electronics

MDPI

Article

Blockchain-Based Pseudonym Management Scheme for Vehicular Communication

Sonia Alice George, Steffie Maria Stephen and Arunita Jaekel *

School of Computer Science, University of Windsor, Windsor, ON N9B 3P4, Canada; georg11o@uwindsor.ca (S.A.G.); shajin@uwindsor.ca (S.M.S.)
* Correspondence: arunita@uwindsor.ca

Abstract: A vehicular ad hoc network (VANET) consists of vehicles, roadside units, and other infrastructures that communicate with each other with the goal of improving road safety, reducing accidents, and alleviating traffic congestion. For safe and secure operation of critical applications in VANET, it is essential to ensure that only authenticated vehicles can participate in the network. Another important requirement for VANET communication is that the privacy of vehicles and their users must be protected. Privacy can be improved by using pseudonyms instead of actual vehicle identities during communication. However, it is also necessary to ensure that these pseudonyms can be linked to the real vehicle identities if needed, in order to maintain accountability. In this paper, we propose a new blockchain-based decentralized pseudonym management scheme for VANET. This allows the vehicles to maintain conditional anonymity in the network. The blockchain is used to maintain a record of each vehicle and all of its pseudo-IDs. The information in the blockchain can only be accessed by authorized entities and is not available to all vehicles. The proposed distributed framework maintains an immutable record of the vehicle data, which is not vulnerable to a single point of failure. We compared the performance of the proposed approach with a traditional PKI scheme and shown that it significantly reduces the authentication delay.

Keywords: vehicular ad hoc network; authentication; blockchain; identity management; location privacy

Citation: George, S.A.; Stephen, S.M.; Jaekel, A. Blockchain-Based Pseudonym Management Scheme for Vehicular Communication. *Electronics* **2021**, *10*, 1584. https://doi.org/10.3390/electronics10131584

Academic Editors: Michele Girolami and Davide La Rosa

Received: 17 May 2021
Accepted: 18 June 2021
Published: 30 June 2021

1. Introduction

A vehicular ad hoc network (VANET) consists of vehicles, roadside units (RSUs), and other infrastructures that communicate with each other with the goal of improving road safety, reducing accidents, and alleviating traffic congestion. VANETs provide support for the deployment of intelligent transportation systems (ITS) and will form an integral part of future smart city infrastructure [1]. Typical VANET applications can be classified as (i) safety applications or (ii) comfort applications. Safety applications such as collision avoidance, lane-changing assistance, intersection coordination, and emergency warning systems provide critical support for preventing road accidents. Comfort applications, also referred to as "infotainment" applications, include items such as weather notifications, gas/restaurant locations, and parking information, which can enhance the driving experience [2].

Different communication standards such as dedicated short-range communication (DSRC), wireless access in vehicular environments (WAVE), and cellular-V2X (CV2X) [3–5] have been proposed for vehicular communication in VANET. Each vehicle is equipped with an onboard unit (OBU) that is responsible for communicating with other vehicles and infrastructure units. The roadside units (RSUs) are infrastructures present on the side of the road that provide support for vehicular communication. Communication in VANET can be vehicle to vehicle (V2V), vehicle to infrastructure (V2I), infrastructure to infrastructure (I2I), or V2X—vehicle to any other Internet-enabled device [6].

VANET safety applications require frequent, up-to-date information on the current state of the neighboring vehicles in order to make important decisions. To achieve the necessary level of awareness, each vehicle periodically broadcasts its current status to other vehicles, using basic safety messages (BSMs). BSMs contain important information about a vehicle, such as its location, speed, heading, and other relevant information that can be used to manage traffic congestion and prevent collisions. For improved awareness, BSMs are sent at a relatively high rate, 10 times per sec [7]. The BSMs can be used to transmit alerts or warning messages in the cases of collision warning, lane change warning, an emergency vehicle at scene warning, forward collision warning, precrash sensing, and blind-spot warning [8]. These messages are sent by the vehicles after analyzing the data received from the neighboring vehicles. For example, when a driver signals a lane change, the OBU uses the communication information to determine whether there is enough gap for a safe lane change based on the position of vehicles in the next lane. If the spacing between vehicles in the adjacent lane is insufficient, the driver is warned [8].

Furthermore, as the BSM data is used in real-time for high-speed applications, it is typically not encrypted to allow fast processing [9]. However, this makes the information in a BSM vulnerable to privacy attacks, as it can be used to reveal precise movement patterns and driving behavior, which, in turn, can lead to long-term driver profiling and vehicle tracking. If messages exchanged in VANET wireless communication carry inferrable personally identifiable information (PII), it can introduce several privacy threats that could limit the adoption of VANET.

A widely accepted approach for preserving privacy in VANET is to use pseudonyms to dissociate the vehicle identifier from the information trail [10–12]. Pseudonyms (also referred to as pseudo-IDs or PIDs) are the temporary identifiers that hide the real identity of the vehicle and can be used for authorizing a vehicle to be a part of the vehicular network. Even with the use of pseudonyms, it is possible to infer personal information about a driver if the same pseudonym is used for an extended period. Therefore, it is important to change these pseudonyms from time to time in order to disconnect the information stream associated with a specific identifier.

Pseudonyms allow vehicles to maintain anonymity and preserve privacy when participating in a VANET. However, for proper functioning, it is also necessary to ensure that:

- participation in the VANET is restricted to authenticated vehicles only and
- there is a way to link pseudonyms with the real vehicle identities, in order to have accountability in case of any misbehavior.

In other words, it is necessary to balance the privacy requirements of a vehicle with the need to have security and accountability for all users [6]. This means that vehicles should only have conditional anonymity [13] rather than full anonymity. This will allow vehicles to communicate using pseudonyms, but will allow (i) detection of unauthenticated vehicles and (ii) linking of pseudonyms to actual vehicle identities in case of misbehavior. Therefore, a suitable pseudonym management scheme that can authenticate valid senders in real-time, detect unauthorized BSMs, and report this information to the relevant authorities is needed.

