DEGREE PROJECT IN COMPUTER SCIENCE AND ENGINEERING, SECOND CYCLE, 30 CREDITS

STOCKHOLM, SWEDEN 2018

A Privacy-preserving Pseudonym Acquisition Scheme for Vehicular Communication Systems

ANDREAS MESSING

KTH ROYAL INSTITUTE OF TECHNOLOGY
SCHOOL OF COMPUTER SCIENCE AND COMMUNICATION

A Privacy-preserving Pseudonym Acquisition Scheme for Vehicular Communication Systems

ANDREAS MESSING

Master in Computer Science
Date: January 11, 2018
Supervisor: Panos Papadimitratos & Mohammad Khodaei
Examiner: Mads Dam
Swedish title: Ett integritetsbevarande protokoll för erhållning av pseudonymer i fordonskommunikationssystem
School of Computer Science and Communication

Abstract

Vehicular communication systems rely on temporary anonymous identities, i.e. pseudonyms, in order to establish security and at the same time avoid the possibility of tracking vehicles. If a vehicle uses only one pseudonym, an adversary would be able to follow the vehicle by observing and linking messages, signed under that pseudonym. Therefore, the vehicles acquire a set of pseudonyms from the VPKI, i.e. infrastructure of the communication system, and switches pseudonym frequently. If a vehicle would be unable to acquire these pseudonyms, it would not be able to utilize the communication system without compromising its privacy. A vehicle is able to create its own pseudonyms using group signatures, i.e. the so-called Hybrid scheme. However, a pseudonym issued by the VPKI and a pseudonym created with a group signature would look different to an observer. If only one vehicle used pseudonyms created with group signature, it would easily be singled out and tracked. This thesis proposes a solution to this problem, but not the broader problem of linking messages by other means, e.g. the content of the message. In the solution, a vehicle is able to generate its own pseudonyms, using the Hybrid scheme, and make them unlinkable at the cost of computational overhead for itself and the vehicles around it, since group signatures are costly. The vehicle achieves this by aligning the lifetime of the pseudonym with other pseudonyms and asking neighboring vehicles to alternate randomly between using pseudonyms issued by the VPKI and pseudonyms created with group signatures. This alternation by neighboring vehicles decreases the linkability of pseudonyms created with group signature without increasing the linkability of pseudonyms created by the VPKI. This results in a trade off between reasonable computational overhead and acceptable linkability for pseudonyms.

A short paper, presenting the scheme and results of this thesis, has been accepted to the IEEE Vehicular Networking Conference in Torino, Italy, 27-29 November, 2017 [1].

Sammanfattning

Fordonskommunikation utnyttjar temporära identiteter, dvs. pseudonymer, för att etablera säkerhet och samtidigt undvika möjligheten att spåra fordon. Om ett fordon skulle använda endast ett pseudonym så skulle en observatör kunna följa fordonet genom att observera och länka meddelanden signerade under det pseudonymet. Varje fordon erhåller därför ett set pseudonymer från kommunikationssystemet och byter pseudonym regelbundet. Om ett fordon inte kan erhålla dessa pseudonymer från systemet, så skulle fordonet inte kunna utnyttja kommunikationssystemet utan att förkasta sin integritet. Ett fordon skulle kunna skapa sina egna pseudonymer genom att använda gruppsignaturer, dvs. det så kallade Hybrid scheme. Problemet är att ett pseudonym som är erhållet från kommunikationssystemet och ett pseudonym som är genererat med en gruppsignatur, ser olika ut för en observatör. Om endast ett fordon skulle använda pseudonymer med gruppsignaturer, så skulle det enkelt filtreras ut och spåras. Den här avhandlingen föreslår en lösning på detta problem, men inte till det större problemet att länka meddelanden på andra sätt, exempelvis använda informationen i själva meddelandet. I lösningen kan fordonet generera egna pseudonymer, genom att använda gruppsignaturer, dvs. Hybrid scheme, och göra dem olänkbara till priset av extra beräkningstid för sig själv och fordonen omkring sig, eftersom gruppsignaturer är kostsamma. Fordonet uppnår det genom att synkronisera pseudonymernas livslängd med de andra pseudonymerna och fråga fordonen i närheten om de kan slumpmässigt växla mellan att använda pseudonymer från systemet och pseudonymer som de skapat med gruppsignaturer. Om fordon i närheten växlar mellan pseudonymer från systemet och pseudonymer genererade med gruppsignaturer så minskar länkbarheten av pseudonymer baserade på gruppsignaturer utan att öka länkbarheten av pseudonymer från kommunikationssystemet. Det resulterar i en avvägning mellan beräkningstid och acceptabel länkbarhet av pseudonymer.

Ett konferens papper, som presenterar protokollet och resultatet av denna avhandling, har blivit accepterat till IEEE Vehicular Networking Conference i Torino, Italien, 27-29 November 2017 [1].

This work was performed with the administration of the School of Computer Science and Communication. However, it was done at the Networked Systems Security (NSS) Group, which is a part of the School of Electrical Engineering.

The result of this work was accepted to the IEEE Vehicular Networking Conference, 27-29 November, 2017, Torino, Italy [1].

I would like to thank my supervisors Prof. Panos Papadimitratos and Mohammad Khodaei for keeping me on track and providing great feedback and discussions. They also motivated me to submit a short version of this work to the conference.

I would like to thank my opponent, Erik Ihrén, for providing feedback.

I would like to thank Prof. Mads Dam for his valuable comments on the early version of this thesis and being my examiner.

Finally I would like to thank my family and friends for great support.

Contents

Chapter 1

Introduction

Vehicles are becoming increasingly interconnected, with several applications being developed for transportation safety and efficiency [2]. At the same time, vehicle are also becoming more independent of the drivers and more integrated with computer systems that allow vehicles to make their own decisions when driving. Several companies, including Google [26] and Tesla [25], are developing self-driving cars that aims to be entirely independent of the person in the driver seat. In the future, vehicles will drive themselves and be connected to the Internet like most other things. To do so, a vehicular communication system needs to be integrated for vehicles to acquire information about traffic and the environment around them to make efficient and correct decisions. Needless to say, the security of the vehicular communication system is crucial. Lack of security could potentially have lethal consequences for the drivers and passengers of the vehicles as well as the surrounding individuals. There have already been reported incidents of cars and airplanes being targeted by malicious hackers [27]. Vehicular communication systems are currently being developed and could hopefully be integrated into society in the near future.

1.1 Background

Secure vehicular communication systems are being researched around the globe. One promising secure communication system architecture, called Secure Vehicle Communication (SeVeCOM) [3], which is a project that started in 2008. Since then, various work have followed the architecture and extended the system with new components and ideas,

e.g. [4] [5]. The basis of the SeVeCOM project relies on a Vehicular Public Key Infrastructure (VPKI) system to ensure secure communication. The most common type of communication in the system are messages that are called Cooperative Awareness Messages (CAM). These messages are broadcast between 3 and 10 times per second from each vehicle to each other vehicle within its wireless range, which ranges up to a few hundred meters. These messages are signed under temporary identities, called pseudonyms, that has been signed and issued by the VPKI to all the vehicles.

Apart from CAMs, vehicles also communicate with the infrastructure of the system via Vehicle-to-Infrastructure (V2I) communication. While CAMs are broadcast to other vehicles in the neighborhood, the messages to the infrastructure are received by Road-Side Units (RSU). These RSUs are placed along the roads and are connected to the rest of the infrastructure with cable.

1.1.1 Vehicular Public Key Infrastructure (VPKI)

Systems that follow SeVeCOM, such as [7], [9], and [16], have extended the notion and use of a VPKI. They have divided areas into regions, based on different parameters including geography, that are being handled by their own VPKI management. The reason for separating into different regions is to make it more manageable. If all vehicles would be registered to the same VPKI, computational costs and memory usage would be too high. An example of this is the process of issuing pseudonyms. If the region is too large, it would be cumbersome to issue pseudonyms to all the vehicles.

The VPKI itself is separated into smaller components based on the functionality. One component would handle issuing pseudonyms, it is called Pseudonym Certificate Authority (PCA), while another handles the Long-Term Certificate (LTC), i.e. the real identities, of the vehicles and it is called Long-Term Certificate Authority (LTCA). Another authority, called Resolution Authority (RA) would be able to link a pseudonym to a LTC, through the LTCA and PCA to reveal real identity of a vehicle, if it needs to. Separating the functionality from one entity into several components is argued to be more secure and privacy preserving [8]. One component cannot uncover the real identity and track a vehicle for a long time on its own.

This makes it possible for a third party to operate a PCA without

gaining sensitive knowledge about the vehicles' real identities. It is undesirable to have a third party being able to make the connection and uncover the real identity of a vehicle. Some proposals, e.g. [10], have proposed a solution to have a proxy server scramble the pseudonym request to make it harder for the PCA to gain knowledge of the vehicles.

To obtain pseudonyms, the vehicle first sends a message to the LTCA, which the vehicle is registered with, and ask for an anonymous authentication ticket [7] [16]. If the vehicle is a valid member of that LTCA, it will receive the ticket that has been signed by the LTCA. This communication is encrypted and signed under the LTC of the vehicle to ensure privacy and membership. The ticket would then be sent to the PCA, during a pseudonym requests, as a proof of being a valid member in the system without revealing the vehicle's actual identity. The PCA then accepts the ticket and issue pseudonyms to that vehicle. This communication is encrypted using TLS encryption, i.e. symmetric encryption. If a third party eavesdrops that communication, it would not be able to see all the pseudonyms that the vehicles will be using. This way, the LTCA will not be aware of the pseudonyms issued to the vehicles and the PCA will not be aware of the vehicles' real identities. Since the ticket is anonymous and looks different every time, the PCA will not be able to link subsequent pseudonym requests coming from the same vehicle. A vehicle is therefore very reliant on the communication with the back-end security infrastructure to acquire pseudonyms and operate the communication system in a privacy preserving manner.

1.1.2 Group Signatures

Group signature was first introduced in [24] as a way for a member of the group to create signatures on behalf of the entire group while protecting the signers identity. It has some valuable features that would seem to be favorable for a vehicular communication system. Group signature schemes are asymmetric cryptography systems that uses many group private keys and only one group public key when signing messages and verifying signatures. If a member of the group uses its group private key to sign a message, the receiver would not be able to tell exactly which member signed it because the group public key corresponds to all the member's group private keys. The receiver

would only be able to tell that the message was signed by a valid member of the group. This would ensure the privacy of the signer of the message. Another important feature of group signatures is that every signature would be different. Even if the same message is signed twice by the same group private key, the signature would look different. This makes it hard to link different messages to the same signer. Using group signatures to sign CAMs sounds good in theory. However, the signing and verification processes of group signatures are expensive both in terms of computation time and memory. Using group signatures for every CAM is simply too expensive for vehicular communication systems that requires each host to sign and verify several CAMs each second.

