# Transmission Power-Control Certificate Omission in Vehicular Ad Hoc Networks

Emmanuel Charleson Dapaah(✉), Parisa Memarmoshrefi, and Dieter Hogrefe

Institute of Computer Science, University of Göttingen, Göttingen, Germany
e.dapaah@stud.uni-goettingen.de,
memarmoshrefi@cs.uni-goettingen.de,
hogrefe@informatik.uni-goettingen.de

**Abstract.** The frequent dissemination of safety-related beacons among neighboring vehicles in VANET is fundamental for cooperative awareness. Nevertheless, this has over the years raised a major security concern hence the current state-of-the-art requires all safety-related beacons to carry a certificate and a digital signature as a security mechanism to ensure authenticity and integrity. Unfortunately, this security mechanism is characterized by an increase in the size of a beacons payload which as a result, induces an overhead in communication under dense traffic conditions.

Several works have been published in the literature investigating how to reduce this overhead without compromising the level of security achieved, as well as vehicle cooperative awareness. The Neighbor-based Certificate Omission scheme, which conveys the general idea of a vehicle attaching a certificate to its beacon based on changes it observes from its neighboring table was proposed to address this issue. However, on evaluating the scheme under a dense traffic scenario, it was observed that the scheme reduced the level of achieved cooperative awareness among vehicles as it was unable to obtain a fair balance between the number of incurred *cryptographic packet loss* (packets dropped because the vehicle had no corresponding certificate to verify it) and *network packet loss* (packets dropped because of network channel congestion).

In this paper, we propose a Transmission Power-control Certificate Omission scheme, which seeks to achieve a better balance between the number of incurred *cryptographic packet loss (CPL)* and *network packet loss (NPL)* to maximize vehicle cooperative awareness even under dense traffic conditions. Unlike previously proposed schemes, we efficiently control channel load by adopting a congestion detection and congestion control algorithm in our scheme. The simulation results indicate that our proposed scheme can achieve a better balance between the number of incurred CPL and NPL and can maximize vehicle cooperative awareness even under dense traffic conditions.

**Keywords:** VANET · Security · Certificate omission · Congestion


L. Foschini and M. El Kamili (Eds.): ADHOCNETS 2020, LNICST 345, pp. 164–176, 2021.
https://doi.org/10.1007/978-3-030-67369-7_12

## 1 Introduction

Critical to the reduction of road accidents is the frequent dissemination of safety-related messages among vehicles. Because, it enables cooperative awareness, which is beneficial for vehicles to make proactive safety decisions. However, in V2V communication, dissemination of safety-related messages is through broadcast. It comprises of two main messages: Periodic Safety Messages (called beacon in this paper) which are broadcasted periodically to announce a vehicles status and Event-Driven Messages which are broadcasted at the detection of an event [1]. In the United States, periodic safety messages are defined as Basic Safety Messages (BSM) according to the SAE J2945/1 standard [2] and as Cooperative Awareness Messages (CAM) by the European Telecommunication Standards Institute (ETSI) [3].

These messages are susceptible to attack as an adversary can inject spoofed messages into the network to mislead vehicles. Therefore to enforce beacon integrity and authenticity, both the IEEE 1609.2 standard and its European counterpart ETSI TS 103 097 mostly rely on the attachment of a digital signature based on Elliptic Curve DSA (ECDSA) and a digital certificate issued by a trusted Certificate Authority (CA) [4].

Despite the benefits of this security mechanism, it increases the beacon payload by approximately 200 bytes [5], which, as a result, induces an overhead in communication and computation. Under high traffic conditions, the periodic broadcast of such a large beacon payload may cause the channel to congest, which in turn increases the number of packet collisions and delay in packet delivery. Therefore, to reduce the overhead and also improve channel efficiency, researchers have proposed several certificate omission schemes and channel congestion control schemes which were described and proven by simulation in [4, 6]. In the omission schemes, if a sending vehicle includes fewer certificates in its subsequent beacons, it increases the number of cryptographic packet loss (CPL) while reducing network packet loss (NPL). Also, if the sending vehicle includes a certificate in all beacons, it eliminates cryptographic packet loss but increases the number of network packet loss.

