A novel active revocation algorithm for Intelligent Transport System security

Nuno R. P. Lopes
Instituto Superior Técnico,
Universidade de Lisboa
Lisboa, Portugal
nunoromeu@tecnico.ulisboa.pt

Naercio Magaia
School of Engineering and Informatics,
University of Sussex,
Brighton BN1 9QJ, U.K.
N.Magaia@sussex.ac.uk

Paulo Rogério Pereira
INESC INOV,
Instituto Superior Técnico,
Universidade de Lisboa, Portugal
prbp@inesc.pt

***Abstract*—Vehicular networks enable vehicles to communicate with each other and with the roadside infrastructure. They are part of the Intelligent Transport System (ITS) framework and provide safety, navigation, and other roadside services. To communicate with each other in the network, ITS stations (i.e., vehicles, roadside and portable units) use pseudonym certificates called Authorization Tickets (ATs). These ATs are issued to certified ITS stations (ITS-S) so they can sign and encrypt messages in the network, building trust in ITS. ATs are of short validity and have to be renovated frequently due to the privacy of ITS stations. Revocation of ATs is done passively, not sending new ATs to compromised ITS-Ss, leaving a space between the moment an ITS-S is classified as compromised and the end of the validity of its ATs, exposing the network to possible misleading messages. This work studies ITS security management and proposes an active revocation algorithm based on an Authorization Ticket Certificate Revocation List (ATCRL). This list is distributed in the ITS network and used by vehicles to discard messages associated with the compromised ATs. An analysis of the proposed algorithm is conducted, where several scenarios were built to compare and analyze different uses of the algorithm, including the two versions proposed, i.e., a decentralized and a centralized version. The decentralized version is faster, and there is a benefit in using delta versions of the ATCRL.**

Keywords*— *ITS, Security Management, Authorization Tickets, Active Revocation

I. Introduction

Vehicular networks are a particularly challenging class of mobile networks that enable vehicles to communicate with each other and with the roadside infrastructure. They are part of the Intelligent Transport System (ITS) framework, providing safety, navigation, and other roadside services. As of today, they are understood as having evolved into a broader Internet of Vehicles (IoV) [1] and are expected to evolve into an Internet of autonomous Vehicles.

ITS message applications, such as Cooperative Awareness Messages (CAMs), the beacon-like messages of ITS, and event-focused Decentralized Environmental Notification Messages (DENMs), have security requirements like authentication, authorization, confidentiality and privacy. To protect users' privacy, ITS messages should not be linked to users' or vehicles' identities and messages coming from the same ITS station (vehicles, roadside or portable units) should not be linked together. To achieve the desired security requirements, ITS stations (ITS-Ss) must be enrolled and authorized to communicate in the ITS network following an enrolment process.

In the enrolment process, an ITS-S communicates with the Enrolment Authority (EA) using its canonical (i.e., unique and immutable) identity to obtain an Enrolment Credential (EC), giving the ITS-S access to communications in the ITS network. The ITS-S then uses the obtained EC to acquire Authorization Tickets (ATs), in the form of pseudonym certificates, from the Authorization Authority (AA), providing the ITS-S with authoritative proof that it may use specific ITS applications.

With the use of ATs, an ITS-S can send misbehaving messages in the ITS network, endangering the safety of other users. To detect compromised messages, a misbehavior detection system embedded in ITS-Ss sends a Misbehavior Report (MR) to the Misbehavior Authority (MA), which classifies it and takes the appropriate response. The response can be on different levels: no action, sending an alert to the user or the ITS station's manufacturer, or initiating the revocation process (e.g., blocking the ITS-S Enrolment Credential) [2].

ATs are revoked passively by blocking the ITS-S EC and not issuing more ATs to the compromised ITS-S. The problem is that even though ATs are of a short validity period and have to be renovated frequently, the time between the ITS-S is classified as compromised by the MA, and the end validity of its ATs remains open to communication from the compromised ITS-S to the ITS network. This work develops an active revocation algorithm based on an Authorization Ticket Certificate Revocation List (ATCRL) to be distributed in the network to tackle this issue.