In this paper, we introduce a new blockchain-based pseudonym management scheme for VANET. In this approach the RSU is responsible for authenticating the sender of a BSM. This reduces the computational overhead on individual vehicle OBUs, which have limited processing power compared to infrastructure units such as the RSU. Detailed information about each vehicle is maintained in a shared, distributed ledger [14] that can only be accessed by authorized entities. We compared the performance of the proposed approach with traditional PKI-based authentication [15] and shown that it leads to reduced delay and packet size. This approach in this paper can be extended and applied to other applications, such as truck-and-drone delivery systems [16] and ITS logistics [17].

The rest of the paper is organized as follows. In Section 2, we discuss the traditional PKI-based authentication in VANET and also review some recent papers that use blockchain technology for authentication. In Sections 3 and 4, we present the communication architecture and the proposed pseudonym management scheme. In Section 5, we

discuss and analyze the simulation results, and in Section 6, we present our conclusions and some directions for future work.

2. Review of Vehicle Authentication in VANET

Traditional VANET authentication uses the public-key infrastructure (PKI) for managing the vehicles' identities in the network [15,18]. Each vehicle in the network is assigned one (or possibly multiple) public–private key pairs. During registration, each vehicle v is assigned a certificate ($Cert_v$) by a trusted certificate authority (CA), and provided with the public key (PK_{CA}) of the CA. The certificate will contain the public key (PK_v) of the vehicle v and the digital signature of the public key signed with the CA's private key (SK_{CA}), as shown in Equation (1) [18]. The signature also contains the identity of the CA, i.e., ID_{CA}. We assume that public keys of CAs are known to registered vehicles.

$$Cert_v = PK_v | Sign_{SK_{CA}}[PK_v | ID_{CA}] \quad (1)$$

Before broadcasting a BSM, the sending vehicle v computes the digital signature of the message using its private key SK_v. This digital signature and the certificate of the vehicle ($Cert_v$) must be transmitted with each BSM. To validate the sender, the receiving vehicle first extracts PK_v from the certificate using the public key of the trusted CA (PK_{CA}). Then, PK_v is used to verify the digital signature of the message. If verified successfully, then the sender of the message is authenticated [18]. A typical packet format for sending BSMs is shown below in Figure 1, where T is a timestamp that is concatenated with the message M_v (M_v contains the PID and other relevant vehicular data for v) to ensure freshness of data.

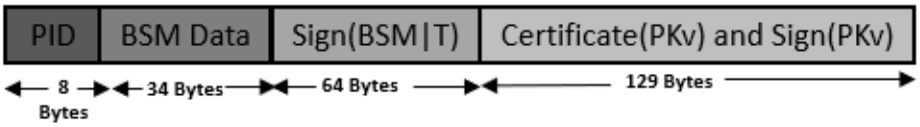

Figure 1. BSM packet format for PKI framework.

Blockchain technology, initially introduced for Bitcoin cryptocurrency [19], supports a decentralized [20] and distributed framework and uses cryptography to store data in an immutable record of data on a shared ledger. Blockchains can be an attractive option for implementing VANET authentication and a number of blockchain-based approaches have been proposed in recent years for a variety of applications.

In [21], Leiding et al. used Ethereum [22], to implement a self-managed VANET framework with challenge–response-based authentication, where the vehicles, RSUs, and the authorities are participants of the network. The limitation of this approach is higher power consumption, as each message must be stored in the blockchain and requires mining as new blocks are added [23]. In [24], Dai et al. proposed a permissionless blockchain, where all vehicles are participants of this system. The vehicles store their reputation scores on the blockchain, instead of storing each BSM. These reputation scores are used by other vehicles to authenticate the senders. The work did not consider the computational complexity for maintaining the reputation on the blockchain. Furthermore, since the participants are individual vehicles, it will become difficult to reach consensus as the number of vehicles in the network increases. In [25], Lasla et al. present a blockchain framework, where the participants include vehicles, RSUs, and authorities. It uses PKI to assign public–private key pairs to the participating vehicles. This method uses proof-of-work consensus, which is slow due to the high computational requirement to add new blocks [23].

In [19,26], permissioned blockchains were used with VANETs. In [19], Malik et al. used PKI to generate public and private keys for the vehicles, which are used by the vehicles to authenticate themselves with the RSUs. The pseudo-ID of the vehicle is digitally signed by the CA and added as blocks in the blockchain. This approach uses proof of authority for consensus, where the validator's identity is kept at stake [27]. In [26], Lu et al.

propose a framework that use three different blockchains with VANET, for storing (i) valid certificates, (ii) revoked certificates, and (iii) messages transmitted by the vehicles. In order to authenticate a vehicle, both the "valid certificates" and "revoked certificates" blockchains must be searched. The vehicle is authenticated only if its certificate is present in the first blockchain and absent from the second blockchain.

In [28], Wang et al. proposed a blockchain-assisted trustworthiness scalable computation-based V2I authentication (B-TSCA) scheme. This scheme aims to reduce the computational cost of authentication when the vehicle travels through multiple RSUs. The previous RSU gives the next RSU and vehicle a handover certificate, which assists the vehicle in resuming communication. In [29], Khalid et al. proposed a secure blockchain-based data storage and incentive provisioning system. The interplanetary file system [30] is used to store messages related to traffic events and to resolve redundancy issues. In this scheme, the reputation of vehicles is measured based on their past events, and consortium blockchain [31] is used to store the vehicle's reputation values.

In [32], Hassija et al. proposed a secure and distributed framework for vehicular communication using an open-source distributed ledger, IOTA. This approach includes a DAG-enabled framework and an auction-based smart contract to address security and privacy. In [33], a decentralized key management mechanism for VANET with blockchain technology (DB-KMM) that can withstand DoS attacks, public key tampering attacks, and collusion attacks is proposed. In this approach, the user's public key is automatically registered, updated, and revoked.