Therefore, the general drawback of the various omission schemes is how to efficiently achieve a fair balance between NPL and CPL to maximize vehicle cooperative awareness. This we believe is as a result of the schemes inability to efficiently manage channel congestion. With this paper, we propose a Transmission Power-control Certificate Omission which alleviates the general drawback of the previously proposed schemes by combining the advantages of the NbCO scheme discussed in [7] with the advantages of the distributed transmission power control algorithm discussed in [8]. Also, we adopted the concept of channel state transition as described in [9] to cooperatively adjust the transmission power of vehicles taking into consideration their current channel state.

The remainder of this paper is organized as follows: In Sect. 2, we discuss some related works. Next, we present the Transmission Power-control Certificate Omission Scheme (TPCO) in Sect. 3. In Sect. 4, we describe the simulation setup and analyze the simulation results. Finally, we present our conclusion and future work in Sect. 5.

## 2 Related Work

In this section, we review related works that exploit certificate omission and channel congestion control to improve the efficiency of secured beaconing.

**Periodic Omission of Certificates (POoC).** In this omission scheme [10], a vehicle attaches a certificate only every nth beacon, therefore omitting its certificate in n–1 beacons sent. Although the approach reduces communication overhead, its performance is dependent on the vehicle's context. For instance, under conditions of high vehicle speed and low beacon frequency, the number of unverified beacons (cryptographic packet loss) increases during the n–1 beacon period (certificate omission period) and this is because a vehicle that has not yet cached the certificate of the sender may have left the senders communication range during the $n^{th}$ beacon period which is the certificate attachment period and as such will have to drop all unverifiable beacons received.

**Neighbor-Based Certificate Omission (NbCO).** The idea of NbCO [7] is for a vehicle to attach a certificate to its beacon based on the changes observed from its neighboring table. Therefore, every vehicle monitors its neighborhood through beacons received from neighboring vehicles and update its neighboring table as at when it receives a beacon from an unknown vehicle. However, when vehicle density is high, the number of certificate omissions performed by the scheme reduces due to the increase of neighbor changes in the network. Though this may positively reduce the number of incurred CPL, it may also impact the channel load negatively and consequently increase packet collisions which in turn increases the number of NPL.

**Congestion-Based Certificate Omission (CbCO).** This scheme [6] aims at reducing the overall packet loss incurred by taking into consideration the channel condition before attaching or omitting a certificate. Thus, the scheme attaches a certificate to all beacons if the communication channel is detected to be free and aggressively omits certificates when the channel is congested. Although this trade-off positively impacts the overall packet loss (CPL + NPL), it compromises the individual packet loss (NPL or CPL) based on the current condition. Therefore, the number of CPL is seen to increase when certificates are aggressively omitted during channel congestion and also NPL is seen to increase when the channel is detected to be free.

**Channel Congestion Control.** Researchers have proposed in literature numerous methods to address the issue of channel congestion and they essentially employ two techniques: beaconing rate control or transmission power control. The concept of beaconing rate control has to do with adapting the transmission rate of a sending node to control its beaconing period. However, several improved beaconing rate control techniques have over the years been proposed in the literature [11, 12]. Sommer [12] proposed an improved approach which considered message utility and channel quality as the baseline for adapting beacon transmission rate to further enhance the adaptation of vehicle transmission rate, for a more effective channel congestion control. Despite the benefits, the general drawback of beacon rate control methods is the lack of sufficient vehicle status information to prevent the degrading of cooperative awareness among vehicles.

Therefore, to better manage channel congestion, a transmission power control scheme [13] was proposed. This scheme controls a vehicles communication range by

adapting its beacon transmission power when the channel is congested. Also, Chang [8] in his approach considered the gradual and distributive adjusting of beacon transmission power to achieve an optimal transmission range for maximum awareness.

## 3 Transmission Power-Control Certificate Omission Scheme

In this paper, we propose an efficient and reliable Transmission Power-control certificate omission (TPCO) scheme which seeks to achieve a better balance between the number of incurred CPL and NPL to maximize vehicle cooperative awareness even under dense traffic conditions and also demonstrate effective control over the communication channel through its ability to adaptively increase or decrease vehicles transmission power based on the observed channel state.

