Efficient Management of Revoked Pseudonyms in VANETs using ID-Based Cryptography

Francisco Martín-Fernández, Pino Caballero-Gil and Cándido Caballero-Gil
Department of Computer Engineering, University of La Laguna, 38271 La Laguna, Tenerife, Spain

Keywords: Certification Revocation List, k-ary hash tree, Huffman Codes, Vehicular Ad-hoc Network.

Abstract: The management of fraudulent users of vehicular ad-hoc networks is one of the most important security issues of these mobile networks. It is necessary to prevent the access of malicious users to the network so that they cannot send false information to other users. This paper defines a new method for managing revoked users, using identity-based authentication, what allows improving both efficiency and security through certificateless authentication. The presented proposal optimizes the performance of classical revocation lists by building a data structure based on two concepts: an authenticated dynamic hash k-ary tree, and the frequency with which revoked pseudonyms are queried. Thus, revoked pseudonyms that are more frequently queried have a higher level in the tree. This provides a better match to urban environments, where there are some types of vehicles that spend more time on the road due to their work tasks.

SCIENCE AND TECHNOLOGY PUBLICATIONS

1 INTRODUCTION

Protecting information security on a wireless network is one of the hardest and most important tasks in our technological world. Regarding security, a key aspect is user authentication because authenticating users securely and quickly is a fundamental requirement in wireless networks. The complexity of this problem increases significantly if network nodes are able to move. Therefore, the authentication mechanism must allow access to legitimate and honest network users and must also be able to deny access to fraudulent users. In this way, malicious and dishonest nodes must be detected and removed effectively from the network in order to protect the network reliability.

There are different methods to authenticate communications network. One such method is the public key cryptography, which is present in many security schemes today. To establish this model, it is necessary to ensure that any used public key is truthful and legitimate. The traditional approach to this problem is through public-key certificates emitted by a Public Key Infrastructure (PKI), in which a Certificate Authority (CA) certifies ownership and validity of public-key certificates. This solution presents many difficulties because the issues associated with certificate management are quite complex and expensive. The so-called Identity Based Cryptography (IBC), where each user's public key is his/her public IDentity (ID), represents a different approach because the need for public key certificates is eliminated.

The use of public key cryptography involves certain level of risk because private keys can get compromised. Therefore, the revocation process must be efficient. This problem has been traditionally solved through a centralized approach based on the existence of a Trusted Third Party (TTP), which is usually a CA. This entity distributes the so-called Certificate Revocation Lists (CRLs), which can be seen as blacklists of revoked certificates. Moreover, in order to achieve a more efficient management of certificate revocation, a different approach based on hash trees used as Authenticated Data Structures (ADS) has been proposed.

As discussed earlier, the wireless networks where it is more difficult to protect information security, are those whose nodes are capable of movement. Within these wireless networks with mobile nature, we focuses on Vehicular Ad-hoc NETworks (VANETs). Their main mission is for efficiently manage traffic on the roads to prevent abnormal circumstances. They can be seen as self-organizing networks built up from moving vehicles that communicate with each other. In particular, these networks are considered an emerging research area of mobile communications because they offer a wide variety of possible applications, ranging from as aforementioned road safety and transport efficiency, to commercial services, passenger comfort, and infotainment delivery. Further-

Martín-Fernández F., Caballero-Gil P. and Caballero-Gil C..
Efficient Management of Revoked Pseudonyms in VANETs using ID-Based Cryptography.
DOI: 10.5220/0005479207010708
In *Proceedings of the 17th International Conference on Enterprise Information Systems* (WOSIS-2015), pages 701-708
ISBN: 978-989-758-097-0
Copyright © 2015 SCITEPRESS (Science and Technology Publications, Lda.)

more, VANETs can be seen as an extension of mobile ad-hoc networks where there are not only mobile nodes, named On-Board Units (OBUs), but also static nodes, named Road-Side Units (RSUs). The so-called Intelligent Transportation System (ITS) includes two types of communications: between OBUs, and between OBUs and RSUs. IEEE 802.11p amendment to IEEE 802.11, which adds a vehicular communication system, is the basis for both the European standard for ITS, called ITS-G5, and its American counterpart, called Wireless Access in Vehicular Environment (WAVE).

