A Model to Evaluate Reliability of Authentication Protocols in C-ITS Safety-Critical Applications

Mir Ali Rezazadeh Baee , *Senior Member, IEEE*
Leonie Simpson , Xavier Boyen, Ernest Foo , *Member, IEEE*, and Josef Pieprzyk

***Abstract*—In the near future, Vehicle-to-Vehicle (V2V) transmission will enable wireless broadcast communication among nearby vehicles. Benefits for users include improved driver safety and potentially optimized traffic. However, this communication is vulnerable to cyber attacks involving message manipulation. Research aimed at tackling this problem has resulted in the proposal of multiple authentication protocols. The security, privacy, and other desirable features of authentication in vehicular networks have been widely studied. However, the efficiency of such authentication schemes has not been suitably addressed. There is no model to evaluate the efficiency of the proposals in a practical context, where the delay introduced by V2V authentication may impact on driver safety. In this paper, we provide such a model for evaluation. We explicitly present the key factors involved to evaluate the computational delay in the V2V authentication protocols. Our model has clearly defined metrics for computing the delay and evaluating the impact. Developing this model enables future research in the design of secure and efficient V2V authentication protocols suitable for practical application. Applying the model to assess proposed authentication protocols permits categorization based on safety service they can support. We demonstrate the applicability of our model through case studies. Our model can effectively analyze the delay introduced by an authentication protocol, and determine whether this would result in a crash, in the real world vehicular environments.**

***Index Terms*—Cryptography, vehicular communication systems, authentication delay, IEEE 802.11p simulation, efficient authentication.**

I. Introduction

EMERGING TECHNOLOGIES employed in future vehicles have enhanced sensing capabilities, and carry computing and communication platforms to enable Cooperative Intelligent Transportation Systems (C-ITS). The C-ITS permits integration of the operations of multiple vehicles. This has the potential to improve vehicular safety through periodic safety message broadcasting, letting vehicles know about environmental conditions and the status of neighboring vehicles [1].

The Institute of Electrical and Electronics Engineers (IEEE) in United States, the European Telecommunications Standards Institute (ETSI) in Europe, and Association of Radio Industries and Businesses (ARIB) in Japan are well-known standards specifying different aspects of the C-ITS communications such as Physical (PHY) and Medium Access Control (MAC) layers, data structures, and security. The IEEE 1609.4 standard defined the first version of the Wireless Access in Vehicular Environment (WAVE) protocol stack, using IEEE 802.11p [2] to support vehicular communications. The WAVE protocol [3] reserves the frequency range 5.850 to 5.925 GigaHertz (GHz) to use in United States (US) Dedicated Short Range Communications (DSRC) spectrum band. This is known as Intelligent Transportation Systems Radio Service (ITS-RS). Similarly, IEEE 802.11p as an access layer is used in the European ETSI ITS-G5 family of standards [4], dedicated to safety and safety-related applications in the frequency range 5.875 GHz to 5.905 GHz. The ETSI ITS-G5 uses a model including state machines and different tunable parameters to control MAC layer operations. In parallel to the American and European C-ITS standards, the Japanese ARIB STD-T109 [5] employs a specific MAC to ensure that all the vehicles have enough time to send safety messages without collisions or delay in the communication channel. This standard also specifies a PHY similar to IEEE 802.11p, but operating on a center frequency of 760 MegaHertz (MHz).

WAVE enabled vehicles can communicate with other nearby vehicles and Road Side Units (RSUs) by establishing a self-organizing network called a Vehicular Ad-hoc Network (VANET). Different communication technologies are used in VANETs, including Vehicle-to-Vehicle (V2V) and Vehicle-to/from-Infrastructure (V2I/I2V) communications. V2V is wireless communication among nearby vehicles. V2I is wireless communications between vehicles and RSUs. Vehicles and RSUs within transmission range exchange beacon messages (high update rate broadcast messages) about critical information, such as location, speed, braking status, traffic conditions, and traffic events [6].

The RSU is an access point, used along with vehicles, to allow information dissemination for the road user community. The RSUs are located along critical sections of roads, such as at traffic light intersections, or at stop signs. The RSUs

Manuscript received January 23, 2021; revised April 16, 2021 and June 14, 2021; accepted July 11, 2021. Date of publication X X, X; date of current version X X, X. The work of Mir Ali Rezazadeh Baee was supported by the Queensland University of Technology Postgraduate Research Award. The work of Josef Pieprzyk was supported in part by the Australian Research Council under Grant DP180102199 and in part by the Polish National Science Center (Narodowe Centrum Nauki) under Grant 2018/31/B/ST6/03003. The review of this article was coordinated by Dr. Yuanxiong Guo. *(Corresponding author: Mir Ali Rezazadeh Baee.)*

Mir Ali Rezazadeh Baee, Leonie Simpson, and Xavier Boyen are with the School of Computer Science, Queensland University of Technology, QLD 4000, Australia (e-mail: info@baee.co; lr.simpson@qut.edu.au; xavier.boyen@qut.edu.au).

Ernest Foo is with the School of Information and Communication Technology, Griffith University, QLD 4111, Australia, and also with the School of Computer Science, Queensland University of Technology, QLD 4000, Australia (e-mail: e.foo@griffith.edu.au).

Josef Pieprzyk is with the Commonwealth Scientific and Industrial Research Organization, Data61, NSW 2122, Australia, also with the Institute of Computer Science, Polish Academy of Sciences, 01-248 Warsaw, Poland, and also with the School of Computer Science, Queensland University of Technology, QLD 4000, Australia (e-mail: josef.pieprzyk@csiro.au).

are connected to the Backbone Network (BN) via high-speed network connections and have data storing, computing, and routing capabilities to support the V2I/I2V communications and increase the V2V communication connectivity [7]. The distributed RSUs are equipped with a higher computational capability and transmission power than vehicle OBUs. The BN and RSUs can be connected to each other through wired connections or the Internet. The RSUs work as gateways to deliver data from the BN to roadside vehicles, and vice versa. The range of I2V communication can be larger than that of the V2V and V2I communications to improve the network availability and performance [3]. This VANET architecture and communication model is illustrated in Figure 1.

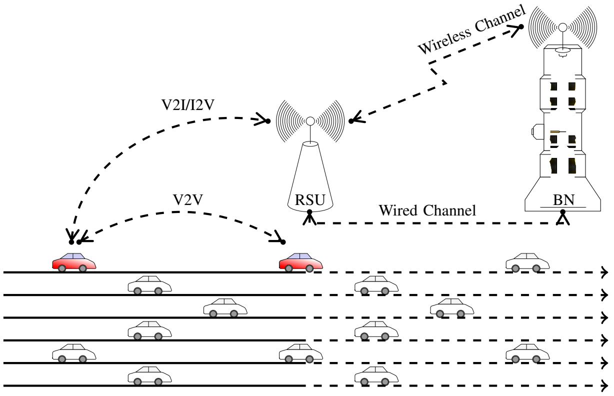


Fig. 1. Vehicular network model.

Smart vehicles equipped with On-Board Units (OBUs), sensors, and Global Positioning System (GPS) move along the roads and communicate with other vehicles and RSUs according to a defined Intelligent Transportation Systems Radio Service (ITS-RS) standard, such as the Dedicated Short Range Communications (DSRC) protocol [3]. A Tamper Proof Device (TPD) can be embedded in each OBU to store the user inaccessible cryptographic keying materials involved in cryptographic operations. Figure 2 illustrates an envisioned smart vehicle prototype.

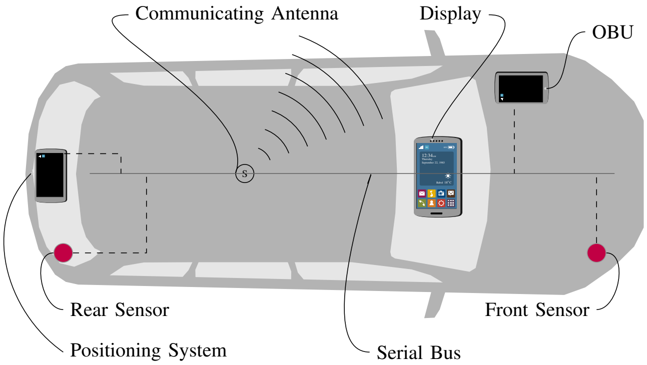


Fig. 2. Envisioned smart vehicle prototype.

A. C-ITS Safety Applications

Applications for C-ITS can be classified based on the safety objectives with classes including safety-critical, safety-related, and non-safety applications. Each of these three classes is described as follows.

Safety-critical applications (also known as latency critical) are the most important applications for hazardous situations, where the danger is high or imminent (e.g., intersection collision warning). Vehicles periodically (automatically at regular intervals) broadcast messages about events in their vicinity, such as collisions, road conditions, and emergency braking. The receiver vehicle can collect relevant information and inform the human driver about relevant events, depending on the context and situation. For this case, the communication requires high reliability and low latency to realize the safety function. The communication technology used in these applications can be V2V, V2I, and I2V. The latency required for most safety-critical applications is 100 ms or minimum update rate of 10 Hertz (Hz) in a communication range of 150 to 500 m [6]. The system utility requires vehicles to receive updated information from surrounding vehicles within the required time frame before sending out a new safety message. These will be regarded as high-priority messages.

