

iTLM: A Privacy Friendly Crowdsourcing Architecture for Intelligent Traffic Light Management

Christian Roth^a, Mirja Nitschke^b, Matthias Hörmann and Doğan Kesdoğan

University of Regensburg, Regensburg, Germany
{firstname.lastname}@ur.de

Keywords: Traffic Light, V2X, Privacy, Attribute-Based-Credentials, Privacy-ABC System, Reinforcement Learning, Privacy-by-design.

Abstract: Vehicle-to-everything (V2X) interconnects participants in vehicular environments to exchange information. This enables a broad range of new opportunities. We propose a self learning traffic light system which uses crowdsourced information from vehicles in a privacy friendly manner to optimize the overall traffic flow. Our simulation, based on real world data, shows that the information gain vastly decreases waiting time at traffic lights eventually reducing CO2 emissions. A privacy analysis shows that our approach provides a significant level of k-anonymity even in low traffic scenarios.

1 INTRODUCTION

Confronted by the climate change nowadays, there is an urgent need to reduce CO2 emissions produced by vehicles. Particularly in cities, the pollution is severe because of frequent stop-and-go traffic. One reason may lie in rather inflexible cyber-physical systems, i.e. traffic lights, unable to quickly adapt to changing situations. Therefore, the field of traffic control requires new economic approaches to optimize the efficiency of existing infrastructure, ultimately protecting the environment by reducing pollutants. In this paper, we investigate an intelligent traffic light management (TLM) using crowdsourced user input in a privacy-friendly manner to achieve this goal.

With an increasing number of vehicles having the ability to communicate with other cars (V2V) or infrastructure (V2I) without additional costs, vehicle-to-everything (V2X) communication is finally reaching the mass market (Abuelsamid, 2019). V2X can be considered to be an enabler for real-time TLM because it is now possible to cheaply distribute the needed information using V2X. This facilitates the mostly academic field of self-learning, self-optimizing traffic light scheduling to become applied in real environments. To present an applicable approach, we assume a mixed environment with some vehicles not being enabled for V2X. With our approach, it is conceivable that such participants could

also (although not necessarily) be integrated using a smartphone-based solution.

However, many security implications have to be considered in the open, loosely-connected V2X environment. In particular, integrity must be considered because a safe system must be ensured at any moment. Furthermore, such a system has to be built on privacy by design principles since its users have to be protected for broad-end user acceptance. One can use e.g. ABC4Trust (Sabouri et al., 2015), a privacy-enhanced attribute-based credential (privacy-ABC) system. We propose a reinforcement learning (RL) powered cyber-physical system to reduce the overall waiting time. Our approach takes into account the wide variety of requirements: optimize the traffic light schedules using (unreliable) information from users while protecting their privacy.

To the best of our knowledge, we are the first to combine traffic light management based on user input in vehicular environments with user privacy. We contribute with 1) a communication protocol for V2X traffic light management based on the ABC4Trust platform, 2) a self-learning traffic light management algorithm called *iTLM* using user input, 3) a simulation using SUMO to evaluate the performance of our approach in comparison to standard, widely applied models, and 4) a study of the contradicting requirements of privacy and integrity. The simulation is based on real data of the City of Hamburg in Germany to allow meaningful conclusions.

Section 2 briefly introduces ABC4Trust and dif-

^a  <https://orcid.org/0000-0002-1668-5441>

^b  <https://orcid.org/0000-0002-2527-6340>

ferent approaches for traffic light systems w.r.t. privacy. Section 3 illustrates our protocol including an attacker model. Section 4 thoroughly evaluates the approach in terms of performance and discusses the impacts of the privacy enhancing techniques (PETs). Section 5 pointedly concludes the paper.

2 RELATED WORK

Traffic light control systems (TLCS) can be organized in static or dynamic approaches (Li, 2012). Table 1 presents an overview of methods for traffic light control. It specifies for every method not only the pros and cons, but also reviews the privacy friendliness of the approaches and discusses if the method can respond to dynamic traffic flows.

We shortly focus on recent developments of reinforcement learning (RL) approaches which try to model the actual traffic conditions to provide highly dynamic traffic light schedules. It does so by predicting the number of cars for each (waiting) lane with basic approaches, e.g. by relying on actuated or camera inputs (Arel et al., 2010). Other superior approaches are more privacy-invasive as they use the car’s current position and speed to predict arrival times (Liang et al., 2019; Gao et al., 2017). Interconnecting multiple traffic lights optimizes the traffic light schedules (Steingröver et al., 2005) by overcoming the limited area of view of camera-based systems. However, as already mentioned, many of these systems use data provided by cameras or environmental sensors to track individual cars and to derive decisions.