Other papers, [14] [15], have investigated a combination of group signatures and pseudonyms, and it is called *Hybrid*. Vehicles uses the group signature to sign the pseudonyms instead of having a PCA sign them. By doing so, the CAMs can be signed under a pseudonym, and the extra computational cost from group signatures would only occur when creating and validating pseudonyms. A vehicle only have to validate the pseudonym once and can then validate subsequent CAMs, that uses the same pseudonym, without having to validate the pseudonym every time. This cuts down on the overhead significantly compared to using group signature on every CAM. Hybrid also have another important feature, it does not require a PCA to be able to generate a pseudonym, the vehicle can do it by itself. Generating a self-signed pseudonym is time consuming, however it can be done beforehand if the lifetime of the generated pseudonym is known. Another issue is that there are no policies that determine the lifetimes of the pseudonyms, meaning that there is no synchronization between the pseudonyms used by different vehicles. This makes it easier to link two pseudonyms to each other based on the timing of the pseudonym change.

1.1.3 Linking Attacks

An adversary could try to eavesdrop the communication system in order to achieve information about the vehicles. After eavesdropping, the adversary would have a list of all the CAMs and pseudonyms, that have been used to sign the CAMs, in different time periods. The adversary would then try to link CAMs or pseudonyms from different

time periods to the same vehicle. There are two types of linking attacks that could be used to link the old and new CAMs and pseudonyms when they change pseudonym [30]. One of them is syntactic linking and it is what will be discussed further in this thesis. That is the ability to link an old pseudonym to a new one based on the information in the pseudonym alone, i.e. lifetime and signature, and not the content of the message that the pseudonym signed. If only one pseudonym disappear and only one new pseudonym appear, it is the same vehicle with high probability. There are several papers that offers solutions to this, e.g. mix-zones [29] [28] and synchronized pseudonym switches [16].

The other one is semantic linking. It relies on the information in the CAMs, that the pseudonym signs, so that, for example, it predicts the next location of the vehicle and this way link successive messages transmitted by the same vehicle even though they are signed under different pseudonyms. In a CAM, there is detailed information regarding the state of the vehicle. This information includes position, speed, trajectory, and angle of the steering wheel. If a new CAM pops up at the predicted location, it is most likely the same vehicle as before, even if it uses a different pseudonym. Semantic linking is not discussed more in this thesis, it is however important to know that it exists and that there are other papers on that topic, such as [19]. Although it is an existing and significant problem, this thesis is concerned with a narrower version of providing privacy enhancements. In particular, how to design the use of pseudonyms so that they themselves do not contain information that can lead an observer to link vehicular messages, such as the CAMs. By proposing a scheme to improve the state of the art, the more general problem, to thwart linking based on the content of the messages, i.e. semantic linking, can have its own treatment in a future work.

However, protection against semantic linking is not entirely safe by itself either, even if it is impossible to predict the next step of the vehicle, if it uses the same pseudonym as before or it is the only pseudonym that changes, it is most likely the same vehicle. Therefore both syntactic and semantic linking protection is required to have a privacy preserving system.

1.2 Problem Statement

The VPKI communication system as described earlier has a single point of failure. If the PCA or LTCA is not accessible, vehicles would not be able to acquire pseudonyms. A system that require vehicles to constantly acquire new pseudonyms, e.g. on-demand systems such as [16], is very dependent on the VPKI being constantly accessible. Not being able to acquire pseudonyms would cause the vehicles to not be able to sign CAMs without reveling their LTC [18]. The subject of the thesis is to find an acceptable solution to this problem. How can we remove this single point of failure such that vehicles are able to participate in the system, without revealing their LTC or use easily trackable pseudonyms, even if the vehicles are unable to access the VPKI to acquire pseudonyms.

The system needs an alternative way of acquiring unlinkable pseudonyms in the case that the VPKI is unavailable. Designing and testing such a solution is the research topic of this thesis. The scheme will not only have to allow the vehicles to continue to broadcast CAMs using pseudonyms, but also ensure acceptable privacy, by making syntactic linking non-trivial, for the pseudonyms. A solution to this problem would most likely be compatible with any future solution to semantic linking.

The proposed scheme relies on self-signed pseudonyms using group signatures, i.e. the Hybrid scheme [14] [15], when needed. The reason for using group signatures is so that vehicles can generate their own pseudonyms without requiring connection to the infrastructure. The Hybrid scheme would allow vehicles to continue to sign CAMs, and other messages, with pseudonyms. The problem is that a limited use of the Hybrid scheme could actually lead to a small subset of CAMs and messages being signed under a few, or possibly a single, such pseudonym(s). This subset would correspond to a small anonymity set and thus make guessing or linking of those pseudonyms (and thus the messages) much easier. This potential imbalance, which depends on extraneous factors, such as the number of neighboring vehicles and the connectivity to the VPKI, needs to be addressed and it is investigated in this thesis. The feasibility of this proposed scheme, as well as policies about how and when vehicles needs to use it, is something that will be designed and tested.

1.2.1 Research Question

In order to address the syntactic linking problem stated above, the research question for the thesis is defined as follows:

To what extent is the limited use of the Hybrid scheme making linking of pseudonyms more likely and how can we reduce the likelihood of linking them if the observer/adversary resorts to information included only in the pseudonyms, i.e. syntactic linking, and no other data in the vehicular transmissions and with credentials/pseudonyms that are sanitized, e.g. as those proposed in [6] [5].

The linking of messages under a single pseudonym are trivially linkable, but that is considered acceptable [4].

Another interesting question that needs to be addressed is:

Is the extra overhead, when using the solution, too computational heavy for the hardware to be considered a practical solution?

1.3 Motivation

Vehicular communication systems will be integrated in vehicles in the near future. In order to do so, a robust system is needed that can handle the dynamic environment and malicious adversaries. The structure of the vehicular communication system is still under construction and all loose ends will eventually need to be addressed. This project aims to help tie up a loose end that has not received much attention.

Current proposals for the standard of the vehicle communication system, e.g. [10], [11], does not have efficient on-demand schemes. In those papers, each vehicle is equipped with pseudonyms for 1-3 years, or even 25 years, and refilling them when inspecting the car. However, the academic world is also currently researching other solutions, e.g. [16], that could potentially be more favorable in the future. One reason is that most of the pseudonyms will not even be used since the vehicle might be turned off during the lifetime of those pseudonyms. If a pseudonym lifetime is about an hour and the vehicle is only active for two hours a day, $\frac{11}{12}$ of all those pseudonyms would be discarded. That would mean that the processing power used to

create those pseudonyms is wasted. In addition, all the pseudonyms would have to be revoked if the vehicle misbehaves, which would be cumbersome. The academic world is researching more efficient on-demand pseudonym acquisition solutions. In these solutions, the research problem investigated in this thesis could be a rather common occurrence and is therefore of interest to research.

One of the reasons that those papers propose such a high amount of pseudonyms is because there will be a low amount of RSUs in the beginning. This means that it will be hard to find an opportunity to communicate with the infrastructure at all times without relying on external communication systems, e.g mobile network. By having pseudonyms for a long time, e.g. 1-3 years, the vehicle requires less communication with the PCA. However, as the distribution of RSUs grows, it will be easier to communicate with the infrastructure and on-demand pseudonym acquisition might become a better solution. Alternative ways to communicate with the PCA might also be adopted as the mobile network becomes more prominent. The PCA would be a good target for malicious attacks that wants to render the system unavailable for a time.

Vehicles could use the Hybrid scheme in order to obtain pseudonyms when disconnected from the VPKI. However, these pseudonyms would belong to a smaller anonymity set and they could potentially be easy to link to the same vehicle, e.g. using timing information or signature type. Therefore, just using Hybrid pseudonyms is not enough to achieve protection against syntactic linking.

1.4 Limitations

This thesis seeks to solve the problem of acquiring pseudonyms that can be used in a privacy preserving way if the VPKI is unavailable. Therefore, linking attacks that uses the information in the acquired pseudonyms in order to link messages to the same vehicle, i.e. syntactic linking, are taken into consideration and are negated.

Linking attacks that uses information in the CAMs to track vehicles, e.g. semantic linking, is not taken into consideration and is out of the scope of this thesis. These linking attacks does not depend on the pseudonyms used and the problem cannot be solved with pseudonyms.

The focus of this thesis is not to find the best suitable group signature scheme to use, but rather how to use it efficiently to not lose syntactic linking protection. Therefore, comparison of different group signatures is not included in this thesis. There are other papers and thesis that have focused on that, e.g. [38]. The group signature implementation is used for timing signing and verification processes. It does not contain the dynamic joining functionality [23] or a limit on the amount of valid signatures that can be created at the same time [20].

Only 7 Nexcom boxes from the PRESERVE project [13] are available for use and in order to emulate a larger neighborhood, some of them are dedicated to emulate multiple vehicles by sending several times the normal amount of CAMs.

Chapter 2

System Model

In this chapter, the functionality of the VPKI, pseudonyms, and CAMs are described in more details. A Group Manager is added such that it would be possible to create self-signed pseudonyms, if the PCA is unreachable. Furthermore, a Baseline Scheme is introduced that is used to compare our solution with.

2.1 VPKI Entities

The VPKI is the system that handles the security in a region. The region is a geographical zone in which the secure communication system is operating. The components of the VPKI are the LTCA, PCA, RA, and Root Certificate Authority (RCA). These components are separate entities such that one of them cannot reveal the identity of vehicles on their own [8].

The LTCA handles the LTCs of the vehicles, i.e. the real identities within a region. There is only one LTCA in a region and vehicles are registered to the LTCA in the vehicle's home region. The vehicle generates a private/public key pair and sends the public key, which has been signed with the private key, to the LTCA. The reason it is signed is to prove possession of the private key. The LTCA then generates and signs a certificate to that vehicle. Whenever a vehicle that has been registered with an LTCA tries to acquire new pseudonyms, it first sends a ticket request to its LTCA [7]. If the vehicle is a valid member of the LTCA, it signs an anonymous ticket and sends it to the vehicle. The vehicle can then anonymously request pseudonyms from a PCA using the ticket to authenticate itself.

The role of an PCA is to issue pseudonyms to the valid vehicles in the region. In on-demand systems, e.g. [16], vehicles periodically sends pseudonym requests to a PCA to acquire a set of pseudonyms for a period. This pseudonym request period is called Γ and a vehicle can ask for sets of pseudonyms for more than one Γ at a time by sending multiple requests. Vehicles first generate private/public key pairs, then the vehicle signs the public keys with their corresponding private keys and sends them to the PCA along with the anonymous ticket from the LTCA [7] [16]. The PCA creates pseudonyms from the public keys and align the lifetimes of those pseudonym to be one after the other. The PCA also aligns the pseudonym lifetimes for each vehicle such that every vehicle switches pseudonym at the same time to protect against syntactic linking [16]. The period in which a single pseudonym is utilized is notated as τ_i. Every vehicle then changes pseudonym in the beginning of τ_{i+1}.

A region could potentially have any number of PCAs that can issue pseudonyms to the vehicles [8]. Every PCA would aligns its pseudonyms with all the other PCAs such that all vehicles have aligned pseudonyms regardless of which PCA issued them. One problem with this is that there would be several pseudonym sets, i.e. pseudonyms could be filtered based on which PCA signed them. Therefore a low number of PCAs would be favorable such that each PCA issues a high number of pseudonyms.

The purpose of the RA is to uncover the identity of a vehicle if needed. By coordinating with the PCA and the LTCA, the RA is able to reveal the identity of a vehicle based on the pseudonym that signed a specific CAM [7]. Misbehaving vehicles can then be evicted from the system by invalidating their long-term certificate and pseudonyms. It is also possible to use the CAMs to resolve what happen in an accident.