Safety-related applications are event-driven (the transmission is triggered by an event) and are used in cases where the latency requirements are not as stringent as for safety-critical applications, and the danger is low, but still foreseeable (e.g., post-crash warning). The communication technology used in these applications can be V2V, V2I, and I2V. The latency required for most safety-related applications is between 500 and 1000 ms (update rate of 1 Hz) in a communication range of 250 to 1000 m [6]. The mechanisms to generate safety-related messages are quite different than the other two classes. First, a vehicle's sensor detects an event, and local sensor information is aggregated. Then, in the case of a dangerous event, a message will be generated and broadcast by the vehicle. Also, a single car may not able to detect events such as traffic jam, which needs multiple cars location information to conclude that it is in or before a traffic jam. This example makes it easy to understand that matching the information received from different vehicles is critical for reliability.

Non-safety applications provide periodic or event-driven traffic information and enhance driving comfort. Examples include traffic updates, electronic toll collection, and infotainment (the Internet, media, and entertainment). The latency required for most non-safety applications is 1000 ms (update rate of 1 Hz) in a communication range of 100 to 400 m [6]. The communication technology used in these applications can be V2V, V2I, and I2V. These services access the channels in the communication system in a low priority mode, compared to safety-critical and safety-related applications [6].

B. Research Challenge

Safety messages are broadcast to reach all vehicles within communication range. This system is useful if all messages are legitimate. However, malicious entities could manipulate messages. Without the use of security mechanisms, activities such as the injection of false messages can be performed without detection [8], [9]. For this reason, mechanisms should be applied to ensure both identification of the data source (entity authentication) and authentication of the message (assurance of data origin and data integrity).

From a practical perspective, different cars may have different processing capacities to support C-ITS applications. For economic reasons, car manufacturers embed small-scale and low-cost hardware for vehicular communications. This constrains the mechanisms applicable to secure modern vehicles against cyber attacks. The limited in-car computational capabilities make complex cryptographic techniques economically unattractive [10][11]. For example, NXP Semiconductors currently offer the RoadLINK SAF5400 [12], with the capacity to process up to 200 authentication requests every 100 ms. Any possible solution for authentication performed by vehicles must have low computational overhead to suit their limited computing resources.

Using V2V technology for safety purposes requires the communication channel to be accessible for latency-critical applications, such as collision avoidance, with the highest priority and reliability. Latency defines the time frame from when information is generated for transmission and when it is received. For system efficiency, vehicles need to receive updated information from surrounding vehicles within the required time frame before sending out a new safety message.

Multiple authentication protocols have been proposed to secure V2V communication. Clearly, any proposal for V2V authentication for the VANET safety applications must be able to process the verification of a large number of broadcast messages received in a short time period before their dedicated deadline, while simultaneously processing other vehicular applications. However, the verification results in a delay in driver notification and may allow insufficient driver reaction time, resulting in potential collisions and serious injuries (assuming the driver does not react independently).

There are many scenarios where a driver is relying completely on the safety messages to react on time. Examples include situations involving aggressive drivers, distracted/inattentive drivers, poor driver decisions, impaired/drowsy drivers, and rough/slick road conditions [6]. In such scenarios, the verification time must be less than driver reaction time. Otherwise the safety goal that the vehicular communications are designed to achieve cannot be obtained with secure communications in place.

The communications overhead, security and privacy aspects of authentication protocols in V2V communication are widely studied in the public literature. However, a model is needed that enables the evaluation of the efficiency of proposed secure communications for practical applications in the real world. Further, a testbed to evaluate the computational overhead of authentication protocols and the practical impact of the real-time delay on messaging within a large-scale network is missing. The available simulation software for vehicular movement, such as Veins *Vehicles in Network Simulation* [13] (an open source vehicular network simulation framework) and SUMO *Simulation of Urban Mobility* [14] do not utilize models for simulating car accidents caused by authentication delay. As a result, the practical applicability of many authentication protocols found in the literature is uncertain for VANET safety purposes.

C. Our Contribution

This work specifically addresses the development of a model to analyze the delay produced by an authentication protocol, determine the impact of the delay and possibility of a crash occurring in real-world scenarios, and categorize authentication protocols into suitable safety categories. The main contributions are summarized as follows:

1. The key factors involved in the computational delay of V2V authentication protocols are identified, through an extensive review of public literature. These factors include the cryptographic method, the credential type, and the privacy principle.
2. The number of beacons successfully received in the required interval for safety-critical applications is evaluated through computer simulations. The beacons are generated in accordance with different C-ITS standards, including: DOT HS 809 859 [6] and DOT HS 811 492D [15] specifications for American IEEE 1609 standard, and ETSI TR 102 861 [16] and ETSI EN 302 637-2 [17] specifications for European ETSI ITS-G5 standard, as well as Japanese ARIB STD-T109 ITS.
3. A static model is presented with clearly defined metrics to evaluate the impact of the delay associated with the use of authentication mechanisms. The model presents three scenarios: a best-case, an average-case, and a worst-case scenario. Applying the model allows the protocols to be grouped into suitable safety categories: safety-critical or non-safety-critical. The model determines whether a crash will occur based on vehicle displacements during the time taken to perform authentication.
4. The model is applied for case studies, evaluating five proposed authentication schemes in the literature to show how and to what extent an authentication protocol is “Not Appropriate”, “Risky”, or “Appropriate” to use in safety-critical applications.

D. Organization of the Paper

The remainder of this paper is organized as follows. Section II provides an overview of the authentication requirements between network entities. Section III outlines related work. Section IV identifies the key factors involved in the computational delay introduced through applying V2V authentication protocols. Section V defines our evaluation model and the related metrics to determine the impact of the delay. Section VI illustrates the use of our model through case studies. Section VII discusses the results and concludes the paper. For the convenience of the reader, a list of abbreviations used throughout the paper is given in Table I.

II. Authentication Between Network Entities

Authentication is a vital part of trust establishment between network entities [18]. It ensures that received messages come from the legitimate entities. Without this security service, messages transmitted by network entities can be altered by an adversary, or a bogus message can be generated by an impersonator. Also, a sender can later deny the message generation.

TABLE I
LIST OF ABBREVIATIONS

Abbreviation	Meaning
ABS	Anti-lock Braking System
ACT	Average Computation Time
ARIB	Association of Radio Industries and Businesses
BN	Backbone Network
C-ITS	Cooperative Intelligent Transportation System
CRL	Certificate Revocation List
DSRC	Dedicated Short Range Communications
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECQV	Elliptic Curve Qu-Vanstone
ETSI	European Telecommunications Standards Institute
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
ITS-RS	Intelligent Transportation Systems Radio Service
MAC	Medium Access Control layer
MACs	Message Authentication Codes
MSR	Model-Specific Register
OBU	On-Board Unit
PHY	Physical layer
RDTSC	Read Time Stamp Counter
RSU	Road-Side Unit
TSC	Time Stamp Counter
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VANET	Vehicular Ad-hoc Network
WAVE	Wireless Access in Vehicular Environment

We define the capabilities of an adversary as possession of impressive communication abilities through powerful receivers, control of the communication channel, monitoring on-the-fly data exchange, and delaying their transmission, as well as tampering with messages and replacing the original messages with modified versions. The adversary may intend to maximize its gains by cheating neighboring vehicles to make a clear path for traveling, or compromising legitimate users identities for impersonation, in order to avoid responsibility for injurious behaviors. Furthermore, a malicious adversary may deliberately generate large amounts of both legitimate and invalid messages in a relatively short period of time to disrupt the VANET safety applications, creating disorder. The most commonly encountered attacks concerning authentication are outlined by Raya and Hubaux [19]. Examples include the GPS spoofing attacks, replay attacks, free-riding attacks, impersonation attacks, and message tampering attacks.

In VANETs, authentication is performed at two levels: the message level and the entity level. Message authentication provides assurance of data origin, and also data integrity. Data origin authentication is where a communicating node can be verified as the original source of data created at some time in the past. Data integrity is a property in which data has not been altered in an unauthorized manner. This property must be maintained from the time the data was created, transmitted, or stored by an authorized source. Note that for any received message, it is essential to ensure both that data actually came from the claimed source (data origin authentication) and is unaltered (data integrity).

Both of these requirements must be met for communicating nodes to trust the system. If data is altered, the new message effectively has a new source; and if the source is not determined, then an investigation into alteration cannot be settled conclusively (data cannot be linked to a source). Thus, integrity mechanisms implicitly provide some assurance of data origin authentication, and vice versa [20].

Entity authentication or identification is a technique designed to assure one communicating node (the verifier) that the identity of another (the prover or claimant) is as claimed, and, as a result, prevents impersonation [21]. From the verifier's point of view, the result of an identification protocol is either acceptance of the prover's identity as authentic, or rejection (leading to termination of the connection without acceptance) [20].

III. Related Work

Multiple authentication protocols have been proposed to address security and privacy issues in V2V communication. Existing papers [22–26] have attempted to evaluate and compare the performance of different authentication protocols based on a limited set of metrics. The existence of a realistic model to evaluate the overhead of these protocols when applied in practical situations with regard to quantitative comparison is a missing component.

Riley et al. [22] provide a comparison of the advantages and disadvantages of several proposed authentication schemes, and identify their suitability under various conditions. They conclude that the quantitative performance comparison among different schemes is challenging for several reasons, including difference in the considered applications within the proposed network (i.e., safety application, platooning, sensing).

