Throughput Aware Authentication Prioritisation for Vehicular Communication Networks

Hu Yuan, Matthew Bradbury, Carsten Maple and Chen Gu
Cyber Security Centre, WMG, University of Warwick, Coventry, CV4 7AL, United Kingdom
{H.Yuan.4, M.Bradbury, CM, Chen.Gu.1}@warwick.ac.uk

***Abstract*—Connected vehicles will be a prominent feature of future Intelligent Transport Systems. Which means that there will be a very high volume of wireless traffic that vehicles will receive and process. Due to this large quantity of traffic, there will be Quality of Service (QoS) constraints on the system that means messages will need to be prioritised. As vehicles will have a finite buffer to hold messages, the prioritisation scheme must consider network throughput to ensure QoS requirements are met. In our throughput authentication prioritisation technique, a Markov model is used to detect abnormally large data traffic users who are potential attackers performing a Denial of Service (DoS). Our results show that the algorithm can efficiently enhance network throughput.**

***Index Terms*—Connected Vehicles, Message Prioritisation and Network Throughput.**

I. Introduction

Connected vehicles will communicate with infrastructure and other vehicles for different reasons such as driving efficiency, road safety and infotainment. There are many different types of information that will be exchanged between vehicles and infrastructure. For example, vehicles will periodically broadcast Cooperative Awareness Messages (CAMs) which include location, speed, identity and acceleration to surrounding vehicles and infrastructure [1]. Vehicles can also be used as public infrastructure to collect and share knowledge on an Area of Interest (AoI) [2]. Connected vehicles even can provide Internet access to other vehicles, advertising information, file carry and transfer [3], and social applications (e.g., micro-blogs or instant messaging) [4].

A. Authentication Prioritisation

To ensure trusted communications connected vehicles need to have the ability to include a proof that they were the sender of a message and receivers need to be able to verify this proof. Digital signatures provide this non-repudiation capability plus the ability to verify the integrity of the message [5]. However, they are expensive to compute and to validate. Which is a problem on two fronts, firstly, the devices signing messages and verifying signatures have limited computational ability meaning that they can only verify a limited number of signatures per second at maximum. Secondly, an adversary may attempt to spam these devices with messages to verify that they do not provide useful information in an attempt to induce a Denial of Service (DoS). The more messages a vehicle receives the greater delay to verifying the signature of an important message. With limited buffer, this will also reduce the effective data rate and even lead to data loss. To resolve it, vehicles need to prioritise which messages to authenticate.

Existing work on authentication prioritisation in vehicular communication has typically investigated two main aspects either: (i) randomly selecting messages to verify and (ii) based on the physical distance of vehicles. In [6], messages in the security queue are randomly picked for verification to reduce data congestion. However, it cannot guarantee the performance or important messages would be verified in time. A distance-based prioritisation scheme was addressed in [7], [8].

Furthermore, those approaches did not consider the network QoS such as network throughput, which is a is a particularly important parameter for network performance. This is because vehicular networks require very low latency and high reliability. In additionally, the previous work did not investigate the impact of an attacker who is broadcasting messages to cause a DoS attack.

B. Contribution and Organisation

In this paper, we presented the technical details regarding: (1) our authentication prioritisation techniques that are able to improve the network throughput, and (2) the method used to detect a data jamming attacker with the authentication prioritisation algorithm. This paper is organised as follows: in Section II the system model is defined, in Section III the throughput maximised authentication was explained, in Section IV the misbehaviour detection model is explained, in Section V are the numerical results and analysis, finally the paper concludes and presents further open challenges in Section VI.

II. System Model

In this paper, the vehicle communication system considered is a multiple access system employing 3GPP LTE-V protocols, specifically Vehicle-to-Vehicle (V2V) communication. Vehicles are able to send and receive CAMs, act as a relay node for a store carry forward (SCF) [9] network or as a social network participant [10]. As shown in Figure 1, the vehicle receives data flows from different vehicles within its communication range. Data is buffered for verification before any further actions are triggered, for example, forwarding to other vehicles in an SCF application or to share images in social networks.

