Manuscript version: Author’s Accepted Manuscript
The version presented in WRAP is the author’s accepted manuscript and may differ from the published version or Version of Record.

Persistent WRAP URL:
http://wrap.warwick.ac.uk/124293

How to cite:
Please refer to published version for the most recent bibliographic citation information. If a published version is known of, the repository item page linked to above, will contain details on accessing it.

Copyright and reuse:
The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher’s statement:
Please refer to the repository item page, publisher’s statement section, for further information.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk.
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 flows from different vehicles within its communication range. A throughput prioritisation algorithm was addressed in [7], [8].

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 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 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 \( \{S_{i,1}, S_{i,2}, \ldots, S_{i,m}\} \).
A. Link Capacity for V2V Communication

The road network is defined as the graph \( G = (J, E) \), where \( J \) is the set of junctions and \( E \subseteq J \times J \) is the set of roads between junctions. There is a function \( L : E \rightarrow \mathbb{R}_{>0} \) 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:

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

where \( \phi_i \) 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:

\[
\gamma (r_{i, i'}) = \frac{H_{i, i'} P_{V2V} \lambda r_{i, i'}^{-\alpha}}{\sigma^2 + I_i}.
\]

where \( P_{V2V} \) is transmission power, \( H_{i, i'} \) is the channel fading between vehicle \( i \) and vehicle \( i' \), \( \sigma^2 \) is the Additive White Gaussian Noise (AWGN) power, \( r_{i, i'} \) is the distance between \( i \) and \( i' \), \( \lambda \) is the frequency dependent pathloss constant, and \( \alpha \) 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:

\[
I_i = \sum_{v \in N(i)} P_{V2V} \lambda r_{i, v}^{-\alpha}.
\]

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

\[
I_i = P_{V2V} \lambda r_{1, i}^{-\alpha} + \frac{\phi_{V2V} \Xi(r, \Psi, 4)}{2 \sqrt{\frac{1}{P_{V2V} \lambda}}} \text{erfc}^{-1}(0.5)^2,
\]

where \( r_1 \) is the distance to the closest vehicle, \( \Xi(r, \Psi, 4) = \arctan(\Psi) - \arctan(r) \), and \( \Psi \) is the radius of the network coverage area and \( \phi_{V2V} \) is the vehicle density 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 \( \gamma \) is the received SINR.

\[
C(r_{i, i'}) = B \log_2 \left( 1 + \gamma (r_{i, i'}) \right)
\]

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

\[
C(r_{i, i'}) = E \left[ C(r_{i, i'}) \right] = \int_0^{+\infty} \int_0^{+\infty} P \left[ B \log_2 \left( 1 + \frac{H_{i, i'} P_{V2V} \lambda r_{i, i'}^{-\alpha}}{\sigma^2 + I_i} \right) > \zeta \right] d\zeta dr.
\]

\[
= \left\{ P_{V2V} \lambda r_{1, i}^{-\alpha} + \frac{\phi_{V2V} \Xi(r, \Psi, 4)}{2 \sqrt{\frac{1}{P_{V2V} \lambda}}} \text{erfc}^{-1}(0.5) \right\}^2 \times \int_0^{+\infty} \exp \left[ -\beta r^\alpha \sigma^2 (2 \zeta - 1) \right] d\zeta
\]

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.
So the effective throughput is:

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

where $T^{\text{Aut}}$ 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 throughput. 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:

$$A_p = \max_{i, i', v \in V \times V} \left\{ C_{\text{eff}} \left( i, i', S, T^{\text{Aut}}, r \right) \right\}.$$  \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.

### Algorithm 1 Message Prioritisation

**function** PRIORITYISATION($S_i, T^{\text{Aut}}, P_{r,2}, \phi_{2,v}, r$)

- When $S_i$ reached, queen in $Bu$ as Eq. 1.
- for $i \in V$ do
  - for $j \in V$ do
    - DETECTION($\omega_r, W, P_{r,j}, P_{v,j}$)
    - if $i$ is a normal vehicle then
      - $Bu(i, j) = \text{SORT}(S_{i,j}, \text{`descending'})$
    - else
      - $i$ is a attacker, drop the $S_{i,j}$

### Algorithm 2 Misbehaviour Detection

**function** DETECTION($\omega_r, W, P_{r,j}, P_{v,j}$)

- When the data reached, check the previous get $\omega_r$
- for $t=1:n$ do
  - Calculate probability $P(O^{1:t})$ from Eq. 17, Eq. 21 and Eq. 22.
  - if $P(O^{1:t})$ matched then
    - $i$ is a normal vehicle
  - else
    - $i$ is a attacker

So the transfer matrix of the different status of data package sending by a vehicle is:

$$Z_1 \quad \omega^1_r \quad \ldots \quad \omega^1_r \quad \omega^2_r \quad \ldots \quad \omega^W_r \quad \ldots \quad \omega^W_r \quad Z_n$$

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

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

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

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

This is the product of the hidden status probability.

$$P(O^{1:t} | \omega_r) = \prod_{t=1}^{W} P(o(t) | \omega_r) = \prod_{t=1}^{W} P_{o(t), \omega_r}.$$  \tag{13}

where $P_{o(t), \omega_r}$ 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\textsuperscript{2}. It presents six different road classification categories. Each different category

\textsuperscript{2}https://www.openstreetmap.org/#map=16/51.4952/0.1469
The digital signature verification time is 5 and the buffer window is from 100 ms authentication, as the results displayed in Fig. 4, the throughput of messages are discarded for non-prioritisation and 50% for increasing of the buffer window size. If the buffer window size is over 450 ms is not reach the limitation of the buffer. When the density climbs to 500 km², it is more difficult to 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 use 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.