To evaluate the use of the developed active revocation algorithm, several scenarios are conceived, assigning different values for the number of ATs of the compromised ITS-S to add to the ATCRL and the number of Road Side Units (RSUs) used to disseminate the list into the ITS network, by broadcasting it. We aim to evaluate different aspects of the algorithm, such as the increase in the number of RSUs to distribute the list in a larger area, the use of a delta version of the ATCRL with only the updated entries, the impact of the cryptographic measures and the use of alternative paths to the reporting ITS-S to send the MR to the MA.

The remainder of this article is as follows: Section II presents the background, and Section III details the proposed active revocation algorithm, with its two versions and a traceability algorithm. Section IV presents the evaluation and results of using the active revocation algorithm in the scenarios considered, and Section V presents concluding remarks.

II. Background

The main elements of the ITS security functional model can be determined by considering a simple ITS communications scenario illustrated in Fig. 1. In this scenario, an ITS-enabled vehicle needs to communicate with the following entities:

- The EA authenticates an ITS-S and grants it access to ITS communications;

- The AA provides an ITS-S with authoritative proof that it may use specific ITS services.
- other ITS-equipped devices:
  - RSUs or central units; and
  - personal units such as portable devices.

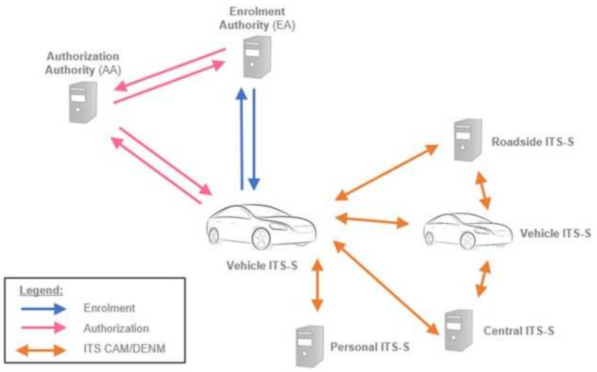

Fig. 1. ITS communications reference scenario [3].

To protect users' privacy, ITS messages should not be linked to users' or vehicles' identities and messages coming from the same ITS-S should not be linked together. In the security reference model, the vehicle (sending ITS-S) communicates with the EA to acquire the EC for access to ITS communications, and then uses the received EC to negotiate authoritative proof to invoke ITS services from the AA, given in the form of ATs. ATs are of a short validity and have to be renovated frequently. [4, 3]

Certificate distribution lists are distributed to ITS stations in the network for key management. The Certificate Revocation List (CRL) and Certificate Trust List (CTL) contain the certificates of the Certified Authorities (CAs) in ITS, such as the EA and the AA, and ITS-Ss use these lists to build trust chains.

III. Proposed Algorithms

A Traceability algorithm was developed to link an AT to an EC, which is linked to the canonical ID of the ITS-S. An example situation of a compromised ITS-S is used, in which a neighbor ITS-S receives a message coming from a compromised ITS-S, classifies it as possibly compromised and sends the corresponding Misbehavior Report (MR) to the MA, containing the AT associated with the possibly compromised message. From this moment on, the MA starts a Traceability process by communicating with the AA and the EA. The developed algorithm is suitable for passive revocation of ITS-Ss, in which the EA revokes an ITS-S by revoking its EC, thus stopping the authorization of new ATs to the compromised ITS-S. The algorithm is illustrated in Fig. 2, and the detailed steps are presented below.

1. An ITS-S reports another ITS-S by sending an MR to the MA, containing the AT associated with the misbehavior situation.
2. The MA analyses the MR and decides that the ITS-S is compromised.