Within the communication range of a vehicles set $V = \{V_1, V_2, \ldots, V_n\}$, V_i is able to communicate with other vehicles. The received data flow at V_i is $\{S_{i,1}, S_{i,2}, \ldots, S_{i,m}\}$

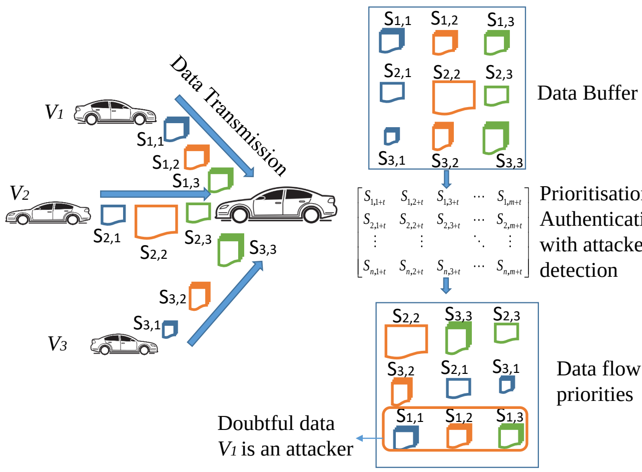

Figure 1: The authentication prioritisation with attacker detection.

where m is the buffer window size which is defined as the time duration T_B, so the $S_{i,m}$ is represented the received data from vehicle i at the time slot of m. If the data package stays in the buffer longer than the time duration T_B and has not been verified, the data would be discard. At anytime t, the whole data matrix in the buffer is defined as:

$$\mathbf{Bu} = \begin{bmatrix} S_{1,t+1} & S_{1,t+2} & \cdots & S_{1,t+m} \\ S_{2,t+1} & S_{2,t+2} & \cdots & S_{2,t+m} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n,t+1} & S_{n,t+2} & \cdots & S_{n,t+m} \end{bmatrix} \tag{1}$$

In this paper, a prioritised authentication algorithm is applied to enhance the network throughput and avoid data loss due to the limited buffer window. However, the potential attacker attempting to consume a finite size buffer to reduce throughput. A attacker detection model is studied in this paper as well.

The assumptions are made for analysis in this paper as: (1) the size of received data in each time slot is normally distributed; (2) the attacker vehicles are broadcasting relatively large data all the time; and (3) the detection is separated from the authentication part and does not reduce authentication computing capability.

III. Link Capacity Based Authentication Prioritisation

A. Link Capacity for V2V Communication

The road network is defined as the graph $\mathfrak{N} = (J, E)$, where J is the set of junctions and $E \subseteq J \times J$ is the set of roads between junctions. There is a function $L : E \to \mathbb{R}_{>0}$ that provides the length of a road in meters. The overall number of vehicles n located along a road i is modelled as Poisson distribution [11], with a probability density function:

$$p_i(n) = \exp\left(\frac{-L(i)}{\phi_i}\right)\left[\frac{(L(i)/\phi_i)^n}{n!}\right], \tag{2}$$

where ϕ_i is the vehicle density on the road i.

For V2V communications the received Signal-to-Interference-Noise-Ratio (SINR) from vehicle i to i' is:

$$\gamma\left(r_{i,i'}\right) = \frac{H_{i,i'} P_{\text{V2V}} \lambda r_{i,i'}^{-\alpha}}{\sigma^2 + I_i}. \tag{3}$$

where P_{V2V} is transmission power, $H_{i,i'}$ is the channel fading between vehicle i and vehicle i', σ^2 is the Additive White Gaussian Noise (AWGN) power, $r_{i,i'}$ is the distance between i and i', λ is the frequency dependent pathloss constant, and α is the pathloss distance exponent. I_i is the interference from co-frequency V2V vehicles. The interference to the vehicle i (I_i) from neighbouring vehicles $N(i)$ is:

$$I_i = \sum_{v \in N(i)} P_{\text{V2V}} \lambda r_{i,v}^{-\alpha}. \tag{4}$$

The expected interference power from the vehicles within its communication range is [12]:

$$I_i = P_{\text{V2V}} \lambda r_1^{-\alpha} + \left[\frac{\phi_{\text{V2V}} \Xi(r, \Psi, 4)}{2\sqrt{\frac{1}{P_{\text{V2V}}\lambda}}\operatorname{erfc}^{-1}(0.5)}\right]^2, \tag{5}$$

where r_1 is the distance to the closest vehicle, $\Xi(r, \Psi, 4) = \arctan(\Psi) - \arctan(r)$, and Ψ is the radius of the network coverage area and ϕ_{V2V} is the vehicle density[1] across the entire road network.