A holistic approach must ensure that the privacy of each individual is protected while taking into account the open and untrusted environment of V2X scenarios (i.e. smart traffic light scheduling) due to its contradicting requirements (Blumberg et al., 2005). Typical pseudonym-based approaches are not feasible in V2X networks (Wiedersheim et al., 2010). Pseudonyms may also be critical when they are shared across multiple messages. Such messages can be linked together to form a location trajectory of such a car. (Schaub et al., 2009) describes concrete requirements for vehicular communication systems which are currently not achieved in any RL-based traffic light approach. We cherry-picked the advantages of RL-based approaches and V2X benefits and overcome the drawbacks. That given, we propose a system combining the dynamics of RL and V2X with privacy properties of conventional methods. Furthermore, for the first time, everything is poured into a new privacy-friendly protocol based on the robust ABC4Trust platform (Sabouri et al., 2015).

ABC4Trust. (Sabouri et al., 2015) is a EU funded privacy enhanced attribute-based credential (privacy-ABC) system. It allows to build trustworthy applications which combine contradicting goals such as reliability, integrity and privacy. A common architecture abstracts the specific implementation of the ABC system, enabling one to build complex yet secure applications. ABC4Trust defines five different roles, i.e. *User*, *Verifier*, *Issuer*, *Inspector* and *Revocator*. Furthermore, it defines `credentials` as containers for `attributes` which are defined either by a user or issuer, (blindly) confirmed by an issuer and owned by a user. Knowing and owning a signed credential can then be used to gain access to a remote system protected by a Verifier. In addition, a `pseudonym` is a (temporary) identity of a user and allows (limited) linkability if needed and prevents replay attacks which is explicitly relevant in our use case since Sybil attacks are an omnipresent risk in V2X environments. Both elements can be bound to a secret only known to a user, adding an additional layer of authenticity. It is a viable foundation for securing communication in our privacy-friendly system architecture.

3 INTELLIGENT TRAFFIC LIGHT MANAGEMENT (iTLM)

We now introduce our system model and present our protocol. Attacks and abuse possibilities including protection mechanisms are discussed as well.

According to our scenario, vehicles try to find the fastest route to a destination using static (road network) and dynamic (traffic congestion) information. However, travel duration is often impacted by the waiting time t^w at traffic lights. To allow a traffic light (TL) to intelligently optimize the light schedule, it needs additional information, e.g. the vehicle’s time of arrival. This information may be sent by vehicles to a traffic light long before arrival. By aggregating the information from vehicles, the traffic light can find the optimal light schedule, which globally minimizes the overall waiting time ($\sum t^w$) at a junction.

The proposed architecture takes the special conditions in V2X environments into account. The protocol is based on an attribute-based credential system to provide privacy. At the same time, the system was designed to handle the open nature of V2X environments with untrustworthy participants. Thus, integrity protecting mechanisms are needed. Both contradicting goals can be achieved using ABC4Trust (Sabouri et al., 2015).

Table 1: Comparison of different approaches for traffic light scheduling

	Method	Pros & Cons	Properties
Static	Different predefined light cycle schedules (optionally time dependent)	+ Common + Easy to deploy - Not dynamic at all	high privacy: no sensors at all; not dynamic
Actuated	1-2 inductive loops per lane detect presence of vehicles to control the length of green phases (e.g. (Darroch et al., 1964))	+ Can adjust to traffic density - High traffic density cannot be handled very well - Short-term information	high privacy: no personal data; limited dynamic
Camera	Cameras per lane detect (number of) vehicles to control the length of green phases (e.g. (Rachmadi et al., 2011; Nirmani et al., 2018; Xing et al., 2018))	+ Can adjust to traffic density + Fair system gives every lane green time - Short-term information	medium privacy: license plate allows tracking; limited dynamic
V2X	Virtual traffic lights communicate directly with cars and receive information of arrival time to model actual traffic flow (e.g. (Gao et al., 2019; Varga et al., 2017))	+ Very dynamic + No physical traffic lights needed + Can find optimal solution - Requires all participants to be enabled for V2X communication	poor privacy: assignable communication allows tracking; full dynamic
RL	Fusion of multiple input sources give feedback for decisions, optionally connected to other TLCs, tries to predict traffic flow (e.g. (Arel et al., 2010; Liang et al., 2019; Steingröver et al., 2005))	+ Dynamic + Constantly optimizing - Seems to be an academic solution - Needs to know trajectory of cars	poor privacy: moving pattern allows tracking; full dynamic

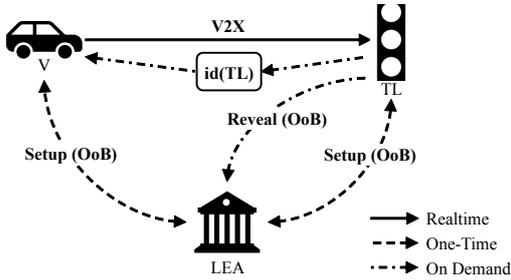


Figure 1: Minimal communication overhead of participants.

3.1 System Model

Junction. The given environment throughout this paper is a junction where a traffic light controls all waiting lanes \mathcal{WL} . A typical junction in our scenario has 12 waiting (3 per incoming direction) and 4 outgoing lanes. Each waiting lane $wl \in \mathcal{WL}$ has a dedicated outgoing orientation of north (n), west (w), south (s) or east (e). Hence, a waiting lane is a combination of two orientations.

Participants. Communication in the system is kept minimal to take into account the limited communication range and unstable connections in V2X environments. We distinguish between V2X communication using one of the existing standards (e.g. WAVE)

and Out-of-Band (OoB) communication happening in special conditions (c.f. Figure 1).

The *User* is a *Vehicle* (V) equipped with an On-Board-Unit (OBU), including a unique ID and cryptographic material enabling it to exchange data in the V2X network. OoB communication is also possible. A vehicle is considered to always know both its current position and its route to a destination. The V uses a scope-exclusive pseudonym P for a specific scope. The scope can be publicly known. We use a scope artifact $ScopeString = \mathcal{H}(id(TL)||TimeWindow)$ and derive a scope-exclusive pseudonym P with a constant, publicly distributed value $id(TL)$ for the traffic light, thus the V uses another pseudonym for every TL to allow limited linkability (Pfitzmann and Borcea-Pfitzmann, 2010). Additionally, the granularity of the dynamic part $TimeWindow$ controls how long a TL can track a V via its unique P , e.g. it can be one day.

The *Traffic Light System* (TL) is a cyber-physical system attached to a communication network, able to communicate via V2X, but also via OoB communication. It controls a real-world traffic light so that traffic can be controlled not only by autonomously driving cars levels 3 and 4 (cooperative driving), but also by non-connected vehicles. TL is also a *Verifier* since it checks incoming messages from V s for validity.

To provide a robust system in terms of integrity and

revocability, a *Law Enforcement Agency (LEA)* is introduced. It knows the real identities of all vehicles in the system. *LEA* itself is not included in traffic control operations but manages the users, which are able to participate (therefore called *Issuer*). Thus, she does not need to know the location of any car at any time. She is a semi-trusted entity since all participants in the system trust digital signatures issued by her. In situations of fraud, she can reveal the identity of a *V* once it is requested by a *TL* and then exclude vehicles (making *LEA* also an *Inspector* and *Revocator*).

3.2 Traffic Cycle Protocol

Setup. The setup phase is performed once. It is desirable to include as many operations as possible in this static one-time phase to take into account the highly dynamic, low-latency, and loosely-connected nature of V2X environments. During the setup phase, the *V* and *TL* exchange with the *LEA* all (cryptography) information and policies needed for participation.

Announcement of Arrival. (*TranVT*) To allow a *TL* to calculate feasible traffic light schedules, it requires information from *Vs*. However, in order to use this information, a *V* has to prove that it is a valid member of the network by 1) having a valid OBU and 2) is still allowed to participate. To guarantee that, one can use the key-binding credentials from the ABC4Trust platform. Credentials are guaranteed to be unforgeable. If a *V* wants to provide information to a *TL*, it has to select a specific amount of verified credentials according to the (static) presentation policy and wrap it along with the actual $arr = (wl, t^a)$ payload, in a so-called presentation token. Then the package is encrypted with the addressed *TL*'s public key. This allows tamper-proof package forwarding in the V2X environment. To overcome "credential pooling", credentials are bound to a specific OBU of a *V* using an implicit proof-of-knowledge (called key-binding). Once a presentation token provides the needed credentials and confirms to the agreed presentation policy, the *TL* buffers arr for further calculation.

Calculation of Traffic Light Schedule. (*TLLC*) We consider that the traffic lights of our junction use a simple four-phase-model. That means that every light cycle consists of 4 traffic flows. In one phase, the vehicles in the vertical direction driving straight ahead and turning right (*srv*) have green, then those in the other direction (*srh*). The same applies to left-turning vehicles (*lv*, *lh*). We use Algorithm 1 to calculate the duration of the corresponding green ΔT^g and yellow Δt_{wl}^y periods in the next light cycle. The *TL* uses all buffered $arr \in \mathcal{A}rr$ where the timestamp of arrival lies before the timestamp of starting the new traffic light

schedule and where no feedback messages arrived. The algorithm also considers the specified length of the whole light cycle Δt^{Cycle} , the total length of the green period for all straight and right lanes Δt_{sr}^g , and the total length of the green period for all left lanes Δt_l^g . First, the traffic intensity per *wl* is calculated. Then, according to the intensities, the green periods are calculated. Finally, the yellow periods of the waiting lanes are calculated according to the given speed limits.