Qu et al. [23] provide a detailed survey of several VANET authentication schemes followed by evaluations and discussions. The authors emphasize that more performance evaluation of these schemes should be conducted on a large-scale vehicular network.

Petit et al. [24] compare different proposed authentication schemes, and identify open research challenges for future research, such as reduction of computation overhead.

Similarly, Manvi et al. [25] and Lu et al. [26] classify VANET authentication strategies, and advise researchers to design and develop efficient authentication schemes.

The evaluations performed in the above-reviewed papers fail to make a connection between the qualitative results and the potential consequences, such as the impact of authentication processing delay on driver safety in high-density VANET scenarios. There are very few academic publications evaluating the impact of authentication delay.

Petit and Mammeri [27] investigate the impact of authentication processing on vehicle braking distance in a highway scenario. However, they did not extend the investigation to include potential accident scenarios. In addition, the authors did not investigate the number of beacons received by a vehicle in a realistic high-density scenario before applying authentication. Their investigation is only based on 49 vehicles in a highway with 6 lanes. This may be a practical scenario in some contexts, but it is not an extreme scenario.

Baee et al. [28] provide a detailed performance evaluation of the authentication algorithms described in IEEE 1609.2

security standard [29]. However, the evaluation is based on a single scenario which is not enough for grouping the protocols into appropriate safety categories.

The lack of a realistic testbed to evaluate the real computational overhead of authentication protocols on a large-scale network may lead protocol designers to misunderstand the resulting impact when evaluating the applicability and effectiveness of their proposals, comparing performance with existing protocols inappropriately. Although a newly proposed protocol may be more efficient than an existing protocol, this does not mean either protocol meets the requirements for practical application. Benchmarks should not be based on other protocols but on the contexts of the application environment. As a result, many of the protocols found in the literature are not applicable and effective in their proposed network environment. We fill this gap in this research by extending the work presented by Baee et al. [28].

IV. Revisiting Computational Delay in Authentication

Three key factors are involved in the delay covered by authentication overhead of protocols, including: the cryptographic method, the credential type, and the privacy principle (see Figure 3). These are derived from observations of protocols reviewed in the literature. The identified key factors help define related metrics for our model, and enable the evaluation of the impact of computational delay.

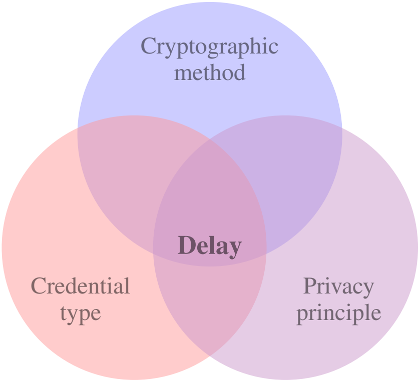


Fig. 3. The key factors affecting computational delay in authentication.

A. Cryptographic Method

Cryptography is the application of advanced mathematical principles to enable the storage and transmission of data in a secure way [20]. A cryptographic algorithm uses a string of bits called a cryptographic key to transform a plain text into a cipher text (encryption) or vice versa (decryption). This cryptographic key must remain private to ensure a secure communication. The length of a key is normally expressed in bits. A longer key makes exhaustive key search more difficult to perform (makes an encrypted data more difficult to crack). However, it may also result in longer time periods to perform encryption and decryption processes. Cryptographic keys can be used for different purposes, such as data encryption, decryption, identification, and message authentication.

A cryptographic method is used within an authentication scheme, with respect to credential type and privacy principle requirements. A computationally heavy cryptographic technique may exceed the latency requirements that the protocol is designed for. There are two major categories for cryptographic method, symmetric and asymmetric.

1) Symmetric Methods: Symmetric methods make use of a secret key such as a string of random letters to change the content of a message in a particular way. Both sender and recipient can encrypt and decrypt all messages using the same secret key. It is highly efficient in terms of computational overhead, and offers the benefits of short encryption and decryption time [20]. Authentication protocols under this category can be further classified into two groups: Hash-based and Message Authentication Code-based (MAC-based).

a) The Hash-based Group: The protocols in this group perform authentication using cryptographic hash functions. A hash function is a one-way function (infeasible to invert) that is used for data integrity assurance. It takes a message as input and produces an output referred to as a hash value. A cryptographic hash implies an unkeyed hash function. The study presented by Han et al. [30] proposes a three-step authentication protocol using cryptographic hash value to provide data integrity assurance between the intra-vehicle network and an external network (mobile device).

b) The MAC-based Group: The protocols in this group perform authentication using a distinct class of cryptographic primitives called Message Authentication Codes (MACs). The output of a MAC algorithm is referred to as a MAC, and is a short piece of information used to confirm that a message comes from the stated sender (its authenticity), and has not been changed [20]. Note that any communicating node with knowledge of shared secret key can be an originator of data. Hence, it does not offer non-repudiation (a sender can later deny the message generation).

Different symmetric cryptographic primitives such as cryptographic hash functions, or block cipher algorithms can be used to construct MAC algorithms. An HMAC implies a keyed-hash function that takes two functionally distinct inputs, a message and a secret key, and produces a fixed-size output. In practice, it should be infeasible to produce the same output without knowledge of the key [20].

HMACs can be constructed from dedicated cryptographic hash functions, such as SHA-256 or SHA3-256 secure hash algorithms. In VANETs, HMACs can provide both data integrity assurance and symmetric data origin authentication, as well as identification in symmetric-key schemes.

Hash-based authentication is highly efficient in terms of computational and communication overhead. It offers the benefits of short generation and verification time as well as less communication overhead. The security of HMACs depends on the cryptographic strength of the underlying hash function, and the size and quality of the key used [20]. The authentication protocol proposed by Choi et al. [31] enables vehicles and RSUs to generate/verify MACs in V2I/I2V communications, resulting in less reliance on availability of bandwidth, and high degree of efficiency.

2) Asymmetric Method: Asymmetric methods make use of two mathematically related keys (a key pair), referred as a public key, and a private key. Any sender node can encrypt a message using the receiver's public key (confidentiality is not required for this public key). The corresponding private key must be kept secret, only known by the receiver. Any message encrypted using a public key can only be decrypted by applying the same algorithm and the matching private key. This method can be used to provide confidentiality, and thus securely distribute symmetric secret keys over vehicular networks. Asymmetric methods can also be used to form digital signatures, enabling authentication of both message and sender [20]. Asymmetric cryptographic primitives require far more processing power for both encryption and decryption, and as a result, they are much slower than symmetric techniques.

Authentication using digital signatures involves generating an output from the content of a message using an algorithm and a private key that is known only to the signer. The signature must be verifiable using the corresponding public key [20]. In VANETs, digital signatures are used to ensure authentication, data integrity, non-repudiation, and for certification of public keys. In this regard, many studies propose authentication mechanisms using digital signature schemes, such as Elliptic Curve Digital Signature Algorithm (ECDSA) [32] which is a digital signature algorithm based on Elliptic Curve Cryptography (ECC). For the interested reader, additional information related to the application of ECDSA and signature schemes in VANETs is presented by Baee et al. [28], [33].

Gollan and Meinel [34] propose the use of digital signatures for authentication in vehicular environments. For vehicular communications, each message broadcast/sent is signed. Recipients must verify the signatures before accepting the messages. Recipients must verify the signatures before accepting the messages. Raya and Hubaux [35] show that in terms of speed and compactness, ECDSA is fit for message authentication in V2V communications.

There are other types of signature schemes used for authentication in VANETs. The group signature scheme applied by Calandriello et al. [36], ring signature scheme applied by Xiong et al. [37], and blind signature scheme applied by Fischer et al. [38] are other examples of signature-based protocols.

B. Credential Type

A credential can take the form of a key (for example, a public key) that is known to be unique to a network communicating node, and used for establishing its identity when communicating with other nodes. Any node holding a credential is usually given secret knowledge (e.g., a private or secret key) as proof of owning that credential. A node wanting to communicate to the other nodes in the network is referred to as a *supplicant*. A node that receives and responds to the authentication requests is referred to as an *authenticator*. The supplicant can assure the authenticator about its identity (credential) by demonstrating that it possesses a cryptographic private/secret key corresponding to that credential.

In VANETs, credentials contain identifiers of vehicles. If these are captured, vehicle tracking may be possible, and as a result, compromising the privacy of drivers. Strategies have to be defined for generation, issuance, distribution, and revocation of credentials. Communicating parties can exchange their credentials for the purpose of identification. The credentials can be transferred either using certificates or without certificates. A digital certificate (also known as certificate) is an electronic document that is used to bind a credential to an entity. Authentication protocols under this category can be further classified into two groups: certificate-based, and certificate-less.