In VANETs, the difficulty of maintaining the security and authenticity of communications is even more difficult than in other mobile networks because most communications are performed in broadcast mode. Furthermore, it is noteworthy that the mobility of the nodes in such networks is frequently at high speeds and in any direction, due to the nature of vehicles. In these networks, any malicious misbehaving user that can inject false information, or modify/replay any previously disseminated message, could be fatal to the others. Therefore, within the family of standards for vehicular communications IEEE 1609 based on the IEEE 802.11p, the standard 1609.2 deals in particular with the issues related to security services for applications and management messages. This standard describes the use of PKIs, CAs and CRLs, and implies that in order to revoke a vehicle, a CRL has to be issued by the CA to the RSUs, who are in charge of sending this information to the OBUs. In particular, the IEEE 1609.2 standard proposes both broadcast authentication and non-repudiation through the use of the Elliptic Curve Digital Signature Algorithm (ECDSA). However, the verification of each signature using ECDSA means a high computational cost. On the one hand, according to these standards, each vehicle is assumed to have a pair of keys: a private signing key and a public verification key certified by the CA; and any VANET message must contain: a timestamp with the creation time, the sender's signature, and the sender's public-key certificate. On the other hand, the so-called Dedicated Short-Range Communications (DSRC), devoted specifically designed for automotive use, defines that vehicles regularly exchange with nearby vehicles beacons containing sender information such as location and speed, because the information of these beacons is very useful for many VANET applications, such as cooperative collision warning.

In order to prevent possible tracking of vehicles, each OBU can have several pairs of certified public keys. These public keys are linked to pseudonyms that allow preventing location tracking by eavesdroppers. In this way, once VANETs are implemented in practice on a large scale, their size will grow rapidly due to the increasing number of OBUs and to the use of multiple pseudonyms. Thus, it is foreseeable that if CRLs are used, they will grow up to become very large and unmanageable. Moreover, this context can bring a phenomenon known as implosion request, consisting of many nodes who synchronously try to download the CRL during its updating, producing a longer latency in the process of validating a certificate due to congestion and overload of the network.

This paper proposes a scheme to achieve certificateless and cooperative authentication in VANETs by implementing IBC. Moreover, the problem of efficient management of pseudonym revocation is solved by using a Huffman k-ary hash tree as an ADS. Thus, the process of query on the validity of public pseudonyms will be more efficient because OBUs will send queries to RSUs, who will answer them on behalf of the TTP. In this way, at the same time this TTP will no longer be a bottleneck, and OBUs will not have to download any entire revocation list. Instead of that, they will have to manage hash trees where the leaf nodes contain revoked pseudonyms. In particular, in order to provide the shortest paths in the tree for the revoked pseudonyms that are the most queried by network users, the use of k-ary Huffman trees is proposed so that we can take advantage of the efficiency of the Huffman algorithm.

This paper is organized as follows. Section 2 presents a review of the state of the art. Section 3 summarizes the main concepts and ideas of the proposed authentication scheme based on the combination of IBC and Huffman k-ary hash trees. Finally, Section 4 discusses some conclusions and open problems.

2 RELATED WORKS

Public-key cryptography is nowadays one of the most popular tools in the protection of information security (Blake-Wilso, 2000). With regard to VANETs, the family of standards IEEE 1609 describes the use of PKI in this type of mobile networks. In particular, the work (J.P. Hubaux and Luo, 2004) analyses a proposal for the use of PKI to protect messages and mutually authenticate entities in VANETs. The paper (Raya and Hubaux, 2007) is a continuation of that work because it describes a PKI-based security protocol where each vehicle preloads anonymous public/private keys and a TTP stores all the anonymous certificates of all vehicles. However, the certificate management process of this scheme is less efficient.