The RCA is the top Certificate Authority (CA) of the VPKI and handles the certificates of the other components. By doing that, it can evict the certificates of the other components if they have been compromised. If the RCA gets compromised, the VPKI is no longer secure. The RCA can extend over multiple regions. This way, trust between LTCA in different regions is established [8].

2.2 Group Manager (GM)

A Group Manager (GM) is included in every region. The GM handles a group signature scheme for vehicles that are within their home region (i.e. are registered with the regions LTCA). This allows vehicles to create self-signed pseudonyms within their home region. The group manager should not be the LTCA itself since it could have the possibility to link LTC and group signatures together. The group manager should be a separate entity within the same region as the LTCA.

When a vehicle registers with a LTCA, the LTCA issues an anonymous ticket to that vehicle. That vehicle then uses the ticket to register with the GM and acquire a group signing key. The result of this is that the GM has no knowledge of the vehicle's LTC, only which LTCA the vehicle is registered with. The LTCA has no knowledge of the vehicles group signing key. If the vehicle misbehaves, the RA can use the anonymous ticket, stored by both the LTCA and the GM, to synchronize the eviction of the vehicle from both the GM and the LTCA.

Other related work have also considered a GM in vehicular networks, but for other reasons, e.g. anonymous traffic reports [34] and participatory sensing [35].

2.3 Pseudonyms

By eavesdropping the CAMs, it would be possible to track the vehicles wherever they go based on the pseudonym used to sign the CAMs, until the vehicle switches to a new pseudonym. Privacy is of very high importance in the system and to be able to track vehicles this way for a long time is a deal breaker as described in [5]. In order to negate this undesirable outcome, pseudonyms have short life-times. The vehicles would use one pseudonym for a brief time, then discard it and switch to a new one. The pseudonym lifetime, notated as τ, is decided by the PCA. Two subsequent CAMs that have been signed with different pseudonyms cannot be linked to the same vehicle, using syntactic linking, by anyone other than the PCA, since it was the PCA that issued those pseudonyms. However, the PCA does not know the real identity of that vehicle. This would keep the real identity, i.e the LTC, of a vehicle confidential and the vehicle could only be tracked by the PCA during a brief time interval until the next Γ, i.e. pseudonym re-

quest. However, if needed, the RA could uncover the LTC of a vehicle through its pseudonym and hold it accountable for its actions by evicting its credentials from the system.

Fig 2.1 shows the structure of a pseudonym, the most interesting fields are the *Public key*, *Validity Restriction*, and *Signature*. The signature is signed by the PCA which makes the pseudonym trustworthy. Since everyone has access to the public key of the PCA, anyone can verify the pseudonym and therefore trust the CAMs that are signed with the private key corresponding to the public key in that pseudonym.

Element	Value	Description	Length in octets
Certificate			
uint8 version	0x01		1
SignerInfo singner_info<var>	0x09	length: 9 octets	1
SignerInfoType type	0x01	certificate_digest_with_ecdsap256	1
HashedId8 digest	[...]		8
SubjectInfo subject_info			
SubjectType type	0x01	authorization_ticket	1
opaque subject_name<var>	0x00	length: 0 → no name	1
[subject name]			0
SubjectAttribute subject_attributes<var>	0x2b	length: 43	1
SubjectAttributeType type	0x00	verification_key	1
PublicKey key			
PublicKeyAlgorithm algorithm	0x00	ecdsa_nistp256_with_sha256	1
EccPoint public_key			
EccPointType type	0x01	compressed_lsb_y_0	2
opaque x[32]	[...]		32
SubjectAttributeType type	0x02	assurance_level	1
SubjectAssurance assurance_level	0x04	level_4	1
SubjectAttributeType type	0x33	its_aid_ssp_list	1
ItsAidSsp its_aid_ssp_list<var>	0x04	length: 4 octets	1
IntX its_aid	[...]		1
opaque service_specific_permissions<var>	0x02	length: 2 octets	1
[service specific permissions]	[...]		2
ValidityRestriction validity_restrictions<var>	0x09	length: 9 octets	1
ValidityRestrictionType type	0x01	time_start_and_end	1
Time32 start_validity	[...]		4
Time32 end_validity	[...]		4
Signature signature			
PublicKeyAlgorithm algorithm	0x00	ecdsa_nistp256_with_sha256	1
EcdsaSignature ecdsa_signature			
EccPoint R			
EccPointType type	0x01	compressed_lsb_y_0	2
opaque x[32]	[...]		32
opaque s[32]	[...]		32
The total size of this certificate is 133 octets.			

Figure 2.1: Structure of a pseudonym, also called certificate. Taken from [40].

There have been a lot of different research about how to switch pseudonyms [16] [29]. If only one vehicle in the area is switching to a new pseudonym, it would be trivial to see the connection between the old pseudonym and the new pseudonym. The purpose of switch-

ing to a new pseudonym is so that no one can track the movements of the vehicle. Since the PCA is the one issuing the pseudonyms, it can decide the policies of them, the PCA can force all vehicles to switch at the same time, making it harder to see the connection to the old pseudonym [8]. While this seems to be a decent solution, one problem is that it overloads the network traffic in that one instant that everybody switches pseudonyms since every new pseudonym needs to be sent. Usually the vehicles can cache the pseudonyms in their neighborhood so that the pseudonym does not have to be sent and verified every time [14] [15]. Since every vehicle switch pseudonyms at the same time, they have to send their new pseudonym in their CAMs. They also have to verify the pseudonym of all the other vehicles in the area. This problem can be somewhat controlled by pre-announcing the pseudonyms as discussed in [14].

2.4 Cooperative Awareness Message (CAM)

CAMs are the most common type of messages in the vehicular communication system. A CAM is a broadcast message to all the surrounding vehicles and contains information about the sender. They are broadcast between 3 to 10 times per second using wireless communication from each vehicle. The content of a CAM ranges from position, speed, acceleration, and angle of the wheel to knowledge about the surrounding environment such as traffic accidents. All the necessary information is available in the CAMs for the receiver to use that information and make appropriate actions of its own. There is normally no need to keep track of other vehicle's old CAMs. However, they are stored so that they can be investigated in case of accidents.

The security of these messages are of high concern since they could be used to cause traffic accidents if used maliciously. Because of the number of CAMs sent all the time from every vehicle, it is of a very high importance to limit the amount of time it takes to manage incoming CAMs. For this reason, CAMs are not encrypted, which is fine since all the vehicles are suppose to read it anyway. However, it is required to have a signature such that other vehicles can be sure that the CAMs come from a trusted source and is not altered on the way. This signature is created using the temporary key pair of the pseudonym.

Fig 2.2 represents the structure of a CAM. At the bottom, we can

see the signature of the CAM that has been signed with the private key corresponding to the current pseudonym. After that, the pseudonym itself is attached in the certificate field and used to verify the signature.

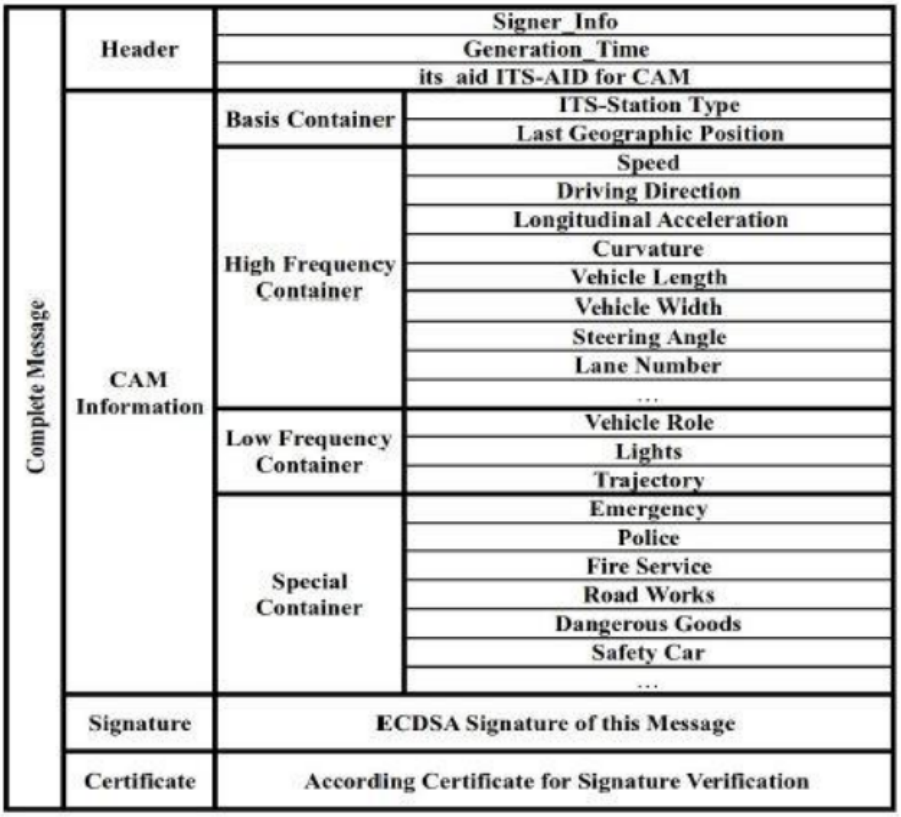

Figure 2.2: Structure of CAM. Figure is taken from [39]

2.5 Vehicular Communication Standards

As the research of the vehicular communication systems are pushing forward, the proposed standards that follows it is also developing to set guidelines and make sure that researchers are on the same page. The current proposed standards of how a CAM is structured and example of what information it contains can be found in the paper [39]. The currently proposed standard say that CAMs should be signed using Elliptic Curve Digital Signature Algorithm (ECDSA) and the signature type is the ANSI X9.62 Prime 256v1 curve [32] [12]. The security operations are done by a Hardware Security Module (HSM) that

is tamper proof such that other components of the system will not be able to access secret information, such as the key pairs [3].

2.6 Baseline Scheme (BS)

With the addition of a group signature scheme and a GM, it is possible for a vehicle to create pseudonyms on its own whenever it has to. This simple scheme is refereed to as the Baseline Scheme (BS) and it is used as a reference to compare our solution with.

In the BS, vehicles that cannot acquire new pseudonyms, from the PCA, instead generate their own self-signed pseudonyms with a self-determined lifetime, i.e. using Hybrid scheme. A vehicle's self-signed pseudonyms will look different from the other vehicles' pseudonyms and therefore the vehicle's CAMs can be distinguished from the others' CAMs and the vehicle could be tracked. The vehicle is now a valid member of the system and other vehicles will successfully verify that vehicle's CAMs, but the syntactic linking protection is gone.

Since the pseudonyms are not issued by the PCA, they do not follow the policies of the PCA and therefore have different lifetimes, even compared to other self-signed pseudonyms. This leads to easy pseudonym linking based on timing information.

Chapter 3

Security and Privacy Requirements

3.1 Security Requirements

For the vehicular communication system to be secure, all messages are required to have authenticity, such that it is possible to verify that the entity that created the message is a part of the system, and integrity, to make sure that messages where not altered on the way, and also non-repudiation, meaning that an entity is not able to deny having sent a message. If all these requirements are met, then the messages in the system can be trusted and their origin proven (For more details see [4]). When a vehicle interacts with the security infrastructure of the system, the messages must also be confidential. If adversaries could read the messages containing the pseudonyms, that are sent to a vehicle from the PCA, it is trivial to link them when used.