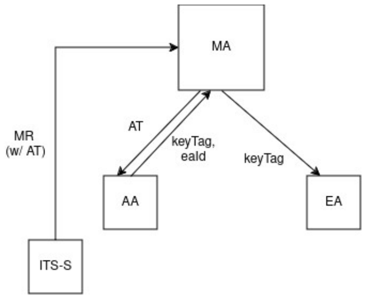

Fig. 2. Traceability algorithm in a compromised situation.

3. The MA initiates the revocation process:
   a) Contacts the AA asking for the keytag associated with the AT and the identifier of the EA associated with the ITS-S that issued the EC associated with the AT.
   b) The AA sends back the associated keytag and the EA identifier (ID).
   c) Contacts the EA, sending the keytag associated with the AT.
   d) The EA links the keytag with the EC of the compromised ITS-S, which is linked to the ITS-S canonical identity.

For linking the AT with its respective keytag, the AA has to store all active ATs, the associated keytags and EA IDs in a database. The EA shall group all the keytags of active ATs by the associated EC.

The proposed active revocation algorithm consists of the traceability algorithm further developed to create an Authorization Ticket CRL (ATCRL) to be disseminated in the ITS network using location-based RSUs. The Algorithm steps are described below, and its illustration is shown in Fig. 3.

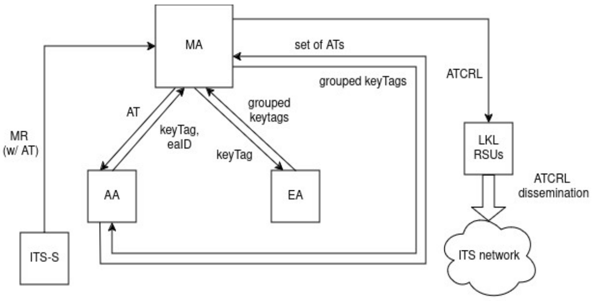

Fig. 3. Active Revocation algorithm.

1. An ITS-S reports another ITS-S by sending an MR to the MA containing the AT associated with the misbehavior situation.
2. The MA analyses the MR and decides that the ITS-S is compromised.
3. The MA initiates the revocation process:
   a) Contacts the AA asking for the keytag associated with the AT and the EA identifier.
   b) The AA sends back the associated keytag and the EA ID.
   c) Contacts the EA sending the keytag associated with the AT.
   d) The EA links the keytag with the EC of the compromised ITS-S.

4. The EA sends back to the MA all the grouped keytags associated with the compromised ITS-S EC.
5. The MA sends the keytags to the AA, asking for all the ATs associated with the keytags.
6. The AA answers the MA by sending a list with the requested ATs.
7. The MA checks the Last Known Location (LKL) of the compromised ITS-S, adds the ATs identifiers (SHA-256 hashes) to the ATCRL containing the identifiers of the previous revoked and active (or in a preloading state) ATs, the respective validity period and, a nextUpdate field and a sequence number, and sends the ATCRL to an RSU close to the LKL (denominated central LKL RSU or LKL RSU) who then sends it to its neighbor RSUs in a predefined distance radius for further dissemination in the network. The list sequence number is increased by one unit.
8. RSUs broadcast the ATCRL through ITS G5 access technology to the ITS network.

ITS-Ss receiving the ATCRL will then compare ATs of new incoming messages against the ATCRL, discarding messages whose ATs are present in the ATCRL. Before comparing it to the ATCRL, ITS-S will first verify the trust chain of the AT (with the CTL and CRL) and its validity period, discarding messages associated with expired ATs. The ATCRL should be updated in the ITS network every time new entries are added to the list and have a nextUpdate field indicating the time when the next update is expected, and consequently, the time after which the CRL is to be expired. The sequence number should be increased by one unit, and the ATCRL should be disseminated in the network. As with the CTL of Root CAs, the sequence number is a monotonically increasing counter.

ITS-Ss should store the list of revoked ATs. The list is updated by RSU dissemination or, using the Internet, by requesting the list to the MA, with possible RSUs and ITS-Ss relaying, as it happens with the CRLs issued by Root CAs. Since ATs' validity period and preloading period, the period of time in which an ITS-S can request and have an AT before its validity starts, are limited, there should not be a high number of revoked active ATs within that period of time.