As discussed above, some interesting works on using blockchain in VANET have been proposed in recent years. Some limitations of the existing works include high power consumption and scalability issues, particularly when it is required to store every message in the blockchain. Scalability issues also arise when each individual vehicle has access to update the blockchain. It becomes harder to reach consensus and requires higher storage and computation capabilities in vehicle OBUs. Finally, there are increased security risks, if individual vehicles have access to the blockchain, as vehicles are more vulnerable to attacks. The main objective of the proposed work is to limit access to private information in the blockchain to infrastructure units only and shift the computational burden of pseudonym authentication from vehicle OBUs to RSUs.

A high-level overview with some preliminary results from this work was presented in [34]. In this paper, we have provided a new algorithm and detailed description of each step in the authentication process, which were not included in [34]. We have also extended the literature review and added new simulation results and comparisons, as well as a discussion on directions for future research.

3. Proposed Architecture

In this section, we discuss the architecture for our proposed blockchain-based pseudonym scheme. The V2V communication uses the DSRC/WAVE protocol stack [4], with a three-tier VANET architecture, similar to that in [35]. The proposed approach would be suitable for use in conjunction with other architectures, such as ITS-5G as well [36]. As shown in Figure 2, there are three main classes of entities that participate in the authentication process. These are: (i) authentication parties (APs), (ii) roadside units (RSUs), and (iii) individual vehicles.

We use the following notation in discussing the operation of each component

- PID_v: pseudonym or pseudo-ID (PID) of vehicle v
- $PK_v(SK_v)$: public (private) key of vehicle v
- M_v: contents of BSM from vehicle v (including its PID)
- T: timestamp indicating when a message M is generated
- $Sign_{SK_v}[X]$: the digital signature for message X, generated using the private key of vehicle v

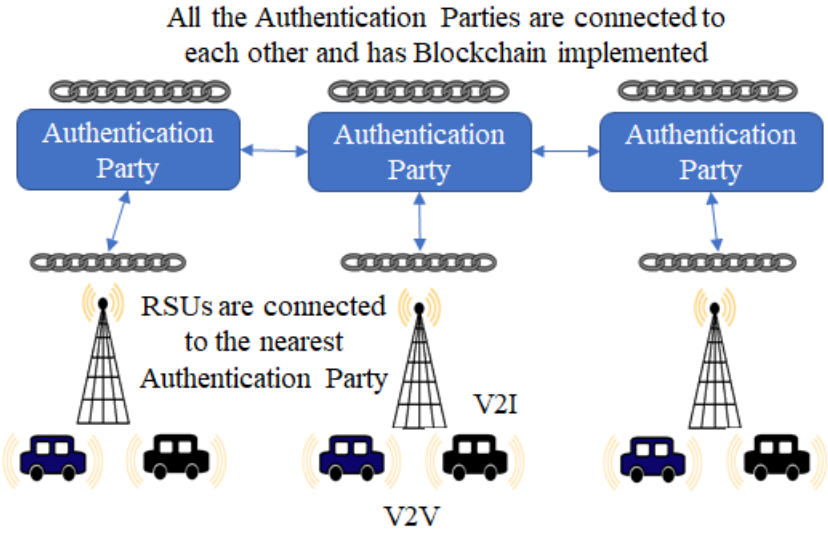

Figure 2. Proposed Architecture.

The main function of the APs is to register new vehicles, to allow them to participate in the network. The APs are also authorized to add transactions to the shared ledger. The APs are interconnected through a wired I2I network and each AP maintains a copy of the shared ledger. This allows vehicles in different regions to register with their nearest authentication party, but the information is available to all APs. If a vehicle leaves the region under one AP and enters another, it can continue to participate in the VANET seamlessly.

Typical transactions performed by an AP include adding a newly registered vehicle or updating the information about a registered vehicle. Before participating in the VANET, a vehicle v first sends a registration request to the AP that is responsible for that region. Upon receiving the request, the AP checks the vehicle credentials to make sure the request is legitimate and the vehicle is authorized to send and receive messages in the VANET. If so, the AP generates a set of public–private key pair and (PK_v, SK_v, and a pseudo-ID PID_v) for the vehicle. In our simulations, we assumed that each vehicle has a single PID and key pair; however, it is possible to allocate mulitple PIDs and key pairs to each vehicle. This information is also added to the blockchain as a registration transaction. The information in the shared ledger can be used to link a PID to the real identity of a vehicle (e.g., a unique 17-character vehicle identification number or VIN) [37]. The shared ledger also contains information on the current PID of the vehicle and expiration time, revocation status of the PID, and any misbehavior reports. In our implementation, we used SOLO [38], the default consensus algorithm for hyperlegder fabric [39]. However, any other suitable algorithm can be used as well. Finally, the AP is also responsible for submitting a misbehavior transaction to the shared ledger, if it receives a misbehavior report for a vehicle, from an RSU.

The RSUs are responsible for actually authenticating vehicles and have backhaul I2I connections to each other and to the APs. If a vehicle is not able to authenticate a sender v locally, it sends an RSU query message to the nearest RSU. When the RSU receives this message, it queries the blockchain to get the most updated information on vehicle. RSUs have read-only access to the shared ledger, so they can retrieve information a about a vehicle, but they are not allowed to add any transactions. The RSU checks if the PID_v and the PK_v of the vehicle v is valid in the blockchain; if so, the RSU validates the signature of the message by using PK_v (retrieved from the blockchain) and, upon validation, broadcasts this information to all vehicles in its region. If the sender cannot be authenticated, the RSU broadcasts a warning message to all vehicles.

The third type of entity in our architecture consist of the individual vehicles. Each vehicle in the network must carry out the following tasks:

1. VEHICLE REGISTRATION: Each vehicle must register itself with an AP, before joining the VANET. During registration, each vehicle sends a registration request, along with

its real identity (e.g., VIN) and related credentials, to the nearest AP and receives a set of pseudo-IDs and corresponding public/private key pairs (PID_v, PK_v, and SK_v, respectively) from the authentication party. These are used for communication with other vehicles, as discussed below.

2. BSM BROADCAST: Each vehicle communicates its current status with neighboring vehicles through BSMs. When sending a BSM, the vehicle v must include additional information such as (PID_v, PK_v) and the digital signature of the message, along with the regular BSM data. This is shown in Equation (2), where M_v is the basic safety message data (including PID and vehicle status information), T is the timestamp, and $Sign_{SK_v}[M_v|T]$ is the digital signature generated using the private key, SK_v.

$$V \rightarrow M_v, Sign_{SK_v}[M_v|T], PID_v, PK_v \quad (2)$$

Figure 3 shows the packet format used for the proposed approach, and we note that the packet size is 171 bytes, compared to 235 bytes in PKI approach, as shown in Figure 1. The packet sizes may change depending the actual content of the BSM data field, and we used typical values found in the literature [40]. The proposed approach requires a smaller packet size compared to PKI. This is mainly due to the additional certificate that must be attached to each BSM, when using PKI. We note that the PKI packet size does not include additional bytes for any certificate revocation lists (CRLs). The inclusion of CRLs will further increase the packet size for each BSM transmission for PKI.

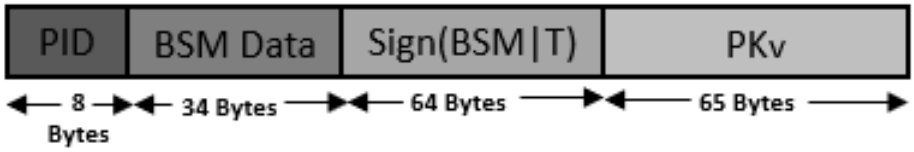

Figure 3. BSM packet format of proposed method.

3. BSM VALIDATION: When a BSM is received from vehicle v, the receiving vehicle will first try to validate the BSM locally. If it succeeds, the received BSM will be processed normally. Otherwise, a request of validation is send to the nearest RSU.This authentication step is discussed in detail in Section 4.

4. Overview of Pseudonym Authentication

Traditional PKI authentication in VANET requires a certificate to be attached to each BSM. This certificate is signed using the private key of an AP, where the public keys of the APs are known to all participants of the network. The public key of the sending vehicle can be extracted from the certificate and then used to authenticate the BSM. This approach does not require the use of RSUs for vehicle authentication; each BSM is authenticated by each receiving vehicle individually. However, it adds an extra level of processing, i.e., extracting PK_v from the certificate, for each BSM that is received. This increases the computational load on the vehicle OBUs, which have limited processing power. It also increases the communication overhead, since a certificate must be attached to each BSM. Furthermore, since vehicle PIDs and/or keys may be revoked due to misbehavior, each vehicle must ensure that the certificate attached to a BSM is actually valid. In other words, vehicles must have access to a certificate revocation list (CRL), with the most up-to-date information, which must be updated and shared frequently. In this section, we propose our approach for BSM authentication, which aims to reduce some of these overheads.

As mentioned in Section 3, the proposed architecture consists of APs, RSUs, and individual vehicles, where APs have full access to the blockchain and RSUs can read from the shared ledger. The reasons for choosing hyperledger fabric include the immutable distributed ledger system, its level of scalability, performance, and trust, as well as the permissioned membership where all participants have known identity. This architecture

is implemented on hyperledger fabric for creating a decentralized and distributed lookup-based authentication for VANET. In our implementation, we make the following assumptions:

- We assume that the APs and RSUs can be trusted. It is possible for infrastructure equipment to be compromised, and different approaches have been proposed in the literature to deal with this [6,41]. We assume suitable measures are in place for dealing with compromised APs and RSUs, but it is outside the scope of this paper.
- We assume that there is an RSU within the range of each vehicle to assist with the authentication of other vehicles' messages.
- We assume that the RSUs have enough computational power to look information up on the blockchain and respond to queries in real time.
- We assume the vehicles OBUs have enough capacity to locally store PID and PK information for a subset of vehicles and perform the necessary computations.

Algorithm 1 shows the steps in the BSM authentication process that is carried out by each vehicle OBU. Each vehicle v in the network uses its pseudo-ID (PID_v) to indicate the sender of the message and attaches its public key (PK_v) and the digital signature of the message generated using its private key. Each vehicle also maintains a local table (LT) consisting of valid (PID_v, PK_v) pairs, along with an expiration time for each entry. We note that the length of time for which the information in local table is valid can affect the performance. If it is too short, vehicles will need to query the RSU more frequently, increasing the delay. If it is too long, the LT may contain stale or incorrect data. Some current standards recommend vehicles to change their pseudonyms at least every 5 min [42]. Therefore, we feel that a validity period of a few seconds in the LT is reasonable to ensure freshness of data. In our simulations, we used a validity period of 5 s. The authentication algorithm is run for each received BSM, and the output is a binary value that represents whether the BSM is valid or not. A BSM from an authenticated sender with correct digital signature is designated as "VALID" and can be used in related safety-critical algorithms or other applications. Otherwise, the BSM is considered to be spurious and immediately discarded.

When a new BSM is received, the receiving vehicle first checks if an entry for (PID_v, PK_v) can be found in LT and the entry is not expired (Step 1). If so, it can authenticate the sender v locally (Step 3); otherwise, the vehicle must wait for a response from the RSU. If local authentication is not possible, the vehicle waits a random amount of time t_w, before sending a query to the RSU. This is done to reduce the communication overhead. Since many nearby vehicles will receive the same BSM, it may cause significant channel congestion if all vehicles try to query the RSU at the same time. Once the RSU receives a query for a sender and confirms its authentication status, it broadcasts the response to all vehicles. It is possible that a vehicle will receive the response during its wait period and will not need to send the query. If no such message is received during the wait period, then the vehicle sends a query to the RSU. Once a response message for (PID_v, PK_v) is received, either during the wait period or after sending the query, the BSM is validated based on this response (Steps 9–24). If the RSU response indicates that public key PK_v is associated with pseudo-ID PID_v, then the sender is authenticated. In this case, (PID_v, PK_v) is added to LT; otherwise, the sender v is not authenticated and the BSM is discarded. For authenticated senders, the next phase is to verify the digital signature (Steps 18–24). If the signature can be verified using PK_v, then the BSM is valid; otherwise, it is discarded.

When the RSU receives a query for a (PID_v, PK_v) pair, it looks up the PID_v in the blockchain to verify the currently valid public key. Each vehicle may have multiple pseudo-IDs and corresponding keys associated with it and these pseudonyms need to be changed frequently to protect privacy. Therefore, it is necessary to ensure that the expired IDs are not being used and each entry in the LTs is only valid for a short period of time. The blockchain can also contain additional information on a vehicle v, such as misbehavior reports and reputation scores. The proposed approach implements authentication of vehicles as a quick lookup for its PID in the blockchain. Thus, we have a lightweight pseudonym authentication mechanism, which significantly reduces the computation burden on vehicle OBUs.

Algorithm 1 BSM Authentication Algorithm.

Input: BSM received from vehicle v, local table at receiving vehicle (LT)
Output: Authentication status of received BSM from v

Check status of PID_v and PK_v in local table
if $(PID_v, PK_v) \in LT$ and not expired **then**
  Sender v is authenticated
else
  Set random wait time t_w and wait
  if No status message for (PID_v, PK_v) received during t_w **then**
    Send validation request to RSU and wait for response
  end if
  Process RSU response.
  if Response indicates an authenticated BSM **then**
    a. add (PID_v, PK_v) to LT
    b. Sender v is authenticated
  else
    Sender v is not authenticated
    b. Received BSM is not VALID
  end if
end if
if sender v is authenticated **then**
  a. Verify digital signature using PK_v
  if Signature valid **then**
    Received BSM is VALID
  else
    Received BSM is not VALID.
  end if
end if

5. Simulation and Results

In this section, we present and analyze the results of our simulations. We used SUMO 0.32.0 [43] to generate the vehicle traffic and OMNET++ 5.3 [44] with Veins 4.7.1 [45], to simulate the network communication. In our simulations, we used the two-ray ground reflection model [46], although other models such as the Nakagami model [46] can also be used. The permissioned blockchain framework was implemented using the hyperledger composer [47], which is an open-source framework for developing blockchain applications. We used a uniform speed of 50 km/h for all vehicles. We note that the primary effect of varying speed would be a change in the vehicle density, as more intervehicle distance is needed as speed increases. This, in turn, would affect the number of packets received. Therefore, we simulated how the performance varies with different number of vehicles in the simulation. Table 1 shows the computer setup for our simulation and the simulation parameters that we used.

To evaluate the performance of the proposed approach, we the compared it to the traditional PKI framework in terms of different parameters such as the additional message overhead, the authentication delay, and the channel busy time (CBT).

Table 1. Simulation Setup.

CPU	Intel(R) Core(TM) i5-8265U CPU @1.60 GHz 1.80 GHz
RAM	7.89 GB
Simulation time	200 s–500 s
Frequency	5.9 GHz
No. of nodes	50–200
Vehicle speed	50 km/h
Length of road segment	2500 m
Physical Layer	IEEE 802.11p
Mac Layer	IEEE 1609.4
Measured Parameters	Delay due to Authentication, Channel Busy Time, BSM Packet Size, Message Overhead

5.1. Additional Messages Sent

Since certificates are not attached to each BSM, two additional types of messages are needed in proposed approach to authenticate the sender, as given below.

- RSU query message: These are messages sent from a vehicle to the RSU, if it cannot find a valid entry for the sender of a received BSM in its LT and
- RSU response message: These are messages broadcast by the RSU to all nearby vehicles in response to a query from a vehicle. It indicates the status (i.e., authenticated sender or not) of the corresponding BSM sender.

Figure 4 shows how the numbers of BSMs, RSU queries, and RSU response messages vary with the number of vehicles as the road traffic density increases. As expected, the number of BSMs increase steadily with the number of vehicles. However, the rate of increase for the number of RSU queries and RSU response messages is much lower. For PKI, there are no additional messages needed, if we assume that certificates are never revoked. However, this is not realistic and additional communication would be needed for PKI as well, for circulating the CRLs.

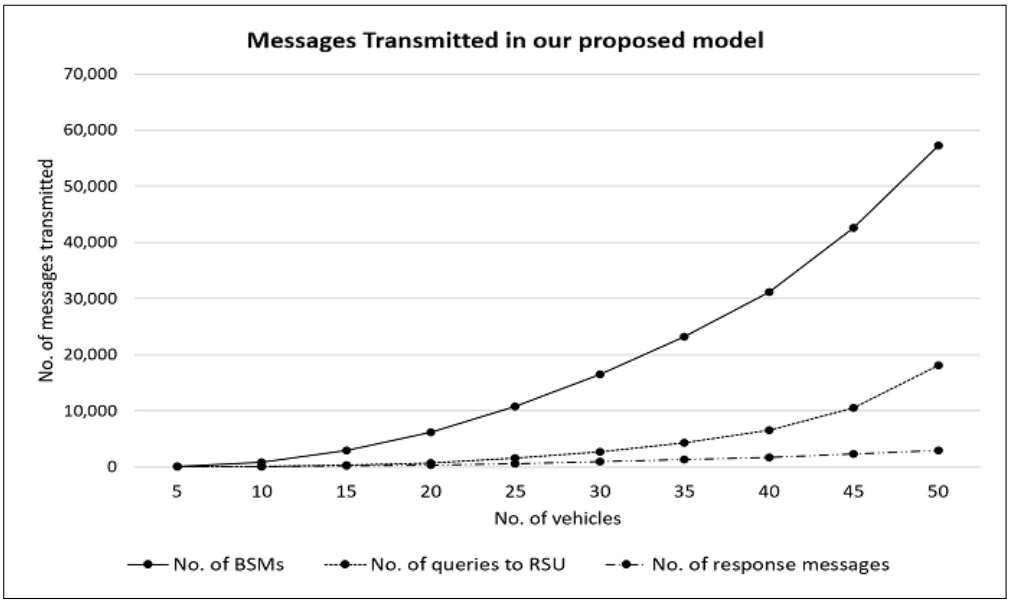

Figure 4. Additional messages transmitted in our proposed method.

5.2. Authentication Delay

The goal of the proposed approach is to create a lightweight authentication mechanism that reduces the computation overhead of the OBUs as well as the authentication delay. The authentication delay is typically of the order of a few ms; however, it depends significantly on the speed/capacity of processor used. This is why we used normalized delays for

comparison, in this section. Figure 5 compares the normalized authentication delay per BSM, for both PKI and the proposed approach. We see that the average delay per BSM does not vary significantly with the number of vehicles. However, the delay for the proposed approach is reduced by about 50% on average. This is due to the additional computational time required for validating two digital signatures in the PKI approach. In the proposed approach, the delay is reduced by using RSU services to authenticate the sender using blockchain, and then verifying the digital signature in the message.

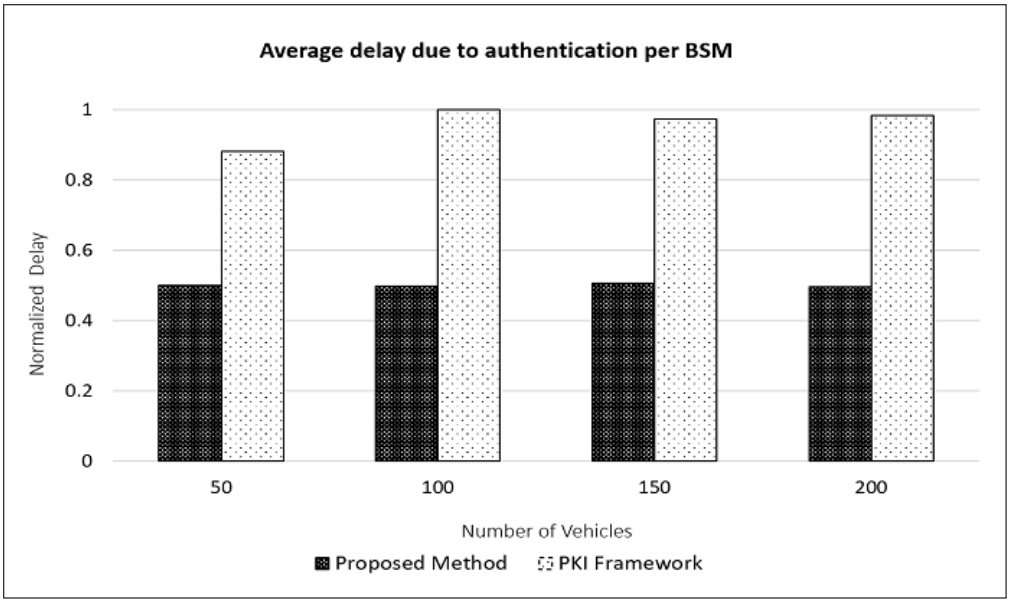

Figure 5. Average delay in authentication for a BSM.

Figure 6 shows the total normalized authentication delay for all the BSMs. As expected, this delay increases as the number of vehicles (and hence the number of BSMs transmitted) in the simulation increases. We see that the proposed approach results in a significant reduction, about 47% on average, in the total delay.

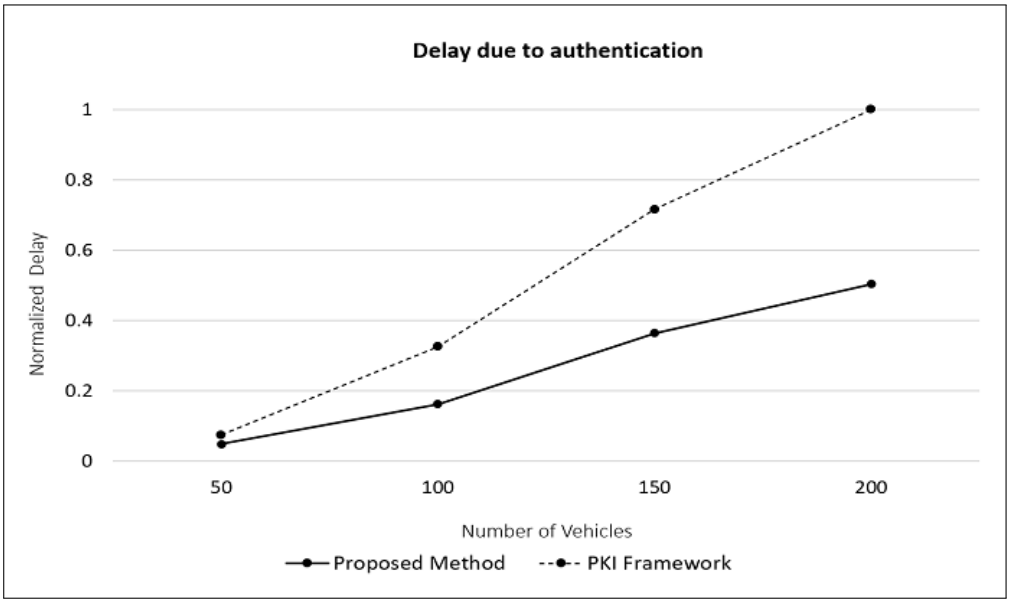

Figure 6. Total delay due to authentication.

Finally, Figure 7 shows the channel busy time (CBT) for the two approaches. We see that for both cases, the CBT increases with the number of vehicles and PKI consistently

shows a lower CBT. This is due to the additional messages, i.e., RSU queries and responses that are needed in the proposed approach.

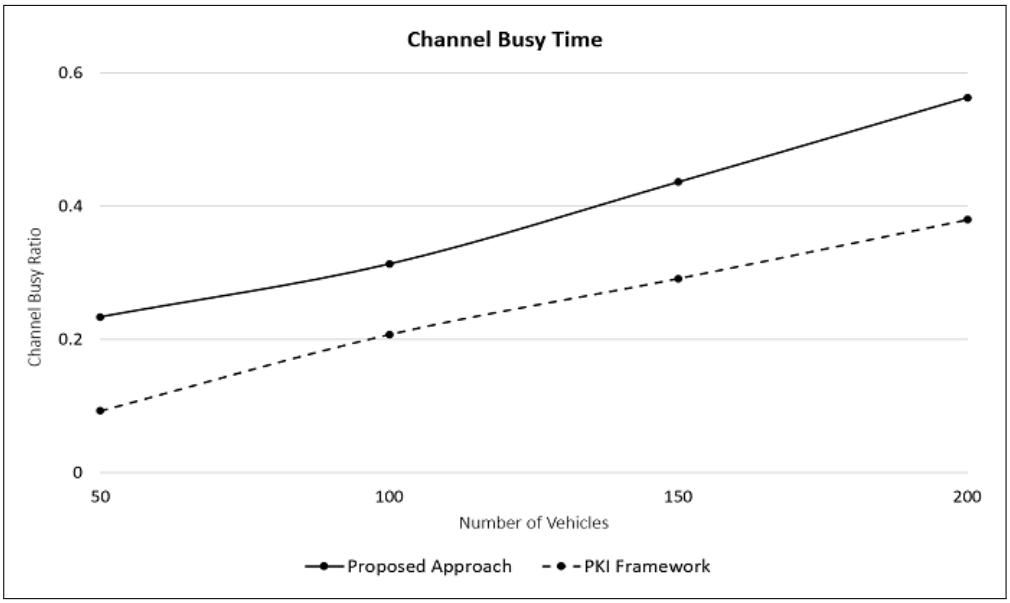

Figure 7. Channel busy time.

Overall, the simulation results indicate that the proposed approach is able to reduce authentication delay and computation overhead on vehicle OBUs. However, this reduction comes at the cost in increased message exchange with the RSUs. Therefore, this approach will be most effective under low to moderate channel loads. For higher loads, it is recommended that additional congestion control mechanisms should be implemented and used in conjunction with the proposed approach.

6. Conclusions and Future Work

In this paper, we present a lightweight pseudonym management scheme for vehicular authentication using blockchain. The proposed approach reduces the computational overhead on vehicle OBUs by shifting the burden of authentication to the RSUs; it results in a significantly lower authentication delay compared to a traditional PKI-based approach. The trade-off is that it requires additional communication between vehicles and RSUs. We expect that appropriate congestion control approaches will be used in conjunction with our proposed approach to mitigate channel congestion.

In this paper, the performance of the proposed approach was studied using simulation results. Additional evaluation using a testbed with actual hardware components, including OBUs and RSUs, are needed to further validate the results for a range of different traffic conditions. A suitable misbehavior detection model that can accurately identify and report malicious vehicles to the APs should be integrated with the proposed authentication approach.

Author Contributions: A.J. was responsible for conceptualization of the paper. S.A.G. developed the software framework, performed analysis and validation, and wrote the paper under the supervision of A.J. and S.M.S. extended the software and collected and analyzed the data. A.J. supervised the research and provided guidance and key suggestions in writing the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by NSERC DG, Grant# RGPIN-2015-05641.

Acknowledgments: The work of A. Jaekel has been supported by a research grant from the Natural Sciences and Engineering Research Council of Canada (NSERC).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Soyturk, M.; Muhammad, K.N.; Avcil, M.N.; Kantarci, B.; Matthews, J. Chapter 8—From vehicular networks to vehicular clouds in smart cities. In *Smart Cities and Homes—Key Enabling Technologies*; Obaidat, M.S., Nicopolitidis, P., Eds.; Elsevier: Cambridge, MA, USA, 2016; Volume 1, pp. 149–171.
2. Yousefi, S.; Mousavi, M.S.; Fathy, M. Vehicular ad hoc networks (VANETs): Challenges and perspectives. In Proceedings of the 6th International Conference on ITS Telecommunications, Chengdu, China, 21–23 June 2006; pp. 761–766.
3. Anwer, M.S.; Guy, C. A survey of VANET technologies. *J. Emerg. Trends Comput. Inf. Sci.* **2014**, *5*, 661–671.
4. Schoch, E.; Kargal, F.; Weber, M.; Leinmuller, T. Communication patterns in VANETs. *IEEE Commun. Mag.* **2008**, *46*, 119–125. [CrossRef]
5. Zeadally, S.; Javed, M.A.; Hamida, E.B. Vehicular communications for ITS: Standardization and challenges. *IEEE Commun. Stand. Mag.* **2020**, *4*, 11–17. [CrossRef]
6. Abassi, R. VANET security and forensics: challenges and opportunities. *Wiley Interdiscip. Rev. Forensic Sci.* **2019**, *1*, e1324. [CrossRef]
7. Kim, T.W.; Jung, J.I.; Lee, J.Y. A congestion control scheme estimating global channel busy ratio in VANETs. *J. IKEEE* **2017**, *21*, 115–122.
8. Eyobu, O.S.; Joo, J.; Han, D.S. A broadcast scheme for vehicle-to-pedestrian safety message dissemination. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717741834. [CrossRef]
9. Saini, I.; Saad, S.; Jaekel, A. Evaluating the effectiveness of pseudonym changing strategies for location privacy in vehicular ad-hoc network. *Secur. Priv.* **2019**, e68. [CrossRef]
10. Liao, J.; Li, J. Effectively changing pseudonyms for privacy protection in VANETs. In Proceedings of the 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, Kaohsiung, Taiwan, 14–16 December 2009; pp. 648–652.
11. Pan, Y.; Li, J.; Feng, L.; Xu, B. An analytical model for random changing pseudonyms scheme in VANETs. In Proceedings of the 2011 International Conference on Network Computing and Information Security, Guilin, China, 14–15 May 2011; pp. 141–145.
12. Bouksani, W.; Bensaber, B.A. An efficient and dynamic pseudonyms change system for privacy in VANET. In Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017; pp. 59–63.
13. Alazzawi, M.A.; Lu, H.; Yassin, A.A.; Chen, K. Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network. *IEEE Access* **2019**, *7*, 71424–71435. [CrossRef]
14. Chaudhary, B.; Singh, K. A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. *Peer-to-Peer Netw. Appl.* **2021**, 1–15. [CrossRef]
15. Liu, X.; Fang, Z.; Shi, L. Securing Vehicular ad Hoc Networks. In Proceedings of the 2007 2nd International Conference on Pervasive Computing and Applications, Birmingham, UK, 26–27 July 2007.
16. Crişan, G.C.; Nechita, E. On a cooperative truck-and-drone delivery system. *Procedia Comput. Sci.* **2019**, *159*, 38–47. [CrossRef]
17. Baniasadi, P.; Foumani, M.; Smith-Miles, K.; Ejov, V. A transformation technique for the clustered generalized traveling salesman problem with applications to logistics. *Eur. J. Oper. Res.* **2020**, *285*, 444–457. [CrossRef]
18. Raya, M.; Hubaux, J.-P. The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '05), Alexandria, VA, USA, 7 November 2005.
19. Malik, N.; Nanda, P.; Arora, A.; He, X.; Puthal, D. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 674–679.
20. Suciu, G.; Nădrag, C.; Istrate, C.; Vulpe, A.; Ditu, M.C.; Subea, O. Comparative analysis of distributed ledger technologies. In Proceedings of the Global Wireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; pp. 370–373.
21. Leiding, B.; Memarmoshrefi, P.; Hogrefe, D. Self-managed and Blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Heidelberg, Germany, 16 September 2016.
22. Rosic, A. What Is Ethereum? [The Most Updated Step-by-Step-Guide!]. Blockgeeks. 2016. Available online: https://blockgeeks.com/guides/ethereum/ (accessed on 6 December 2019).
23. Frankenfield, J. Consensus Mechanism (Cryptocurrency), Investopedia, 25 June 2019. Available online: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp (accessed on 6 December 2019).
24. bai, C.; Xiao, X.; Ding, Y.; Xiao, L.; Tang, Y.; Zhou, S. Learning based security for VANET with blockchain. In Proceedings of the 2018 IEEE International Conference on Communication Systems (ICCS), Chengdu, China, 19–21 December 2018.
25. Lasla, N.; Younis, M.; Znaidi, W.; Arbia, D.B. Efficient distributed admission and revocation using blockchain for cooperative ITS. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018.
26. Lu, Z.; Wang, Q.; Qu, G.; Liu, Z. BARS: A Blockchain-based anonymous reputation system for trust management in VANETs. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018.