Using PKI to sign each message is one of the best-

known solutions to establish a robust authentication method in VANETs (IEEE-1609, 2006). However, the use of a traditional approach to PKIs may fail to satisfy the real time requirement in vehicular communications because according to the DSRC protocol, each OBU will periodically transmit beacons so even in a normal traffic scenario, it is a very rigorous requirement to deploy an authentication scheme that allows at the same time efficient revocation of invalid public keys and efficient use of valid public keys.

There is a revocation method known as Online Certificate Status Protocol (OCSP), where multiple validation agents are constantly responding to requests about the status of certificates. This ensures that only these agents have the ability to inform whether a certificate is revoked or not. This explicit revocation method has an unpleasant side effect because it divulges too much information. Since validation agents constitute a global service, they must involve enough replication to handle the load of all validation queries, what means that the method is either insecure or expensive because the signature key must be replicated across many servers.

Other authors (Kocher, 1998) propose an improvement of the OCSP solution through what is called Certificate Revocation Tree (CRT). The CRT is based on that a single highly secure entity periodically publishes a CRL, represented as a signed data structure. Thus, multiple secure or insecure agents can validate certificates safely thanks to to the signature of the tree root by the single highly secure entity because in CRTs, the leaf nodes are statements concerning revoked certificates, and the CA signs the root. By using CRTs, the responder can prove the status of any certificate by showing the path from the root to the leaf node without signing the response, because the signatures of all leaf nodes are identical, and given by the signature contained in the root. Therefore, there is no need to trust the responder. The certificateless proposal described here is based on this idea.

Another interesting idea is proposed in (Kocher, 1998), where a Merkle hash tree (Merkle, 1980) is used as an ADS where leaf nodes represent the revoked certificates, sorted by serial number. A client sends a query to the nearest agent, which produces a short proof that the target certificate is (or not) on the CRT. The paper (M. Jakobsson and Szydlo, 2003) introduces several methods to traverse Merkle trees allowing time space trade-offs. Other ADSs based on multi-dimensional tree structures are studied in (Miller, 1986) to support efficient search queries, allowing the retrieval of authenticated certificates from an untrusted repository used for dissemination by various credential issuers. Besides, many tree-balancing algorithms have been proposed in the bibliography for hash trees (T. Cormen and Rivest, 1990). For instance, AVL trees are balanced by applying rotation, B-trees are balanced by manipulating the degrees of the nodes, and 2-3 trees contain only nodes with at least 2 and at most 3 children. However, in the particular application of public-key revocation, balanced trees do not necessarily minimize communication.

The management of CRTs has associated several challenges that have to be faced. One of the problems to be addressed is related to recalculating and restructuring the tree when a certificate is revoked. Skip-lists proposed in (M. Goodrich and Winsborough, 2003), (M. Goodrich and Cohen, 2003) can be seen as a natural and efficient structure for the purpose of reducing communication by balancing the CRT. However, for problems such as insertion of new leaf nodes, these are not good solutions.

In these types of trees, it is necessary to use a hash function to represent the internal nodes according to their child nodes. This work uses SHA-3 (G. Bertoni and Assche, 2010), which is a cryptographic hash function recently selected as winner of the NIST hash function competition based on the Keccak function and a sponge construction (G. Bertoni and Assche, 2010).

However, the biggest problem os revocation is the one concerning the management of valid public-key certificates. The work (Shamir, 1985) proposes the idea of an identity-based cryptosystem in which arbitrary strings can act as public keys so that there is no need for public-key certificates. The first practical identity-based encryption scheme was described in (Boneh and Franklin, 2001) using a bilinear map. Weil and Tate pairings on elliptic curves are the most efficient ways of constructing such bilinear maps (Joux, 2002). For the implementation of the identity-based authentication in the proposal here described, the Tate pairing was used.

3 IDENTITY-BASED AUTHENTICATION SCHEME

The nomenclature used in this paper to describe the tree-based model is detailed in Table 1.