Therefore, to reduce CPL we employed the use of neighboring tables as was proposed by the NbCO scheme [7]. With this concept, each vehicle within the network updates its neighboring table as at when it receives a beacon from an unknown vehicle. And if a vehicle detects such an update, it attaches a certificate to the next beacon it schedules for broadcast. On the other hand, if no such changes are observed, it omits its certificate from all subsequent beacons.

The concept of vehicles maintaining a neighboring table has the advantage of significantly reducing the number of CPL incurred under dense traffic conditions because the frequent update of a neighboring table will force a vehicle to attach a certificate to almost every beacon it sends.

Nevertheless, this will introduce the issue of channel congestion leading to increase in NPL as observed in the NbCO. But peculiar to our Transmission Power-control Certificate Omission scheme is the combination of a congestion detection algorithm and a congestion control algorithm to address the channel congestion drawback introduced by the adopted neighboring table mechanism. Therefore, our TPCO scheme drastically reduces the number of NPL incurred when the channel is congested, causing it to scale very well under dense traffic conditions.

As a congestion detection algorithm, we switch the channel among three states (Relaxed, Active and Restrictive) based on the estimated channel load as was proposed in the ETSI TS 102 687 standards [14]. Each channel state, therefore, determines the transmission power assigned for beacon transmission. In this work, we estimate the channel load using the formula:

$$\text{Estimated\_CL} \;=\; \text{N} * \left(\text{beacon\_rate} \; * M_{length}\right) \tag{1}$$

In Eq. (1), Estimated_CL represents the measured channel load, N represents the number of vehicles within the communication range, beacon_rate represents the number of periodic beacons generated per second and Mlength represents the beacon payload length. The automaton state transition of the congestion detection algorithm is demonstrated in Fig. 1.

Also, to effectively control channel congestion and enhance vehicle cooperative awareness, we employed the concept of a distributed transmission power-control algorithm [8]. Hence, we control channel congestion by adjusting the vehicle transmission power when the estimated channel load exceeds the allowed thresholds. Our maximum

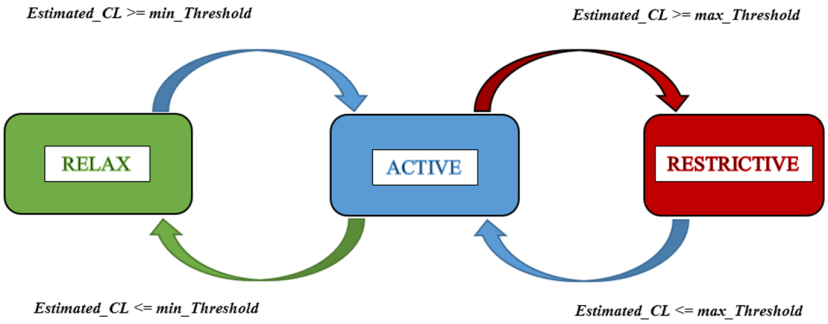


**Fig. 1.** Channel state transition.

and minimum transmission power assignment were defined in line with the parameter definition Chang et al. [8].

The node state is then switched into a distressed state (Active or Restrictive) and it broadcasts a distress signal to all neighboring vehicles. Vehicles that receive a distress signal gradually adjust their transmission power by a step size (ε) until the estimated channel load of the node in a distressed state gradually converge to a reasonable value below the allowed threshold. The step size is defined to increase or decrease the communication range of the vehicle by 50 m.

Figure 2 describes the operational flow of our channel congestion detection and congestion control algorithm for a sending vehicle. Within a defined time frame of $\Delta T$, the algorithm checks if the estimated channel load (*Estimated_CL*) exceed the allowed thresholds. If the estimated channel load exceeds the allowed thresholds, the vehicle state is changed to a distressed state (Active or Restrictive). It then decreases its transmission power by ε and broadcasts a distress signal to its neighboring nodes and waits for $\Delta T$. This process is continued until the vehicles transmission power reaches the minimum allowed transmission power. However, if the algorithm checks and the estimated channel load has converged to a reasonable value below the allowed threshold, the vehicle state is changed to the non-distressed state (Relax) and its transmission power is increased by ε and waits for $\Delta T$. This process also continues until the vehicles transmission power reaches the maximum allowed transmission power. The pseudocode of the algorithm is illustrated in Table 1.