As defined by Shannon theory, the network capacity related to SINR is defined in Equation 6 where B is the channel bandwidth and γ is the received SINR.

$$C\left(r_{i,i'}\right) = B \log_2\left(1 + \gamma\left(r_{i,i'}\right)\right) \tag{6}$$

So the mean capacity of a link between i and i' is as follows, with a detailed explanation presented in Appendix A.

$$\begin{aligned} \overline{C\left(r_{i,i'}\right)} &= \mathbb{E}\left[C\left(r_{i,i'}\right)\right] \\ &= \int_0^{+\infty} \mathbb{P}\left\{B \log_2\left[1 + \frac{H_{i,i'} P_{\text{V2V}} \lambda r_{i,i'}^{-\alpha}}{\sigma^2 + I_i}\right] > \zeta\right\} \mathrm{d}\zeta\, \mathrm{d}r. \\ &= \left\{P_{\text{V2V}} \lambda r_1^{-\alpha} + \left[\frac{\phi_{\text{V2V}} \Xi(r, \Psi, 4)}{2\sqrt{\frac{1}{P_{\text{V2V}}\lambda}}\operatorname{erfc}^{-1}(0.5)}\right]^2\right\} \\ &\times \int_0^{+\infty} \exp\left[-\beta r^\alpha \sigma^2 \left(2^{\frac{\zeta}{B}} - 1\right)\right] \mathrm{d}\zeta \end{aligned} \tag{7}$$

The effective throughput of a V2V link is defined as that the actual data processing capacity from a vehicle to the destination vehicle, which includes the two components: the data transmission capacity and the data authentication capacity.

[1]The vehicles within the vehicle communication coverage area are considered as the same Poisson distribution as they are on roads.

Algorithm 1 Message Prioritisation

function PRIORITISATION($S_i, T^{\text{Aut}}, P_{\text{v2v}}, \phi_{\text{v2v}}, r$)
  When S_i reached, queen in $\mathbf{Bu}$ *as Eq. 1.*
  for $i \in V$ **do**
    for $j \in V$ **do**
      DETECTION(ω_r, W, $P'_{i,j}$, $P_{i,j}$)
      if i is a normal vehicle **then**
        $\mathbf{Bu}(i,j) = \text{SORT}(S_{i,j}, \text{'descending'})$
      else
        i is a attacker, drop the $S_{i,j}$

Algorithm 2 Misbehaviour Detection

function DETECTION(ω_r, W, $P'_{i,j}$, $P_{i,j}$)
  When the data reached, check the previous get ω_r
  for t=1:1:m **do**
    Calculate probability $\mathbb{P}\left(O^{1:W}\right)$ from Eq. 17, Eq. 21 and Eq. 22.
    if $\mathbb{P}\left(O^{1:t}\right)$ matched **then**
      i is a normal vehicle
    else
      i is a attacker

So the effective throughput is:

$$\mathbb{C}_{\text{eff}}\left(i, i', S, T^{\text{Aut}}, r\right) = \frac{\sum_{t=1}^{t=m} S_{i,t}}{\sum_{t=1}^{t=m}\left(\frac{S_{i,m}}{C\left(r_{i,i'}\right)}\right) + mT^{\text{Aut}}} \tag{8}$$

where T^{Aut} is the message verification time.