1) Certificate-based Group: The protocols in this group convey credentials using certificates. A certificate consists of information to identify an entity. Each entity's credential is embedded in a certificate which is either explicitly (signed by a trusted authority or self-signed) or implicitly (without attaching signature) certified. Any party can use a copy of the certificate to extract the provided credential and use it to uniquely identify the holder [20]. To provide a more accurate discrimination, certificate-based credentials can be further classified into two subgroups: explicit and implicit.

a) Explicit Certificate: The explicit certificate is a data structure used to store, distribute, or forward credentials (e.g., public keys) over unsecured networks without fear of undetectable manipulation. It is composed of two different parts: a data part and a signature part. The data part contains a credential and a unique string identifying the associated entity. The signature part of the certificate contains the signature of the certificate owner or a trusted authority. This binds the subject entity's unique identity to the specified credential. An intended recipient can verify this signature and be assured that the credential belongs to the subject entity. During an authorized system user registration, the authentic public key of the trusted authority is made available to all communicating nodes. This public key enables communicating nodes to verify the certificates signed by that trusted authority, and as a result, transfers trust. The scheme presented by Jung et al. [39] is an example where RSUs issue multiple explicit certificates to vehicles for authentication purposes.

b) Implicit Certificate: The implicit certificate is a variation of the digital certificates used with cryptography for which an explicit user's credential can be implicitly certified. The main difference here is that a credential must be reconstructed from public data, rather than transported within a certificate, as occurs with explicit certificates. The implicit certificate is still comprised of the three main elements/parts (identifier, public credential, and digital signature), but superimposed into the same space as the size of a public credential, resulting in reduced data transfer. The Elliptic Curve Qu-Vanstone (ECQV) implicit certificate is an example that falls into this subgroup. The IEEE 1609.2 security standard [29] recommends use of ECQV as a more efficient alternative to traditional certificates, as described in the document *Standards for Efficient Cryptography 4* [40]. For the interested reader, additional information related to the application of ECQV algorithm in VANETs is presented by Baee et al. [28], [41].

2) Certificate-less Group: The protocols in this group assume that credentials are not presented in certificates. Unlike the certificate-based group of protocols, these have no dependence on signed certificates. The application of identity-based cryptography and signature schemes [42–44] is common among protocols in this group. The study presented by Kamat et al. [45] is an example of schemes that fall into this group, where vehicles implicitly validate the identity-based signatures on the messages by verifying that the vehicle using the credential actually has the private key corresponding to it. This eliminates the need for certificate exchange between vehicles, resulting in reduced communication overhead.

C. Privacy Principle

Authentication protocols use different approaches to provide conditional privacy for vehicles/drivers in VANETs. For both identification and message authentication, protection of the driver's identity during authentication should be guaranteed. Identity privacy refers to the ability to prevent others from learning and linking a network node identifier to a driver/vehicle. When a unique identifier is provided to a vehicle and its embedded communicating nodes for authentication purpose, this information can be associated with an identifiable individual. In this case, the data becomes personal information. An adversary can capture the communications and link the identifiers to the vehicles, and consequently to the drivers (ID disclosure), providing a means for surveillance. Ideally, to mitigate the surveillance risk, it should be impossible for any observer to learn if a specific node has transmitted or will transmit a message.

In VANETs, each node relies on messages received from other nodes. To preserve a driver's privacy during authentication, a mechanism should be employed to keep messages anonymous to other nodes. Authentication protocols under this category can be further classified into two groups: pseudonym-based and group signature-based.

1) Pseudonym-based Group: The protocols in this group rely on pseudonymous credentials. A pseudonym or alias is an alternative identity that is verified by the node itself or a trusted party. This ensures that services can be used without disclosing the driver's identity, e.g., enabling a vehicle to avoid being tracked by periodically creating new pseudonym certificates [36]. To provide unlinkability, a pseudonym-change strategy using a set or different sets of pseudonyms is required. The credential holder can change pseudonyms over time or different contexts to break linkability [46].

2) Group Signature-based Group: The protocols in this group assume that the network nodes form a group, and utilize a group-oriented signature scheme (e.g., group signature [47] or ring signature [48]) to provide anonymous authentication, while eliminating the issuance of certificates. On behalf of a group, any member of the group can sign a message using its private key, and the signature can be verified with a group-wide public key. Group-oriented signature schemes provide non-traceability, unlinkability, and unforgeability. That is computationally infeasible for an adversary to learn whether two signatures on the message have been signed by the same group member, as only one public key is used for a group. The study presented by Studer et al. [49] is an example that uses a group signature scheme for anonymous authentication in vehicular communications.

V. The Proposed Evaluation Model

This section introduces our model and defines the related metrics to evaluate the impact of any delay resulting from the use of authentication mechanisms. The metrics are defined based on the key factors identified in the computational delay of authentication protocols, as discussed in Section IV. The model can be applied to determine whether a crash is likely to occur for a given scenario.

A. Evaluation Metrics

This section defines the metrics used in our evaluation model. These are the Number of Beacons, the Time Stamp Counter, the Average Computation Time, the Distance Traveled, and the Crash Time.

1) Number of Beacons (N_b): By means of simulations, we evaluate the number of beacons successfully received in the required interval for safety-critical applications. The beacons are generated in accordance with different C-ITS standards, including: DOT HS 809 859 [6] and DOT HS 811 492D [15] specifications for the American IEEE 1609, and ETSI TR 102 861 [16] and ETSI EN 302 637-2 [17] specifications for the European ETSI ITS-G5, and for the Japanese ARIB STD-T109 ITS.

To evaluate N_b, this study uses Veins *Vehicles in Network Simulation* [13] which is an open source vehicular network simulation framework. The Veins utilizes the models provided in the OMNeT++ discrete event simulator [50] and SUMO *Simulation of Urban Mobility* [14] for network simulation and vehicular movement, respectively. Veins is frequently used in academic research and contains a fully functioning implementation of IEEE 802.11p [51].

We focus on a use case scenario, representing the broadcasting of safety-critical messages between vehicles on a highway, similar to the scenario assumed by Raya and Hubaux [35]. The scenario considers a uniform presence of vehicles moving on a highway with the number of lanes $N_l = 12$ (6 in each direction), where each lane is 3 m wide (as shown in Figure 4). To enable comparisons with existing research, we adopt the vehicle speed used in the simulation study presented by Baee et al. [28]. It is assumed that vehicles travel at a fixed speed $u = 30$ m/s (108 Km/h) with an inter-vehicle space $Gap = 30$ m and the drivers rely on the received safety-critical messages to react on time. Moving vehicles generate, and transmit safety-critical messages every 100 ms over a 300 m communication range. For safety, vehicles are equipped with Anti-lock Braking System (ABS) with a maximum deceleration value $a = -9$ m/s^2 [52]. The scenario also considers an RSU. Calculations are performed for communication between the two vehicles, v_A and v_B, located in the middle of the highway. The vehicles correspond with a maximum of N_b received beacons from $N_v = 240$ other vehicles within their communication range.

TABLE II
SIMULATION PARAMETERS

	Standards		
Parameter	**American IEEE 1609**	**European ETSI ITS-G5**	**Japanese ARIB STD-T109**
Medium access control	IEEE 802.11p	IEEE 802.11p	ARIB-T109
Physical layer	IEEE 802.11p	IEEE 802.11p	IEEE 802.11p
Frequency	5.89 GigaHertz	5.90 GigaHertz	760 MegaHertz
Bitrate (megabits/seconds)	6	6	6
Max Transmission power (milliwatts)	20	126	10
Clear channel assessment threshold (decibel-milliwatts)	-65	-65	-53
Sensitivity (decibel-milliwatts)	-89	-85	-89
Thermal noise (decibel-milliwatts)	-110	-110	-110
Beacon size (bytes)	100	300	100
Update rate (hertz)	10	10	10
	Scenario		
Parameter	**Symbol**		**Value**
Number of vehicles	N_v		240
Number of lanes	N_l		12
Vehicles speed (meters/seconds)	u		30
Deceleration (meters/seconds squared)	a		-9
Inter-vehicle space (meters)	Gap		30
Simulation time (seconds)	t_{sim}		186

—Note: Bitrate is the number of bits that are conveyed or processed per unit of time. Transmission power is the amount of power input into the signal to the device. The clear channel assessment is a mechanism for determining whether the medium is idle or not. Sensitivity is the lowest power level at which a receiver can detect a radio signal. Thermal noise is generated by the random motion of free electrons in a conductor resulting from thermal agitation. All values are set in accordance with the corresponding C-ITS standard.

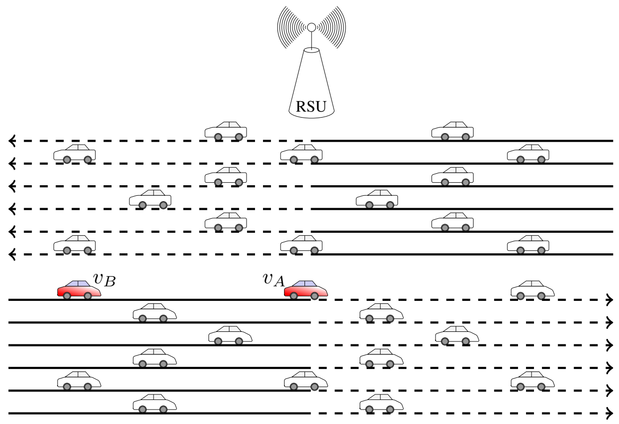


Fig. 4. Simulation scenario.

Depending on the C-ITS standard, each vehicle performs one of the following steps to generate and broadcast safety messages:

1) For IEEE 1609 standard, generate beacons in accordance with DOT HS 809 859 [6] and DOT HS 811 492D [15] specifications.
2) For ETSI ITS-G5 standard, generate cooperative awareness messages (European implementation of the beacons for ITS-G5) in accordance with ETSI TR 102 638 [53], ETSI TR 102 861 [16], and ETSI EN 302 637-2 [17] specifications, and transmit them on a dedicated channel in accordance with IEEE 802.11p MAC specification [54].
3) For ARIB STD-T109 standard, generate beacons in accordance with DOT HS 809 859 [6] and DOT HS 811 492D [15] specifications.