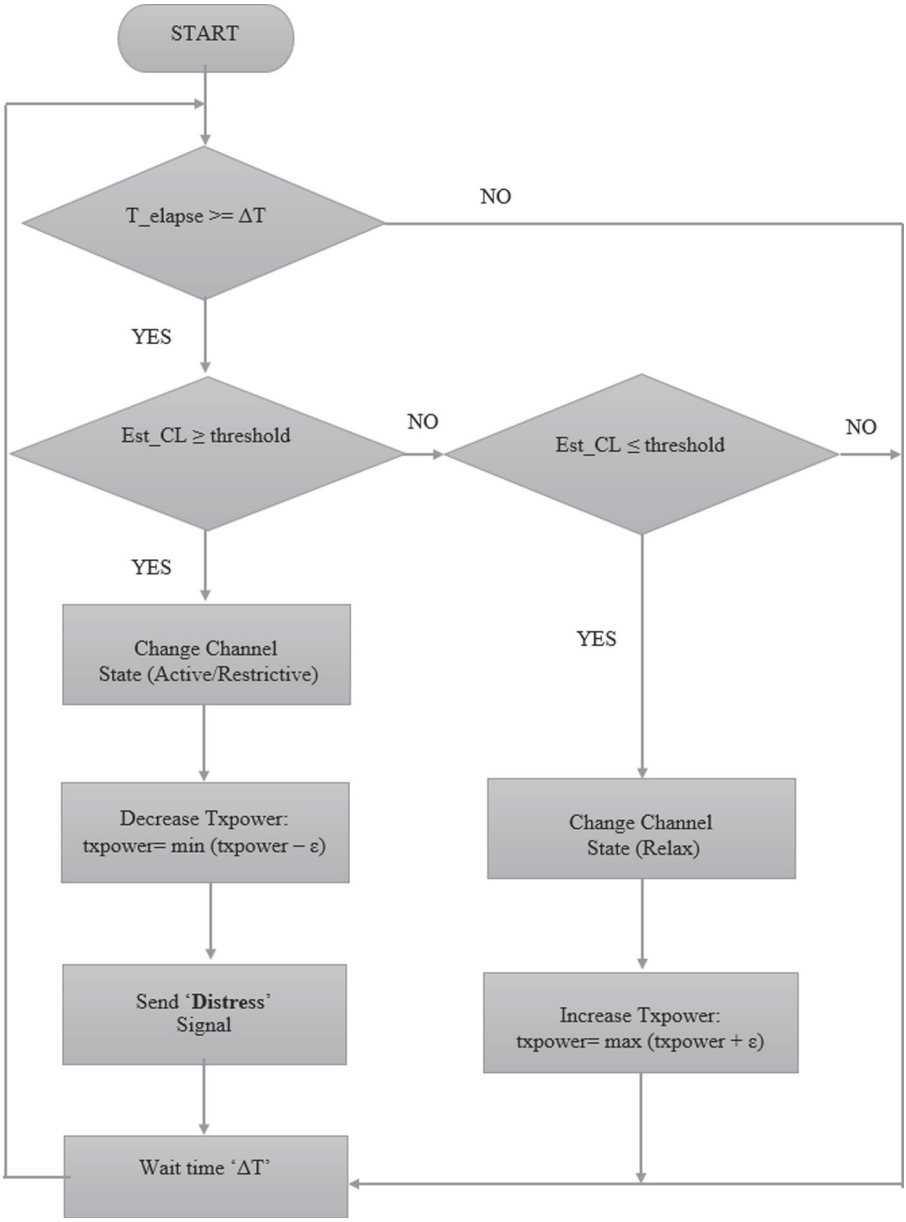


**Fig. 2.** Flow chart of channel congestion detection and control algorithm for a sending vehicle.

Figure 3 describes the operational flow for receiving vehicles. If a vehicle receives a distress signal, it decreases its transmission power by ε and waits until it receives another distress signal. This process continues until the vehicles transmission power reaches the minimum allowed transmission power. If the vehicle has not received a distress signal and