Feedback. (*TranVT*) To further optimize the time of loss at a junction, *TL* collects feedback fb of the experienced waiting time from *Vs*. Using all received fb s, *TL* can first calculate the actual t_j^w of V_j and then find $\sum t_{i,wl_k}^w$ for the *i*-th traffic light cycle and wl_k . The sum can be used to calculate the actual throughput per *wl*. Putting this in relation to the theoretic throughput allows the *TL* (via Q-Learning) to adjust the weights $\vec{\alpha}$ and to select specific actions via its selection policy (Q-function).

Algorithm 1: Traffic light logic calculation (TLLC) for the four-phase-model.

Data: $\mathcal{A}rr, \Delta t^{Cycle}, \Delta t_{sr}^g, \Delta t_l^g, \vec{\alpha}, speedlimit_{wl}$
Result: $\Delta T^g = (\Delta t_{srv}^g, \Delta t_{srh}^g, \Delta t_{lv}^g, \Delta t_{lh}^g), \Delta t_{wl}^y$

- 1 Calculate traffic intensity per *wl*:
- 2 Count arr per *wl* and store in $\mathcal{A}rr_{wl}$
- 3 Traffic intensity per *wl*: $q_{wl} = \frac{\mathcal{A}rr_{wl}}{\Delta t^{Cycle}}$
- 4 Define maximum of green period per *wl*:
- 5 $\Delta t_{srv}^{g,max} = \alpha_{srv} \cdot \max(q_{ns}, q_{nw}, q_{sn}, q_{se})$
- 6 $\Delta t_{srh}^{g,max} = \alpha_{srh} \cdot \max(q_{we}, q_{ws}, q_{en}, q_{ew})$
- 7 $\Delta t_{lv}^{g,max} = \alpha_{lv} \cdot \max(q_{ne}, q_{sw})$
- 8 $\Delta t_{lh}^{g,max} = \alpha_{lh} \cdot \max(q_{wn}, q_{es})$
- 9 Calculate ΔT^g per green periods:
- 10 $\Delta t_{srv}^g = \frac{\Delta t_{srv}^{g,max}}{\Delta t_{srv}^{g,max} + \Delta t_{srh}^{g,max}} \Delta t_{sr}^g$
- 11 $\Delta t_{srh}^g = \Delta t_{sr}^g - \Delta t_{srv}^g$
- 12 $\Delta t_{lv}^g = \frac{\Delta t_{lv}^{g,max}}{\Delta t_{lv}^{g,max} + \Delta t_{lh}^{g,max}} \Delta t_l^g$
- 13 $\Delta t_{lh}^g = \Delta t_l^g - \Delta t_{lv}^g$
- 14 Set $\Delta t_{wl}^y = \text{round}\left(\frac{speedlimit_{wl}}{15}\right)$

3.3 Attacks and Abuses

As in most V2X scenarios, two main security threats arise, namely for privacy and integrity.

Traffic Light System. We assume that a traffic light performs only passive attacks and is not actively manipulating traffic in a bad way (e.g. red light for all $\mathcal{W}L$). The main objective is to track *Vs* passing a junction controlled by the *TL*. It can there-

fore record any received message and derive individual movement patterns. This threat becomes more severe when multiple *TLs* start exchanging information about seen cars, allowing them to create location trajectories. Precisely, the location privacy of a user is threatened if (one or cooperating) *TLs* are able to find a list $\mathcal{T} = (TL_1, \dots, TL_n)$ with $n > 1$ of traffic lights passed during a trip. Knowing that list may be used to identify a *TL* without the need for a unique identifier (such as the ID of a OBU). Section 4.2 provides empirical proof that it is hard for different traffic lights to link multiple scope-exclusive pseudonyms of the same user. Adding additional information to a pseudonym to facilitate linking is not possible due to protocol design: the $id(TL)$, $TimeWindow$, and \mathcal{H} are public knowledge. Other manipulation conflicts with the public presentation policy.

Vehicle. In contrast, *Vs* are considered untrustworthy and thus try to actively influence a *TL* i.a. for their own benefit. One can identify four different goals. First, a *V* can change the impact of its message by trying to appear towards a *TL* as multiple vehicles (Sybil attack). Furthermore, it is possible to send either a wrong time of arrival t^a or a wrong wl , both potentially resulting in inaccurate calculation of the traffic light schedule, eventually downgrading service quality. Furthermore, in the context of reinforced learning, not providing feedback to a *TL* also may impact service quality. Sybil attacks are prevented by a combination of key-bound credentials and scope exclusive pseudonyms, which are indirectly also key-bound. Absolute privacy contradicts the integrity of the system since vehicles can lie without fearing any consequences, ultimately resulting in poor service quality. Therefore, privacy-ABC systems introduce an (trusted) inspector (i.e. *LEA*) who can reveal a *V*'s identity under well-defined conditions (i.e. policy conditions \mathcal{L}) on request of a *TL*. The inspection grounds are clear for all included parties. since they are signed into the presentation token in a tamper-proof way, protecting against malicious *TL*.

Law Enforcement Agency. *LEA* has no knowledge about package flow and payload because she is not involved in the actual traffic light calculation procedure and does not participate in V2X communication. She is bound to the inspection policy which every participant in the system agrees on. Hence, she is unable to illegitimately reveal the identity of a *V*. Therefore, she has to use pseudonyms in the same way cooperating *TL* do and does not have additional knowledge.

External Eavesdropper. Like *TLs*, external entities can also have an interest in deriving individual movement patterns. However, similar to *LEA*, external

eavesdroppers need to link pseudonyms in order to derive a location trajectory.

Furthermore, the system allows revoking a specific set of attribute values without revealing the actual values. The revocation process can be triggered either by a *V* or a *TL*. For example, revocation can be used by a car owner if his *V* gets stolen.

4 EVALUATION

We now evaluate *iTLM* with the reinforcement learning extension in order to assess performance, privacy and emission aspects.

Simulation Environment. We evaluated our approach using SUMO, which is a microscopic simulator for urban mobility. Our testbed is a standard 4-arm intersection with $|\mathcal{WL}| = 12$ according to our system model. Traffic light switching schedules can be controlled in SUMO, using *tlLogic* elements with states G, g, y, r applied¹. Each simulation was run for 900 simulation seconds, resulting in 10 traffic light cycles for a fixed time (*STA*) approach, an actuated approach using induction loops in every wl (*ACT*), and our new dynamic traffic light logic (*TLL*) approach. The evaluation is accomplished with real-world data from the City of Hamburg² in Germany. The traffic counts of three years illustrate the traffic densities of all roads in the annual average weekday traffic, that was broken down to provide a realistic simulation and come up with feasible results.

Scenarios. We formulate three hypotheses (H1-3) which are evaluated in six traffic scenarios. Fig. 2 illustrates the spawn frequency of vehicles/sec in relation to the simulation cycle. Exit lanes are selected with a static distribution.

- H1.** *TLL is capable to quickly adapt the green light phase to alternating traffic flow intensities.*
- H2.** *TLL is capable of detecting and monitoring the rush direction while adapting to changing intensities.*
- H3.** *TLL is capable of reacting to asymmetric incoming lanes and prefers the major arteries.*

4.1 Performance

In order to evaluate the performance, we focus on the waiting time of *Vs* and the related traffic density. The

¹sumo.dlr.de/docs/Simulation/Traffic_Lights.html

²www.hamburg.de/bwvi/verkehrsbelastung/

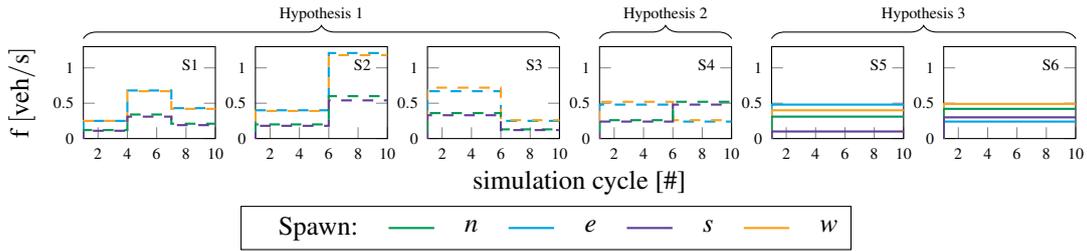


Figure 2: Overview of all scenarios used to verify our hypotheses.