This scenario is implemented for each of the three C-ITS standards, including: American IEEE 1609, European ETSI ITS-G5, and Japanese ARIB STD-T109 using the detailed models published in [55][56]. Table II lists IEEE 1609, ETSI ITS-G5, and ARIB STD-T109 application layers and simulation parameters.

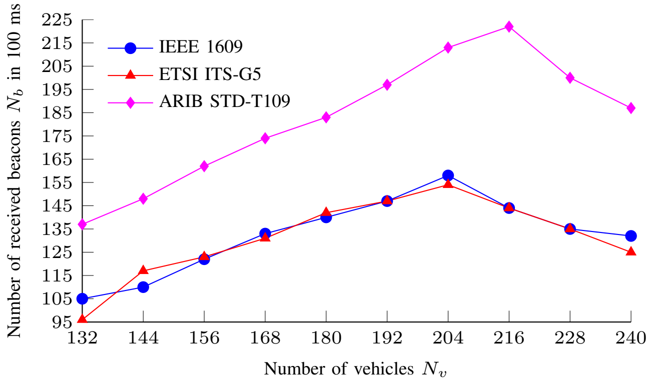


Fig. 5. Number of received beacons by vehicle v in the three different C-ITS standards.

The number of beacons N_b received in every 100 ms by a vehicle (e.g., v_A or v_B) is estimated (Figure 5). Note that v_A and v_B are moving in the middle of the highway. The performance comparison demonstrates that the maximum number of beacons received by the vehicle under the application of Japanese ARIB STD-T109 standard is 222 beacons per 100 ms, which is much greater than either the American IEEE 1609 or European ETSI ITS-G5 standards, with 158 and 154 beacons respectively. Processing a greater number of beacons has obvious benefits for safety applications. The U.S./European IEEE 802.11p suffers much more from shadow fading compared to the Japanese ARIB STD-T109 due to differences in the physical layer (5.9 GHz vs. 700 MHz band), as well as their very different MAC layer characteristics [56]. Therefore, this research considers the upper bound to be 222 beacons for further calculations.

2) Time Stamp Counter (TSC): The TSC is a hardware counter found in all contemporary x86 processors. The counter is implemented as a 64-bit Model-Specific Register (MSR) that is incremented at every clock cycle. The Read Time Stamp Counter (RDTSC) register has been present since the original Pentium. It is the most precise counter available on x86 architecture [57]. A processor requires a fixed number of clock ticks (or clock cycles) to execute each instruction. The faster the clock, the more instructions the processor can execute per second. Clock cycles are useful, because this study (or future studies) can more fairly compare the execution time across processors of different speeds by calculating how many cycles it takes to process each operation [58]. Using a given TSC (number of clock cycles) and Equation 1, the execution time of an operation can be calculated for different speed processors.

$$T_{Execution} = \left(\frac{number\ of\ clock\ cycles}{processor\ clock\ frequency}\right) \tag{1}$$

3) Average Computation Time (ACT): This metric is used to calculate average computation time in second/s (sec) for each operation (refer to Equation 2). We repeat the benchmarking 10000 times to have accurate results.

$$T^{AVG}_{Operation} = \left(\frac{Duration}{10000}\right) \tag{2}$$

4) Distance Traveled: When responding to a dangerous situation, drivers need an average mental reaction time or thinking time $T_{Thinking}$ in seconds, which is the duration between the occurrence of an event and starting to touch the brake pedal. According to experimental measurements studied by Hugemann [59], an average thinking time of a driver to be $T_{Thinking} = 0.63$ s. The average time between reacting the driver's muscle and receiving the first braking response is given to be $T_{Braking} = 0.2$ s. Added together, an average reaction time $T_{Reaction} = 0.83$ s is required before a braking process begins to happen. According to the constant power equations of motion [60], we have $v = u + at$, $x = ut + \frac{1}{2}at^2$, $x = vt - \frac{1}{2}at^2$, and $v^2 = u^2 + 2ax$, where u (m/s) is the initial velocity, v (m/s) is the final velocity, a (m/s^2) is the constant acceleration/deceleration, t (s) is the time of motion, and x (m) is the distance traveled. When the car stops, final velocity is $v = 0$, and so:

$$d_b = \frac{u^2}{2a}, \tag{3}$$

solving for d_r, we have:

$$d_r = u \times T_{Reaction} = u \times 0.83, \tag{4}$$

hence, the final stopping distance d_s is obtained such that $d_s = d_r + d_b$, where d_r is the distance traveled before receiving the first braking response, and d_b is the distance the car then travels before coming to rest.

Vehicles continue to move while processing received authentication requests, before sending a new message. During each verification operation a distance d_{Verify} with speed u will be passed. To calculate total distance traveled $T^{distance}_{Verify}$ during verification of N_b signature/s received from N_v vehicles in communication range, we have:

$$T^{distance}_{Verify} = u \times \sum_{i=1}^{N_b} T_{Verify(i)}. \tag{5}$$

The sum of all verification times for both vehicles results an extra delay, which will be added to the driver's reaction time and gives total delay as follows:

$$T^{total}_{Delay} = \sum_{i=1}^{N_b} \left(T_{Verify(Mi)}\right) + T_{Reaction}. \tag{6}$$

Solving for distance traveled $T^{distance}_{Delay}$, we have:

$$T^{distance}_{Delay} = u \times T^{total}_{Delay}. \tag{7}$$

5) Crash Time: Let t denote the time in seconds from when v_A brakes. Let $x_A(t)$ denote the position of the back of v_A and $x_B(t)$ denote the position of the front of v_B at time t. Figure 6 shows the situation at time $t = 0$. For vehicle speed $u = 30$ m/s (108 Km/h), inter-vehicle space $Gap = 30$ m, and deceleration value $a = 9$ m/s^2, we have:

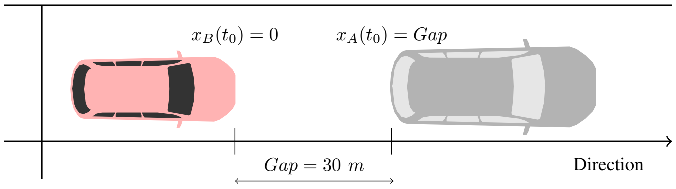


Fig. 6. Scenario at time $t = 0$.

$$u = \frac{1000}{3600} \times 108 = 30\ m/s.$$

The velocity and position of the back of v_A at time t is given by:

$$u_A(t) = 30 - 9t,\ x_A(t) = 30t - \frac{9}{2}t^2 + Gap,$$

and the velocity and position of the front of v_B at time t is given by:

$$u_B(t) = \begin{cases} 30, & \text{if } t \leq T^{total}_{Delay} \\ 30 - 9\left(t - T^{total}_{Delay}\right), & \text{if } t > T^{total}_{Delay}, \end{cases}$$

$$x_B(t) = \begin{cases} 30t, & \text{if } t \leq T^{total}_{Delay} \\ 30t - \frac{9}{2}\left(t - T^{total}_{Delay}\right)^2, & \text{if } t > T^{total}_{Delay}. \end{cases}$$

We solve the equation $x_A(t)$ and $x_B(t)$ to determine whether the beacon safety messages will be processed and acted on in time to prevent a crash, or whether a crash is unavoidable such that v_B runs into v_A at time t due to the verification overhead.

The position of the back of v_A and the position of the front of v_B at crash time t_{Crash} are equal $x_A(t_{Crash}) = x_B(t_{Crash})$, and can be calculated by:

$$30(t_{Crash}) - \frac{9}{2}\left(t_{Crash}\right)^2 + Gap = \\ 30(t_{Crash}) - \frac{9}{2}\left(t_{Crash} - T^{total}_{Delay}\right)^2,$$

where $t_{Crash} > T^{total}_{Delay}$, and

$$30(t_{Crash}) - \frac{9}{2}\left(t_{Crash}\right)^2 + Gap = 30(t_{Crash}),$$

where $t_{Crash} \le T^{total}_{Delay}$. Solving for t_{Crash}, we have:

$$t_{Crash} = \frac{Gap + \frac{9}{2}\left(T^{total}_{Delay}\right)^2}{9T^{total}_{Delay}}, \tag{8}$$

if $t_{Crash} > T^{total}_{Delay}$, and $u_A(t_{Crash}) \ge 0$. Then,

$$t_{Crash} = \sqrt[2]{\frac{Gap}{\frac{9}{2}}}, \tag{9}$$

if $t_{Crash} \le T^{total}_{Delay}$.

B. Scenarios

This section defines three scenarios, which we refer to as best-case, average-case, and worst-case. For each case, we apply the model to determine whether a crash will occur based on vehicle displacements during the time taken to perform authentication. The scenario is successful if no crash occurs.

1) Best-Case Scenario: Assume the first vehicle, v_A, has processed all incoming authentication requests, and is ready to broadcast a new message. During movement, v_A applies its brakes, and therefore should generate, sign, and broadcast a safety-critical message over the network. As soon as the message is received, v_B must authenticate the message transmitted from v_A, before making use of the information content and responding to the situation. Assume that the message number $N_b/2 = 111$ belongs to v_A. This results in a delay in v_B performing message authentication, as vehicle v_B must first verify $N_b/2 = 111$ messages, where each message contains a signature.

2) Average-Case Scenario: Assume the first vehicle, v_A, has processed all incoming authentication requests, and is ready to broadcast a new message. During movement, v_A applies its brakes, and therefore should generate, sign, and broadcast a safety-critical message over the network. As soon as the message is received, v_B must authenticate the message transmitted from v_A, before making use of the information content and responding to the situation. Assume that the message number $N_b = 222$ belongs to v_A. This results in a delay in v_B performing message authentication, as vehicle v_B must first verify $N_b = 222$ messages, where each message contains a signature.

3) Worst-Case Scenario: Assume the first vehicle, v_A, has not processed all incoming authentication requests. The vehicle should be able to verify a maximum of N_b received messages containing authentication requests, before broadcasting a new message. During movement, v_A applies its brakes, and therefore (after processing current received messages) should generate, sign, and broadcast a safety-critical message over the network. As soon as the message is received, v_B must authenticate the message transmitted from v_A, before making use of the information content and responding to the situation. Assume that the message number $N_b = 222$ (the last message) belongs to v_A. This results a delay in v_A and v_B performing message authentication, as each vehicle v_A and v_B must first verify $N_b = 222$ messages (together $N_b \times 2 = 444$ messages), where each message contains a signature.

Note that

1) Authentication protocols that only succeed in the best-case scenario are “Not Appropriate” for use in safety-critical applications in the real world.
2) Authentication protocols that succeed in the average-case scenario are “Risky” for use in safety-critical applications in the real world.
3) Authentication protocols that succeed in the worst-case scenario are “Appropriate” for use in safety-critical applications in the real world.

VI. Case Studies

In this section, a case study approach is employed to demonstrate the usefulness of the proposed evaluation model. We use the defined metrics to evaluate the impact of the delay. Then, we group the protocols into appropriate safety categories. Using our model, we determine whether a crash will occur based on vehicle displacements during the time taken to perform authentication in three best-case ($N_b/2 = 111$), average-case ($N_b = 222$), and worst-case ($N_b \times 2 = 444$) scenarios.

A. Implementation

We implement the cryptographic primitives used in the following five schemes: BP [35], GSIS [61], VAST [62], 2FLIP [63], and BAEE [28]. We investigate the time complexity of various cryptographic operations providing $\approx$ 128-bit security level used in each of these five schemes, including: ECDSA-256 signature generation (T^{ecdsa}_{sign}) and verification (T^{ecdsa}_{ver}), ECQV-256 public-key certificate reconstruction (T^{ecqv}_{rec}), SHA-256 hash (T^{hash}_{sha}), HMAC-256 (T^{hmac}_{sha}), and optimal Ate pairing-382 (T^{oate}_{pair}). The investigation is performed using the newest stable release branch (1.1.1 series) of the OpenSSL software library [64]. All ECC operations (except for GSIS) are evaluated over the NIST P-256 curve (achieving 128-bit security level [29]). As GSIS is a pairing-based scheme [33], the elliptic curve arithmetic and optimal Ate pairing computations [65] are over the Barreto-Naehrig curve [66] in our evaluation, where the minimum bit-length of p is estimated as 382-bits (achieving 127-bit security level [67]), an optimistic parameter to use in cryptographic pairings for

TABLE III
THE NUMBER OF CPU CLOCK CYCLES AND AVERAGE COMPUTATION TIME OF DIFFERENT OPERATIONS

	$ecdsa$ $sign$	$ecdsa$ ver	$ecqv$ rec	$hash$ sha	$hmac$ sha	$oate$ $pair$
CPU (clk)	3.15×10^5	7.14×10^5	4.62×10^5	1×10^3	7.77×10^3	11.34×10^6
ACT (sec)	1.5×10^{-4}	3.4×10^{-4}	2.2×10^{-4}	4.8×10^{-7}	3.7×10^{-6}	5.4×10^{-3}

TABLE IV
COMPARISONS OF FIVE DIFFERENT V2V AUTHENTICATION SCHEMES OVERHEAD DURING MESSAGE GENERATION AND VERIFICATION

	V2V Authentication Overhead	
Schemes	**Message Generation Overhead (sec)**	**Message Verification Overhead (sec)**
BP	$T^{ecdsa}_{sign} = 1.5\times10^{-4}$	$6.8\times10^{-4} = T^{ecdsa}_{ver} + {}_{cert}T^{ecdsa}_{ver}$
GSIS	$3T^{oate}_{pair} + T^{hash}_{sha} = 1.62\times10^{-2}$	$2.7\times10^{-2} + x^* = 5T^{oate}_{pair} + T^{hash}_{sha} + (2\times\sum_{i=1}^{crl} T^{oate}_{pair})$
VAST	$T^{ecdsa}_{sign} + T^{hmac}_{sha} = 1.53\times10^{-4}$	$6.87\times10^{-4} = T^{ecdsa}_{ver} + {}_{cert}T^{ecdsa}_{ver} + 2T^{hmac}_{sha}$
2FLIP	$7T^{hash}_{sha} + T^{hmac}_{sha} = 7.06\times10^{-6}$	$4.18\times10^{-6} = T^{hash}_{sha} + T^{hmac}_{sha}$
BAEE	$T^{ecdsa}_{sign} = 1.5\times10^{-4}$	$5.6\times10^{-4} = T^{ecdsa}_{ver} + T^{ecqv}_{rec}$

—Note: [x^*] The value $x = (2\times\sum_{i=1}^{crl} T^{oate}_{pair})$, where crl denotes the number of elements in the CRL.

128-bit security level (384 bits p) [68]. The implementation for GSIS is performed using the newest efficient and stable release branch (0.5.0 series) of the RELIC cryptographic meta-toolkit [69]. The experiment for each cryptographic operation involved 10^6 trials in Debian Linux distribution running on an Intel Core 2 Duo Processor T6570 (2M Cache, 2.10 GHz, 4GB RAM). Note that the latest high-performance automotive single chip modem for vehicular communications made by NXP Semiconductors (the RoadLINK SAF5400 [12]) offers same performance as the processor used in this study [28], [41].

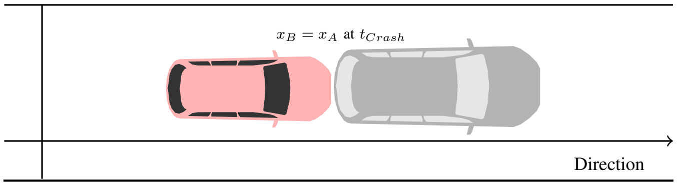
B. Results

Table III lists the results of our investigation of the number of CPU clock cycles (clk) and ACT in seconds associated with the various cryptographic operations used in the protocols. The message signing cost comparisons is shown in Table IV. Recipient vehicles must verify the signatures before accepting the messages. As the vehicles broadcast one beacon in each 100 ms, they receive many beacons in the time between broadcasts. Hence, the signature verification speed is far more important than signature generation speed.

The message verification cost comparisons is shown in Table IV. The BP scheme requires two ECDSA signature verification operations (one for the message and one for the explicit certificate). In GSIS, verification of each broadcast message requires five bilinear-pairing operations, one hash computation, and two paring operations for each Certificate Revocation List (CRL) item, the largest verifying cost among the schemes listed in the table. The verification in VAST requires two HMAC computations, and two ECDSA signature verification operations (one for the message and one for the explicit certificate authentication). For 2FLIP, one hash calculation and one HMAC computation are needed. BAEE requires one ECDSA signature verification and one ECQV public-key reconstruction computation. We note that message verification in BP, VAST, and BAEE includes CRL checking through string comparison, hence, their computation costs could be ignored. Table V lists the total delay T^{total}_{Delay}, positions $x_{A,B}$, speeds u_A, and speed u_B at accident time t_{Crash}.

Solving Equation 8 and Equation 9 shows if a crash will occur such that v_B runs into v_A at time t due to verification overhead, where $0 \geq u_A(t)$. Table V lists the total delay

TABLE V
RESULTS FOR SCENARIO AT CRASH TIME



Scenario for a vehicle equipped with 2.10 GHz processor					
Best-case	T^{total}_{Delay}	t_{Crash}	$x_{A,B}$	u_A	u_B
BP	0.90sec	-	-	0.0m/s	0.0m/s
GSIS	3.82sec	2.58sec	77.45m	6.7m/s	30.0m/s
VAST	0.91sec	-	-	0.0m/s	0.0m/s
2FLIP	0.83sec	-	-	0.0m/s	0.0m/s
BAEE	0.89sec	-	-	0.0m/s	0.0m/s
Average-case	T^{total}_{Delay}	t_{Crash}	$x_{A,B}$	u_A	u_B
BP	0.98sec	-	-	0.0m/s	0.0m/s
GSIS	6.82sec	2.58sec	77.45m	6.7m/s	30.0m/s
VAST	0.98sec	-	-	0.0m/s	0.0m/s
2FLIP	0.83sec	-	-	0.0m/s	0.0m/s
BAEE	0.95sec	-	-	0.0m/s	0.0m/s
Worst-case	T^{total}_{Delay}	t_{Crash}	$x_{A,B}$	u_A	u_B
BP	1.13sec	3.51sec	80.0m	0.0m/s	8.6m/s
GSIS	12.8sec	2.58sec	77.45m	6.7m/s	30.0m/s
VAST	1.13sec	3.51sec	80.0m	0.0m/s	8.6m/s
2FLIP	0.83sec	-	-	0.0m/s	0.0m/s
BAEE	1.07sec	3.65sec	80.0m	0.0m/s	6.8m/s

—Note: The value $x_{A,B}$ denotes the position of v_A and v_B at crash time (if there is a crash).