A decentralized Active Revocation algorithm was also proposed and is shown in Fig. 4.

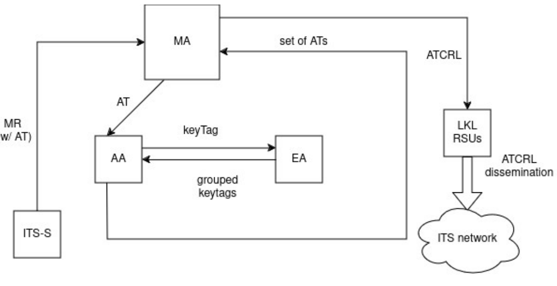

Fig. 4. Active Revocation algorithm – the decentralized approach.

ITS-Ss should store the list of revoked ATs. The list is updated by RSU dissemination or, using the Internet, by requesting it from the MA, with possible RSUs and ITS-Ss relaying, as it happens with the CRLs issued by Root CAs.

If scalability or distribution problems arise, several strategies can be adopted for the dissemination of the ATCRL. The division of the ATCRL into multiple ATCRLs and distribution based on the compromised ITS-S last location, calculating a possible distance range considering the remaining validity of the ITS-S ATs and distributing the ATCRL within that range, or by an extensible perimeter approach, where the list is first distributed within a specified perimeter around the LKL and to RSUs in the border and in a small distance outside of the specified perimeter, and if these RSUs detect the use of any of the revoked ATs the perimeter is enlarged and the list distributed in the added area and to new border and external RSUs, repeating the process. These strategies can be adopted besides the main geographical factor of the division of the ATCRL, the ATs use range. For dissemination of the revoked ATs belonging to a compromised ITS-S in a broader distance range, the list can be sent directly from the MA to other RSUs than the central LKL RSU, and the same strategy of dissemination adopted, or a broader distance radius can be specified, where RSUs transmit the list in a sequential manner within that radius.

Another option for solving eventual ATCRL list scalability (i.e., size) problems that may arise is the distribution of delta ATCRLs by RSUs instead of distributing the full ATCRL. A delta ATCRL contains the added entries in relation to the last issued ATCRL, with a sequence number and a next update field, usually being of a smaller size than the full ATCRL. The sequence number is one unit more than the full ATCRL from which it is generated, and it is equal to the new and updated ATCRL sequence number. For the use of delta ATCRLs, an extra field should be added to lists, an isFullList flag indicating if the list is a full list (true) or delta list (false).

The decentralized approach has the advantage of being faster than the previous active revocation algorithm since it requires fewer communications. In scenarios where the MA does not need full control over the Active Revocation process for keyTag data information retrieving and processing, the decentralized algorithm should be selected over the centralized one.

Fig. 5 presents three possible options for ITS-S communication with the PKI to support security management services. Three communication paths are presented: one path via cellular network (reference point S0) and two alternative paths via ITS G5 to the ITS infrastructure (reference point S1 or reference points S2 and S3) using a relaying ITS-S roadside gateway to communicate with PKI authorities through the Internet (reference point S4).

ETSI ITS defines specific ITS-G5 frequency channels for Security management services. RSUs should use the allocated channels for security management services (ITS-G5A frequency band, channels G5-SCH1 and G5-SCH2 [5]) or the supplementary channels when available (G5B to G5D [5]) for distribution of the ATCRL in the ITS network. The specified channels for security management purposes should also be used for communication between the reporting ITS-S and the MA via ITS-G5 (reference points S1, S2, and S3).

Several communication profiles are possible, depending on the path chosen for communication and the entities involved. As defined in ETSI TS 102 941[4] for the security management messages of enrolment and authorization, in all communications using the IP protocol (directly, over reference points S0 and S4, or after forwarding, via reference points S1 or S2 and S3) the protocols HTTP over TCP/IP should be used.