Avoiding the need of public-key certificates is possible thanks to the Identity-Based Signature (IBS). The idea is based on the fact that the public identity of the signer can be used as verification key of a received signature. In tha proposal, such an identity is a public pseudonym P_j sent by the signer node together with the signed message. In the used ID-based system, each node receives all the signing private keys

Table 1: Notation.

Symbol	Meaning
$h(\cdots)$	hash function used to define the revocation tree
$h(A0\|A1\|\cdots)$	Digest obtained with the hash function h applied on the concatenation of the inputs $Ai, i = 0, 1\cdots$
$D(\geq 1)$	Depth of the hash tree
t	total number of revoked pseudonyms
$RP_j(j = 1, 2, \geq, t)$	$j-th$ Revoked Pseudonym
N_0	Root Node of the hash tree
N_{path}	Node of the hash tree. where $path$ indicates the branches from the root to the leaf node
k	Maximum number of children for each node in the hash tree
$f(\cdots)$	Keccak function used in SHA-3
n	Bit size of the digest of h
s	Bit size of the input to f
r	Bit size of the input blocks for h after padding
l	Bit size of the output blocks that build the digest of h, which is here assumed to be lower than r

P_rP_j linked to all its pseudonyms P_j from a TTP, because it cannot generate them by itself.

A TTP, called in IBC the Private Key Generator (PKG), is in charge of computing and delivering to each node via a confidential channel, the signing private keys linked to each of its pseudonyms. On the other hand, the PKG publishes a master public key MP_u and retains the corresponding master private key MP_r. Thus, given the master public key MP_u, any party will be able to compute the public key P_uP_j corresponding to any pseudonym P_j by combining it with MP_u. In order to use the corresponding private key, the node authorized to use a pseudonym must have received it from the PKG, which uses the master private key MP_r to generate all the private keys corresponding to all the pseudonyms.

Thus, the main algorithms in the proposed IBS are: Setup (see Algorithm 1), Extraction (see Algorithm 2), Signature (see Algorithm 3) and Verification (see Algorithm 4).

This paper does not describe any new ID-based cryptosystem because that is out of scope of this paper. The ID-based system that has been implemented in the proof of concept prototype is the Boneh-Franklin scheme (Boneh and Franklin, 2001), which

Algorithm 1: Setup Algorithm.

1 $MP_r \leftarrow$ Generate Random Key;
2 $MP_u \leftarrow$ Generate Master Public Key from MP_r;
3 Publish MP_u;

Algorithm 2: Extraction Algorithm.

1 **for** $j \leftarrow 1$ ***to*** $Total_{Pseudonyms}$ **do**
2 $\quad P_rP_j \leftarrow$ Generate Private Key from MP_r, P_j;
3 $\quad$ Send Securely (P_j, P_rP_j) from the PKG to the corresponding owner;

Algorithm 3: Signature Algorithm.

1 $(P_j, P_rP_j) \leftarrow$ Pseudonym Signer Node, Private Key Signer Node;
2 $P_rP_j(M) \leftarrow$ Signature of a message M;
3 Send Openly $(P_rP_j(M), P_j)$;

Algorithm 4: Verification Algorithm.

1 A Node Receives $(P_rP_j(M), P_j)$;
2 $P_uP_j \leftarrow MP_u(P_j)$;
3 Verify $P_rP_j(M)$ Signature using P_uP_j;

uses a bilinear pairing over elliptic curves and bases its security on the Bilinear Diffie-Hellman problem.

The building process used in the ID-based system applies a bilinear map $e : G_1 \times G_1 \rightarrow G2$ between two groups G_1 and G_2 so that according to the bilinearity of $e : e(aP, bQ) = e(P, Q)ab \; \forall \; P, Q \in G_1$ and $a, b \in Z$. Specifically, an ID-based system can be built from a bilinear map e if and only if a variant of the Computational Diffie-Hellman problem in G_1 is hard. The considered Bilinear Diffie-Hellman problem in G_1 is defined as follows: Given P, aP, bP, cP, compute $e(P, P)abc$, where $P \in G_1$ and $a, b, c \in Z$. In particular, the used bilinear pairing e is described for an elliptic curve E defined over some field K, so it maps a pair of points of E to an element of the multiplicative group of a finite extension of K.