T^{total}_{Delay}, positions $x_{A,B}$, speeds u_A, and speed u_B at accident time t_{Crash}.

The time window T^{total}_{Delay} is ≤ 1 second (including driver reaction time) to stop the vehicle before a possible crash. Please note that without authentication delay, v_A and v_B would stop in positions $x = 80$ and $x = 74.9$, respectively.

As shown in Table V, the pairing-based GSIS protocol fails to succeed the best-case, average-case, and worst-case scenarios, as vehicle v_B runs into v_A before even starting to break (speed 30 m/s). This scheme is "Not Appropriate" for use in safety-critical applications. The BP, VAST, and BAEE fail to succeed the worst-case scenario, and as a result, these protocols are "Risky" for use in safety-critical applications. The 2FLIP is "Appropriate" for use in safety-critical applications, since there is no crash recorded for this scheme, even in the worst-case scenario (the T^{total}_{Delay} is less than 1 second).

C. Summary of the Steps Performed

The number of beacons successfully received in the required interval for safety-critical applications is evaluated through computer simulations for a large-scale VANET (see Section V-A1). The maximum number of beacons received by the vehicle under the application of Japanese ARIB STD-T109 standard is 222 beacons per 100 ms. Therefore, we consider 222 as the upper bound for further calculations. We determine whether a crash will occur based on vehicle displacements during the time taken to perform authentication in three scenarios (see Section V-B), best-case ($N_b/2 = 111$), average-case ($N_b = 222$), and worst-case ($N_b \times 2 = 444$). The required steps to evaluate an authentication protocol are as follows:

1. Implement the cryptographic primitives used in the V2V authentication scheme and investigate the time complexity of various cryptographic operations (in accordance with a C-ITS security standard).
2. Solve Equation 6 to calculate the total delay (the sum of all verification times plus the driver's reaction time).
3. Solve Equation 8 and Equation 9 to show if a crash will occur, such that v_B runs into v_A at time t due to the verification overhead, where $0 \geq u_A(t)$.
4. Consider the protocol as "Appropriate" for use in safety-critical applications if it succeeds in the worst-case scenario, where $N_b \times 2 = 444$.

VII. Conclusion and Recommendation

Multiple schemes have been proposed for V2V authentication in VANETs. The existence of a realistic model to evaluate the overhead of these schemes when applied in practical situations with regard to quantitative comparison was a missing component. This paper proposed such a model with clearly defined metrics. The model was applied for case studies, evaluating five proposed authentication schemes in the literature.

The numerical experiments in Section VI-B showed that only one of those five evaluated authentication schemes can be marked as "Appropriate" for use in safety-critical applications. This demonstrates that most of the proposed schemes in the literature are not applicable and effective in their proposed network environment. Thus, more performance evaluation of the existing schemes and future proposals should be conducted on a large-scale network.

Enabling safety-critical applications in VANETs requires extensive beaconing exchange between vehicles. Based on the results listed in Section VI-B, care is needed when designing authentication protocols to cater for processing a large number of exchanged beacons. We advise researchers to identify a balance between satisfying security/privacy requirements and developing efficient authentication schemes for practical applications. The beacon verification process results in a delay in driver notification and allows insufficient driver reaction time, resulting in potential collisions and serious injuries (assuming the driver does not react independently). There are many scenarios where a driver is relying completely on the safety messages to react on time. Examples include situations involving aggressive drivers, distracted/inattentive drivers, poor driver decisions, impaired/drowsy drivers, and rough/slick road conditions. Hence, the verification time must be less than driver reaction time. Otherwise the safety goal that the vehicular communications are designed to achieve cannot be obtained with secure communications in place.

We recommend protocol designers assess proposed authentication protocols through applying our model and determine the impact of authentication processing delay on driver safety in high-density VANET scenarios. We believe this model will be useful, and it is our hope that the model is broadly adopted.

References

[1] P. Papadimitratos, A. D. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation," *IEEE Communications Magazine*, vol. 47, pp. 84–95, November 2009.

[2] IEEE, "IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications amendment 6: Wireless access in vehicular environments," *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007)*, pp. 1–51, July 2010.

[3] R. A. Uzcategui, A. J. D. Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Communications Magazine*, vol. 47, pp. 126–133, May 2009.

[4] ITS.Europa, "Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band," Standard ETSI - ES 202 663, European Telecommunications Standards Institute, January 2010.

[5] ARIB.Japan, "700 MHz Band Intelligent Transport Systems," Standard ARIB STD-T109, Association of Radio Industries and Businesses, July 2017.

[6] CAMP, "Vehicle Safety Communications Project: Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC," Tech. Rep. DOT HS 809 859, National Highway Traffic Safety Administration - U. S. Department of Transportation (USDOT), March 2005.

[7] L. Xue, Y. Yang, and D. Dong, "Roadside infrastructure planning scheme for the urban vehicular networks," *Transportation Research Procedia*, vol. 25, pp. 1380 – 1396, 2017. World Conference on Transport Research - WCTR 2016 Shanghai. 10-15 July 2016.

[8] S. Goudarzi, A. H. Abdullah, S. Mandala, S. A. Soleymani, M. A. R. Baee, M. H. Anisi, and M. S. Aliyu, "A systematic review of security in vehicular ad hoc network," in *Proc. 2nd Symp. WSCN*, pp. 1–10, 2013.

[9] M. A. R. Baee, L. Simpson, X. Boyen, E. Foo, and J. Pieprzyk, "Authentication strategies in vehicular communications: a taxonomy and framework," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1–50, 2021.

[10] K. Han, A. Weimerskirch, and K. G. Shin, "Automotive cybersecurity for in-vehicle communication," in *IQT QUARTERLY*, vol. 6 of *1*, pp. 22–25, 2014.

[11] J. Siegel, D. Erb, and S. Sarma, "Algorithms and architectures: A case study in when, where and how to connect vehicles," *IEEE Intelligent Transportation Systems Magazine*, vol. 10, pp. 74–87, Spring 2018.

[12] "NXP Semiconductors; RoadLINK SAF5400 single chip modem." https://www.nxp.com. Accessed: 2020-02-10.

[13] C. Sommer, Z. Yao, R. German, and F. Dressler, "Simulating the influence of IVC on road traffic using bidirectionally coupled simulators," in *IEEE INFOCOM Workshops 2008*, pp. 1–6, April 2008.

[14] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of SUMO - Simulation of Urban Mobility," *International Journal On Advances in Systems and Measurements*, vol. 5, pp. 128–138, December 2012.

[15] CAMP, "Vehicle Safety Communications Applications (VSC-A) Final Report: Appendix Volume 3 Security," Tech. Rep. DOT HS 811 492D, National Highway Traffic Safety Administration - U. S. Department of Transportation (USDOT), September 2011.

[16] ITS.Europa, "Intelligent Transport Systems (ITS); STDMA recommended parameters and settings for cooperative ITS; Access Layer Part," Standard ETSI TR 102 861, European Telecommunications Standards Institute, January 2012.

[17] ITS.Europa, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," Standard ETSI EN 302 637-2, European Telecommunications Standards Institute, September 2014.

[18] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. Rezazadeh Baee, and S. Mandala, "Trust management in vehicular ad hoc network: a systematic review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, p. 146, May 2015.

[19] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, pp. 39–68, Jan. 2007.

[20] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, Inc., 1st ed., 1996.

[21] D. Gollmann, "What do we mean by entity authentication?," in *Proceedings 1996 IEEE Symposium on Security and Privacy*, pp. 46–54, May 1996.

[22] M. Riley, K. Akkaya, and K. Fong, "A survey of authentication schemes for vehicular ad hoc networks," *Security and Communication Networks*, vol. 4, pp. 1137 – 1152, 10 2011.

[23] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, pp. 2985–2996, Dec 2015.

[24] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 17, pp. 228–255, Firstquarter 2015.

[25] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Vehicular Communications*, vol. 9, no. Supplement C, pp. 19 – 30, 2017.

[26] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–17, 2018.

[27] J. Petit and Z. Mammeri, "Authentication and consensus overhead in vehicular ad hoc networks," *Telecommunication systems*, vol. 52, no. 4, pp. 2699–2712, 2013.

[28] M. A. R. Baee, L. Simpson, E. Foo, and J. Pieprzyk, "Broadcast authentication in latency-critical applications: On the efficiency of IEEE 1609.2," *IEEE Transactions on Vehicular Technology*, vol. 68, pp. 11577–11587, Dec 2019.

[29] IEEE, "IEEE standard for wireless access in vehicular environments–security services for applications and management messages - amendment 1," *IEEE Std 1609.2a-2017 (Amendment to IEEE Std 1609.2-2016)*, pp. 1–123, Oct 2017.

[30] K. Han, S. D. Potluri, and K. G. Shin, "On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks," in *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems*, ICCPS '13, (New York, NY, USA), pp. 160–169, ACM, 2013.

[31] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proceedings of the 1st ACM International Workshop on Quality of Service &Amp; Security in Wireless and Mobile Networks*, Q2SWinet '05, (New York, NY, USA), pp. 79–87, ACM, 2005.

[32] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International journal of information security*, vol. 1, no. 1, pp. 36–63, 2001.