27. Proof of Authority: Consensus Model with Identity at Stake, POA Network. 11 November 2017. Available online: https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256 (accessed on 6 December 2019).
28. Wang, C.; Shen, J.; Lai, J.F.; Liu, J. B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs. *IEEE Trans. Emerg. Top. Comput.* **2020**. [CrossRef]
29. Khalid, A.; Iftikhar, M.S.; Almogren, A.; Khalid, R.; Afzal, M.K.; Javaid, N. A blockchain based incentive provisioning scheme for traffic event validation and information storage in VANETs. *Inf. Process. Manag.* **2021**, *58*, 102464. [CrossRef]
30. Nyaletey, E.; Parizi, R.M.; Zhang, Q.; Choo, K.K.R. BlockIPFS—Blockchain-enabled interplanetary file system for forensic and trusted data traceability. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 18–25.
31. Boualouache, A.; Sedjelmaci, H.; Engel, T. Consortium blockchain for cooperative location privacy preservation in 5G-enabled vehicular fog computing. *IEEE Trans. Veh. Technol.* **2021**. [CrossRef]
32. Hassija, V.; Chamola, V.; Gupta, V.; Chalapathi, G.S. A framework for secure vehicular network using advanced blockchain. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 1260–1265.
33. Ma, Z.; Zhang, J.; Guo, Y.; Liu, Y.; Liu, X.; He, W. An efficient decentralized key management mechanism for VANET with blockchain. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5836–5849. [CrossRef]
34. George, S.A.; Jaekel, A.; Saini, I. Secure identity management framework for vehicular ad-hoc network using blockchain. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; pp. 1–6.
35. Liang, W.; Li, Z.; Zhang, H.; Wang, S.; Bie, R. Vehicular ad hoc networks: Architectures, research issues, methodologies, challenges, and trends. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 745303. [CrossRef]
36. Tahir, M.N.; Katz, M. Heterogeneous (ITS-G5 and 5G) vehicular pilot road weather service platform in a realistic operational environment. *Sensors* **2021**, *21*, 1676. [CrossRef] [PubMed]
37. What Is a Vehicle Identification, AutoCheck. Available online: https://www.autocheck.com/vehiclehistory/vin-basics (accessed on 6 December 2019).
38. Gaurav, K. Consensus in Hyperledger Fabric. Available online: https://jktech.com/insight/blogs/consensus-in-hyperledger-fabric/ (accessed on 6 December 2019).
39. Introduction—Hyperledger Fabric. 2019. Available online: https://hyperledger-fabric.readthedocs.io/en/release-1.4/blockchain.html (accessed on 10 August 2019).
40. Miao, L.; Djouani, K.; Wyk, B.J.V.; Hamam, Y. Performance evaluation of IEEE 802.11p MAC protocol in VANETs safety applications. In Proceedings of the 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 7–10 April 2013; pp. 1663–1668.
41. Zeadally, S.; Hunt, R.; Chen, Y. Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241. [CrossRef]
42. Brecht, B.; Therriault, D.; Weimerskirch, A.; Whyte, W.; Kumar, V.; Hehn, T.; Goudy, R. A security credential management system for V2X communications. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3850–3871. [CrossRef]
43. Simulation of Urban mObility, SUMO. 10 December 2019. Available online: https://sumo.dlr.de/docs/index.html (accessed on 26 December 2019).
44. OMNET++, OMNET++. 9 November 2019. Available online: https://omnetpp.org/ (accessed on 26 December 2019).
45. Vehicles in Network Simulation, Veins. 12 December 2019. Available online: https://veins.car2x.org/ (accessed on 26 December 2019).
46. Salous, S. *Radio Propagation Measurement and Channel Modelling*; John Wiley & Sons.: Hoboken, NJ, USA, 2013.
47. Hyperledger Composer, Hyperledger Composer. 29 August 2019. Available online: https://hyperledger.github.io/composer/latest/ (accessed on 26 December 2019).