**Table 1.** Channel congestion detection and control algorithm for a sending vehicle

| Data: | Estimated channel load |
|---|---|
| Result: | Change in vehicle state and transmission power |
| 1 | **If** Est_CL $\geq$ threshold **then** |
| 2 | channel_state = Active or Restrictive |
| 3 | decrease_txpower = min(txpower-$\varepsilon$) |
| 4 | Broadcast 'Distress signal' |
| 5 | Wait time '$\Delta$T' |
| 6 | **else** |
| 7 | channel_state = Relax |
| 8 | increase_txpower = max(txpower + $\varepsilon$) |
| 9 | Wait time '$\Delta$T' |
| 10 | **endif** |

**Table 2.** Channel congestion detection and control algorithm for receiving vehicles

| Data: | Distress signal (beacon) from neighboring nodes |
|---|---|
| Result: | Change in vehicle transmission power |
| 1 | **If** Distress signal = true **then** |
| 2 | decrease_txpower = min(txpower-$\varepsilon$) |
| 3 | Wait time '$\Delta$T' |
| 4 | **else** |
| 5 | increase_txpower = max(txpower + $\varepsilon$) |
| 6 | Wait time '$\Delta$T' |
| 7 | **endif** |

its transmission power is below the maximum allowed transmission power, it increases its transmission power by $\varepsilon$ until the maximum allowed transmission power is reached. The pseudocode of the algorithm is illustrated in Table 2.

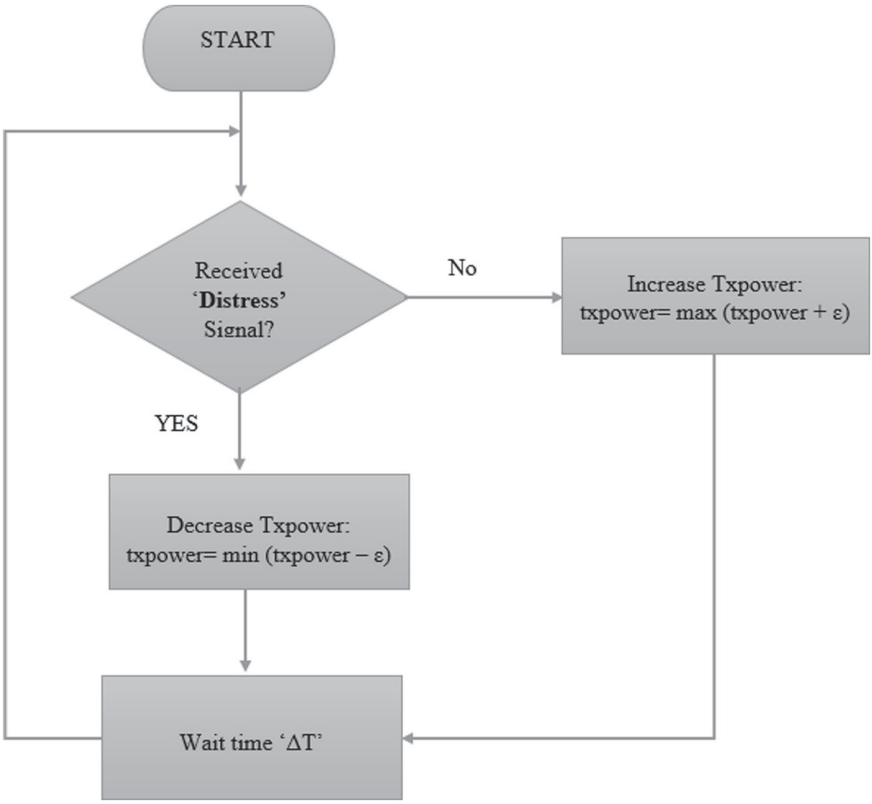


**Fig. 3.** Flow chart of channel congestion detection and control algorithm for receiving vehicles.

## 4 Evaluation

To evaluate the performance of our proposed scheme, we focus on a two-directional highway scenario as shown in Fig. 4 and to achieve a dense traffic condition with frequent neighborhood changes we scheduled a total of 100 vehicles where 50 (green vehicles) move on the right lane and the remaining 50 (red vehicles) move on the left lane. Without loss of generality, we focus on the Basic Safety Message (BSM) format as specified in the SAE J2945/1 standard [2].