[33] M. A. R. Baee, L. Simpson, X. Boyen, E. Foo, and J. Pieprzyk, "On the efficiency of pairing-based authentication for connected vehicles: Time is not on our side!," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2021.

[34] L. Gollan and C. Meinel, "Digital signatures for automobiles?!," in *in Systemics, Cybernetics and Informatics (SCI)*, Citeseer, 2002.

[35] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '05, (New York, NY, USA), pp. 11–21, ACM, 2005.

[36] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, VANET '07, (New York, NY, USA), pp. 19–28, ACM, 2007.

[37] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu, "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication," in *2010 IEEE International Conference on Communications*, pp. 1–6, May 2010.

[38] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, "Secure revocable anonymous authenticated inter-vehicle communication (sraac)," in *4th Conference on Embedded Security in Cars (ESCAR 2006), Berlin, Germany*, pp. 1–9, Citeseer, 2006.

[39] C. D. Jung, C. Sur, Y. Park, and K.-H. Rhee, "A robust conditional privacy-preserving authentication protocol in VANET," in *Security and Privacy in Mobile Information and Communication Systems* (A. U. Schmidt and S. Lian, eds.), (Berlin, Heidelberg), pp. 35–45, Springer Berlin Heidelberg, 2009.

[40] M. Campagna, "Sec 4: Elliptic curve qu-vanstone implicit certificate scheme (ECQV)," *Standards for Efficient Cryptography, Version*, vol. 1, 2013.

[41] M. A. R. Baee, *Privacy-Preserving Authentication and Key-Management for Cooperative Intelligent Transportation Systems*. PhD thesis, Queensland University of Technology, 2021.

[42] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology* (G. R. Blakley and D. Chaum, eds.), (Berlin, Heidelberg), pp. 47–53, Springer Berlin Heidelberg, 1985.

[43] M. A. R. Baee, "Implementation and performance analysis of identity-based authentication in wireless sensor networks," Master's thesis, Universiti Teknologi Malaysia, 2014.

[44] B. Palaniswamy, S. Camtepe, E. Foo, L. Simpson, M. A. Rezazadeh Baee, and J. Pieprzyk, "Continuous authentication for VANET," *Vehicular Communications*, vol. 25, p. 100255, 2020.

[45] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for VANETs," in *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*, VANET '06, (New York, NY, USA), pp. 94–95, ACM, 2006.

[46] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, pp. 86–96, Jan 2012.

[47] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Advances in Cryptology – CRYPTO 2004* (M. Franklin, ed.), (Berlin, Heidelberg), pp. 41–55, Springer Berlin Heidelberg, 2004.

[48] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology — ASIACRYPT 2001* (C. Boyd, ed.), (Berlin, Heidelberg), pp. 552–565, Springer Berlin Heidelberg, 2001.

[49] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 1–9, June 2009.

[50] A. Varga, "The OMNeT++ discrete event simulation system," in *In ESM01*, 2001.

[51] D. Eckhoff, C. Sommer, and F. Dressler, "On the Necessity of Accurate IEEE 802.11p Models for IVC Protocol Simulation," in *75th IEEE Vehicular Technology Conference (VTC2012-Spring)*, (Yokohama, Japan), pp. 1–5, IEEE, May 2012.

[52] N. Kudarauskas, "Analysis of emergency braking of a vehicle," *Transport*, vol. 22, no. 3, pp. 154–159, 2007.

[53] ITS.Europa, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions," Standard ETSI TR 102 638, European Telecommunications Standards Institute, June 2009.

[54] IEEE, "IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements - part 11: Wireless LAN Medium Access

Control (MAC) and Physical Layer (PHY) specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, Dec 2016.

[55] D. Eckhoff and C. Sommer, "A Multi-Channel IEEE 1609.4 and 802.11p EDCA Model for the Veins Framework," in *5th ACM/ICST International Conference on Simulation Tools and Techniques for Communications, Networks and Systems (SIMUTools 2012): 5th ACM/ICST International Workshop on OMNeT++ (OMNeT++ 2012), Poster Session*, (Desenzano, Italy), ACM, March 2012.

[56] J. Heinovski, F. Klingler, F. Dressler, and C. Sommer, "Performance comparison of IEEE 802.11p and ARIB STD-T109," in *2016 IEEE Vehicular Networking Conference (VNC)*, pp. 1–8, Dec 2016.

[57] G. S. Tian, Y. C. Tian, and C. Fidge, "High-precision relative clock synchronization using time stamp counters," in *13th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2008)*, pp. 69–78, March 2008.

[58] J. Viega and M. Messier, *Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation & More*. O'Reilly Media, 2003.

[59] W. Hugemann, "Driver reaction times in road traffic," in *European Association for Accident Research and Analysis Annual Convention*, (Portoro, Slovenija), September 2002.

[60] R. Stephenson, "Constant power equations of motion," *American Journal of Physics*, vol. 50, no. 12, pp. 1150–1155, 1982.

[61] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, pp. 3442–3456, Nov 2007.

[62] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *Journal of Communications and Networks*, vol. 11, pp. 574–588, Dec 2009.

[63] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 896–911, Feb 2016.

[64] The OpenSSL Project, "OpenSSL: The open source toolkit for SSL/TLS." www.openssl.org, April 2003.

[65] F. Vercauteren, "Optimal pairings," *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 455–461, 2009.

[66] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," in *Selected Areas in Cryptography* (B. Preneel and S. Tavares, eds.), (Berlin, Heidelberg), pp. 319–331, Springer Berlin Heidelberg, 2006.

[67] Y. Sakemi, T. Kobayashi, and T. Saito, "Pairing-Friendly Curves," Internet-Draft draft-irtf-cfrg-pairing-friendly-curves-00, Internet Engineering Task Force, Nov. 2019. Work in Progress.

[68] A. Menezes, P. Sarkar, and S. Singh, "Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography," in *Paradigms in Cryptology – Mycrypt 2016. Malicious and Exploratory Cryptology* (R. C.-W. Phan and M. Yung, eds.), (Cham), pp. 83–108, Springer International Publishing, 2017.

[69] D. F. Aranha and C. P. L. Gouvêa, "RELIC is an Efficient LIbrary for Cryptography." https://github.com/relic-toolkit/relic.

Mir Ali Rezazadeh Baee (Senior Member, IEEE) completed his Doctoral research in computer science information security at the Queensland University of Technology, Brisbane, QLD, Australia. He has over 15 years of experience working in computer science, and since 2012, he has been involved in computer science research with a strong focus on applied cryptography and information security. He is a Sessional Academic and Information Security Researcher with the Queensland University of Technology, designing authentication and key-management protocols for privacy-preserved secure vehicular communications. He also collaborates with the Cyber Security Cooperative Research Center (CSCRC), Australia, to solve pressing real-world cyber security challenges. His contributions have led to novel and important scientific outcomes. He has actively served as a reviewer for flagship journals and conference proceedings, such as *IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, and ASIACRYPT sponsored by International Association for Cryptologic Research (IACR)*.

Leonie Simpson received her Ph.D. degree from the Queensland University of Technology, Brisbane, QLD, Australia, in 2000. She has been involved in information security research for over 20 years. She has extensive experience analyzing cryptographic algorithms and finding weaknesses that reduce the security provided. She has applied her knowledge of design flaws in algorithms to help develop more secure ciphers, working in teams with Australian and international researchers. She is a Senior Lecturer and Information Security Researcher at the Queensland University of Technology. She is currently researching efficient authenticated encryption methods for use in securing data transmissions between small, low-power devices in the rapidly growing Internet of Things. Her main research interests include symmetric cryptology, widely used for data protection.

Xavier Boyen is a world expert on cryptography, from theory and efficient designs to liberty-promoting applications, and whose contributions have attracted over 15,000 scholarly citations, industry standards, and a diverse set of tangible real-world benefits. Prof Xavier is an Associate Professor with QUT, a Future Fellow from the ARC, and a PhD from Stanford.

Ernest Foo (Member, IEEE) received his Ph.D. degree from the Queensland University of Technology, Brisbane, QLD, Australia, in 2000. He is an Associate Professor with School of Information and Communication Technology, the Griffith University, Brisbane, QLD, Australia. From 2007 to 2019, he has been a Senior Lecturer and Researcher at the Information Security Discipline, Queensland University of Technology, Brisbane, QLD, Australia. His research interests can be broadly grouped into the field of secure network protocols with an active interest in the security of industrial controls systems employing machine learning and data mining as well as cryptographic protocols and network simulations. He has authored or coauthored over 90 refereed papers including 20 journal papers.

Josef Pieprzyk is a Senior Principal Research Scientist with the Commonwealth Scientific and Industrial Research Organization, Data61, Sydney, NSW, Australia, a Professor with Institute of Computer Science, Polish Academy of Sciences, and an Adjunct Professor with the Queensland University of Technology, Brisbane, QLD, Australia. His main research interests include cryptology and information security. He has authored or coauthored five books, edited ten books (conference proceedings), six book chapters, and more than 300 papers in refereed journals and refereed international conferences. He is a member of the editorial boards for *International Journal of Information Security (Springer), Journal of Mathematical Cryptology (De Gruyter), Open Access Journal of Cryptography (MDPI), International Journal of Applied Cryptography (Inderscience Publishers), Fundamenta Informaticae (IOS Press), International Journal of Security and Networks (Inderscience Publishers), and International Journal of Information and Computer Security (Inderscience Publishers).*