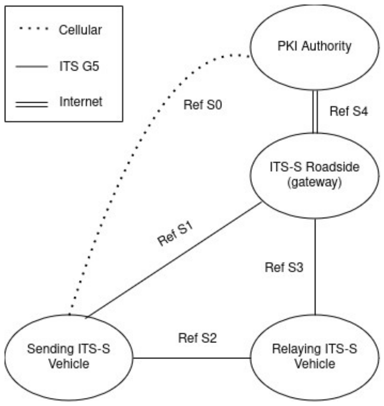

Fig. 5. Communication paths for ITS-S communication with the PKI.

The developed algorithms have the following security requirements:

- Messages are encrypted using Elliptic Curve Integrated Encryption Scheme (ECIES) as defined in ETSI TS 103 097 [6];
- Messages are encrypted with the public key of the receiving PKI authority certificate;
- All messages, except the ATCRL dissemination messages, shall be encrypted;
- No supplementary cryptographic layer, such as TLS, is required over HTTP;
- The ATCRL should be publicly accessible, thus not encrypted.
- Messages are signed using the Elliptic Curve Digital Signature Algorithm (ECDSA) as defined in ETSI TS 103 097 [6];
- Messages are signed using entities' certificates:
  - ITS Stations sign using the Authorization Tickets (ATs) issued for the effect, i.e. with Security Management permissions;
  - PKI authorities sign with their private keys associated with their public keys.
- All messages must be signed;
- When forwarding messages in ITS-G5, no additional cryptographic procedures are needed, such as a new signature over the signed message.

Message types are to be incorporated in ETSI TS 103 097 data structures [6], namely in the field tbsData.payload.content of the EtsiTs103097Data-Signed data structure. Signed and encrypted messages are composed of encrypted messages containing a signed message.

IV. Evaluation

This section evaluates the Active Revocation (AR) algorithms in multiple scenarios and a comparison between them.

Fig. 6 shows the ATCRL components. Specifically, it comprises the ATs entries, each containing the AT identifier and the respective validation period, a sequence number, and a nextUpdate field, plus a flag isFullList to indicate whether the list is a full or delta list.

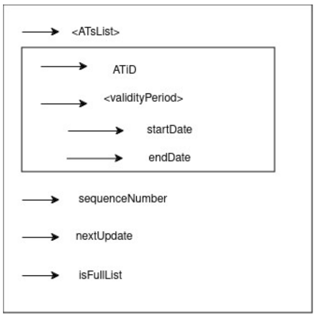

Fig. 6. ATCRL components illustration.

Table I presents the AR algorithms' various message types and sizes, with common ITS messages, such as CAM and DENM, that may be sent as evidence in the MR to the MA. The MR size was estimated to contain long CAMs or DENMs and the respective ITS-S AT certificate for the message application, plus extra space for the report message with the AT of the reporting ITS-S [2]. The eaID was estimated as a typical URL address size.

TABLE I. MESSAGE TYPE AND THEIR SIZES

Message type	Data size
short CAM	190 bytes [7]
long CAM	300 bytes [7]
DENM	300 bytes [7]
AT certificate	132 bytes [8]
MR	1 Kbyte
keyTag	16 bytes [4]
eaID	75 bytes

Table II represents the types of ATCRL and the respective data sizes.

Table III's cryptographic data and sizes are used to sign and encrypt messages. A certificate identifier is the SHA256 hash of a certificate. The ciphertext to plaintext ratio of an ECIES with a key length of 512 bits, the key length of ITS entities encryption key (public key) is taken from [9] and is negligible when encrypting more than 1 KB of data, the key length of ITS entities encryption key (public key) used to encrypt messages, the SHA-256 hashing algorithm execution time used to digest messages for signing with the ECDSA is taken from [6], being negligible for sizes in the order of dozens of KBs. Table IV presents encryption and decryption rates using an ECIES [9] with the ITS entities' private key size of 256 bits for decryption and the associated public key size of 512 bits for encryption.