VI. CONCLUSIONS AND OPEN CHALLENGES

In this paper, we studied how to enhance the network throughput by prioritising which messages to authenticate based on 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 detect 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.

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).

ACKNOWLEDGEMENT

APPENDIX

A. Average Network Capacity

The expectation of a non-negative continuous random variable $X$ is $E[X] = \int_{t>0} \mathbb{P}(X > t) \, dt$. With the Poisson
Point Process (PPP) and fading distribution, the expectation capacity for any single V2V link is [13]:

\[
\mathbb{E} \left[ C \left( r_{i,i'} \right) \right] = \int_0^{+\infty} \mathbb{P} \left[ H_{i,i'} > \gamma \right] \frac{1}{P_{2V} \lambda} \left( \frac{\sigma^2 + I_i}{\sigma^2} \right) \left( 2^{\frac{\phi}{2} - 1} \right) d\zeta, \quad (14)
\]

where \( H_{i,i'} \) is the channel fading from the vehicle \( i \) to the receiver vehicle \( i' \), \( P_{2V} \) is the transmission power, \( B \) is the bandwidth, and \( I_i \) is the interference to the vehicle \( i \).

\[
\mathbb{E} \left[ C \left( r_{i,i'} \right) \right] = \int_0^{+\infty} \log_2 \left[ 1 + \frac{H_{i,i'} P_{2V} \lambda r^{-\alpha}}{\sigma^2 + I_i} \right] > \zeta \right] d\zeta dr
\]

\[
= \left\{ \frac{P_{2V} \lambda r^{-\alpha} + \frac{1}{2} \sqrt{\frac{1}{r_{2V} \lambda}} \text{erfc}^{-1}(0.5)}{2} \right\}^2
\]

\[
\times \int_0^{+\infty} \exp \left[ -\beta r^\alpha \sigma^2 \left( 2^{\frac{\phi}{2} - 1} \right) \right] d\zeta. \quad (16)
\]

### B. Hidden Probability

The whole set of the possible hidden status is \( \Omega \), so the expectation probability of the observed status \( O^{1:T} \) is:

\[
\mathbb{P} \left( V^{1:T} \right) = \sum_{r \in \Omega} P \left( V^{1:T} \left| \omega_r \right. \right) P \left( \omega_r, \omega_{r_1}, \ldots, \omega_{r_T} \right) \quad (17)
\]

then,

\[
\mathbb{P} \left( V^{1:T} \right) = \sum_{r \in \Omega} \prod_{t=1}^{T} P \left( \omega_t \mid \omega_{t-1} \right) = \sum_{r \in \Omega} \prod_{t=1}^{T} P \left( o(t) \mid \omega_r \right) P \left( \omega_r(t) \mid \omega_r(t-1) \right)
\]

\[
= \sum_{r \in \Omega} \prod_{t=1}^{W} P' \left( \omega_r(t), o(t) \right) P \left( \omega_r(t) \mid \omega_r(t-1) \right). \quad (18)
\]

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

\[
\mathbb{P} \left( O^{1:T} \right) = \sum_{\omega(W)} P \left( O^{1:T-1}, \omega(W) \right)
\]

\[
= \sum_{\omega(W)} P \left( O^W \mid O^{1:T-1}, \omega(W) \right)
\]

\[
\times P \left( O^{1:T-1}, \omega(W) \right), \quad (19)
\]

from the conditions the \( O^T \) and \( O^{1:T-1} \) are independent, so

\[
\mathbb{P} \left( O^{1:T} \right) = \sum_{\omega(W)} P \left( O^{1:T}, \omega(W) \right)
\]

\[
= \sum_{\omega(W)} P \left( O^W \mid \omega(W) \right) P \left( O^{1:T-1}, \omega(W) \right)
\]

\[
= \sum_{\omega(W)} P \left( O^W \right) P \left( O^{1:T-1}, \omega(W) \right).
\]

where

\[
\mathbb{P} \left( V^{1:T}, \omega(W) \right) = P' \left( \omega(W), O^W \right) \sum_{\omega(W-1)} P \left( O^{1:W-1}, \omega(W-1) \right).
\]

Where as the sets:

\[
\varphi_j = P \left( O^{1:T}, \omega(t) = j \right) = P' \left( \omega(t) \right) \sum_i P_{i,j} \varphi_i(t-1).
\]

### REFERENCES