Vehicles should not be able to have multiple valid pseudonyms at a single point in time. If this is the case, misbehaving vehicle could pose as several entities and abuse protocols, e.g. Sybil attacks [33]. In some protocols, e.g. [17], vehicles can use voting to recommend revoking a vehicle. By posing as several identities, a vehicle could vote several times. These protocols might not require the physical presence of the vehicle. Since the votes are sent to the infrastructure, it might not be possible to use sensors to confirm its existence. An adversary should also not be able to launch a Denial of Service (DoS) attack by clogging the network with legitimate-looking traffic. Whenever a misbehaving vehicle is found, it needs to be evicted from the system such that it

cannot continue to cause harm.

3.2 Privacy Requirements

A single VPKI entity should not be able to fully disclose the real identity of a vehicle and track it for a long time by linking the pseudonyms from different pseudonym requests.

Semantic linking is disregarded here since it is a separate problem from what this thesis seeks to solve. It is however a known issue that eventually needs to be addressed for the vehicular communication system to be entirely privacy preserving.

The privacy metric in this thesis is defined as the ability to link two subsequent pseudonyms to the same vehicle, but not which vehicle. Low privacy means that it is easy, e.g. have a high probability, to link the pseudonyms and the vehicle is therefore easily trackable by an adversary using syntactic linking. This would be the case if the content of the pseudonyms belonging to a single vehicle is different such that it is easy to single them out from the rest.

High privacy means that the probability to link is low, this is the case when the pseudonyms look like the pseudonyms of the other vehicles such that an adversary would have to guess with a low probability of guessing correctly. For a vehicular communication system, the privacy of the pseudonyms must be acceptably high.

There is no clear threshold and the privacy, i.e. probability of linking, will be different in every situation. It depends on the amount of neighbors in the area and also the amount of disconnected vehicles.

3.3 Adversarial Model

An adversary is defined as an entity that is trying to abuse the system for its own benefit or track a vehicle by linking pseudonyms to the same vehicle. The adversary is assumed to be eavesdropping the system. By doing this it acquires a list of all the pseudonyms in a pseudonym lifetime. The adversary then tries to link a pseudonym from one lifetime to a pseudonym in the next lifetime using syntactic linking. The adversary is assumed to be knowledgeable about the system and picks the two pseudonyms that are most likely to belong to the same vehicle. If there are several pseudonyms that are equally

probable, the adversary picks one of them at random and tries to link them.

An adversary could try to utilize a Sybil-based attack [33] by creating several self-signed pseudonyms and abusing the system by posing as several vehicles. An adversary could also attack the PCA with a Denial of Service attack, thus hindering vehicles from acquiring pseudonyms. This problem is solved by the solution introduced in chapter 4.

3.4 Assumptions

Some assumptions have been made about the system, such as the assumption that every vehicle is from the region it is currently in. The size of a region is not defined and as such, the region could be arbitrary large. For the sake of argument and visualization, a country such as Sweden could be divided into regions based on provinces. Under that assumption, most vehicles will stay within their region for a longer time. Vehicles from other regions, e.g. foreign vehicles, do not have preinstalled group keys to use in that region. It is possible to use a group signature system where vehicles can dynamically join the group when entering a region [23].

For this thesis, vehicles are assumed to refill their pseudonyms a few times whenever the vehicle is in use, e.g. the system is an on-demand system as in [16] [18]. If the destination is known by the vehicle, the vehicle could request pseudonyms for several Γ periods by sending multiple requests at the same time. Otherwise, the vehicle sends a new request each Γ. The reason is to increase efficiency by lower the amount of pseudonyms that are never used since they cost processing power and memory as well. For such frequent VPKI interaction, availability is of high importance.

Pseudonym updates, i.e. changing pseudonyms every τ, are assumed to be short-lived, e.g. 1-5 minutes. Having frequent pseudonym updates is important when evaluating the performance of the scheme. The most overhead happens when validating pseudonyms, if updates only happens every 10 minutes or so, the overhead would pale in comparison.

Furthermore, the vehicles are equipped with a HSM [3] to make sure that cryptographic keys are protected and only one pseudonym

is active at any point in time. Without it, a vehicle could be able to utilize multiple pseudonyms at once.

Chapter 4

Solution Design: Rhythm

Γ	Time period between pseudonym requests.
τ	Lifetime of a single Pseudonym.
$\mathbf{V_{GS}}$	"Vehicle Group Signature", vehicle that only has self-signed pseudonyms.
$\mathbf{V_R}$	"Vehicle Rhythm", vehicle that uses the designed Rhythm protocol to support neighboring vehicles V_{GS}.
self-signed pseudonym	A self generated pseudonym that is signed with the vehicle's group signature key.
VPKI Pseudonym	A pseudonym that is issued and signed by a PCA in the VPKI.
R	R is a number, $0 \leq R \leq 1$. A threshold for whether or not to use self-signed pseudonym.

4.1 High-level Design

We propose Rhythm, "Randomized Hybrid scheme To Hide in a Mobile crowd". It allows vehicles to operate in the communication system with privacy preserving pseudonyms. If a vehicle runs out of pseudonyms and is not able to acquire new pseudonyms from the PCA, we call this vehicle V_{GS}, it can use the self-signed pseudonyms to preserve its membership in the system, e.g. [14] [15]. However, there is a distinct difference between pseudonyms signed by the PCA and pseudonyms signed with a group signature. If only V_{GS} uses self-signed pseudonyms, it would stand out because the signature of the pseudonyms generated by V_{GS} is different from signatures from

the PCA. Because of this difference, its pseudonyms are easily linkable to the V_{GS} vehicle. Also, the self-signed scheme does not have synchronized pseudonym lifetimes with the VPKI pseudonyms, i.e. pseudonym issued by the PCA. If another vehicle decides to help, by switching to self-signed pseudonyms, the pseudonyms belonging to V_{GS} might be harder to link. However, the other vehicle would lose privacy by switching entirely to a pseudonym type that is easier to link. Therefore, vehicles would be reluctant to help. Furthermore, having every vehicle in a city switch to self-signed pseudonyms to hide one vehicle is not a realistic option. To solve this problem, the protocol Rhythm is presented in this thesis, Rhythm allows vehicles, i.e. V_{GS}, to hide with the help of neighboring vehicles, called V_R, in a crowd of vehicles. Rhythm allows neighboring vehicles to hide V_{GS} without compromising their own privacy by balancing the usage of self-signed pseudonyms and VPKI pseudonyms in a way that does not increase the probability of linking the pseudonyms belonging to V_R.

4.2 Rhythm Operation

The lifetime policy for the VPKI pseudonyms is fixed and decided by the PCA. The lifetime is decided such that every vehicle, using VPKI pseudonyms, changes its VPKI pseudonyms at the same time as described in chapter 2 and the paper [16].

In Rhythm, vehicles would not compromise their own privacy for helping the vehicles in need. Rhythm achieves this by blurring the line between the two sets (those using VPKI pseudonyms and those using self-signed pseudonyms). The first proposed adjustment in the Rhythm protocol is to align the lifetimes of the self-signed pseudonyms with the VPKI pseudonyms. The lifetimes of the VPKI pseudonyms are fixed and decided beforehand by the PCA, any vehicle would be able to acquire this information without requiring a connection to the PCA. Whenever a vehicle needs to create a new self-signed pseudonym, the vehicle looks at the time for which the last pseudonym expired and apply the same lifetime from that point. This way, it becomes harder to link self-signed pseudonyms with other self-signed pseudonyms since they are all synchronized. In the case that the vehicle does not have an old pseudonym to look at, the information can be found in the neighbors' pseudonyms as well.

However, pseudonyms will still be divided into two sets, one which uses self-signed pseudonyms and one which uses VPKI pseudonyms. Therefore the next proposal in the Rhythm protocol is to interleave the two sets using randomization. This is accomplished by the following actions.

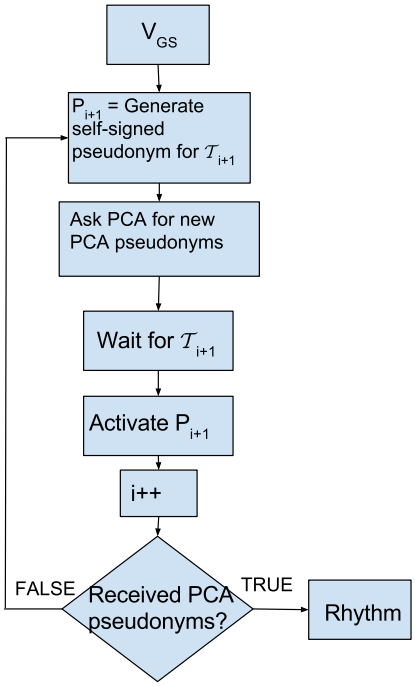

Figure 4.1: Flowchart of a vehicle unable to use VPKI pseudonyms

Vehicle using Group Signatures (V_{GS})

V_{GS} is a vehicle without VPKI pseudonyms and therefore needs to rely on self-signed pseudonyms using group signature. Whenever vehicle V_{GS} is unable to acquire pseudonyms for the next Γ. In order to stay anonymous in the system, it does the following:

1. Asking neighboring vehicles to initialize the Rhythm protocol, V_{GS} includes a field "Rhythm" in its upcoming CAM to inform other vehicles that *"There is a vehicle that does not have pseudonyms for the next Γ, i.e. pseudonym request period*, you should switch to using Rhythm in that period."

2. V_{GS} continuously tries to connect to the PCA to acquire pseudonyms for that Γ as well as the next.
3. V_{GS} uses self-signed pseudonyms until it acquires new pseudonyms from the PCA. It then continues as a V_R vehicle for the rest of the Γ.

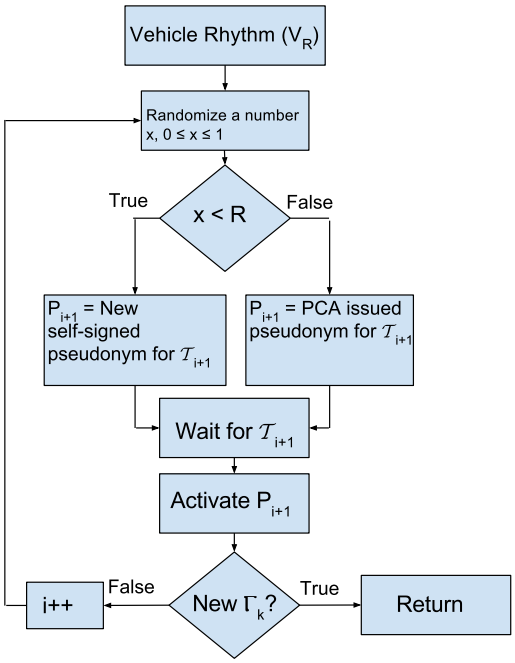

Figure 4.2: Flowchart of a vehicle using the Rhythm protocol

Vehicle Rhythm (V_R)

V_R is a vehicle with VPKI pseudonyms but helping to preserve the privacy of V_{GS} by randomly opting to use self-signed pseudonyms based on the probability R. Neighboring vehicles V_R receives the CAM sent by V_{GS} and does the following:

1. Verify incoming CAM. Include the same section "Rhythm" in the next CAM.
2. Randomize a number x between 0 and 1, if x is less than R, create a self-signed pseudonym to use as the first pseudonym in the next Γ.

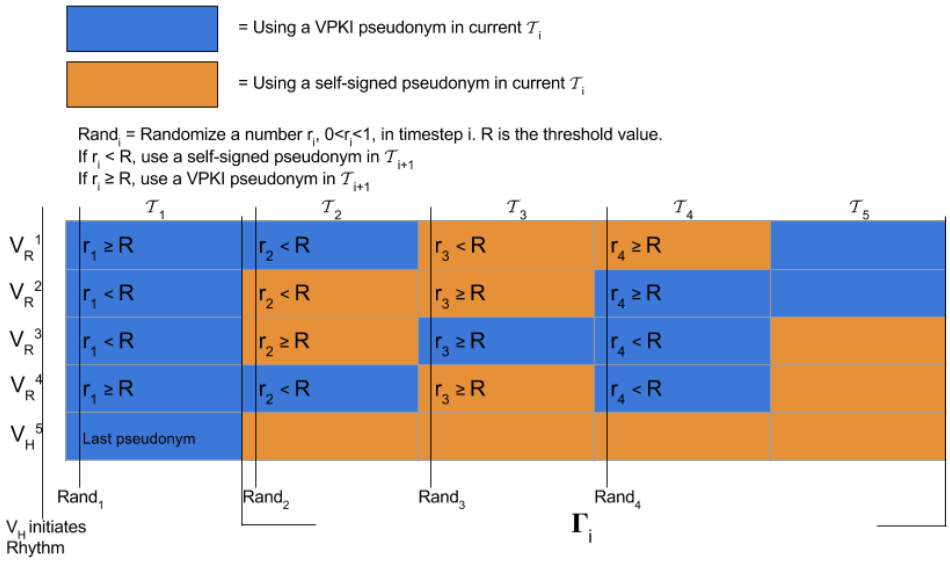

Figure 4.3: Visualization of Rhythm using 5 vehicles. V_H runs out of pseudonym and initiates Rhythm for the next time interval Γ_i.

3. At the start of every pseudonym lifetime, τ_i, in the next Γ, randomize a new x between 0 and 1.
   (a) If x is less than R, V_R creates a self-signed pseudonym to use in the τ_{i+1} time slot.
   (b) If x is equal to or higher than R, V_R uses its VPKI pseudonym in the τ_{i+1} time slot.
4. If a new CAM is received with the section "Rhythm" at the end of the current Γ, then do the same in the next Γ as well.

If a vehicle is starting to receive self-signed pseudonyms in the middle of the Γ, it can switch to become a V_R for the rest of the Γ.

When eavesdropping the communication during Rhythm, an average of 50% of the V_R vehicles, using Rhythm with $R = 0.5$, will be using self-signed pseudonyms in every τ_i alongside the V_{GS} vehicles. This will greatly decrease the linkability of the V_{GS} vehicles, thus increasing their syntactic linking protection.

As an example, let's say that there are 5 vehicles in the neighborhood as in figure 4.3. V_{GS} would only use self-signed pseudonyms and can therefore be linkable to an average of 3 other pseudonyms in any τ_i. The probability of linking V_{GS} is $\frac{1}{3}$ since it could be any one of

the 3 vehicles using self-signed pseudonyms. Every other vehicle (V_R) could have either a VPKI pseudonym or a self-signed pseudonym at any given τ_i. Since the randomization is independent and the vehicle itself is the only one that knows if it uses a self-signed or VPKI pseudonym, any of the 5 pseudonyms could belong to a V_R vehicle. If the VPKI is unreachable, there might be more than one vehicle that runs out of pseudonyms. In such a case, the optimal value of R will be different.

4.2.1 Determination of R

If there are N VPKI pseudonyms and M self-signed pseudonyms in the current τ, the probability of linking a V_R pseudonym in the former τ to a VPKI pseudonym in the current τ would be $\frac{1}{N} \times (1 - R)$ and the probability of linking a V_R pseudonym to a self-signed pseudonym would be $\frac{1}{M} \times R$. In order to achieve a probability of $\frac{1}{(N+M)}$, which would be the optimal goal, R must represent the actual resulting sets of N and M. However, one problem is that not all vehicles would use R since some of them will not have VPKI pseudonyms and always use self-signed ones, i.e the V_{GS} vehicles.

Using self-signed pseudonyms is computational expensive in comparison to VPKI pseudonyms for the entire system. The reason for this is that signing and verifying signatures using the group signature is much more expensive than the algorithm used by the VPKI, which is ECDSA. Therefore, the value of R have to take this overhead into consideration. The system needs to minimize the cost while providing acceptable protection against syntactic linking. If M is already quite large, it would be sufficient with a small contribution from the vehicles in N to get a decent protection level. The optimal choice of R is left as future work.

Chapter 5

Security and Privacy Analysis

5.1 Security Analysis

Some of the security requirements are supported directly by the VPKI [3] [4] [5]. A PKI is a system design that ensures confidentiality, integrity, and authenticity between trusted hosts through the use of asymmetric cryptography. Asymmetric cryptography means that there are two different keys used for encrypting and decrypting a message, in comparison to symmetric cryptography which would use the same key for both encryption and decryption. Every host in the PKI would therefore have two keys, one key called "public key" that is easily obtainable by everyone, and one key called "private key" that is only known by that particular host.

Confidentiality is achieved by the VPKI through TLS encryption. Only the messages to the security infrastructure, such as the PCA, requires confidentiality. CAMs are not confidential, and therefore not encrypted, since they are supposed to be read by everyone. A symmetric key is established between the two entities, e.g. using Diffie-Hellman key exchange [21], when required. Afterwards, messages are sent using symmetric encryption, e.g. AES-encryption. Using asymmetric encryption with the real identity credentials, i.e. LTC, is not a good option, partly because revealing those to the PCA is a privacy risk, but also because encrypting such a long message takes a lot of time for asymmetric encryption systems. When sending several pseudonyms to a vehicle, the asymmetric encryption becomes inefficient in comparison.

Integrity means that there is a way to discover if the messages have

been altered by a third party before arriving at the receiver. This property is supported by the VPKI system through signatures. Before sending a message, the sender hashes the message and then encrypt the hash value with its private key. The receiver can then decrypt the hash value from the sender with the sender's public key and compare it with its own hashed version of the message using the same hash algorithm. If the two hash values are equal, the content of the message is the same as when it was signed by the sender.

This would also prove authenticity since the sender's public key is used to decrypt the hash value, meaning that it could only have been encrypted by the sender's private key which is only known by the sender. This is close but not enough to be sure of the authenticity of the message. The thing that is missing is proving the connection between the senders identity and the key pair that is used to ensure that the sender is a trusted member in the system. When broadcasting CAMs, integrity and authenticity is provided by the pseudonyms. However, pseudonyms does not reveal the LTC of the sender, only that the sender is a trusted member. In a VPKI, the privacy of the members are protected by using pseudonyms instead of their LTC.

Certificates and pseudonyms are used to prove the ownership of a public key. They are a testament of the connection between a trusted host in the system and that host's public key. The LTC has a signature from the LTCA, which proves its authenticity and makes the host trustworthy, since the LTCA is trusted. In the same way, pseudonyms are trusted because of the PCA signature or group signature they have. As long as the pseudonym or certificate of a host is valid, that host is a trusted member of the system. The use of a certificate is quite useful in a PKI because it gives the VPKI a few ways to exclude the host from the system if needed, e.g. if the host is a malicious user.

When validating a certificate or pseudonym in the system, there are three different things to consider, the first thing to check is the signature. This is done in the same way as with a message, by using the singer's public key to decrypt the hash value and then compare it to its own hashed version of the certificate or pseudonym. The second thing to do is to check that the lifetime of the certificate or pseudonym has not expired. Every certificate has an expiration date to make sure that it is not valid forever. The third thing to check is that it is not in the Revocation List (RL). If a member misbehaves, its certificate or pseudonyms can get revoked before the time has expired to exclude

that member from the system. This is done by adding it to a RL. If a certificate is in the RL it is not considered valid anymore. Whenever a host receives a message from another host in the system, the messages will only be considered by the receiver if the sender's certificate or pseudonym is valid. It is not possible to send a message on someone else's behalf because the private key is kept secret by every vehicle. The RA can link the pseudonym of a member to its LTC, by interacting with the LTCA, PCA, and GM, and thus find and revoke the owner. The certificate or pseudonym proves who the sender is and therefore the system have non-repudiation, i.e., a sender cannot deny having sent a message. This is important when trying to revoke a misbehaving vehicle, since the vehicle cannot deny what it has done.

Sybil-based attacks cannot be used by an adversary in order to abuse the system in different ways. By introducing self-signed pseudonyms, adversaries could potentially create several pseudonyms at the same time and act like different vehicles. This can be negated by allowing only one verifiable signature to be produced at the same time. Some group signature schemes can restrict the number of valid signatures a member can use at the same time [20]. In the current version, Sybil attacks is thwarted using the Hardware Security Module (HSM) to make sure that the vehicle only have one valid pseudonym at a time [3]. The HSM handles the cryptographic operations on the On-Board Unit and is considered to be tamper-proof.

An adversary could potentially try to overload the system by repeatedly initiate the Rhythm protocol, thus increasing the network load by having all neighbors utilizing as much self-signed pseudonyms as possible. The extra overhead from Rhythm only occurs when vehicles are using self-signed pseudonyms. Rhythm is designed such that every vehicle can confirm the connection to the PCA before deciding to trust the vehicle that claims to have no connection. A vehicle could ping the PCA or ask for a status report. If the PCA is up and running, vehicles could either ignore that vehicle or use Rhythm with a low R and no harm has been done. If some vehicles cannot connect to the PCA or the status shows that the PCA is having problems, they can propagate the initialization query and choose the R value to be appropriate such that the system can handle the overhead. This would make the initiation more believable for other vehicles as well.

VPKI entities, e.g. the LTCA, PCA, GM, might also try to track the

vehicles. They might even have a higher chance of success. However, the separation of functionality in the VPKI is done so that the LTCA and PCA cannot disclose all information about a vehicle on their own. A PCA can trace a vehicle since it issued the pseudonyms to that vehicle. However, it can not disclose the real identity of the vehicle and it can not link pseudonym requests to the same vehicle. If a vehicle asks for new pseudonym every Γ, it will only be able to track the vehicle until the end of that Γ. The interaction with the GM is done so that the GM does not know the real identity of the vehicles either. By alternating between self-signed and PCA issued pseudonyms, neither the PCA or the GM can fully link the pseudonyms used by a vehicle the same way it can be done in the Baseline Scheme.

5.1.1 Safety Mechanism

Old CAMs from other vehicles usually do not need to be tracked since all the information needed is present in the latest CAM. However, in some cases a safety protocol might need to keep track of a vehicle's CAMs up to a few seconds to avoid an accident. If two vehicles are about to collide, such that the safety protocol is activated, it might be dangerous if the vehicles need to change their pseudonyms. However, vehicles could discard their privacy for safety reason by signing the next CAMs with both the old and the new pseudonyms, thus purposely link their two pseudonyms. Since safety is of higher priority than privacy, this is considered an acceptable solution [18].

5.2 Privacy

Rhythm is compared to the case when some vehicles are only using self-signed pseudonyms, and the rest are using VPKI pseudonyms. This situation is referred to as the baseline.

For the baseline scheme, the self-signed pseudonyms are not timely aligned since this is a property introduced in the Rhythm scheme. Baseline gives every V_{GS} a probabilistic syntactic linkability equal to the number of V_{GS} vehicles that changes pseudonym simultaneously. Every V_R vehicle have a probabilistic syntactic linkability equal to the number of V_R vehicles since those all change simultaneously. That is, the vehicles are separated into two distinct sets, with V_R most likely being the bigger set. Rhythm would give every V_{GS} lower syntactic

linkability, by aligning their pseudonyms and by having some V_R vehicles joining the self-signed pseudonym set, thus increasing the set size, without sacrificing their own syntactic linkability since it is hard to know which vehicles joined in a given pseudonym lifetime. This makes V_R vehicles more willing to cooperate. Foreign vehicles (vehicles from other regions) are not able to use the group signature of this region and can therefore not create self-signed pseudonyms in this region. Foreign vehicles are therefore in the V_R set all the time and if a foreign vehicle is unable to connect to the PCA, it is unable to participate in the system. How to have foreign vehicles join the group and utilize self-signed pseudonym is left as future work.

In figure 5.1, we can see an example of the result when eavesdropping an area that uses the baseline in comparison to Rhythm.

When using the baseline scheme, there are some problems that makes it a bad solution. The set M, which is the set of vehicles unable to use VPKI pseudonyms, is clearly visible. These vehicles have a syntactic linkability of at least $\frac{1}{|M|}$, however, since the pseudonym switches are not coordinated, it is most likely higher.

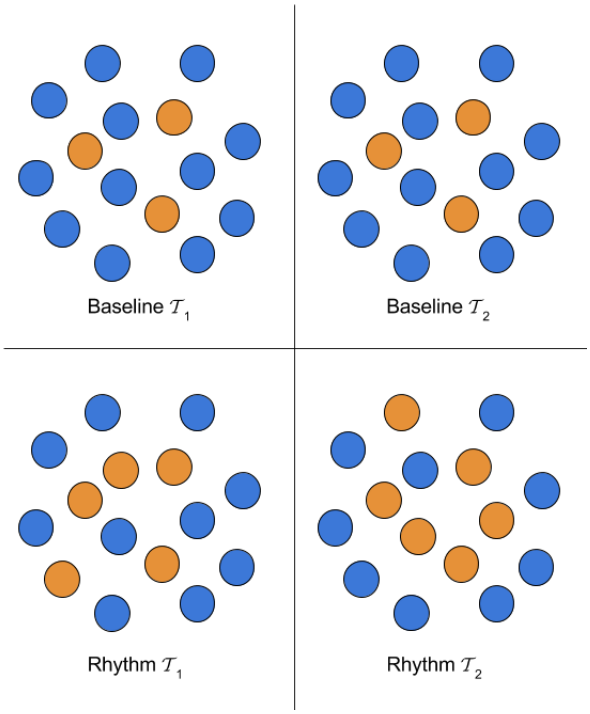

Figure 5.1: Visualization of baseline vs Rhythm

However, when using Rhythm, this is what happens: The exact number of vehicles in the M set is hidden by allowing some V_R vehicles to utilize self-signed pseudonyms and thus increases the number of vehicles that are indistinguishable from the set M. The syntactic linkability of vehicles in the M set becomes $\frac{1}{|M|+x}$, where x is the number of V_R vehicles that utilized self-signed pseudonym in that time slot. The result is that syntactic linking is protected to a higher level.

If a region have multiple PCAs, the V_R vehicles would be divided into separate pseudonym sets because the signatures from the PCAs would be different. This would be the same whether or not Rhythm is used and the analysis would hold for each set.

5.3 Quantitative Analysis

When trying to link two consecutive pseudonyms to the same vehicle, an optimal adversary should pick two pseudonyms from the same pseudonym set. That means, if the adversary wishes to link a VPKI pseudonym, the adversary should try to link it to another VPKI pseudonym. The reason for this is that the size of the resulting VPKI set is only dependent on the value of R. If the average size of that set is notated as $|VPKI|$, the probability of linking to one of those pseudonyms is $\frac{1}{|VPKI|} \times (1 - R)$, since $(1 - R)$ is the probability of the pseudonym to be in that set.

The probability of linking from a VPKI pseudonym to a self-signed pseudonym is $\frac{1}{|self\text{-}signed|} \times R$. However, the average set size, $|self\text{-}signed|$, is not only dependent on R, but on the total number of vehicles that uses self-signed pseudonyms, including V_{GS} vehicles. Let us say that the set size of vehicles that have VPKI pseudonyms and uses Rhythm is notated as $|Rhythm|$ and the set size of those vehicles without VPKI pseudonyms is notated as $|M|$. The set size $|VPKI|$ is equal to $|Rhythm| \times (1 - R)$, and the probability of linking a VPKI pseudonym to a VPKI pseudonym, i.e. P_{V2V}, is

$$P_{\text{V2V}} = \frac{1}{|Rhythm| \times (1 - R)} \times (1 - R) = \frac{1}{|Rhythm|} \tag{5.1}$$

The set size $|self\text{-}signed|$ is equal to $(|Rhythm| \times R) + |M|$. Therefore, the probability of linking VPKI-to-Self-signed, i.e. P_{V2S}, is

$$P_{\text{V2S}} = \frac{1}{(|Rhythm| \times R) + |M|} \times R = \frac{1}{|Rhythm| + \frac{|M|}{R}} \tag{5.2}$$

since $\frac{|M|}{R} > 0$, it results in

$$P_{\text{V2S}} < P_{\text{V2V}} \tag{5.3}$$

This shows that when trying to link a VPKI pseudonym, the proba-

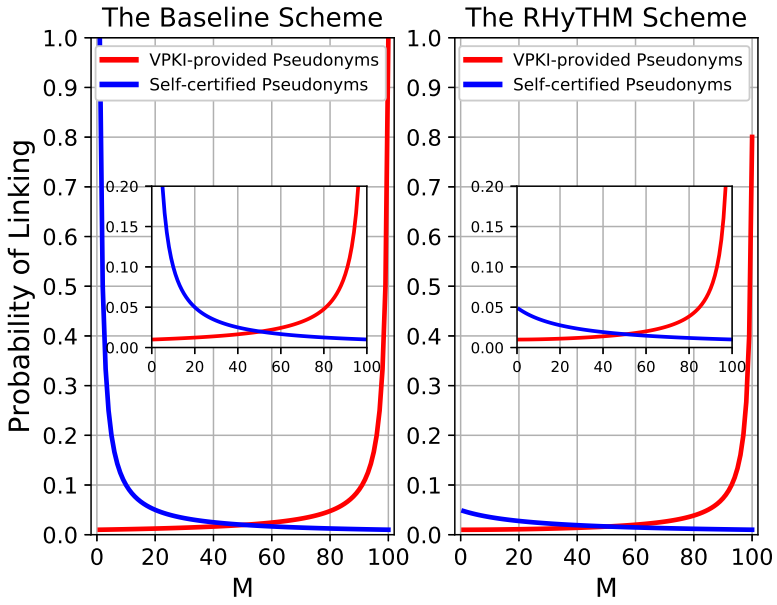

Figure 5.2: This figure shows the probability of linking when using Rhythm compared with the Baseline depending on how many vehicles do not have VPKI pseudonyms (M). (R = 0.2)

bility of linking is higher when linking it to another VPKI pseudonym rather than to a self-signed pseudonym.

When linking a self-signed pseudonym, the probability of linking it to another self-signed pseudonym is higher since there is a probability that the pseudonym belongs to the set M, i.e. a vehicle that does not possess a VPKI pseudonym. If that is the case there is a 100% change of it being in the self-signed set again in the next τ. The probability of being one of those vehicles is $\frac{|M|}{|self\text{-}signed|}$ and the probability of finding that pseudonym in the next τ is $\frac{1}{|self\text{-}signed|}$. The probability of the pseudonym belonging to a vehicle that might switch to a VPKI pseudonym in the next τ is $\frac{|self\text{-}signed|-|M|}{|self\text{-}signed|}$ and the probability of finding it in the next τ is $\frac{1}{|self\text{-}signed|} \times R$. The total probability of linking a self-signed pseudonym to another self-signed pseudonym, i.e. P_{S2S}, is

$$P_{S2S} = \frac{|M|}{|self\text{-}signed|^2} + \frac{|self\text{-}signed| - |M|}{|self\text{-}signed|^2} \times R \tag{5.4}$$

When linking from a self-signed pseudonym to a VPKI pseudonym, only the case where the pseudonym belong to a vehicle

using Rhythm needs to be considered and thus the probability is

$$P_{\text{S2V}} = \frac{|self\text{-}signed| - |M|}{|self\text{-}signed|} \times \frac{1}{|VPKI|} \times (1 - R) = \frac{1}{|Rhythm| + \frac{|M|}{R}}. \tag{5.5}$$

To show that $P_{\text{S2V}} < P_{\text{S2S}}$, the following equation is constructed

$$\frac{1}{|Rhythm| + \frac{|M|}{R}} < \frac{|M|}{|self\text{-}signed|^2} + \frac{|self\text{-}signed| - |M|}{|self\text{-}signed|^2} \times R \tag{5.6}$$

and by substituting $|self\text{-}signed|$ with $(|Rhythm| \times R + |M|)$ and simplifying the equation, it leads to

$$(|Rhythm| \times R + |M|)^2 < (|M| + |Rhythm| \times R^2) \times (|Rhythm| + \frac{|M|}{R}). \tag{5.7}$$

Finally it results in

$$|Rhythm| \times R + |M| < |Rhythm| + \frac{|M|}{R}. \tag{5.8}$$

Since $0 \leq R < 1$, because equation 5.5 does not allow $R = 1$, and both $|Rhythm|$ and $|M|$ are positive integers, $|Rhythm| \times R < |Rhythm|$ and $|M| < \frac{|M|}{R}$. Therefore, equation 5.8 holds.

Figure 5.2 compares the baseline scheme with Rhythm in terms of linkability. On the x-axis we can see how many vehicles does not have VPKI pseudonyms and therefore have to rely on self-signed pseudonyms. On the y-axis we see the probability of linking two consecutive pseudonyms belonging to the same vehicle.

As mention before, the probability of finding two consecutive pseudonyms is highest when choosing them from the same set. That is, if an adversary wants to link a VPKI pseudonym, the adversary should try to link it to another VPKI pseudonym in the next pseudonym update.

Figure 5.3 shows the probability of linking pseudonyms of a vehicle that chooses not to participate in Rhythm. A seen in the figure, the probability is always higher for a vehicle that is never switching to use self-signed pseudonyms. As a result, foreign vehicles or vehicles that cheat in order to not spend the extra overhead on creating self-signed pseudonyms has a higher probability of being linked and has therefore

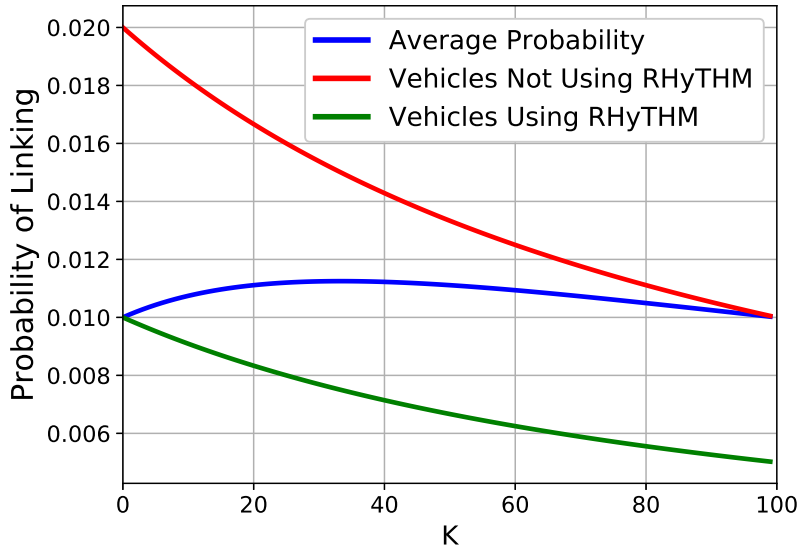

Figure 5.3: This figure shows the linkability of a vehicle that has VPKI pseudonyms and does not comply with the request of using Rhythm in order to not spend the extra processing time. The x-axis is the number of vehicles choosing not to use Rhythm. The total number of vehicles in the neighborhood is 100.

a lower syntactic linking protection.

This shows that an optimal adversary would choose another pseudonym of the same kind when trying to link two pseudonyms together. Equations 5.1 and 5.2 shows that the linkability does not increase when a V_R vehicle uses Rhythm. In fact, equation 5.2 shows that the linkability of a V_R vehicle decreases when switching to a self-signed pseudonym.

Chapter 6

Performance Evaluation

6.1 Implementation

The implementation was done in C to have a high speed as it is highly time sensitive. Table 6.1 shows the specifications of the hardware boxes used for implementation and testing of the scheme.

Table 6.1: NexCom Specifications

	NexCom
Number of boxes	9
Dual-core CPU (Ghz)	1.66
BogoMips	3333.36
Memory	1GB

To follow the proposed standards in vehicle communication systems and especially for the CAMs that have been decided in [39], the libraries that was used in the implementation was OpenSSL [37] and Pairings_in_C [36]. The proposal for the standard in vehicular communication states that the type of signatures used to sign CAMs have to be ECDSA [32] of the type ANSI X9.62 Prime 256v1 curve. The same signature type is used by the PCA for the signature on the pseudonyms. OpenSSL contains this type of signature. Because of the limited amount of boxes available, some of them sent more CAMs per second in order to emulate a larger neighborhood.

For the group signature on the self-signed pseudonyms, the group signature system invented by Boneh et.al in [22] was used. One of the reason it was selected was because in their paper, they specif-

ically referenced vehicular communication as a motivation for their work. Since the focus of this thesis is not to find the perfect group signature system to use, this system seemed decent enough. There are other papers, e.g. [38], that have focused more on comparing group signatures for vehicular communication which has also included this specific scheme by Boneh et.al. However, their implementation was in JAVA and also used different hardware to do the comparison on. Therefore their specific results of the same system is not comparable to the result for this project, but the systems relations to other group signature systems should be similar.

In the library Pairings_in_C, there is an implementation of this particular scheme in C that was used. However, this library was only capable of producing signatures of length 252 bytes and 396 bytes. The authors of this group signature scheme, i.e. [22], claims that the security level of the scheme is about the same as a RSA signature with the same signature length. This would argue that the security level of this group signature scheme is around 110-bit. Although more bytes would have a higher security level, the reason for the length is to limit computation cost and the amount of traffic in the network even on the cost of better security. It is therefore deemed appropriate to use the 252 bytes version for this work as a reference for signing and verifying pseudonyms.

One of the reasons that group signature schemes have not had much success in the vehicle communication systems is that the process of signing and verifying messages is more expensive. Both in terms of time and also in terms of memory usage. While the above group signature is 252 bytes long, ECDSA is only 72 bytes long and is more than 10 times faster.

To be able to determine if the protocol would be practical or not, different parts of the code are timed, i.e. the time it takes to generate pseudonyms, signing, and verify signatures with GS and ECDSA. However, due to time constraints and simplicity when testing, there is no reason to implement an entirely functioning system. Other papers such as [14] [15] have suggested optimizations that would make the implementation of an entire system unnecessary complicated for our purposes. Therefore it is easier to implement different parts of the code separately and then adding the timings of whichever parts are needed. An example of this would be that the pseudonym of a vehicle does not need to be verified for every CAM. If the pseudonym has

already been verified by a vehicle, that vehicle can skip the process of verifying it again.

6.2 Computational Overhead

The table below compares the processing time and features of the cryptographic operations for the ECDSA algorithm and the group signature scheme used. The timings are extracted from 5000 examples.

Operations	ECDSA	GS
Sign	Min: 0.969ms Max: 1.4ms Average: 0.977ms	Min: 55ms Max: 73ms Average: 56ms
Verify	Min: 2.323ms Max: 3.228ms Average: 2.346ms	Min: 81.789ms Max: 86.747ms Average: 82.538ms
Signature length	72 bytes	252 bytes
Security level	80-bit	110-bit[1]

The table shows the processing time required to create signatures and verify signatures. CAMs are all signed and verified using ECDSA, while pseudonyms are usually signed and verified using ECDSA, but sometimes using GS instead based on the protocol proposed. The security level measures how hard it is to break the algorithm [31].

Figure 6.1 shows the delay from starting to produce pseudonyms to the point of having 10 pseudonyms. VPKI delay is not processing time in the vehicle, but external, which means that the vehicle can spend that time doing other things. VPKI delay is measured as the time it takes from that a vehicle sends its public keys to the PCA, until the vehicle receive pseudonyms, which includes creating the pseudonyms by the PCA. The communication delay times was given to me by the NSS group. It is a part of their work for the paper [16].

When a vehicle goes from using only VPKI pseudonyms to using Rhythm, the extra overhead for that vehicle is only present when acquiring group signature pseudonyms, which would increase the privacy of that vehicle in exchange. The extra overhead for 10 pseudonyms is 422 - 135 = 287 ms. Dividing that by 10 gives 28.7 ms.

[1]This is not an exact value. It is derived from the paper of the group signature scheme[22].

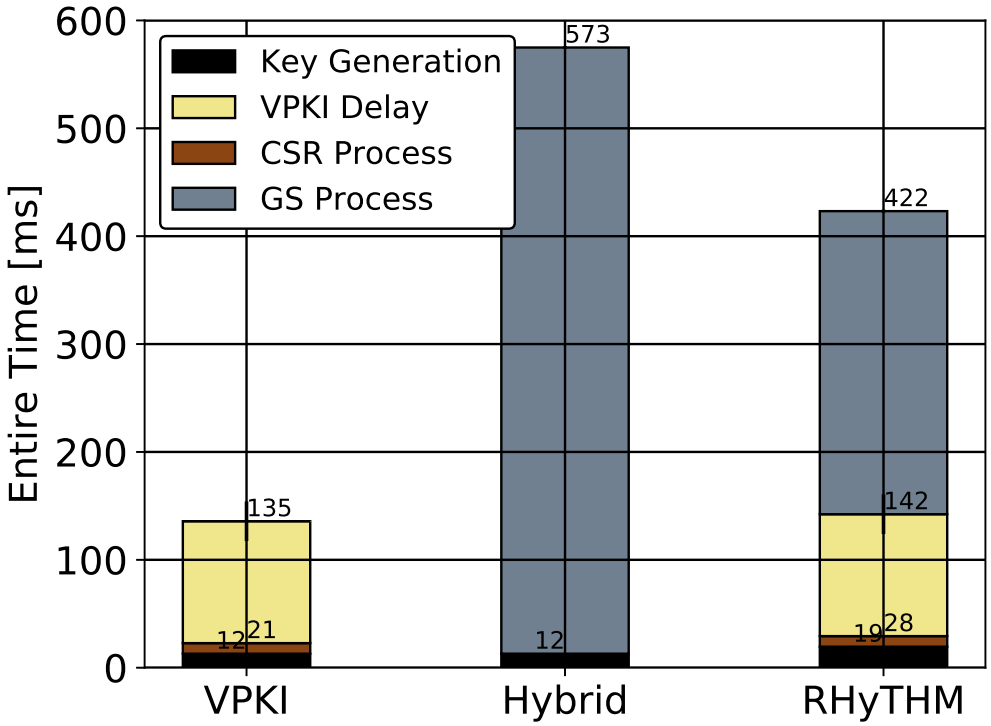

Figure 6.1: End-to-end delay of acquiring pseudonyms for 10 lifetimes. In the case of Rhythm, this means acquiring 15 pseudonyms and discarding 5 of them, when using R = 0.5.

This means that every vehicle have an average of 28.7 ms extra overhead per pseudonym when it is using Rhythm. Since the pseudonyms lifetime is at least 30 s, there is most likely enough time to spend 28.7 ms extra on a pseudonym.

Figure 6.2 shows how many neighboring vehicles a vehicle can process, including itself, each second when using different schemes. The figure shows that if every vehicle is using self-signed pseudonyms, a vehicle can handle at most about 100 neighbors. If every vehicle uses VPKI pseudonyms, which is the normal case, it can handle about 140 neighbors. Using Rhythm, it is a linear function between only self-signed and only VPKI pseudonyms, depending on the value of R. These results are calculated when each vehicle sends 3 CAMs every second and has a pseudonym lifetime of 30 second.

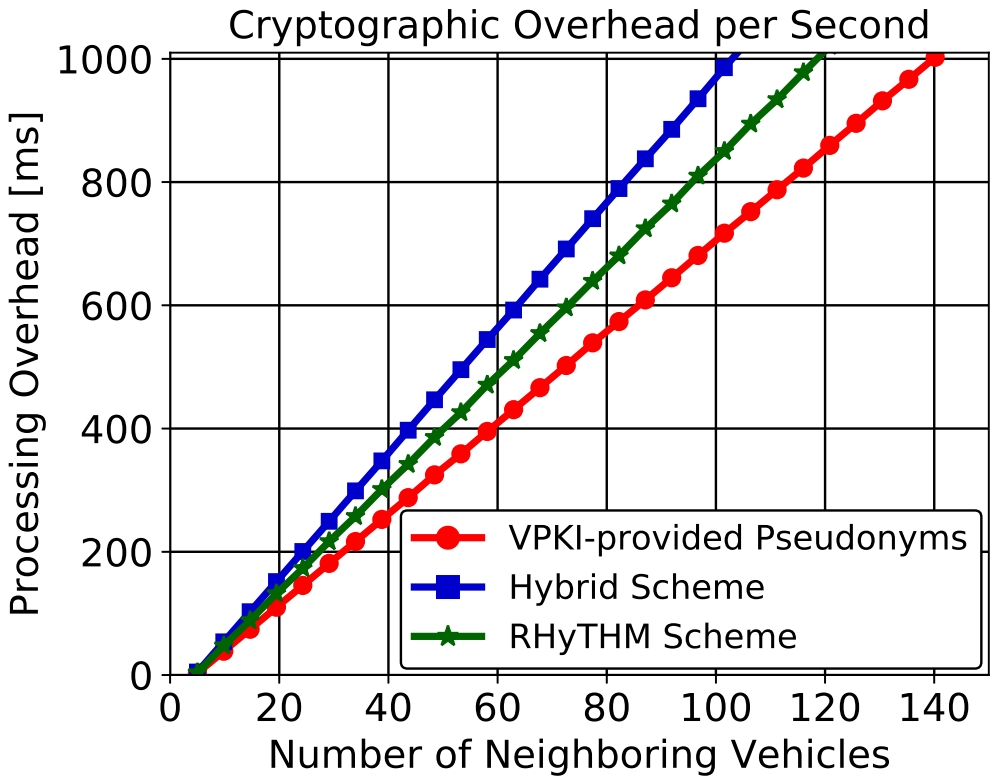

Figure 6.2: This figure shows the time it takes to process incoming CAMs, sending outgoing CAMs, verifying pseudonyms, creating self-signed pseudonyms as a function of the number of neighbors each second. That is, how many neighbors a vehicle can handle each second using different schemes.

Chapter 7

Conclusions and Future Work

The conclusion is that, by using Rhythm, vehicles are able to continue to sign CAMs with privacy preserving pseudonyms, even if the PCA cannot issue pseudonyms to those vehicles. The result of this is that an adversary cannot collapse the privacy of the vehicle-to-vehicle communication on the road by targeting the VPKI with Denial of Service attacks. Vehicles are able to communicate using pseudonyms based on group signatures, i.e. using the Hybrid scheme, that do not require communication with the VPKI. The vehicles would achieve acceptable syntactic linking protection by having neighboring vehicles cooperate at the cost of extra computational overhead. The neighboring vehicles are willing to cooperate in order to preserve their own syntactic linking protection, since it would decrease if it is not cooperating while other vehicles do. It is a manageable trade off between syntactic linking protection and computational overhead on the system.

When joining Rhythm, the extra 28.7 ms computation time on average for a pseudonym seems manageable, even for a 30 seconds pseudonym lifetime, which is considered very short. The vehicles would be able to handle between 100 and 140 neighboring vehicles dependent on the value of R. The lower boundary could become even better by implementing a faster group signature scheme.

The group signature system used in this thesis have some drawbacks and other alternatives should be considered. By choosing a group signature scheme with the JOIN feature and a limit on the number of signatures created simultaneously, Rhythm could be extended to encompass foreign vehicles and an additional layer of Sybil-based attack prevention.

From an ethical point of view, Rhythm would move the vehicular communication systems one step forward towards having acceptable privacy. By offering syntactic linking protection to vehicles that are unable to acquire pseudonyms from the VPKI, the system no longer abandons the syntactic linking protection of those vehicles. Companies and individuals no longer has to rely on potentially easily linkable pseudonyms if the VPKI is unavailable, perhaps due to a Denial of Service attack by another company. This strengthens the acceptance of the communication system for companies and individuals that might want to hide the destinations of their trips. Safety and security are the higher priorities for vehicular communication systems, however, companies and individuals might not be inclined to use them if they do not offer enough privacy.

Future work should include more incentive mechanisms for joining Rhythm. A vehicle that has VPKI pseudonyms will increase its own syntactic linkability if the vehicle decides not to use Rhythm while other vehicles do use Rhythm. This might not be enough of a incentive for the vehicle to start using Rhythm. However, the cost for a single vehicle to use Rhythm is not that high for the vehicle itself. Most overhead comes from verifying group signatures rather than creating pseudonyms. More research might conclude that more incentive is necessary.

The optimality of R, which is the probability of using self-signed pseudonyms, is left as an open question. It should dynamically change with the number of neighboring vehicles and how many of them that needs help. The value R needs to take into consideration what an acceptable level of syntactic linking protection might be and balance it with the extra amount of overhead it will introduce.

Another open question that remains is how far the propagation of the initialization query should be. Whether to propagate with a decreasing value of R, propagate far with a low value of R, or propagate short with a high value of R could be dynamically decided. The propagation should adapt to different situations and is highly dependent on the number of vehicles in the neighborhood.

Bibliography

[1] M. Khodaei, A. Messing, P. Papadimitratos, "RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile-crowd", IEEE Vehicular Networking Conference, Torino, Italy, November 2017.

[2] P. Papadimitratos, A. de La Fortelle, K. Evenssen, R. Brignolo, S. Cosenza, "Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation", in IEEE Communications Magazine, Vol. 47, pp 84-95, November 2009.

[3] T. Leinmuller, L. Buttyan, J-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch, "SEVECOM - Secure Vehicle Communication", IST Mobile and Wireless Communication Summit. No. LCA-POSTER-2008-005. 2006.

[4] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing Vehicular Communications - Assumptions, Requirements, and Principles," Workshop on Embedded Security in Cars (ESCAR), No. LCA-CONF-2006-021. 2006.

[5] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communication Systems: Design and Architecture," IEEE Communications Magazine, November 2008.

[6] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for Secure and Private Vehicular Communications", in IEEE International Conference on ITS Telecommunications (IEEE ITST), Sophia Antipolis, France, June 2007, pp. 1-6.

[7] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, P. Papadimitratos, "VeSPA: Vehicular Security and Privacy-preserving Architecture" in HotWiSec '13 Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy, Budapest, Hungary, pp. 19-24, April 19, 2013.

[8] M. Khodaei, H. Jin, and P. Papadimitratos, "Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure," IEEE Vehicular Networks Conference (IEEE VNC), Paderborn, Germany, December 2014.

[9] M. Khodaei and P. Papadimitratos, "The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems," IEEE Vehicular Technology Magazine, Vol. 10, No. 4, pp. 63 - 69, December 2015.

[10] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn. "A security credential management system for V2V communications". In 2013 IEEE Vehicular Networking Conference, Boston, MA, USA, December 16-18, 2013. 1–8. https://doi.org/10.1109/VNC.2013.6737583

[11] V. Kumar, J. Petit, and W. Whyte. "Binary hash tree based certificate access management for connected vehicles", In Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '17). 2017, ACM, New York, NY, USA, 145-155. DOI: https://doi.org/10.1145/3098243.3098257

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

[13] "Preparing Secure Vehicle-to-X Communication Systems - PRESERVE." [Online]. Available: http://www.preserve-project.eu/

[14] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "On the Performance of Secure Vehicular Communication Systems," IEEE TDSC, vol. 8, no. 6, pp. 898-912, November 2011.

[15] P. Papadimitratos, G. Calandriello, J.-P. Hubaux, and A. Lioy, "Impact of Vehicular Communications Security on Transportation Safety," in IEEE INFOCOM Mobile Networking for Vehic-

ular Environments (MOVE) Workshop (IEEE MOVE), Phoenix, AZ, USA, April 2008, pp. 1–6.

[16] M. Khodaei, H. Jin, and P. Papadimitratos, "SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems" In IEEE Transaction on Intelligent Transportation Systems, April, 2018. Online: https://arxiv.org/abs/1707.05518.

[17] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," In IEEE Journal on Selected Areas in Communications, pp. 1557–1568, October 2007.

[18] M. Khodaei and P. Papadimitratos, "Evaluating on-demand pseudonym acquisition policies in vehicular communication systems", Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet, Paderborn, Germany, July 2016.

[19] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough", Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference. Kranjska Gora, Slovenia, February 2010.

[20] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich, “How to Win the Clone Wars: Efficient Periodic n-Times Anonymous Authentication,” Proc. 13th ACM Conf. Computer and Comm. Security (CCS), Alexandria, Virginia, USA, October 2006.

[21] W. Diffie and M. Hellman. "New Directions in Cryptography". IEEE Trans- actions on Information Theory, November 1976.

[22] D. Boneh, X. Boyen, H. Shacham, "Short Group Signatures". In: Franklin M. (eds) Advances in Cryptology – CRYPTO 2004. CRYPTO 2004. Lecture Notes in Computer Science, vol 3152. Springer, Berlin, Heidelberg

[23] J. Camenisch and M. Stadler. "Efficient group signature schemes for large groups". In B. S. K. Jr., editor, Advances in Cryptology

– CRYPTO ’ 1997, volume 1294 of Lecture Notes in Computer Science, pages 410–424. International Association for Cryptologic Research, Springer, 1997.

[24] D. Chaum, E. van Heyst. "Group Signatures". In: Davies D.W. (eds) Advances in Cryptology — EUROCRYPT ’91. EUROCRYPT 1991. Lecture Notes in Computer Science, vol 547. Springer, Berlin, Heidelberg

[25] Tesla.com. Autopilot. [online] Available at: https://www.tesla.com/autopilot?redirect=no [Accessed on Oct. 2017].

[26] Google, Waymo, [online] waymo.com, Available at: https://waymo.com/ [Accessed on Oct. 2017]

[27] Evan Perez, C. (2015). "FBI: Hacker Chris Roberts claimed to hack into flights" - CNN. [online] CNN. Available at: http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html [Accessed on Oct. 2017].

[28] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, "Mix-zones for Location Privacy in Vehicular Networks" in ACM Workshop on Wireless Networking for Intelligent Transportation Systems (ACM WiN-ITS), Vancouver, British Columbia, Canada. August 2007.

[29] L. Buttyán, T. Holczer, and I. Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs" Published in ESAS 2007: Security and Privacy in Ad-hoc and Sensor Networks, pp 129-141. Cambridge, UK, July 2007.

[30] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A Practical pseudonym changing scheme for location privacy in VANETs". Vehicular Networking Conference (VNC), 2009 IEEE, Tokyo, Japan, October 2009.

[31] N. Koblitz and A. Menezes, "Pairing-Based Cryptography at High Security Levels", Cryptography and Coding 10th IMA International Conference Cirencester, UK, December 2005, p 13-36

[32] "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages",

IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), Mars, 2016.

[33] R. Douceur, “The Sybil Attack,” in ACM Peer-to-peer Systems, London, UK, Mars, 2002.

[34] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, "Secure and Privacy-Preserving Smartphone-Based Traffic Information Systems," IEEE Transactions on Intelligent Transportation Systems (IEEE ITS), vol. 16, no. 3, pp. 1428–1438, 2015.

[35] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "SPPEAR: Security and Privacy-preserving Architecture for Participatory-sensing Applications," in ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec), Oxford, United Kingdom, 2014, pp. 39–50.

[36] T. Unterluggauer, E. Wenger, R. Spreitzer, M. Werner, R. Hölbling, https://github.com/IAIK/pairings_in_c, [Accessed on Dec. 2017]

[37] OpenSSL Foundation, [online] Openssl.org. Available at: https://www.openssl.org/ [Accessed on Oct. 2017].

[38] V. Agrawal, "Performance evaluation of Group Signature schemes", Master’s Degree Project, Stockholm Sweden, December 2012.

[39] http://rondetafels.ditcm.eu/sites/default/files/images/2017.03.01_Processing_personal_data_C_ITS_context_vF.PDF

[40] "Intelligent Transport Systems (ITS), Security header and certificate formats", ETSI TS 103 097 V1.1.1, 04/2013