 & -(q_{ap}+q_{an}+q_{ad}) & q_{ap} & q_{an} & q_{ad} & 0 \\ q_{ps} & 0 & 0 & -q_{ps} & 0 & 0 & 0 \\ q_{ns} & 0 & 0 & 0 & -q_{ns} & 0 & 0 \\ q_{ds} & 0 & 0 & 0 & 0 & -(q_{ds}+q_{df}) & q_{df} \\ q_{fs} & 0 & 0 & 0 & 0 & 0 & -q_{fs} \end{bmatrix} \tag{23}$$

Q is a matrix that transitions states by triggering events. At the same time, Q is composed of $Q^{(i,j)}$ for the following 11 events, so the first task is to request $Q^{(i,j)}$.

$$Q = Q^{(SV)} + Q^{(VS)} + Q^{(VA)} + Q^{(AP)} + Q^{(AN)} + Q^{(AD)} + Q^{(PS)} + Q^{(NS)} + Q^{(DF)} + Q^{(DS)} + Q^{(FS)} \quad (24)$$

$Q^{(i,j)}$ in the matrix is the transition rate from state$i$ to state j. Since the transition rate satisfies the Poisson distribution, the intensity of the Poisson process ${\lambda_{u/d}}^{(ij)}$ is used to represent the state transition rate, that is:

$$q_{ij} = {\lambda_{u/d}}^{(ij)} \quad (25)$$

Substituting (20) and (21) into (17), the probability that VANETs in each state can be obtained:

$$\delta(t) = \sum_{n=0}^{\infty} \delta(0) \cdot e^{-\Lambda} \frac{(\Lambda)^n}{n!} \left(\sum_{i,j \epsilon I} P^{(i,j)}\right)^n \quad (26)$$

The transition probability among states can provide theoretical help for the security mechanism of VANET. The following three examples are given to illustrate the scheme in this article. Firstly, VANET will enter a more vulnerable state when the probability of the security state is low. In this case, the system tries to activate its defense mechanisms to strengthen its security level while minimizing the threats. Secondly, the system will transfer to the attacked state according to the transition matrix $\delta(t)$ if it sensed that the fragile state's probability is high, i.e., the system is exposed to more attacks. In this case, the system will be reminded to carry out intrusion detection to avoid potential threats. Thirdly, the system will transfer to the degraded state if the probability of the attacked state is high. In such a case, the system makes the best effects to eliminate the threats to ensure the applications running normally; unnecessary applications may be paused until the security is restored.

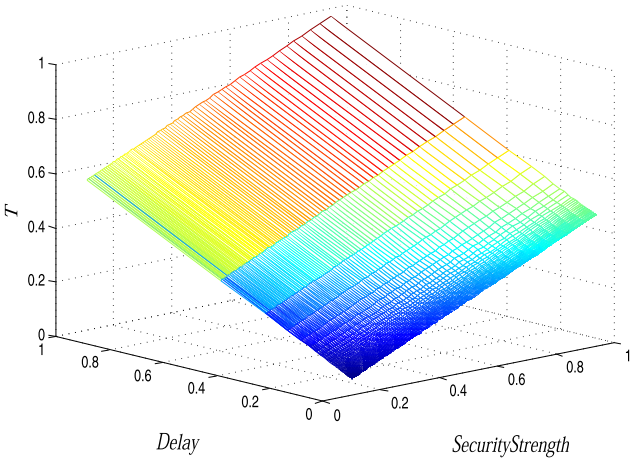

FIGURE 4. Relationship between security strength S_e, delay D_e and objective function T.

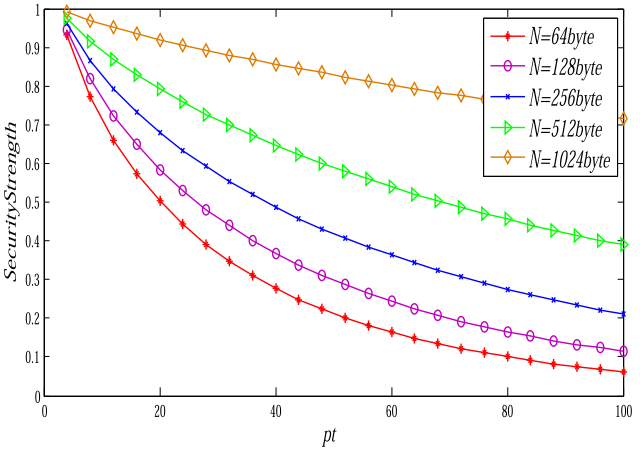

FIGURE 5. Effect of encryption block length N on security strength α.