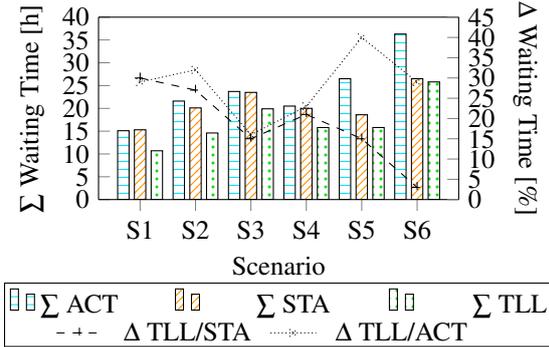


Figure 3: Overview of performance for all approaches across all scenarios.

waiting time defines the overhead of time spent during the simulation because of waiting periods at the junction (i.e. red lights). Due to space constraints, we can only highlight some particularities.

Figure 3 gives a thorough overview of the total waiting time of vehicles and shows that our TLL reduces the waiting time in every scenario.

Figure 4a gives insight into the scenario S1. At the beginning, there is not much difference in the performance because the road network is slowly filling up with cars. However, it can be seen that with a rapidly increasing number of vehicles during rush hour (cycle 4-6), TLL can adapt to this situation and is able to convey the increasing number of cars, resulting in 30% less waiting time and lower overall density. TLL achieves this by increasing the green period for the high traffic flow horizontal lane (c.f. Fig. 4b).

The results of S2 and S3 illustrate a major deficit of the classical methods. In fact, the more vehicles are in the system, the worse ACT performs, because light cycles are changed when a timeout is reached (all bars have similar heights). Regarding green times, the actuated system detects ongoing cars on the lanes and hence keeps the lane on priorities, i.e. giving it green light. However, due to an overcrowded junction, vehicles are unable to leave it on their target lane. TLL however, is able to count the incoming number of cars and then prioritize the lanes with the highest

count. This may lead to an unbalanced light cycle where less dense lanes are neglected for the sake of the majority. Fig. 5 illustrates that vividly for S2: it is easy to understand that lanes going straight or right have a much higher throughput than left turns since this always conflicts with other participants and overall allows lesser directions to drive. TLL draws the right conclusions independently: It detects that major traffic goes $e \leftrightarrow w$ and since left turns have a lower throughput, their time has to be increased in the TLL high scenario. Also, TLL relinquishes the less dense vertical direction by giving it small amounts of green time. H1 can thus be considered to be confirmed.

To confirm H2 we use S4. We can see from Fig. 6 that TLL detects the change of the major traffic axes, and thus intelligently optimizes the green light periods. This results in less waiting times at red lights (TLL: \emptyset 15.8 sec, ACT: \emptyset 20.5 sec, STA: \emptyset 20.0 sec).

S5 and S6 show TLL's advantage more distinctly. TLL is able to calculate the distribution of all lane combinations. Hence it is able to correctly prioritize lanes e, n, w in S5, resulting in much shorter waiting times compared to the other two approaches (see Fig. 3). In fact, ACT performs worse for this high density scenario with a sum of 26.5 hours of waiting after the simulation. STA achieves 18.6 hours while our TLL approach shines with 15.8 hours (less than 40% of ACT). Interestingly enough, in S6 this picture repeats, although TLL calculates traffic light schedules very similar to the STA model ($s+r$ 33 ± 2 seconds, l 6 ± 2 seconds). We assume that the benefit compared to STA is rather low because the number of vehicles from horizontal and vertical lanes is similar making equally distributed green phases feasible by coincidence. ACT fails again by almost evenly distributing the green light period between all lanes, unable to detect and clean a blocked junction. Finally, we can confirm H3.

4.2 Impact of PET

We now discuss some important privacy impacts of our system as it was designed to enable privacy-by-

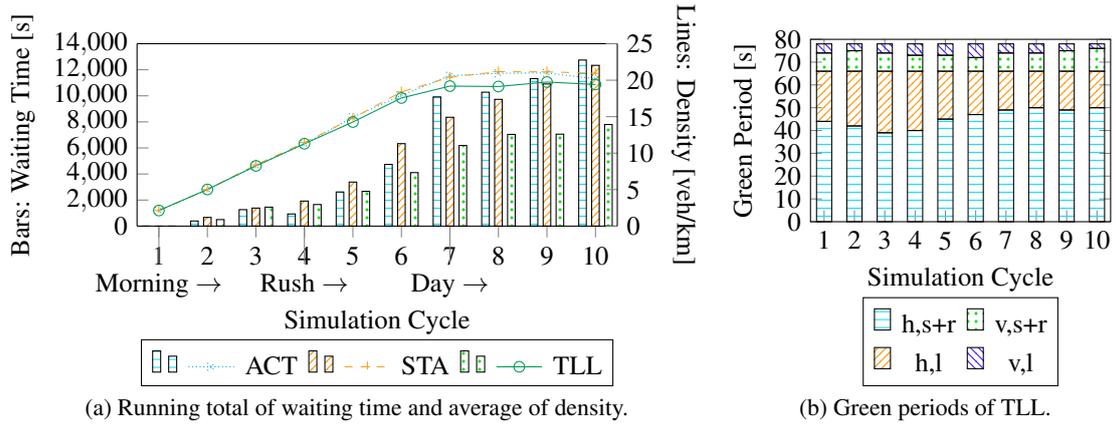


Figure 4: Performance results for S1.

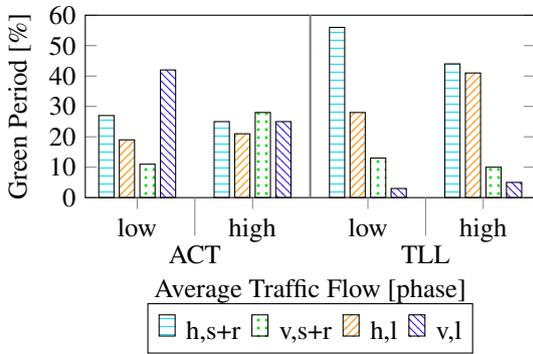


Figure 5: Green periods per approach and phase of S2.

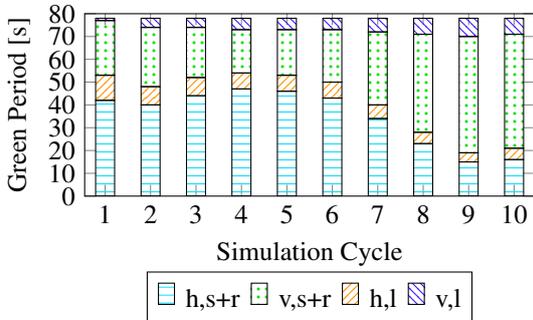


Figure 6: TLL adapts the green periods to the orientation change in S4.

design. In particular, we want to find out how robust the system is in terms of integrity and anonymity. We do not focus on the communication layer since it is based on ABC4Trust.

When talking about integrity, the two transmitted parameters wl and t^a by a V are of interest. If a V sends another wl , then it falsifies the actual number of vehicles per waiting lane, similar to reducing the number of participants (see Figure 7). Also sending a wrong t^a or not receiving data at all (equals not partic-

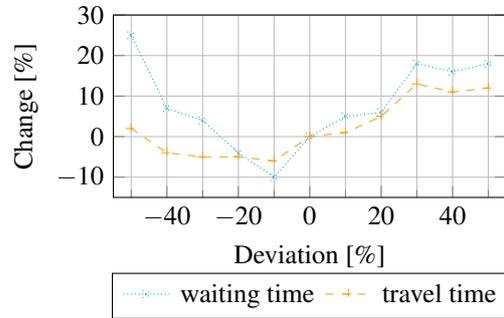


Figure 7: Deviation of KPI in the non-optimal case where not all cars are participating (S3).

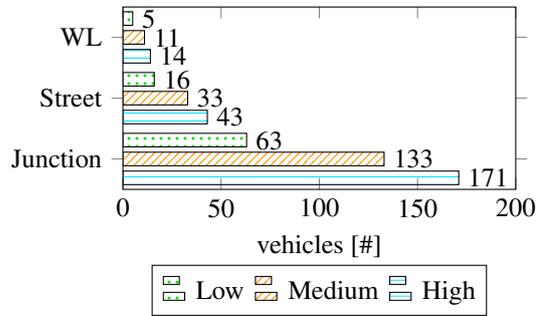


Figure 8: k-anonymity at traffic light for different vehicle densities (one light cycle).

ipating vehicles) might influence the calculation. Figure 7 shows that the calculation is, of course, influenced when corruption happens, although the system can handle inaccuracies regarding transmitted information. If the inaccuracies are similarly distributed as the occurrences of the vehicles, TLL distributes 90 seconds of a light cycle accordingly, resulting in a feasible light schedule. If this is not the case, TL can rely on fb to gain information about that current distribution to update its internal policy. In this manner,

targeted denial of service attacks can be identified and handled appropriately.

From Fig. 8, one can see that even with low traffic, on average, five vehicles pass a junction in a single queue. Therefore, these five vehicles form a k-anonymity set of 5 as long as nobody can derive in which order they arrive at and leave the junction. Although the presentation tokens are generally cryptographically unlinkable and untraceable, conclusions could be drawn from the content or time of transmission. Therefore, it is necessary that V communicate independently of their location with TL and that the arrival time is not exact to the second, but should be given in buckets of e.g. 5 seconds. The independence from the location can be achieved by sending the messages to the traffic light with a random delay.