The Weil pairing (Boneh and Franklin, 2001) is the basis of the first version of the Boneh-Franklin scheme. However, the scheme implemented in this work uses the Tate pairing because this is considered the most convenient bilinear function for the Boneh-Franklin scheme in terms of computational cost. In particular, the implementation of the proposal includes the use of Miller's algorithm to compute the Tate pairing (Miller, 1986).

Although the use of IBC for revocation has been previously proposed, new solutions to provide efficient mechanisms for key revocation in those schemes

are necessary. Here we propose a scheme to manage revoked pseudonyms in IBC-based VANETs, built on the idea of revocation hash trees.

4 AUTHENTICATED DATA STRUCTURE

Researchers in vehicular ad-hoc networks have focused on classical revocation lists so now improving the efficiency of these structures is a purpose of most current research. Some authors have proposed the use of particular ADSs such as Merkle trees (C. Ganan and Alins, 2012), Huffman Merkle trees (J. Munoz and Manel, 2005) and skip lists (Jakobsson and Wetzel, 2004). However, to the best of our knowledge no previous work has described in detail the use of Huffman k-ary trees as hash trees for revoked pseudonym management.

Hash trees are very useful to represent large pieces of data that have to be verified. These structures are characterized by containing the digest of the children nodes in the parent node. The leaf nodes in a hash tree are hashes of data blocks while nodes further up in the tree are the hashes of their respective children so that the root of the tree is the digest representing the whole structure. Most implemented hash trees require the use of a cryptographic hash function h in order to prevent collisions.

Like most hash trees, the Merkle tree is a binary tree, so each internal node Nij is the hash value of the concatenation of its two children: $N_{ij} = h(N_{i-1},0|N_{i-1},1)$, where i is the depth of node in the tree. This work proposes the use of a more general structure known as k-ary tree, which is a rooted tree in which each node has no more than k children, and each internal node is obtained by hashing the concatenation of all the digests contained in its children. Specifically, we propose the use of a Huffman k-ary tree in which leaf nodes are ordered from left to right, based on which revoked pseudonyms the most queried. Thus, we propose the introduction of the combination of both concepts of Huffman coding and k-ary trees applied to trees based revocation.

One of the data compression algorithms more commonly used in any discipline of information systems is the Huffman code (Huffman, 1952). The term refers to the use of a table of variable length codes for encoding certain symbols, where the table is filled in a specific way based on the estimated probability of occurrence of each possible value of the symbol. Our proposal is to bring that idea to the CRLs, and use the shortest paths for the revoked pseudonyms that are more queried. Thus, the tree will be built according

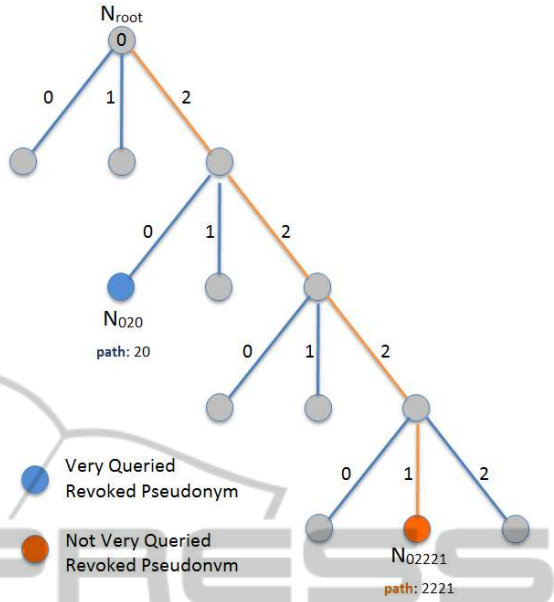

Figure 1: Revocation Path on a 3-ary Huffman Tree.

to the query frequency. In this way, the query of the most queried revoked pseudonyms will be more efficient.