TABLE II. ATCRL COMPONENTS SIZE

ATCRL component/field	Size
AT identifier (SHA-256)	32 bytes
startDate	4 bytes
endDate	4 bytes
sequenceNumber	2 bytes
nextUpdate	4 bytes
isFullList	1 bit

To sign with the ECDSA, the times taken by the SHA-256 hash over messages plus the encryption and decryption of the 256 bits were used. Signature generation uses private key encryption, and signature verification uses public key decryption. The rates of encryption and decryption using

ECIES are equal for the same key length [9]. The resulting times are presented in Table V.

TABLE III. CRYPTOGRAPHIC OPERATIONS DATA AND SIZE

Cryptographic Data	Size
public key	64 bytes [8]
private key	32 bytes [8]
certificate	132 bytes [8]
certificate identifier	32 bytes
signature	69 bytes [8]

TABLE IV. ENCRYPTION AND DECRYPTION RATES FOR ITS ENTITIES PUBLIC AND PRIVATE KEY SIZES

Operation	Key Length	Rate (ms/byte)
Encryption	512 bits	0.08 [9]
Decryption	256 bits	0.0167 [9]

The typical average access rates used are presented in Table VI. The fiber optics rate is a common data rate for professional fiber optics connections.

TABLE V. SIGNATURES OPERATIONS TIME OVER THE SHA-256

Cryptographic Operation	Time
Signature generation	0.53 ms
Signature verification	2.56 ms

TABLE VI. ACTIVE REVOCATION ALGORITHM ACCESS TECHNOLOGIES DATA RATE

Access Technology	Typical Data Rate
ITG-G5	6 Mb/s [5]
Cellular upload	12 Mb/s [10]
Fiber Optics	1 Gb/s

We consider the Round-Trip Time (RTT) between each entity present in the algorithm to be the same and equal to the average RTT in the same country, which is considered Portugal: $RTT = 15$ ms.

The transport layer algorithm used in the algorithm communications is TCP, requiring an initial RTT to establish a session between the communication parties before sending a message. TCP is chosen for reliability purposes since the messages involved in the algorithm are critical and sequential; all messages require confirmation of reception from the destination entity, given in the TCP protocol at the transport layer. The RTT with the TCP slow start is considered for calculating the time taken by each message sent in the Algorithm. In disseminating the ATCRL in the ITS network through ITS-G5, the RTT is not considered due to the proximity of the entities. For the transmission of the ATCRL from the LKL RSU to its neighbors RSUs, the RTT is considered as $RTT = 3$ ms since the entities are close to each other.

As for the headers of the diverse protocols corresponding to the protocol stack of a message, the sizes of Table VII are considered:

The sizes represented in Table VII are added to the messages when calculating the time each message sent with the fiber optics links takes. The protocol header sizes are fixed, except for the HTTP protocol, where the typical header size for the type of services employed in the algorithms (without cookies and user agent extended features) is considered. For the ITS-G5 dissemination, the transport and network protocols used are the Basic Transport Protocol (BTP) over GeoNetworking (GN) [4]. The sizes of these protocols are considered negligible when calculating the time taken by the message since the message (ATCRL) size is much bigger than the size of the protocol headers, similar to the TCP and IP protocol header sizes.

TABLE VII. PROTOCOL HEADER SIZES

Protocol	Header Size
Ethernet	26 bytes
IPv6	40 bytes
TCP	20 bytes
HTTP	500 bytes

The configurable variables in the different scenarios for the use of the algorithm are the following:

- Number of ATs belonging to the compromised ITS-S stations to be revoked ($n0$);
- Number of ATs present in the ATCRL before the addition of new ATs ($n1$);
- Number of RSUs in the pre-defined radius receiving the ATCRL from the LKL RSU to broadcast it into the ITS network (*RSUs*).