### 4.1 Simulation Setup

To conduct our simulation, we used SUMO as the traffic generator, OMNET ++ as the network simulator and VEINS as the VANET simulator. We extended the VEINS simulator by modifying the application layer to implement our beaconing mechanism which encapsulated the neighboring table based certificate omission and attachment strategy. We also modified the mac layer to implement our congestion detection and control algorithm. Table 3 contains a summary of all other relevant simulation parameters which are in line with the previous works by Schoch et al. [7].

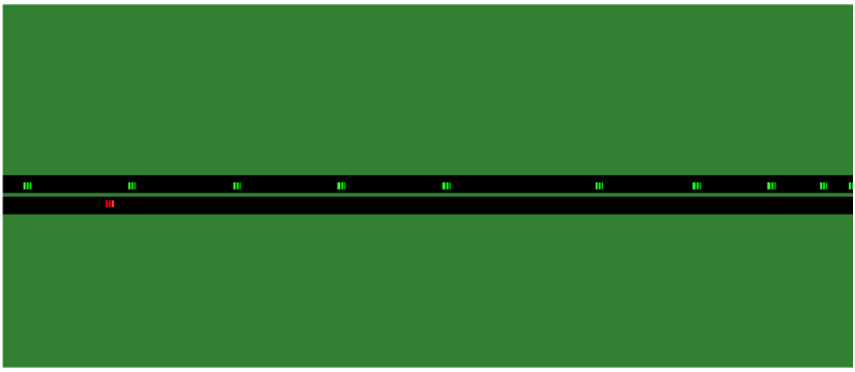

**Fig. 4.** Two-directional highway scenario.

**Table 3.** Overview of simulations parameters.

| Parameter | Value |
|---|---|
| Number of nodes | 100 |
| Field size | 3 km × 3 km |
| Node density (neigh./node) | 1–35 |
| Node velocity (m/s) | 40 |
| MAC | 802.11p, 3Mbit/s |
| Transmit power | Adaptive |
| Beacon frequency | 10 Hz |
| Payload size | 50 Bytes |
| ECC Key type | Nistp256, compressed |
| Certificate size | 125 Bytes |
| Signature size | 56 Bytes |
| Simulation time (s) | 100 |
| Simulation runs | 10 |

### 4.2 Analysis

To evaluate the performance of our TPCO scheme, we compared it to two previously proposed certificate omission schemes; NbCO [7] and POoC [10] by considering three evaluation metrics. First, we measured the percentage of cryptographic packet loss (CPL) incurred by each scheme and from Fig. 5 we observe that our TPCO scheme performs better than the POoC scheme which recorded a high CPL percentage 7.40%. However, in literature [5], the NbCO scheme is known to outperform other certificate omission schemes in regards to reducing the number of CPL incurred under dense traffic conditions. Yet, our TPCO scheme was able to achieve its goal of not incurring a CPL greater than that of the NbCO scheme and rather went further to slightly outperformed the

NbCO scheme by a margin of 0.30%. Though this performance gap may be considered negligible, we still regard it as an achievement of our scheme and we attribute this slight improvement to the dynamic increasing and decreasing of the communication range of vehicles by adjusting its transmission power.