Each node N_{path} of our Huffman hash tree is given by a hash value. For each node N_{path}, path is defined by the path from the root N_0 to the node N_{path} (see Figure1). The length of the path, given by the number of levels in the tree used in it, is related to the number of hash applications that are needed to represent the leaf node that corresponds to a revoked certificate. When a revoked node is very queried, it will appear higher up in the tree to have a much shorter path. This improves the efficiency of both the search node in the tree, and the verification of the path that proves revocation because the size of the paths is greatly reduced.

Thus, thanks to the TTP signature of the root N_0, it is possible to guarantee the authenticity of the used hash tree structure. When a RSU answers to an OBU about a query on a pseudonym, it proceeds in the following way. If it finds the digest of the pseudonym among the leaf nodes of the tree, which means that it is a revoked pseudonym, the RSU sends to the OBU the route between the root and the corresponding leaf node, along with all the siblings of the nodes on this path. After checking all the digests corresponding to the received path, and the TTP signature of the root, the OBU gets convinced of the validity of the received evidence on the revoked pseudonym. Conceptually, thanks to the proposed use of a Huffman tree, queries regarding the most usually queried certificates involve less data transmission and computation.

One of the innovations proposed in this paper is to optimize the query time and computation about re-

voked pseudonyms in VANETs, using the Huffman codes in the Certificate Revocation Tree. Generally, vehicles that spend more time on the roads are those that are more likely to communicate with other vehicles. Typical systems based on CRLs do not take into account this factor, so the average cost of finding any revoked pseudonym is the same. However, the general cost can be optimized by assigning less deep positions in the hash tree, to the most queried pseudonyms corresponding to the vehicles that stay longer on the road.

Therefore, the proposal presented in this paper includes the assumption that the RSU counts the number of queries that are performed for each revoked pseudonym. During the update of the tree the nodes are rearranged based on the new frequencies. Furthermore, taking into account the type of vehicle we can see that public vehicles (buses, taxis, etc.) are more likely to be among the most queried ones because they spend much time on the road.

In order to build the tree, the first thing to consider is how many children per node are allowed. This parameter defines the k of the k-ary tree to be built. If this k is equal to 2, we get the typical binary Huffman tree. The proposed system allows other values for k, such as $3,4,5$, etc. Thus, if we propose a k-ary tree with a maximum of 5 children per node, we have a 5-ary Huffman tree like the one in Figure 2.

Once we know how many children per node are allowed as maximum, what we do is to create the Huffman tree so that internal nodes are assigned from the query frequencies calculated by the RSU. Whenever k revoked pseudonyms are grouped in an internal node, this node is created with the sum of the frequencies of its children. In this way, the tree is constructed by grouping, first all revoked pseudonyms that are less queried, and so on to leave the most queried revoked pseudonyms in the top positions of the tree. Thus, the search of these nodes is much faster and the route to the root node is much shorter.

In order to learn how to find a node in the tree, a hash table is used to map each revoked pseudonym with the exact path that defines the tree. Thus, if for example we have a 3-ary Huffman tree, we have that a node pseudonym N_{02221} has a path in the tree $[2,2,2,1]$ (see Figure 1), what means that from the root node we have to go through the branches starting by the branch 2, then the 2 ... and so on to the internal node that is linked to it and choose the branch 1 to get to it.

5 REVOCATION SCHEME

This paper proposes a scheme where a node does not need any certificate to prove the binding to its public key. Instead of that, an ID-based authentication scheme and revocation trees are used. We consider the following basic authentication architecture, which includes three main parties:

- **TTP.** This entity acts as key distribution centre because it is responsible for generating and assigning related parameters for VANET nodes, and for revoking pseudonyms of misbehaving OBUs and public keys of misbehaving RSUs.
- **RSU.** This entity serves as a gateway to provide OBUs within its transmission range with any requested information about revoked pseudonyms.
- **OBU.** Each vehicle is equipped with an OBU, which periodically broadcasts signed beacons that are received by neighbour OBUs and RSUs.