IV. RESULTS

We first analyze how the utility function T determines the security state of VANETs in Section IV-A. Furthermore, effects of various environmental parameters on state transition are presented in Section IV-B.

A. ANALYSIS OF THE STATE OF SECURITY

The seven states of VANETs in the state transition model in Fig.1 is divided corresponding to the values of objective function T. 1) VANET is in the safe state if $T \in (0.7, 1]$; 2) VANET is in the vulnerable state if $T \in (0.6, 0.7]$; (3) VANET is in the attacked state if $T \in (0.5, 0.6]$. (4) VANET is in the positive state if $T \in (0.4, 0.5]$; (5) VANET is in the negative state if $T \in (0.3, 0.4]$; (6) VANET is in the degradation state if $T \in (0.2, 0.3]$; (7) VANET is in the failure state if $T \in (0, 0.2]$.

Fig.4 shows the relationship between the function T and the security strength and delay. From the figure, it can be concluded that the value of T is dynamically updated with the varies of delay and safety strength. This scheme enables vehicles to adopt context-aware security strategies adaptively in the dynamic VANET environments.

Fig.5 plots the effect of the encrypted block length N on the security strength α. It can be seen from the figure that the security strength is enhanced as the length of the encrypted block increasing from 64 bytes to 1024 bytes with an exponential ratio of two. This uptrend is obvious since the the attacker's strength (i.e., the vulnerability of a data frame) is weakened as the length of encryption block increases according to (4). Therefore, the security level of a data frame and the system's security can be enhanced accordingly.

Fig.6 illustrates the effect of packet arrival rate ξ on delay D. It can be observed that the communication delay decreases with the increase of the packet's arrival rate. Furthermore, D approaches positive infinity when the service rate p_t equals to ξ. This is because the network becomes dense with a high volume of arrival packets, leading to a significant degradation of the delay. Moreover, the inequality $p_t(1 - p_{cf}) < \xi$ can be satisfied if $p_t = \xi$. In this case, D is approximately equals to infinity according to (13).

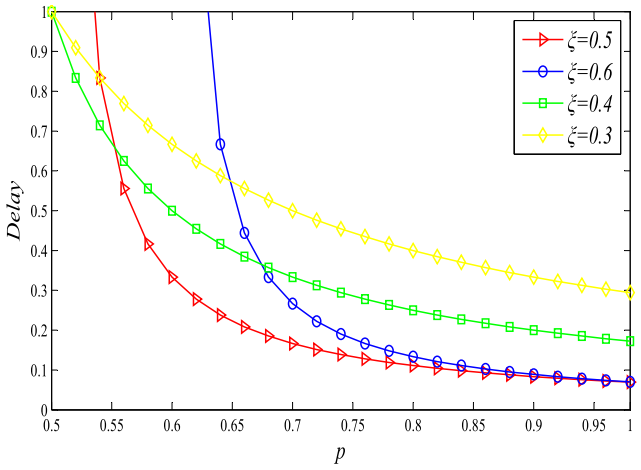

FIGURE 6. Effect of packet arrival rate ξ on delay D.

B. STATE TRANSITION ANALYSIS

In this section, we first set the initial values of k_{ij} for each state as: $k(sv) = 1$, $k(vs) = 0.7$, $k(va) = 0.3$, $k(ad) = 0.5$, $k(ap) = 0.3$, $k(an) = 0.2$, $k(ps) = 0.3$, $k(ns) = 0.2$, $k(ds) = 0.3$, $k(df) = 0.1$, $k(fs) = 0.1$. Furthermore, the initial value of $\delta(0)$ is given as: $\delta(0) = \{0.4, 0.21, 0.1, 0.06, 0.04, 0.16, 0.03\}$.