For scenario 1, there are no ATs previously present in the ATCRL, and the number of ATs to be revoked is the maximum number of active ATs an ITS-S can hold simultaneously [11]. The number of RSUs was considered to be 20 for the initial area in which the ATCRL is to be disseminated. We have obtained the transmission times in Table VIII. We can observe the difference between using the centralized and decentralized versions of the Active Revocation algorithm. There is a difference of 30 ms, representing fewer messages needed by the decentralized AR algorithm version.

TABLE VIII. ACTIVE REVOCATION ALGORITHMS TRANSMISSION TIMES

	AR centralized	AR decentralized
Cellular	23.5 ms	23.5 ms
Fiber Optics	427.5 ms	397.5 ms
ITS-G5	5.3 ms	5.3 ms
Total	456.3 ms	426.3 ms

For scenario 2, we maintained the values of scenario 1, increasing the number of RSUs. We compared three cases (*RSUs* = 20, *RSUs* = 100, *RSUs* = 1000). Since there is no difference between the algorithm versions in this step, the faster version, the decentralized algorithm, was used. The delays are in Table IX.

As expected, the number of RSUs (*RSUs*) in the pre-defined area receiving the ATCRL from the neighbor LKL RSU for disseminating it to the network significantly impacts the total time of the AR algorithm.

For scenario 3, we compared the difference in time between the use of a delta ATCRL and the full ATCRL. The scenario was thought of having an ATCRL with 1000 ATs (if each compromised ITS-S holds 100 ATs to be revoked, it is the equivalent of having the ATs of 10 compromised ITS-Ss in the list) and adding the ATs of a new compromised ITS-S to the ATCRL, the maximum number of active ATs an ITS-S can hold of 100. The number of RSUs chosen is 100, representing a larger area than in scenario 1. The delays are in Table X.

TABLE IX. DECENTRALIZED AR ALGORITHM TIME WITH THE DIFFERENT NUMBERS OF RSUS

#RSUs	20	100	1000
Cellular	23.5 ms	23.5 ms	23.5 ms
Fiber Optics	397.5 ms	1237.5 ms	10687.5 ms
ITS-G5	5.3 ms	5.3 ms	5.3 ms
Total	426.3 ms	1266.3 ms	10716.3 ms

TABLE X. DECENTRALIZED AR ALGORITHM TIMES WITH THE USE OF A DELTA ATCRL AND THE FULL ATCRL

Communication	delta ATCRL	full ATCRL
Cellular	23.5 ms	23.5 ms
Fiber Optics	521.2 ms	6278.3 ms
ITS-G5	5.3 ms	59.5 ms
Total	550 ms	6361.3 ms

The difference is due to the size of the ATCRL transmitted through the algorithm, with the full ATCRL being significantly bigger and taking more RTTs to transmit from one entity to another, from the MA to the LKL RSU or between the RSUs in the pre-defined area. With this result, the benefits in terms of time of using delta versions of the ATCRL become evident. Delta versions also transmit less data, which is easier to transmit and less prone to errors.

For scenario 4, we added the cryptographic operations. All messages except the ATCRL are signed, encrypted and decrypted, and the signature is verified in every communication exchange in the Active Revocation algorithm. The ATCRL is signed by its issuing entity, the MA, and its forwarding by the RSUs does not require any additional cryptographic operations, such as re-signing the ATCRL. The scenario contemplates the revocation of 100 ATs of a reported compromised ITS-S and the use of a delta ATCRL ($n0 = 100$ and $n1 = 0$), the same values considered for Scenario 1 without security operations. The number of RSUs considered in the pre-defined area to disseminate the ATCRL is 100 ($RSUs = 100$). The times taken with the two versions, the Decentralized Active Revocation Algorithm (DARA) and the Centralized Active Revocation Algorithm (CARA), are shown in Table XI and Table XII, respectively.