B. The Authentication Prioritisation

For a normal verification process, the data will be authenticated based on the arrival time in a first come first serve order. Because of the limited computing capacity and buffer window size, vehicles cannot process all the messages within the time duration T_B, so first come first serve order will lead to data loss and reduce the effective data capacity. An alternate approach is for the vehicle to prioritise which messages to verify based on the size of the packet. The simplest and fundamental way is to give a higher priority to larger package. The algorithm of Authentication Prioritisation is to maximise effective throughput across all vehicles:

$$\boldsymbol{A}_{\text{p}} = \max_{i,i' \in V \times V}\left\{\mathbb{C}_{\text{eff}}\left(i, i', S, T^{\text{Aut}}, r\right)\right\}. \tag{9}$$

However, there is a potential attack that the attacker vehicle is randomly broadcasting large messages leading to data loss. In this paper, we now apply a dynamic Markov model to detect the misbehaving vehicles which broadcasting jamming data in the V2V network. The process is shown in Algorithm 1 and detailed in the next section.

IV. ATTACKER DETECTION MODEL

This section describes the dynamic Markov model to help distinguish the data jamming attacker when prioritising the authentication order. This analysis is based on the assumption that an individual vehicle does not transmit large packets all the time, but the size of the data follows the Normal distribution. Therefore, a vehicle is considered an attacker if its transmission data size follows a non-standard way.

The considered Hidden Markov Model uses a set of non-visible states $(X_1, X_2, \ldots, X_n)$ which determine whether the vehicle broadcasting the jamming data or not, while the visible states $(Z_1, Z_2, \ldots, Z_n)$ represent the package data received. So the transfer matrix of the different status of data package sending by a vehicle is:

$$\begin{array}{cccccc}
\text{Z}_1 & \omega_r^1 & \text{Z}_2 & \omega_r^2 & \omega_r^i & \text{Z}_n \\
\bigcirc & \rightarrow & \bigcirc & \rightarrow & \cdots & \bigcirc \\
\downarrow & & \downarrow & & & \downarrow \\
\odot & \rightarrow & \odot & \rightarrow & \cdots & \odot \\
\text{X}_1 & P\left(V^1 \,\middle|\, \omega(1)\right) & \text{X}_2 & P\left(V^2 \,\middle|\, \omega(2)\right) & P\left(V^i \,\middle|\, \omega(i)\right) & \text{X}_n
\end{array} \tag{10}$$

The problem can thus be modelled as a Hidden Markov Model, with a transition probability matrix $\mathbf{A}$ for the observed states, where $P_{i,j}$ is the probability that the data $S_{n,i}$ at the time slot i the vehicle will receive the the data $S_{n,j}$ at the time slot j.

$$\mathbf{A} = \begin{bmatrix} P_{1,1} & P_{1,2} & \cdots & P_{1,n} \\ P_{2,1} & P_{2,2} & \cdots & P_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ P_{m,1} & P_{m,2} & \cdots & P_{m,n} \end{bmatrix} \tag{11}$$

Let set a hidden status of $\omega_r = \left\{\omega_r^1, \omega_r^2, \ldots, \omega_r^W\right\}$. So under the hidden status condition, the probability of the observed status $O^{1:W}$ where W is the observed window size is

$$\mathbb{P}\left(O^{1:W} \,\middle|\, \omega_r\right) = \prod_{t=1}^{W} P\left(o(t) \,\middle|\, \omega_r\right), \tag{12}$$

This is the product of the hidden status probability.

$$\mathbb{P}\left(V^{1:W} \,\middle|\, \omega_r\right) = \prod_{t=1}^{W} P\left(o(t) \,\middle|\, \omega_r\right) = \prod_{t=1}^{W} P'_{\omega(t),o(t)}, \tag{13}$$

where $P'_{\omega(t),o(t)}$ is the probability of the hidden probability under the hidden status condition. The detailed explanation is in Appendix B.

After the data packet arrives in the buffer, the Hidden Markov Model can calculate the observed status probability of each time slot and compare it with the probabilities of expected data size distribution, as shown in Algorithm 2.

V. NUMERICAL RESULTS AND ANALYSIS

The urban environment used in this study is a $1.7\,\text{km} \times 1.3\,\text{km}$ area of the city of Westminster, London[2]. It presents six different road classification categories. Each different category

[2]https://www.openstreetmap.org/#map=16/51.4952/-0.1469

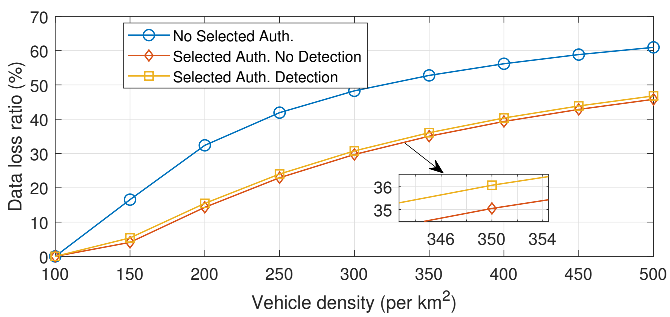

Figure 2: The data loss ratio with different vehicle density.

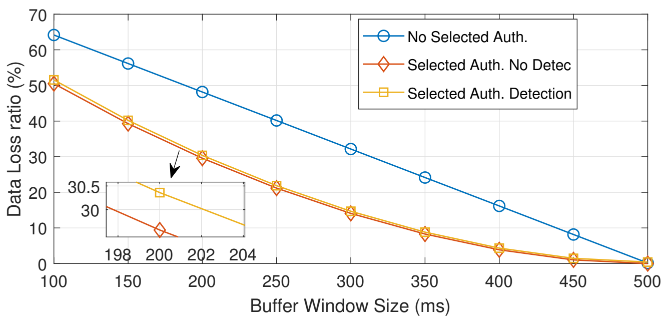

Figure 3: The data loss ratio with different buffer window sizes.

relates to different vehicle traffic intensities and speed limits. The carrier frequency is $5.9\,\mathrm{GHz}$, vehicle transmission power is $13\,\mathrm{dBm}$ and with $10\,\mathrm{MHz}$ bandwidth. The mean size of data distribution is $1\,\mathrm{MB}$ and the variance is 5. The attacker data size is $10\,\mathrm{MB}$ (only one attacker for a vehicle communication range) and the vehicle density is from 100 to 500 per km^2. The digital signature verification time is $5.7\,\mathrm{ms}$ for OpenSSL and the buffer window is from $100\,\mathrm{ms}$ to $500\,\mathrm{ms}$.

The data loss ratio goes up when there are more vehicles on the road, as shown in Fig. 2. It is shown that when the vehicle density is low there is no data loss because the data flow did not reach the limitation of the buffer. When the density climbs to 500 km^2 the loss ratio increased to 60% without prioritised authentication. If the messages are prioritised, the data loss ratio is 15 percentage points lower. The average data loss ratio performance of prioritisation authentication is 14% better than the non-prioritisation authentication. Another obviousness is that attacker detection scheme has a negligible effect on data loss.

In Fig. 3, the relationship between buffer window size and loss ratio is addressed. The data loss ratio drops with the increasing of the buffer window size. If the buffer window size is over $450\,\mathrm{ms}$, all the messages are verified. Oppositely, 63.7% of messages are discarded for non-prioritisation and 50% for prioritised authentication when the buffer is only $100\,\mathrm{ms}$.

The network throughput has increased by applying prioritised authentication, as the results displayed in Fig. 4, the throughput is $20.7\,\mathrm{MB/s}$ but this figure was only $13.79\,\mathrm{MB/s}$ without the authentication prioritisation. If the buffer size size is fixed,

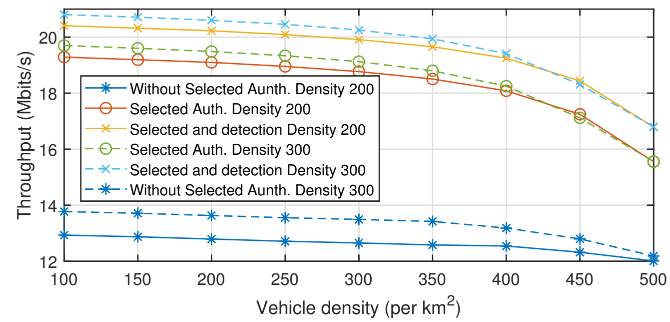

Figure 4: The effective throughput with different vehicle density and buffer window sizes.

the number of the vehicle slightly drops down the network throughput. This is the increasing number of the user's greats the interference by the co-frequency using. The buffer window size still has a positive correlation with the throughput. It is noticed that, compared with the non-detection prioritised authentication, the detection model only increased the network throughput about 7% that is because, in the simulation part, only one attacker introduced. So it is still worth applying the detection model.

VI. Conclusions and Open Challenges

In this paper, we studied how to enhance the network throughput by prioritising which messages to authenticate based packet size. The results show that prioritised authentication reduces the data loss ratio and increases network throughput. At the same time, we applied a Markov model to detected an attacker who aims to jam the data buffer with a Denial of Service attack, which gets a good performance to success detect the attacker. Actually, the data size distribution could be a binomial distribution (small size CAM with large multimedia data), it is more difficult to detect the attacker.

However, another attack type is that an attacker may using small message to consume the CPU resources. There are still challenges remaining. For example, the prioritisation and detection algorithms would consume extra computational resources that could otherwise be used to verify signatures. Practical experiments need to be performed to determine the impact this analysis has on signature verification performance. The attacker may also use a more intelligent strategy instead of continually sending large packets.

Acknowledgement

This work was supported in part by the EPSRC project PETRAS Internet of Things Research Hub under Grant EP/N02298X/1 and Innovate UK project, CAPRI (TS/P012264/1).

Appendix

A. Average Network Capacity

The expectation of a non-negative continuous random variable X is $\mathbb{E}[X] = \int_{t>0} \mathbb{P}(X > t)\,\mathrm{d}t$. With the Poisson

Point Process (PPP) and fading distribution, the expectation capacity for any single V2V link is [13]:

$$\begin{aligned}&\mathbb{E}\left[C\left(r_{i,i'}\right)\right]\\&=\int_0^{+\infty}\mathbb{P}\left[H_{i,i'}>r^{\alpha}\frac{1}{P_{\mathrm{V2V}}\lambda}\left(\sigma^2+I_i\right)\left(2^{\frac{\zeta}{B}}-1\right)\right]\mathrm{d}\zeta,\end{aligned}\tag{14}$$

where $H_{i,i'}$ is the channel fading from the vehicle i to the receiver vehicle i', P_{V2V} is the transmission power, B is the bandwidth, and I_i is the interference to the vehicle i.

$$\mathbb{E}\left[C\left(r_{i,i'}\right)\right]=\int_0^{+\infty}\exp\left[-\beta r^{\alpha}\sigma^2\left(2^{\frac{\zeta}{B}}-1\right)\right]I_i\,\mathrm{d}\zeta\tag{15}$$

If we applied Equation (5) in, the mean theoretical capacity for a V2V link is:

$$\begin{aligned}&\mathbb{E}\left[C\left(r_{i,i'}\right)\right]\\&=\int_0^{+\infty}\mathbb{P}\left\{B\log_2\left[1+\frac{H_{i,i'}P_{\mathrm{V2V}}\lambda r^{-\alpha}}{\sigma^2+I_i}\right]>\zeta\right\}\mathrm{d}\zeta\,\mathrm{d}r\\&=\left\{P_{\mathrm{V2V}}\lambda r_1^{-\alpha}+\left[\frac{\phi_{\mathrm{V2V}}\Xi(r,\Psi,4)}{2\sqrt{\frac{1}{P_{\mathrm{V2V}}\lambda}}\mathrm{erfc}^{-1}(0.5)}\right]^2\right\}\\&\times\int_0^{+\infty}\exp\left[-\beta r^{\alpha}\sigma^2\left(2^{\frac{\zeta}{B}}-1\right)\right]\mathrm{d}\zeta.\end{aligned}\tag{16}$$

B. Hidden Probability

The whole set of the possible hidden status is Ω, so the expectation probability of the observed status $O^{1:W}$ is:

$$\mathbb{P}\left(V^{1:W}\right)=\sum_{r\in\Omega}P\left(V^{1:T}\;\middle|\;\omega_r\right)P\left\{\omega_r^1,\omega_r^2,\ldots,\omega_r^W\right\}\tag{17}$$

then,

$$\begin{aligned}\mathbb{P}\left(V^{1:W}\right)&=\sum_{r\in\Omega}P\left(V^{1:W}\;\middle|\;\omega_r\right)\prod_{t=1}^{T}P\left(\omega_t\mid\omega_{t-1}\right)\\&=\sum_{r\in\Omega}\prod_{t=1}^{T}P\left(o(t)\mid\omega_r\right)P\left(\omega_r(t))\mid\omega_r(t-1)\right)\\&=\sum_{r\in\Omega}\prod_{t=1}^{W}P'_{\omega_r(t),o(t)}P_{\omega_r(t),\omega_r(t-1)}.\end{aligned}\tag{18}$$