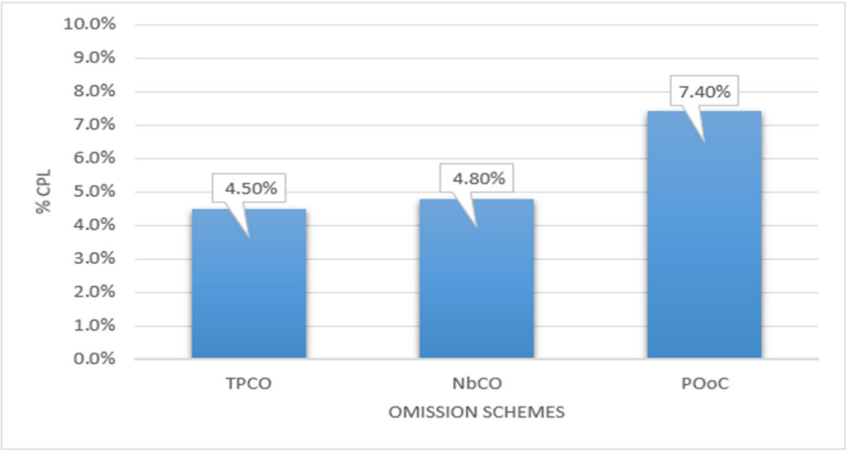


**Fig. 5.** The average percentage of cryptographic packet loss.

Second, as shown in Fig. 6 we compared each certificate omission scheme by measuring the percentage of network packet loss (NPL) incurred when the channel is congested and in so doing, our TPCO scheme proved to be more efficient than the other schemes as it recorded only 23.10% of NPL. Which was as a result of the channel detection and control algorithm we incorporated into our TPCO scheme to adaptively reduce the communication range of vehicles based on their observed channel state. Hence, justifying our claim that the TPCO scheme increases vehicle cooperative awareness under dense traffic conditions through its ability to effectively control communication channel load to minimize NPL.

Finally, in Fig. 7 we further compared each certificate omission scheme based on the percentage of bandwidth saved as this is directly reflected in the percentage of beacons sent without a certificate attached [7]. We thereby observe that our proposed scheme outperformed the others by saving up to 88.40% of channel bandwidth induced by certificate transfer. In contrast, the POoC is observed to perform worse than the other schemes due to its static certificate transfer which is determined by its predefined $n^{th}$ value.

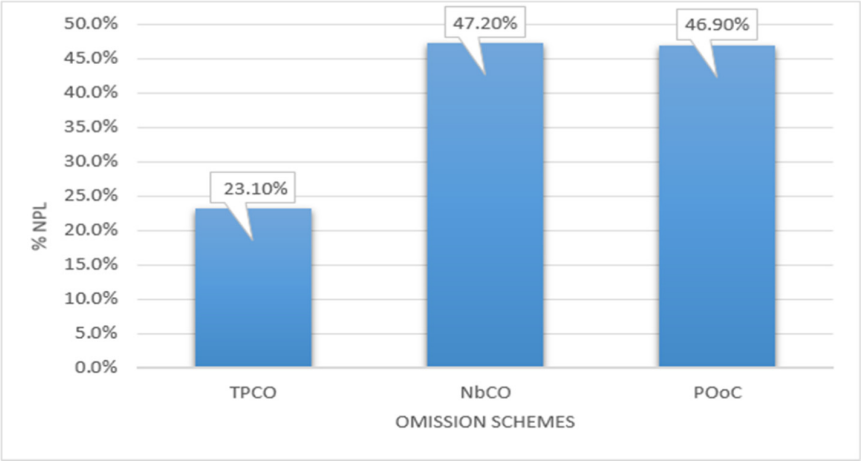


**Fig. 6.** The average percentage of network packet loss.

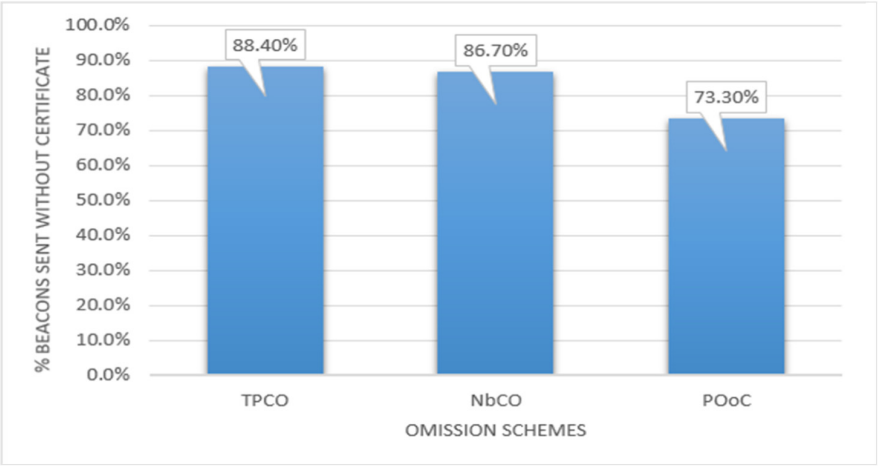


**Fig. 7.** The average percentage of certificate omissions.

## 5 Conclusion and Future Work

In this paper, the issue of decreased vehicle cooperative awareness due to an imbalanced trade-off in cryptographic packet loss and network packet loss by certificate omission schemes under dense traffic conditions have been investigated. Based on our analysis we reason that it is as a result of the lack of an efficient congestion detection and control algorithm in previously proposed certificate omission schemes. We addressed this issue by proposing a Transmission Power-control Certificate Omission scheme which performed certificate omissions based on neighbor changes and further control channel load by the cooperative adjustment of the transmission power of vehicles to gradually

converge the estimated channel load to a value within a reasonable range. The simulation results show that our scheme increases vehicle cooperative awareness by efficiently controlling the channel load to achieve a reasonable balanced between cryptographic packet loss and network packet loss under dense traffic conditions. Also, in the situation where malicious vehicles decide to ignore distress signals, we believe our scheme will slightly still outperform the NbCO since the distressed node will continue to decrease its communication range until its estimated channel load reaches a value within a reasonable range.

As future work, we aspire to test the performance of our omission scheme in a more realistic scenario by making use of real map scenarios as well as comparing the complexity of our model with already existing models. Also, considering the growth of the number of vehicles in future, secure and privacy-preserving beaconing mechanism need to be optimized with respect to the communication load. Furthermore, centralized authentication mechanisms, which are responsible to issue and prove the authenticity of the certificates may not be efficient and scalable. Therefore, as future work, we also plan to focus on the distributed secure beaconing mechanisms and an investigation of their performance.

## References


1. Liu, X., Jaekel, A.: Congestion Control in V2V Safety Communication: Problem, Analysis. Approaches. Electron. **8**(5), 1–24 (2019)
2. Anon: Dedicated Short Range Communications (DSRC) Message Set Dictionary™ (2016)
3. Anon: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service.Etsi.org (2019)
4. Feiri, M., Petit, J., Schmidt, R., Kargl, F.: The impact of security on cooperative awareness in VANET. In: 2013 IEEE Vehicular Networking Conference, pp. 127–134 (2013)
5. Feiri, M., Petit, J., Kargl, F.: Evaluation of congestion-based certificate omission in VANETs. In: 2012 IEEE Vehicular Networking Conference (VNC), pp. 101–108 (2012)
6. Feiri, M., Petit, J., Kargl, F.: Congestion-based certificate omission in VANETs. In: Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications – VANET'12, pp. 135–138 (2012)
7. Schoch, E., Kargl, F.: On the efficiency of secure beaconing in VANETs. In: Proceedings of the Third ACM Conference on Wireless Network Security – WiSec'10, pp. 111–116 (2010)
8. Chang, H., Song, Y., Kim, H., Jung, H.: Distributed transmission power control for communication congestion control and awareness enhancement in VANETs. PLoS ONE **13**(9), 1–25 (2018)
9. Sommer, C., Dressler, F.: Vehicular Networking, pp. 185–188 (2015)
10. Calandriello, G., Papadimitratos, P., Hubaux, J., Lioy, A.: On the performance of secure vehicular communication systems. IEEE Trans. Dependable Secure Comput. **8**(6), 898–912 (2011)
11. Egea-Lopez, E., Pavon-Marino, P.: Distributed and fair beaconing rate adaptation for congestion control in vehicular networks. IEEE Trans. Mob. Comput. **15**(12), 3028–3041 (2016)
12. Sommer, C., Tonguz, O., Dressler, F.: Traffic information systems: efficient message dissemination via adaptive beaconing. IEEE Commun. Mag. **49**(5), 173–179 (2011)

13. Lu, H., Poellabauer, C.: Balancing broadcast reliability and transmission range in VANETs. ACM SIGMOBILE Mob. Comput. Commun. Rev. **14**(4), 25 (2011)
14. Anon: Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part. Etsi.org (2018)