TABLE XI. DECENTRALIZED AR ALGORITHM TIMES WITH SECURITY OPERATIONS

	DARA w/ security	DARA w/o security
Cellular	145.15 ms	23.5 ms
Fiber Optics	3129.6 ms	1237.5 ms
ITS-G5	7.96 ms	5.3 ms
Total	3282.71 ms	1266.3 ms

TABLE XII. CENTRALIZED AR ALGORITHM TIMES WITH SECURITY OPERATIONS

	CARA w/ security	CARA w/o security
Cellular	145.15 ms	23.5 ms
Fiber Optics	3341.46 ms	1267.5 ms
ITS-G5	7.96 ms	5.3 ms
Total	3494.57 ms	1296.3 ms

From the results, we can observe the influence of the cryptographic operations of encryption and decryption, signature generation and signature verification of messages over the Algorithm. Since the cryptographic procedures are very computationally demanding, they are also very time-consuming, making for most of the time taken by the Active Revocation algorithm. Scenario 5 tests the three alternative paths for sending the MR by the reporting ITS-S. Considering a scenario of 3 hops, two relaying ITS-S vehicles and a relaying RSU, we can compare the times taken by the three alternative paths. The results are presented in Table XIII.

TABLE XIII. COMMUNICATION TIME OVER THE VARIOUS COMMUNICATION PATHS FOR SENDING THE MR

Communication Path	Time
Direct	145.15 ms
Relaying RSU	146.27 ms
Relaying vehicles and RSU	150.72 ms

V. CONCLUSION

From Scenario 1, we concluded that using the decentralized active revocation algorithm is faster than using the centralized approach, which is the preferred choice. With Scenario 2, we saw a significant increase in the time required to distribute the ATCRL with the number of RSUs. In Scenario 3, we could observe the large benefit of using delta versions of the ATCRL to update the revoked ATs in the ATCRL instead of sending the full ATCRL to ITS stations every time the list is updated. In Scenario 4, we observed the high impact on the time of the cryptographic operations for signing and encryption of messages, which is necessary for the algorithms. In Scenario 5, we compared the difference in time between the use of the different communication paths to send the MR to the MA, understanding the low impact on time of the use of alternative paths through ITS-G5 to send the MR when the sending ITS-S does not have access to cellular networks.

VI. ACKNOWLEDGMENT

This work was supported by H2020-MSCA-RISE under grant No. 101006411.

REFERENCES

[1] L. Silva et al., "Computing Paradigms in Emerging Vehicular Environments: A Review," in IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 3, pp. 491-511, March 2021, doi: 10.1109/JAS.2021.1003862.

[2] ETSI. TS 103 759 - v2.1.1 - intelligent transport systems (ITS); security; misbehaviour reporting service; release 2.

[3] ETSI. TS 102 940 - v2.1.1 - intelligent transport systems (ITS); security; its communications security architecture and security management; release 2, 2021.

[4] ETSI. TS 102 941 - v1.4.1 - intelligent transport systems (ITS); security; trust and privacy management, 2021.

[5] ETSI. EN 302 663 - v1.2.0 - intelligent transport systems (ITS); access layer specification for intelligent transport systems operating in the 5 ghz frequency band, 2012.

[6] ETSI. TS 103 097 - v2.1.1 - intelligent transport systems (ITS); security; security header and certificate formats; release 2, 2021.

[7] L. M. Lopez, C. F. Mendoza, J. Casademont, and D. Camps-Mur, "Understanding the impact of the pc5 resource grid design on the capacity and efficiency of LTE-V2X in vehicular networks", Wireless Communications and Mobile Computing, 2020, 2020.

[8] C2C-CC. Survey on ITS-G5 cam statistics. 2018

[9] V. G. Martínez, L. H. Encinas, and A. Q. Dios, "Security and practical considerations when implementing the elliptic curve integrated encryption scheme", Cryptologia, 39:244–269, 7 2015.

[10] Speedtest global index – internet speed around the world, date accessed: 14/11/2024. [Online]. Available: https://www.speedtest.net/global-index

[11] E. Comission. Certificate policy for deployment and operation of european cooperative intelligent transport systems (C-ITS), 2018. last access on 02/2024.