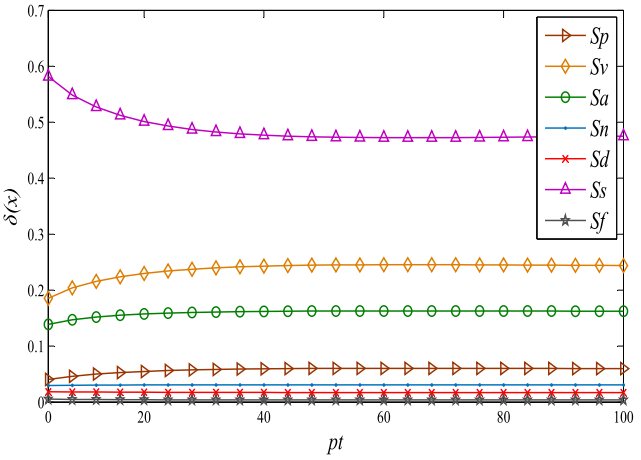

FIGURE 7. Effect of transmit power p_t on state probability $\delta(t)$.

Fig.7 shows that the effect of transmit power p_t on state probabilities. It can be noted that with the increase of the transmission power, the probability of a vehicle entering the safe state decreases, and that of a vehicle accessing to other states (unsafe) increases accordingly. This is because increasing the transmit power p_t enlarges the average transmission range $\bar{r}$ according to (9), leading to a high risk of exposure to the attackers. Obviously, both security strength S_e and objective function T show downtrends according to (5) and (1), respectively. Therefore, the upward transfer intensity $\lambda_u{}^{(ij)}$ decreases according to (19), and the downward transfer intensity $\lambda_d{}^{(ij)}$ increases according to (20). That is to say, the vehicle's system tends to transfer into an insecure state with the increase of transmit power. In conclusion, the VANET will be likely to enter unsafe states to prompt the insecure communication environment when the vehicle transmits with higher power. Therefore, being reminded of the insecure environment, the vehicle can adjust its transmit power to protect VANET against the potential threats.

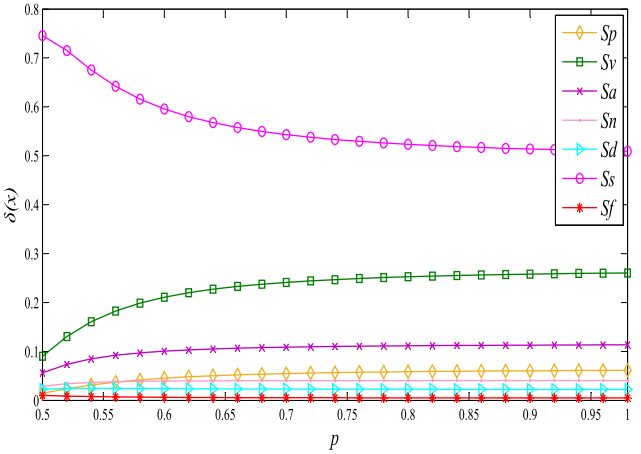

FIGURE 8. Effect of packet transmission probability p on state probability $\delta(t)$.

Fig.8 illustrates the effect of packet transmission probability p on state probability $\delta(t)$. It can be observed that the VANET is less likely to stay in the secure state Ss as the packet transmission probability increases. The reason for this trend is that increasing the packet transmission probability results in a high communication delay, according to (15). Long delay undoubtedly weakens the security strength because the communication of VANET is more likely to be threatened by attackers. Furthermore, according to (19) and (18), the downward transfer intensity $\lambda_d{}^{(ij)}$ increases while the upward transfer intensity $\lambda_u{}^{(ij)}$ decreases with the increase of p. Therefore, the system of VANET is more like to move into the vulnerable state Sv, as shown with the green curve in Fig.8. In this case, the system will prompt the vehicle to adjust the packet transmission probability or carry out monitoring strategies to avoid possible attacks.

Fig.9 describes the effect of data frame length N_f on the probability of each state. It can be observed that the probability of a secure state is in a growing trend but then shows a significant decline as N_f increases. An appropriate frame size suggests a positive effect on the objective function T since it can provide good communication performance by sending more messages. In this case, the upward transfer rate $\lambda_u{}^{(ij)}$ is large, and the downward transfer rate $\lambda_d{}^{(ij)}$ is small. Therefore, the value of the security state probability $\delta(s)$ increases in a short time. However, the excessive size of the data frame burdens the security strength of the messages according to (5), causing the risk of exposure to an insecure environment. As a result, the probability of the VANET in a security state Ss shows a sharp decline. Fig 9 demonstrates that keeping the length of the data frame as 700 bytes approximately could be the best conductive strategy for the security of VANET.

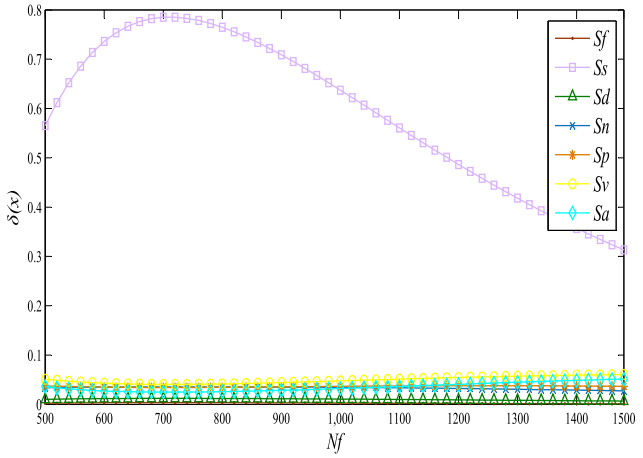

FIGURE 9. Effect of data frame length N_f on state probability $\delta(t)$.

V. CONCLUSION

This article proposes a context-aware and environment adaptive security quantification scheme for VANET based on the Markov chain. An HCTMC-based security quantification model is first constructed by incorporating the dynamic and randomness of the vehicular channel, along with the QoS consideration. Furthermore, the state transition matrix is derived based on the HDTMC and HPP, which provides a guideline for VANET's security defense mechanisms. Finally, extensive numerical calculations are conducted using various combinations of environment variables such as encryption block length, transmit power, and packet arrival rate. The results show that the proposed security measurement is capable of confirming the current security state of VANET based on the sufficient understanding of ''context'', environment, or situation. The system can make effective context-aware secure strategies according to the result of security quantification. This article constructs an HCTMC model with limited states of security levels. Future work will focus on designing quantitative VANET's security model with unlimited or continuous state space.

REFERENCES

[1] F. Qu, Z. Wu, F. Wang, and W. Cho, ''A security and privacy review of VANETs,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[2] Z. Wei, J. Li, X. Wang, and C.-Z. Gao, ''A lightweight privacy-preserving protocol for VANETs based on secure outsourcing computing,'' *IEEE Access*, vol. 7, pp. 62785–62793, 2019.

[3] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, ''Security in vehicular ad hoc networks,'' *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.

[4] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, ''VANet security challenges and solutions: A survey,'' *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.

[5] Z. Sun, Y. Liu, J. Wang, F. Mei, W. Deng, and Y. Ge, ''Non-cooperative game of throughput and hash length for adaptive merkle tree in mobile wireless networks,'' *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4625–4650, May 2019.

[6] N. Guo, L. Ma, and T. Gao, ''Independent mix zone for location privacy in vehicular networks,'' *IEEE Access*, vol. 6, pp. 16842–16850, 2018.

[7] O. Rehman, R. Qureshi, M. Ould-Khaoua, and M. F. Niazi, ''Analysis of mobility speed impact on end-to-end communication performance in VANETs,'' *Veh. Commun.*, vol. 26, Dec. 2020, Art. no. 100278. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209620300498

[8] H. El-Sayed, H. A. Ignatious, P. Kulkarni, and S. Bouktif, ''Machine learning based trust management framework for vehicular networks,'' *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100256. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209620300279

[9] M. Arif, G. Wang, V. E. Balas, O. Geman, A. Castiglione, and J. Chen, ''SDN based communications privacy-preserving architecture for VANETs using fog computing,'' *Veh. Commun.*, vol. 26, Dec. 2020, Art. no. 100265. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S221420962030036X

[10] S. Mihai, N. Dokuz, M. S. Ali, P. Shah, and R. Trestian, ''Security aspects of communications in VANETs,'' in *Proc. 13th Int. Conf. Commun. (COMM)*, Jun. 2020, pp. 277–282.

[11] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, ''Cybersecurity challenges in vehicular communications,'' *Veh. Commun.*, vol. 23, Jun. 2020, Art. no. 100214. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S221420961930261X

[12] G. Yan, S. Olariu, and M. C. Weigle, ''Providing VANET security through active position detection,'' *Comput. Commun.*, vol. 31, no. 12, pp. 2883–2897, Jul. 2008.

[13] A. A. Wagan, B. M. Mughal, and H. Hasbullah, ''VANET security framework for trusted grouping using TPM hardware: Group formation and message dissemination,'' in *Proc. Int. Symp. Inf. Technol.*, Jun. 2010, pp. 607–611.

[14] K. Szczypiorski, P. Smietanka, D. Khadraoui, and M. Seredynski, ''Security framework with active defence system for vehicular ad hoc networks,'' in *Proc. 2nd Int. Conf. Frontiers Signal Process. (ICFSP)*, Oct. 2016, pp. 121–125.

[15] N. R. Siddiqui, K. A. Khaliq, and J. Pannek, ''VANET security analysis on the basis of attacks in authentication,'' in *Proc. 5th Int. Conf. Dyn. Logistics (LDIC)*, in Lecture Notes in Logistics, M. Freitag and H. Kotzab, Eds. Bremen, Germany: Springer, Feb. 2016, pp. 491–502.

[16] L. Chen, H. Tang, and J. Wang, ''Analysis of VANET security based on routing protocol information,'' in *Proc. 4th Int. Conf. Intell. Control Inf. Process. (ICICIP)*, Jun. 2013, pp. 134–138.

[17] W.-M. Li, J. Lei, J. Dong, and Z.-T. Li, ''An optimized method for real time network security quantification,'' *Chin. J. Comput.*, vol. 32, no. 4, pp. 793–804, Aug. 2009.

[18] Q. Zhang, ''Research on quantitative analysis of security of network risk based on big data,'' in *Proc. Int. Conf. Robots Intell. Syst. (ICRIS)*, Jun. 2019, pp. 159–162.

[19] C. Griffin, B. Madan, and K. Trivedi, ''State space approach to security quantification,'' in *Proc. 29th Annu. Int. Comput. Softw. Appl. Conf. (COMPSAC)*, Scotland, U.K., Jul. 2005, pp. 83–88.

[20] J. Almasizadeh and M. A. Azgomi, ''Intrusion process modeling for security quantification,'' in *Proc. Int. Conf. Availability, Rel. Secur.* Fukuoka, Japan: IEEE Computer Society, 2009, pp. 114–121.

[21] A. U. Rahman, A. W. Malik, V. Sati, A. Chopra, and S. D. Ravana, ''Context-aware opportunistic computing in vehicle-to-vehicle networks,'' *Veh. Commun.*, vol. 24, Aug. 2020, Art. no. 100236. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209620300073

[22] X. Y. Tian, Y. H. Liu, J. Wang, W. W. Deng, and H. Oh, ''Computational security for context-awareness in vehicular ad-hoc networks,'' *IEEE Access*, vol. 4, pp. 5268–5279, 2016.

[23] Z. Sun, Y. Liu, J. Wang, W. Deng, and S. Xu, ''Non-cooperative game of effective channel capacity and security strength in vehicular networks,'' *Phys. Commun.*, vol. 25, pp. 214–227, Dec. 2017.

[24] M. A. Haleem, C. N. Mathur, R. Chandramouli, and K. P. Subbalakshmi, ''Opportunistic encryption: A trade-off between security and throughput in wireless networks,'' *IEEE Trans. Depend. Sec. Comput.*, vol. 4, no. 4, pp. 313–324, Oct. 2007.

[25] I. Atencia and P. Moreno, ''A discrete-time Geo/G/1 retrial queue with general retrial times,'' *Queueing Syst.*, vol. 48, nos. 1–2, pp. 5–21, Sep. 2004.

[26] G. Falin, ''A survey of retrial queues,'' *Queueing Syst.*, vol. 7, no. 2, pp. 127–167, Jun. 1990.

[27] Y. Zhong, X. Ge, T. Han, Q. Li, and J. Zhang, ''Tradeoff between delay and physical layer security in wireless networks,'' *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1635–1647, Jul. 2018.

JIAN WANG received the B.Sc., M.Sc., and Ph.D. degrees in computer science from Jilin University, in 2004, 2007, and 2011, respectively. He is currently a Professor with Jilin University. He has published over 50 articles on international journals. His research interests include wireless communication and vehicular networks, especially for network security and privacy protection.

HONGYANG CHEN received the B.Sc. degree in network engineering from Shenyang Aerospace University, China, in 2017. She is currently pursuing the master's degree with the College of Software, Jilin University. Her research interest includes vehicular *ad hoc* networks, especially for vehicle safety.

ZEMIN SUN received the B.Sc. and M.Sc. degrees in software engineering and computer science from Jilin University, China, in 2015 and 2018, respectively, where she is currently pursuing the Ph.D. degree. Her research interests include communication quality and security in vehicular networks, and game theory.