By recursing Equation (18), the expectation observed status probability is

$$\begin{aligned}\mathbb{P}\left(O^{1:W}\right)&=\sum_{\omega(W)}P\left(O^{1:W-1},O^W,\omega(W)\right)\\&=\sum_{\omega(W)}P\left(O^W\;\middle|\;O^{1:W-1},\omega(W)\right)\\&\times P\left(O^{1:W-1},\omega(W)\right),\end{aligned}\tag{19}$$

from the conditions the O^T and $O^{1:W-1}$ are independent, so

$$\begin{aligned}\mathbb{P}\left(O^{1:W}\right)&=\sum_{\omega(W)}P\left(O^{1:W},\omega(W)\right)\\&=\sum_{\omega(W)}P\left(O^W\;\middle|\;\omega(W)\right)P\left(O^{1:W-1},\omega(W-1)\right)\\&\times\sum_{\omega(W-1)}P\left(\omega(W)\mid\omega(W-1)\right).\end{aligned}\tag{20}$$

where

$$\begin{aligned}\mathbb{P}\left(V^{1:W},\omega(W)\right)=P'_{\omega(W),O^W}&\sum_{\omega(W-1)}P_{\omega(W-1),\omega(W)}\\&\times P\left(O^{1:W-1}\omega(W-1)\right),\end{aligned}\tag{21}$$

Where as the sets:

$$\varphi_j=P\left(O^{1:W},\omega(t)=j\right)=P'_{j,O^W}\left[\sum_i^N P_{i,j}\varphi_i(t-1)\right].\tag{22}$$

References

[1] T. ETSI, "Intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," *ETSI TS*, vol. 1.3.2, pp. 448–451, 2014.

[2] F. Meng, X. Gong, L. Guo, X. Cai, and Q. Zhang, "Software-reconfigurable system supporting point-to-point data communication between vehicle social networks and marketers," *IEEE Access*, vol. 5, pp. 22 796–22 803, 2017.

[3] Y. Wang, Y. Liu, J. Zhang, H. Ye, and Z. Tan, "Cooperative store–carry–forward scheme for intermittently connected vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 1, pp. 777–784, 2017.

[4] Q. Yan, M. Li, Z. Yang, W. Lou, and H. Zhai, "Throughput analysis of cooperative mobile content distribution in vehicular network using symbol level network coding," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 484–492, 2012.

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

[6] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, 2007.

[7] X. Xue and J. Ding, "Lpa: a new location-based privacy-preserving authentication protocol in vanet," *Security and Communication Networks*, vol. 5, no. 1, pp. 69–78, 2012.

[8] S. Biswas and J. Mišić, "Location-based anonymous authentication for vehicular communications," in *2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, 2011, pp. 1213–1217.

[9] H. Yuan, C. Maple, and K. Ghirardello, "Dynamic route selection for vehicular store-carry-forward networks and misbehaviour vehicles analysis," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2018, pp. 1–5.

[10] A. M. Vegni and V. Loscri, "A survey on vehicular social networks," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2397–2419, 2015.

[11] S.-I. Sou and Y. Lee, "End-to-end performance for SCF-based vehicular routing over multiple communication gaps," in *IEEE Communication Letters*, vol. 18, no. 6, Jun. 2014, pp. 1015–1018.

[12] H. Yuan, W. Guo, Y. Jin, S. Wang, and M. Ni, "Interference-aware multi-hop path selection for device-to-device communications in a cellular interference environment," *IET Communications*, vol. 11, no. 11, pp. 1741–1750, 2017.

[13] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on communications*, vol. 59, no. 11, pp. 3122–3134, 2011.