5 CONCLUSION

Here, we proposed an intelligent traffic light system using crowdsourced user input transferred via V2X to optimize the traffic light cycle and thus reduce overall waiting time and emissions. A simulation has shown that up to 40% of waiting time can be reduced in complex situations. Therefore, the emissions can also be lowered by around 5% for the same number of vehicles. This is done by i.a. avoiding unnecessary stops. Furthermore, our approach achieves a significant level of privacy by adapting ABC4Trust to our needs.

For future work, we plan to analyze the potential of our approach by extending the range of information available, i.e. interconnecting the traffic light network, allowing two or more traffic lights to exchange information and knowledge. However, the impact of privacy for vehicles has to be taken into account. Our existing k-anonymity results only allow a specific level of interconnection, which is of further interest. Furthermore, we want to analyse the influence of even more flexible light schedules.

REFERENCES

- Abuelsamid, S. (2019). Volkswagen Adds ‘Vehicle-To-Everything’ Communications To Revamped Golf With NXP Chips.
- Arel, I., Liu, C., Urbanik, T., and Kohls, A. G. (2010). Reinforcement learning-based multi-agent system for network traffic signal control. *IET Intelligent Transport Systems*, 4(2).
- Blumberg, A. J., Keeler, L. S., and Shelat, A. (2005). Automated traffic enforcement which respects “driver privacy”. In *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, volume 2005.
- Darroch, J. N., Newell, G. F., and Morris, R. W. J. (1964). Queues for a Vehicle-Actuated Traffic Light. *Operations Research*, 12(6).
- Gao, J., Shen, Y., Liu, J., Ito, M., and Shiratori, N. (2017). Adaptive Traffic Signal Control: Deep Reinforcement Learning Algorithm with Experience Replay and Target Network. Technical report.
- Gao, K., rong Han, F., fei Wen, M., hua Du, R., Li, S., and Zhou, F. (2019). Coordinated control method of intersection traffic light in one-way road based on V2X. *Journal of Central South University*, 26(9).
- Li, Y. (2012). *Netzweite Lichtsignalsteuerung auf Basis Rekurrenter Neuronaler Netze*. Dissertation, Technische Universität München.
- Liang, X., Du, X., Wang, G., and Han, Z. (2019). A Deep Reinforcement Learning Network for Traffic Light Cycle Control. *IEEE Transactions on Vehicular Technology*, 68(2).
- Nirman, A., Thilakarathne, L., Wickramasinghe, A., Senanayake, S., and Haddela, P. S. (2018). Google Map and Camera Based Fuzzified Adaptive Networked Traffic Light Handling Model. In *2018 3rd International Conference on Information Technology Research, ICITR 2018*. Institute of Electrical and Electronics Engineers Inc.
- Pfitzmann, A. and Borcea-Pfitzmann, K. (2010). Lifelong privacy: Privacy and identity management for life. In *IFIP Advances in Information and Communication Technology*, volume 320. Springer New York LLC.
- Rachmadi, M. F., Al Afif, F., Jatmiko, W., Mursanto, P., Manggala, E. A., Ma’sum, M. A., and Wibowo, A. (2011). Adaptive traffic signal control system using camera sensor and embedded system. In *TENCON 2011 - 2011 IEEE Region 10 Conference*. IEEE.
- Sabouri, A., Krontiris, I., and Rannenber, K. (2015). *Attribute-based Credentials for Trust*. Springer International Publishing, Cham.
- Schaub, F., Ma, Z., and Kargl, F. (2009). Privacy requirements in vehicular communication systems. In *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, volume 3.
- Steingröver, M., Steingröver, M., Schouten, R., Peelen, S., Nijhuis, E., and Bakker, B. (2005). Reinforcement learning of traffic light controllers adapting to traffic congestion. *Benelux Conference on Artificial Intelligence, BNAIC 2005*.
- Varga, N., Bokor, L., Takacs, A., Kovacs, J., and Virag, L. (2017). An architecture proposal for V2X communication-centric traffic light controller systems. In *Proceedings of 2017 15th International Conference on ITS Telecommunications, ITST 2017*. Institute of Electrical and Electronics Engineers Inc.
- Wiedersheim, B., Ma, Z., Kargl, F., and Papadimitratos, P. (2010). Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In *WONS 2010 - 7th International Conference on Wireless On-demand Network Systems and Services*.
- Xing, S.-Y., Lian, G.-L., Yan, D.-Y., and Cao, J.-Y. (2018). Traffic Signal Light Optimization Control Based on Fuzzy Control and CCD Camera Technology. *DEStech Transactions on Computer Science and Engineering*, (csmms).