The proposed model is based on the use of a pseudonym P_j set by each OBU, so that for each one the TTP provides the OBU with a corresponding private key $P_r P_j$. If any of those pseudonyms is revoked by the TTP, it inserts all the pseudonyms corresponding to the same OBU in the revocation tree. The TTP is also responsible for periodically updating the tree by deleting the expired pseudonyms, and for restructuring the tree when necessary. After each update, the TTP sends the corresponding modifications of the updated tree to all RSUs.

The RSU has to search vehicle pseudonyms in the revocation tree each time an OBU requests it. The RSU must provide the requesting OBU either with a verifiable revocation proof of any revoked pseudonym or with a signed message indicating that the requested pseudonym has not been revoked and is labelled as 'OK'. In the first case, by using the answer data, the OBU can verify the TTP signature of the received signed root, recompute the root of the revocation tree, and check it by comparing it with the received signed root. The proposed scheme is computationally efficient since it obviates the need to sign each RSU reply, as it removes most of the trust from it. The only case when the RSU's trust is questioned is when it provides an 'OK' answer because that could be a fraud. In this regard, when an OBU receives an 'OK' message signed by a cheating RSU, it trusts it momentarily. However, when it contacts another RSU, it asks it again about the same pseudonym. If this RSU provides the OBU with a proof of revocation whose timestamp contradicts the 'OK' answer signed by the questioned RSU, the OBU sends to the latter RSU an impeachment on the questioned RSU, so that

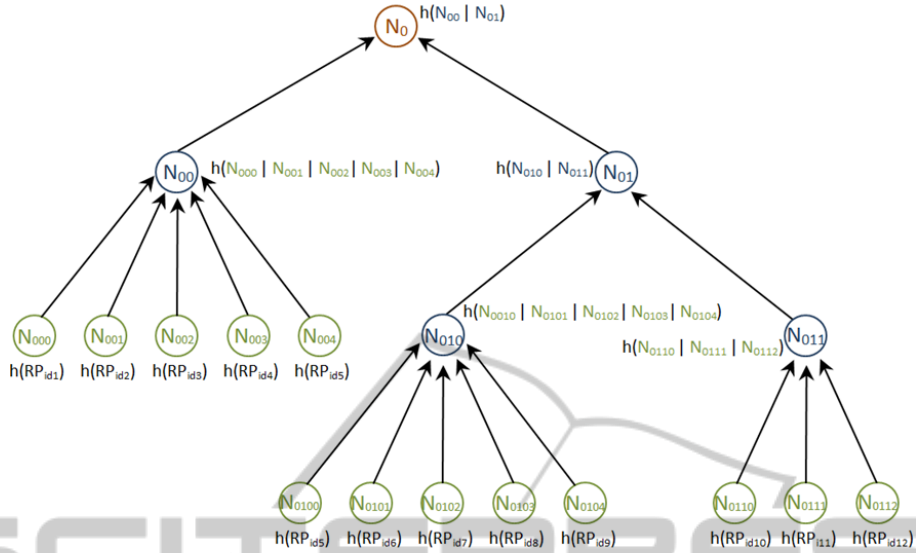

Figure 2: Hash Tree Based on a 5-ary Huffman Tree.

the honest RSU can send it to the TTP who will revoke its public key by deleting it directly from the revoked RSU. Otherwise, if the second RSU also sends a signed 'OK' message, the OBU goes on asking about the same pseudonym until it reaches either a contradiction or a prefixed trust threshold.

Thus, each OBU stores locally in two separate and complementary structures, the pseudonyms of those OBUs that it has previously checked as unreliable, and of those OBUs that have been reliable till then. Therefore, in the future, if it reconnects with any of these vehicles, it can use such information to decide how to proceed. If there is no RSU nearby, it uses these data to decide whether to establish the communication or not. Otherwise, even if there is an RSU nearby, there is no need to re-ask it about a checked revoked pseudonym.

6 CONCLUSIONS

User authentication is one of the most crucial security issues in vehicular ad-hoc networks. In order to improve traditional solutions, this work proposes, on the one hand, the use of identity-based cryptography to achieve certificateless authentication, because this increases efficiency of authentication of honest users. On the other hand, this work also proposes a scheme based on authenticated dynamic hash k-ary trees combined with Huffman codes to use them as revocation trees, because this solution increases efficiency of revocation of keys of dishonest users. Thus, a Huffman tree is constructed where the revoked pseudonyms that are in the upper levels are those corresponding to the nodes that are the most queried by network users. In this way, the proposed tree reflects better the real environments, where some vehicles, such as public transport or freight delivery vehicles, spend much more time on the road and so have a bigger probability to be queried. This work is part of work in progress, so there ase several questions that deserve further study, such as the properties of the used version of k-ary Huffman trees, and the optimal values of the used parameters. Also, a full implementation of the proposal to obtain results useful to make a full comparison with other proposals is being done.

ACKNOWLEDGEMENT

Research supported under TIN2011-25452, IPT-2012-0585-370000, BES-2012-051817, and RTC-2014-1648-8.

REFERENCES

Blake-Wilso, S. (2000). Information security, mathematics, and public-key cryptography. *Designs, Codes and Cryptography 19(2-3)*, pages 77–99.

Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. *Crypto. LNCS 2139*, pages 213–229.

C. Ganan, J. Munoz, O. E. J. M.-D. and Alins, J. (2012). Toward revocation data handling efficiency in vanets. *Communication Technologies for Vehicles*, pages 80–90.

G. Bertoni, J. Daemen, M. P. and Assche, G. (2010). Keccak sponge function family main document. *Updated submission to NIST (Round 2)*, 2.1.

Huffman, D. (1952). A method for the construction of minimum-redundancy codes. *Proceedings of IRE 40 (9)*, pages 1098–1101.

IEEE-1609 (2006). Family of standards for wireless access in vehicular environments (wave). *U.S. Department of Transportation*.

J. Munoz, J. Forne, O. E. and Manel, J. (2005). Efficient certificate revocation system implementation: Huffman merkle hash tree (huffmht). *TrustBus*, pages 119–127.

Jakobsson, M. and Wetzel, S. (2004). Efficient attribute authentication with applications to ad hoc networks. *ACM workshop on vehicular ad hoc networks*, pages 38–46.

Joux, A. (2002). The weil and tate pairings as building blocks for public key cryptosystems. *Algorithmic Number Theory Symposium. LNCS 2369*, pages 20–32.

J.P. Hubaux, S. C. and Luo, J. (2004). The security and privacy of smart vehicles. *IEEE Security and Privacy 2(3)*, pages 49–55.

Kocher, P. (1998). On certificate revocation and validation. *FC98. LNCS 1465*, pages 172–177.

M. Goodrich, R. Tamassia, N. T. and Cohen, R. (2003). Authenticated data structures for graph and geometric searching. *CT-RSA. LNCS 2612*, pages 295–313.

M. Goodrich, M. Shin, R. T. and Winsborough, W. (2003). Authenticated dictionaries for fresh attribute credentials. *Trust Management. LNCS 2692*, pages 332–347.

M. Jakobsson, T. Leighton., S. M. and Szydlo, M. (2003). Fractal merkle tree representation and traversal. *CT-RSA. LNCS 2612*, pages 314–326.

Merkle, R. (1980). Protocols for public key cryptosystems. *IEEE Security and privacy 1109*, pages 122–134.

Miller, V. (1986). Short programs for functions on curves. *Unpublished manuscript, 97*, pages 101–102.

Raya, M. and Hubaux, J. (2007). Securing vehicular ad hoc networks. *Computer Security 15(1)*, pages 29–68.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. *Crypto. LNCS 196*, pages 47–53.

T. Cormen, C. L. and Rivest, R. (1990). Introduction to algorithms. *MIT Press*.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS