V’CER: Efficient Certificate Validation in Constrained Networks
David Koisser and Patrick Jauernig, Technical University Darmstadt; Gene Tsudik, University of California, Irvine; Ahmad-Reza Sadeghi, Technical University Darmstadt
https://www.usenix.org/conference/usenixsecurity22/presentation/koisser

This paper is included in the Proceedings of the 31st USENIX Security Symposium.
August 10–12, 2022 • Boston, MA, USA
978-1-939133-31-1

Open access to the Proceedings of the 31st USENIX Security Symposium is sponsored by USENIX.
Abstract

We address the challenging problem of efficient trust establishment in constrained networks, i.e., networks that are composed of a large and dynamic set of (possibly heterogeneous) devices with limited bandwidth, connectivity, storage, and computational capabilities. Constrained networks are an integral part of many emerging application domains, from IoT meshes to satellite networks. A particularly difficult challenge is how to enforce timely revocation of compromised or faulty devices. Unfortunately, current solutions and techniques cannot cope with idiosyncrasies of constrained networks, since they mandate frequent real-time communication with centralized entities, storage and maintenance of large amounts of revocation information, and incur considerable bandwidth overhead.

To address the shortcomings of existing solutions, we design V’CER, a secure and efficient scheme for certificate validation that augments and benefits a PKI for constrained networks. V’CER utilizes unique features of Sparse Merkle Trees (SMTs) to perform lightweight revocation checks, while enabling collaborative operations among devices to keep them up-to-date when connectivity to external authorities is limited. V’CER can complement any PKI scheme to increase its flexibility and applicability, while ensuring fast dissemination of validation information independent of the network routing or topology. V’CER requires under 3KB storage per node covering $10^6$ certificates. We developed and deployed a prototype of V’CER on an in-orbit satellite and our large-scale simulations demonstrate that V’CER decreases the number of requests for updates from external authorities by over 93%, when nodes are intermittently connected.

1 Introduction

Spurred by new and emerging applications—ranging from IoT to satellite networks—there has been a growing trend of interconnecting large numbers of heterogeneous resource-constrained devices in recent years. In such settings, both devices and networking are constrained: devices have anaemic computation and storage abilities, while networking is characterized by limited bandwidth, low transmission range, dynamic topology, and more critically, by intermittent connectivity due to mobility and/or device hibernation. We use the term constrained networks to describe such settings.

In particular, satellite networks constitute an emerging class of constrained networks [27]. Due to decreased satellite costs (e.g., $22,000 for a CubeSat, including launch [26]) and their increased accessibility (e.g., AWS Ground Station service [2]), the number of operational satellites has doubled to over 4,000 since 2019 [49]. Moreover, the trend towards constellations, i.e., deployment of a network of small satellites (instead of few large ones), will dramatically increase this growth in the years to come. SpaceX’s Starlink alone plans to deploy around 42,000 satellites [48].

However, small satellites have many constraints, such as strict power budgets, radiation-resistant hardware components with limited computing and storage capabilities [3], and physical transmission limitations, e.g., due to periodic line-of-sight blockage by planets and other celestial bodies. While satellite networks might seem to be an extreme example of constrained networks, similar problems arise in terrestrial settings. For example, a number of mesh protocols have been designed to handle poor network conditions for low-power Internet of Things (IoT) devices [7, 25, 55, 56]. Also, similar to line-of-sight disruptions in satellite communication, home/office automation devices often hibernate to conserve power. Unattended outdoor IoT devices that use natural sources of power (solar, wind, etc.) tend to hibernate. Moreover, mobile terrestrial devices can go out of range or encounter communication obstacles. All these conditions result in intermittent or unstable connectivity.

Efficient and secure trust establishment in constrained networks is essential. While small, static, homogeneous networks could rely on symmetric cryptography, large heterogeneous networks require scalable asymmetric cryptography. Public Key Infrastructure (PKI) and public-key certificates are common tools deployed for establishing mutual trust between...
devices. However, timely certificate revocation of malfunctioning or compromised devices is critical for retaining trust in the whole network. Since satellites also suffer from software bugs [13] and can be subject to attacks [47], timely revocation is very important. In fact, the Internet Engineering Task Force (IETF) already recognized the difficulty of revocation in a protocol slated for satellite networks [20].

There is also a large body of literature on PKI in distributed settings, such as observer-based approaches [5, 30, 33, 43], schemes that enable end-users to distributively check their certificates [37, 53], blockchain-based approaches [1, 10], and PKI that is specifically geared towards networks with delay tolerance [15, 17, 41] as well as mobile ad-hoc networks [12, 36, 51, 52]. Furthermore, recent efforts focus on PKI for IoT [24, 45, 50].

As discussed in Section 9, current techniques have some important shortcomings with regard to revocation checks in constrained networks: First, they make strong assumptions about network connectivity or incur heavy communication overhead for the entire network. For instance, on-demand revocation checking, such as Online Certificate Status Protocol (OCSP) [44], requires a reliable connection and separate request for every certificate validation. However, a reliable connection to a central entity cannot be guaranteed in constrained networks. Second, storage and distribution of explicit revocation information, e.g., using Certificate Revocation Lists (CRLs) [8], consumes high bandwidth and storage, including regular updates. However, devices in a constrained network can be highly limited in terms of storage and networking abilities, e.g., the popular Z-Wave low-power IoT technology has a bandwidth of 100Kbps at best [54]. Even recent results that significantly reduce storage and update overheads of CRLs [32, 46] are specifically designed for (generally reliable) Web-based revocation. Thus, they are poorly suited for an environment where devices frequently miss revocation updates. We discuss this in more detail in Section 8.

In summary, efficient certificate validation in constrained networks is still a challenging open problem that we aim to tackle in this paper.

Goals & Contributions: We present V’CER, a novel certificate validation scheme for constrained networks. V’CER provides lightweight certificate validation directly between devices, with minimal communication overhead, by defining operations that allow nodes to epidemically keep each other’s revocation information up-to-date. In a network with 10^6 active certificates, V’CER requires under 3KB of storage per device to allow all devices to mutually authenticate each other, using widely available cryptographic primitives. Furthermore, if devices miss revocation updates, V’CER reduces (by over 93%) the number of devices that need to request fresh validation information from the CA. Our main contributions include:

• V’CER enables flexible and lightweight revocation checks in PKI schemes, especially for device-to-device trust establishment, thus enabling PKI in constrained networks.

• V’CER defines novel algorithms that utilize the deterministic structure of Sparse Merkle Trees (SMTs), which allows devices to keep each other up-to-date. This eliminates the need for the vast majority of devices to contact the CA when updates were missed.

• V’CER introduces the Validation Forest (VF) data structure for efficient exchange of validation information among devices, whenever they come in contact. VF allows for epidemic dissemination of validation information, without the need to consider application-specific network aspects, such as the underlying topology or routing protocols.

• V’CER involves no on-demand requests, while requiring very little storage overhead for devices. At the same time, it offers better security guarantees for constrained networks than prior approaches.

• We evaluate V’CER’s proof-of-concept implementation on the European Space Agency’s OPS-SAT satellite. We then thoroughly evaluate V’CER in a large-scale simulation modeling a constrained network. We also open-source our prototype to the research community.4

2 Background

This section provides background on the data structure that is central for V’CER operation.

2.1 Sparse Merkle Trees

First proposed by Merkle [38], an Merkle Hash Tree (MHT) is an accumulator that efficiently represents a set of data elements and allows to construct Proofs of Inclusion for individual elements [38]. It requires a secure hash function, the digest of which is used to label each element contained in the set. Knowing only the root hash of the tree, anyone can verify whether a given element (leaf) is part of the set by using a small set of hashes (co-path) corresponding to all sibling nodes on the path to root, i.e., a Proof of Inclusion (PoI), which is O(logn) where n is the number of leaves.

An Sparse Merkle Tree (SMT) [34] is a type of MHT which contains all possible hash values, e.g., an SMT for SHA256 has 2256 leaves and depth of 255. When inserting a new element into an SMT, the leaf representing a placeholder is replaced by the new element. Because of the deterministic position of elements in the tree, removing elements is easy. When an element is removed, the root hash changes and a previously valid PoI for the removed element becomes invalid.

4https://github.com/vcer4pki/VCER
While a complete SMT for a reasonable hash function (e.g., SHA256) is not computable, in practice, most leaves need not be assigned. Specifically, all “empty” leaves can be assigned $H(\emptyset)$. Going up such a tree, all hashes above any two empty leaves amount to: $H(H(\emptyset) || H(\emptyset))$, and so on. Therefore, using SHA256 as an example, we can construct all 256 empty branch hashes for all depths in the tree stored in an EmptyHashesList, which covers all hashes in the empty parts of the tree. Since most parts of this SMT are empty, we only need to consider assigned leaves to compute the root.

![SMT example diagram](image)

Figure 1: SMT examples: (a) depicts how the position of hashes is determined and (b) shows a Pol and how depth numbering works.

Figure 1 (a) shows a sample SMT with the five elements $c_1, \ldots, c_5$ for a hash function with a 3-bit digest. Branch colors show how the positioning of the elements works: blue represents an unset bit going left along the branch, and red is a set bit going right. For example, leaf $c_5$ has the hash digest $H(c_5) = 101$, which represents its position in the tree. The three hash digests 010, 100 and 111 are not assigned in this example. Figure 1 (b) shows the path for leaf $c_1$ as green lines in the tree. To construct its Pol, we need its sibling, and all siblings of its ancestors, corresponding to the nodes in green. A Pol for $c_1$ is verified as follows:

(i) The verifier knows the (signed) root and the Pol:

$[H(\emptyset), H(H(c_4) || H(c_2)), H(H(H(\emptyset) || H(c_5)) || H(H(c_3) || H(H(\emptyset))))]$

(ii) The verifier computes the hash of $c_1$, combines it with the first element in the Pol, and hashes both. Next, the result is combined with the second element in the Pol and hashed. Finally, the last hash is combined with the third element in the Pol and hashed.

(iii) The verifier compares the last hash from (ii) with the root value. If they match, the Pol is valid. However, note that, since the sibling leaf of $c_1$ is empty, we can omit it. In a more complex example using SHA256, a Pol would need 256 elements, though most of them will be empty, which can be omitted with the help of the EmptyHashesList. This requires an additional bitmap the same size as the tree height, e.g., 256 bits for SHA256. The bits in the bitmap at every tree level indicate whether an empty hash or an element of the PoI should be used (see Algorithm 6 in Appendix A for details). Because the digest of a strong cryptographic hash function is a pseudo-random value, the hashes of elements are uniformly distributed. Therefore, assigned leaves are evenly spread over the SMT, implying a Pol size of $\log n$ hashes, on average.

3 System Model

We consider three types of entities: CA, Nodes, and cacher Nodes. Nodes are devices that need to validate each other’s public key certificates. We use the term “validation” to focus on the revocation check, i.e., the chain-of-trust verification of certificates is implied. Although a Node can compute hashes and verify signatures, it has limited processing power and storage. A subset of Nodes play the role of cacher Nodes by storing additional information. Communication is constrained due to low bandwidth, mobility, and intermittent connectivity that can result in frequent network partitions. Nodes exchange contact messages whenever they meet. CA is the certificate-issuing authority. Communication with the CA is particularly restricted. We treat CA as a single entity, albeit it might be distributed in practice. Each Node knows CA’s certificate and trusts CA’s signatures. The number of certificates in the system is denoted by $n$. For simplicity, we assume that each Node has exactly one certificate. Further, we assume a coarse time synchronization among Nodes and CA in the range of hours, e.g., to check certificate expiration.

3.1 Adversary Model

We consider the Dolev-Yao model adversary (Adv) that can eavesdrop on, intercept, or inject any number of messages [16]. However, Adv is naturally bound to physical constraints of the network, such as not being able to reach a disconnected Node. In particular, we assume that Adv acts locally, and cannot block all communications in the network at the same time. We assume the Sparse Merkle Tree construction to be secure, i.e., collision-resistant.

3.2 Requirements

As mentioned earlier, designing an efficient distributed certificate validation scheme for constrained networks is challenging, especially since nodes can miss updates, due to connectivity issues. We believe that an ideal scheme must satisfy the following requirements:

R.1: Handle arbitrary delays: Responses from a central entity (CA) might be delayed or lost.

---

\(^*\)Section 7 discusses the setting with multiple CAs.
R.2: Avoid single points of failure: Although centralized systems are easy to set up, they fail when the central entity loses connectivity. Thus, we must avoid relying solely on central entities.

R.3: Consistency: While there is always current local state, validation decisions must be derived from a common trust anchor to ensure consistency.

R.4: Handle constrained devices: A certificate validation scheme must have minimal impact on nodes’ scarce resources.

R.5: Timeliness: Since freshest validation information is crucial for security, an ideal scheme must ensure regular updates and their fastest dissemination.

4 V’CER Overview

V’CER consists of three main components:

(i) Certificate validation via an individual PoI for each Node.

(ii) Efficient spreading of fresh validation information using the Validation Forest ($VF$) data structure. $VF$ is the trust anchor used to validate any PoI.

(iii) Distributed repair whereby up-to-date Nodes directly help outdated Nodes to recover from missed updates.

![Legend:](image)

Figure 2: Example of CA updates being spread in a distributed manner.

Figure 2 is a high-level overview of V’CER operation when there are CA updates, e.g., some certificates are newly revoked. After CA updates the validation information aggregated in $VF$, all Nodes become outdated. In step 1, CA spreads its update information, with which each Node can update both its $VF$ and its PoI. However, in a constrained network, an update would not reach all Nodes. Specifically, the update reaches only the solid green Nodes in step 1, while all the rest miss this update (dotted red Nodes), e.g., by not being connected to the network or by simply hibernating.

After some time, in step 2, some outdated Nodes meet up-to-date Nodes and start to exchange information. Up-to-date Nodes update outdated nodes’ $VF$ (dashed yellow arrows). With a fresh $VF$, a Node can correctly validate other Nodes’ certificates, e.g., reject newly revoked ones. This illustrates one key feature of V’CER: any Node encountering an up-to-date node obtains the latest $VF$ on contact. Thus, fresh validation information spreads very quickly and epidemically.

An outdated Node’s own PoI can become outdated if it misses some updates. Although such a Node can still validate certificates of up-to-date nodes correctly, it cannot provide a proof for its own certificate validity to other Nodes (dashed yellow). However, nodes with up-to-date Pols can help nodes with outdated ones to update their PoI via distributed repair (green dashed arrows). For this, we exploit the deterministic structure of SMTs to design operations for distributed repair, as shown in Section 5.4. In step 2 this succeeds for the node in the center. However, after some time passes in step 3, nodes continue to exchange others, increasing their chance for distributed repair to succeed. Eventually, most nodes would successfully repair their outdated PoI, with only a few having the need to directly request a fresh one from the CA. We demonstrate this in Section 6.3.2.

5 V’CER Certificate Validation Scheme

This section describes all components of V’CER. For certificate validation, Nodes use Proofs of Inclusion to verify that a Node’s certificate is valid. In a simplified example, the CA can build an SMT with all the active certificates’ hashes and Nodes only need to know the root hash of the SMT to verify any PoI. Each Node then stores the PoI for its own certificate, and becomes capable of proving validity of its certificate to others. This is done by computing the PoI’s root hash (see Algorithm 6 in Appendix A) and if it matches the root hash given by CA, the certificate is valid. Thus, Nodes only need to store the respective tree root and their own PoI.

Figure 3 shows individual operations in V’CER. In step 1, the CA constructs the Validation Forest $VF$, as described in Section 5.1. Instead of using a single SMT, $VF$ is a data structure used by Nodes to efficiently keep their certificate validation information up-to-date. Upon any changes in $VF$, e.g., revocations, the CA constructs updates that are processed by the Nodes in step 2, which is described in Section 5.2. As some Nodes may miss these updates, in step 3, Nodes exchange information to keep each other updated and identify which parts of $VF$ are outdated (see Section 5.3). Finally in step 4, Nodes repair each other’s Pols when CA updates are missed, as presented in Section 5.4. We accompany our description with a running example that uses practical parameters. The evaluation in Section 6.3 is also based on this.
example. In terms of cryptographic primitives, the example uses SHA256 and ECDSA signatures based on the secp256r1 curve.

5.1 Validation Forest

The Validation Forest $\cal V$F is the core data structure for validating certificates in V’CER. As long as a Node’s $\cal V$F is up-to-date, it can correctly validate another Node’s certificate with its Pol. $\cal V$F has three main parts. (i) A number of SMT roots for Pol validation. (ii) Aggregator $\cal Aggr$ is a small data structure used for efficient exchange between Nodes to keep their $\cal V$F up-to-date. (iii) CA’s signature of $\cal Aggr$ ($A_r$), which is the trust anchor for all operations in V’CER. Add phrasing that VF represents active cert set.

The number of trees in $\cal V$F is the number of epochs it models. Certificates have a defined maximum lifetime and this lifetime is split into $e$ epochs. A certificate’s expiration date is then used to assign it to the respective epoch tree $T_r$, represented by the epoch root $E_r$ stored in $\cal V$F. Each node stores the $\cal V$F including all $E_r$ and keeps it up-to-date. A Node’s own proof is valid for a single $E_r$, which can be inferred from the certificate’s expiration date. This stabilizes the individual SMTs, significantly reducing the number of potentially outdated Pols on any updates by CA. After an epoch has passed, a forest prune occurs, i.e., the oldest tree is pruned, as it contains only expired certificates. This means that CA and Nodes can discard the oldest $E_r$ and the corresponding $E_r$.

For our accompanying example, we define certificates with a maximum lifetime of around one year, split into weeks as epochs. Thus, $e=52$, meaning that the $\cal V$F stores a maximum of 52 $E_r$, each representing certificates for the corresponding week of expiration. This requires each node to store up to 52 hashes for the tree roots, resulting in ~1.7kB of storage. Assuming that changes occur mostly in the newest epoch, e.g., when new certificates are issued, other epoch trees are left untouched, including their $E_r$. Thus, all current Pols depend on them. This amount of overhead fulfills requirement R.4 for low-storage devices. Other certificate lifetime configurations are possible; however, the primary overhead factor is the revocation update frequency, as we show in Section 6.3.2.

5.1.1 Aggregator

The Aggregator $\cal Aggr$ is used to exchange key information by Nodes about the current $\cal V$F state to help keep it up-to-date among each other. It is designed to be lightweight to allow its inclusion in contact messages Nodes exchange when they meet (cf. Section 5.3). $\cal Aggr$ includes Aggregator root $A_r$, timestamp $A_t$, and checksums $A_c$ to identify outdated tree roots. Furthermore, $\cal Aggr$ is signed by CA. Aggregator signature $A_t$ serves as the trust anchor for Nodes to confirm outcomes of all operations (requirement R.3).

$A_t$ is computed by simply concatenating all tree roots in $\cal V$F and hashing resulting information. Thus, any change in any tree would result in a different $A_t$, and Nodes can use it to check if any parts of their $\cal V$F is outdated. To distinguish among multiple Aggr in terms of freshness, each contains a timestamp $A_t$.

Aggr also contains the checksums $A_c$ for all $E_r$ in $\cal V$F to efficiently identify outdated $E_r$. This avoids having a Node send all tree roots to its peer with an outdated $\cal V$F every time. $A_c$ is split into two types: main and aggregated. Each checksum type has a configurable size. Main checksums are applied directly to tree roots representing newest epochs in $\cal V$F. Aggregated checksums are applied on a number of concatenated tree roots that come after the ones covered by main checksums. The number that is aggregated into a single checksum is configurable in V’CER. Note, while we use the term “checksum”, it is sufficient to simply use some bytes of the hash, as the SMT protects against collisions. This way, tree roots that are expected to change more often than others are covered by their own checksum, e.g., newly issued certificates are inserted into the newest tree. In contrast, $E_r$ that are expected to be more stable get aggregated checksums.

In our example, we use 2 main checksums and aggregate 10 tree roots per aggregated checksum, resulting in 5 aggregated checksums for a total of 7. For $A_t$, we use a 4-Bytes-long UNIX-timestamp. Using 2 Bytes per checksum, this results in $\cal Aggr = 50$ Bytes ($A_r = 32B, A_t = 14B, A_c = 4B$). Also, CA’s signature $A_t$ over $\cal Aggr$ is 64 Bytes. This amount of overhead fulfills requirement R.4 for low-bandwidth devices.

5.2 CA Updates

When any changes occur, CA updates the respective $E_r$ resulting in changes for both $\cal V$F and Pols. Thus, CA needs to distribute updates for Nodes to be up-to-date. To keep the Nodes’ $\cal V$F updated, CA simply needs to distribute new $\cal Aggr$, including new $A_r$ and $E_r$ for affected epochs. Also, if there are no updates for a while, CA can regularly send out current $\cal Aggr$ with new $A_r$. This way, Nodes eventually realize that they are outdated, e.g., even when disconnected for a while.
While this keeps \emph{Nodes}' validation information updated, any PoI found in epochs affected by an update becomes invalid, and respective \emph{Nodes} can no longer provide a valid proof for their certificates. Instead of CA individually distributing updated PoIs to all affected \emph{Nodes}, it constructs universal updates for all \emph{Nodes}. This is done by distributing PoIs for all updated certificates, including revoked ones. Due to the deterministic order of elements in SMT, \emph{Nodes} can process the update PoIs affecting their own epoch to update their PoI. Afterwards, the update PoIs are discarded. Furthermore, when an update contains many PoIs, there are likely many redundant PoI elements that can be aggregated to reduce update size.

Algorithm 1 shows how \emph{Nodes} process update PoIs provided by CA. The operation takes an up-to-date PoI and updates an outdated PoI found in the same epoch. This is then done for all PoIs in the update. The path-bitmaps work as described in Section 2.1. First, the hash of the outdated certificate is XOR-ed with the updated hash and the position of the left-most set bit shows where both PoIs split in the tree. Afterwards, the algorithm checks if the outdated PoI already has an element at the split position, triggering an overwrite of this existing element in the PoI. Otherwise, the outdated PoI needs an additional element at the split position, including a set bit in the bitmap. The hash is computed by calling \texttt{calc_path_root} (see Algorithm 6 in Appendix A), the same algorithm used to validate PoIs, except the optional last parameter indicates the need to stop at the specified depth, instead of the root hash.

Before the split position is reached, every PoI element is updated along the way. This effectively allows to blindly apply updates, meaning a \emph{Node} does not need to worry about the order of applying updates. As long as the PoIs are up-to-date, Algorithm 1 does not perform any destructive updates. Afterwards, the executing \emph{Node} can simply check if the resulting PoI is valid. Under the right circumstances, this may even cover for previously missed updates. We take advantage of this aspect for the distributed repair, described in Section 5.4.1.

\textbf{Epoch Change.} Whenever a new epoch starts, there might be many newly issued certificates. On one hand, the aforementioned forest prune occurs (see Section 5.1), i.e., many certificates will expire. At this point, many \emph{Nodes} will get a new certificate. On the other hand, new \emph{Nodes} may join the network, likewise with new certificates. In V'CER, the issuing of new certificates should be aggregated until an epoch change occurs to increase efficiency. This way, instead of constructing an update bundling many new PoIs, CA can distribute all the certificates hashes as the update, i.e., all epoch tree leaves. This reduces the update size for the epoch change and all \emph{Nodes} that have been issued a new certificate can construct their PoI themselves. Further, this update only needs to be sent to \emph{Nodes} that are affected by the epoch change. The rest of \emph{Nodes} only need the new epoch root for their VF. Additionally, in case an epoch does not contain any revoked certificates, the respective $E$ can be set to $H(\emptyset)$, indicating to the network that any certificates in this epoch are not revoked.

5.3 Aggregator Exchange

When a \emph{Node} missed any updates from CA, its VF will be outdated, and thus it will not have fresh certificate validation information. A key aspect of V'CER is for \emph{Nodes} to be able to efficiently keep each other up-to-date. For this, \emph{Nodes} exchange their Aggregator CERT (cf. Section 5.1.1) with the contact message when they meet. Additionally, \emph{Nodes} will add information about which epoch they belong to and if they have any caches ready. Both are important for the distributed repair, explained in Section 5.4, and in our accompanying example 1 Byte is sufficient (6 bits for the epoch and 2 bits as flags for caches).

\emph{Nodes} only need an up-to-date VF to be able to correctly validate PoIs for any certificate. This ensures that the current
validation information spreads as quickly as possible throughout the network, without the need to consider any transmission aspects, such as acknowledgments from each Node to CA to all Nodes are up-to-date. For example, if a certificate was revoked and CA sends out an update, even a Node missing this update will meet an up-to-date node eventually and after the Aggr exchange, inherently know about the revocation, i.e., reject the revoked certificate’s PoI. Thus, this meets the requirement R.2 and R.5 for validating certificates.

Figure 4 depicts such an exchange in detail. After both exchanged their Aggr, the outdated Node on the right will see a new Aggregator root A, as well as a newer timestamp A, and realize its V_F is outdated. To identify which trees are actually affected by the change, the outdated Node will check the parities A, and send the up-to-date Node the respective outdated checksum identifiers. The up-to-date Node will answer with the respective E_r and add A. The outdated Node is then able to update all of the tree roots in its V_F, re-calculate its Aggr, and finally check if A_r is valid. If one of the actually changed E_r is found in the same epoch as the Node’s own certificate, it can imply that its PoI is outdated. There is also the case that E_r has changed; yet, the corresponding A_r resulted in the same as before. In this unlikely case, the outdated Node has to request all E_r, i.e., V_F.

In our example, let us assume there has been a change in the second newest epoch (covered by a main checksum) and 26th epoch in the middle. Thus, the outdated Node will request the second and fifth checksum. The up-to-date Node will respond with the 11 respective E_r, which allows the outdated Node to update its V_F. This entire exchange will require around 470 Bytes of communication overhead \((Aggr + 11 \cdot E_r)\) directly between the two Nodes.

### 5.4 Distributed Repair

While the Aggr exchange ensures that Nodes update their certificate validation information as fast as possible, missed updates may also lead to a Node’s own PoI to be outdated. However, a key goal of V’CER is to avoid having the outdated Node to contact CA and request a fresh PoI. Otherwise, many Nodes individually requesting fresh PoIs at a similar time leads to a significant overhead for the entire network. Thus, in this section we will present ways how an up-to-date Node can directly help an outdated Node to repair its PoI. After an outdated Node updated its Aggr, it will realize its PoI is not valid and can start requesting repair information from up-to-date Nodes it meets. In the following, we will present two different approaches for this. One is directly leveraging up-to-date PoIs from other Nodes. The other approach introduces a cache, stored and maintained by a share of Nodes in the network for increased efficacy of distributed repairs. With these operations, V’CER meets requirement R.2 for a Node’s own validation proof.

![Figure 4: Exchange of Nodes for distributed repair for the three main operations.](image-url)
5.4.1 Direct PoI Repair

With the direct PoI repair strategy, an outdated Node can collect up-to-date PoIs from other Nodes it meets to potentially repair its outdated PoI. Figure 4 depicts how such an exchange proceeds. After the initial repair exchange on contact, the outdated Node knows if the other is up-to-date and if its certificate is found in the same epoch. If both are true, the outdated Node will request the other’s PoI, check if it is actually valid regarding the current \( E_r \), and if so, use it for repair.

The outdated Node leverages Algorithm 1 for this, as mentioned in Section 5.2. The operation replaces all applicable elements in the outdated PoI with the elements in the up-to-date PoI. If the position of the up-to-date Node’s leaf is favorable, it will update one or more elements in the outdated PoI. In an unfavorable case, elements will simply remain unchanged. This process can be repeated with other up-to-date PoIs in the same epoch, until the Node’s own PoI is valid regarding the current \( E_r \). This gets more difficult the more updates a Node missed for its epoch, which we evaluate in Section 6.2. As Algorithm 1 works by blindly replacing elements in the PoI, the outdated Node must first verify the PoI used for the repair is actually valid for the current

5.4.2 Level-Cache Repair

For the Level-Cache (LC) strategy, a share of Nodes with larger storage capacity, called cacher, may additionally keep all hashes of each \( E_r \) on a specified depth, i.e., the cache level \( clvl \). This results in a storage overhead of \( 2^{clvl} \) hashes per epoch. As mentioned in Section 2.1, the leaves of an \( E_r \) are uniformly distributed. Due to this fact, the higher depth levels of the SMT are likely to be assigned before the lower ones. If enough elements were inserted, the first few depth levels of a SMT will form a fully filled sub-tree. Further, most updates in its PoI from the perspective of one Node will likely be in this sub-tree.

To clarify this phenomenon, consider the example of a SMT with one leaf that is only zeros. Any new leaf that is inserted will go to a different path at one point in the tree, which creates the need for an additional element in the PoIs for both leaves. The chances that any new leaf will branch off to the second half of the tree, i.e., the leaf having a set bit on the most-left position, are 50%. The likelihood of branching off on the second depth level is 25%, and halves for any further depth level. Thus, when inserting many leaves, the first depth levels in the SMT will likely branch off first. This implicitly means, that given an up-to-date LC, outdated Nodes are likely able to repair their own PoI with it. The exact probabilities of this are discussed in Section 6.2. Furthermore, Nodes may use LCs with different \( clvl \)s, e.g., more resourceful Nodes may keep a larger cache and more limited Nodes a smaller one, if any at all. To avoid having to send the entire LC to an outdated Node, it will instead send its outdated PoI to the cacher Node, as shown in Figure 4.

In our example, we chose to equip a share of Nodes with a LC for \( clvl = 7 \). This means that these cacher Nodes will store an additional 4KB per epoch, and thus 208KB in total. In Section 7, we will discuss possible alternative strategies; yet, for our purposes we set all cachers to store a LC with the same \( clvl \) for all epochs.

Algorithm 2 update_lvl_cache_with_poi for updating the level-cache regarding a new proof of inclusion

\[ \text{Input: } LC, clvl, new\_leaf\_hash, new\_path, new\_path\_bitmap \]
\[ \text{Output: } LC \]
1: \( delete\_bits \leftarrow 2^{(clvl - clvl)} - 1 \)
2: \( part\_no \leftarrow new\_leaf\_hash \& \neg delete\_bits \)
3: \( part\_no \leftarrow part\_no >\rangle (\lll - clvl) \)
\( \triangleright \) take \( clvl \) left-most bits that define position in LC
4: \( update\_hash \leftarrow calc\_path\_root\_new\_leaf\_hash, new\_path, new\_path\_bitmap, clvl \)
\( \triangleright \) calculate path’s root, but stop at depth \( clvl \)
5: \( LC[part\_no] \leftarrow update\_hash \)
6: return \( LC \)

However, the cacher needs to keep its LC up-to-date as well. The construction of the LC is described in Appendix A.2.4. The cacher uses Algorithm 2 to process \( CA \) updates for one epoch. First, it extracts the correct position in LC to be updated by the new PoI. Afterwards, it uses the PoI root hash calculation, with the only difference that it stops at \( clvl \) and inserts the resulting hash at the respective position of LC. When the cacher itself misses \( CA \) updates, it may also meet other cacher Nodes and request up-to-date LCs from them.

Algorithm 3 update_poi_with_lvl_cache for updating a proof of inclusion with a given level-cache

\[ \text{Input: } my\_leaf\_hash, my\_path, LC, clvl \]
\[ \text{Output: } my\_path \]
1: \( delete\_bitmap \leftarrow 2^{(clvl - clvl)} - 1 \)
2: \( part\_no \leftarrow my\_leaf\_hash \& \neg delete\_bitmap \)
3: \( part\_no \leftarrow part\_no >\rangle (\lll - clvl) \)
4: \( part\_neg \leftarrow \neg part\_no \)
\( \triangleright \) negated bits of \( part\_no \) define its hash-neighboring in LC
5: for \( i \leftarrow 0 \) to \( clvl \) do
6: \( new\_hash \leftarrow calc\_pos\_in\_LC(part\_neg, (i + 1), LC) \)
\( \triangleright \) constructs a hash at position \( part\_neg \) at depth \( (i + 1) \) with the LC
7: \( my\_path[my\_path - 1 - i] \leftarrow new\_hash \)
8: \( part\_neg[clvl - 1 - i] \leftarrow part\_neg[clvl - 1 - i] \)
\( \triangleright \) flip bit to get hash-neighbor for next depth
9: return \( my\_path \)

To update a PoI with a LC, Algorithm 3 is used. Like in Algorithm 2, the first three lines construct the position of the targeted cache element in LC. Then, for all \( clvl \), the respective neighborhood hash of the outdated PoI is constructed with the help of \( calc\_pos\_in\_LC \). This function simply takes a position and depth, which are used to construct a hash further up the tree in LC. The resulting hash is then set in the correct position in the outdated PoI. This process is repeated for all.
depth levels in $LC$, as the lower depth PoI elements can be updated as well. This operation blindly replaces PoI elements and may not entirely repair the leaf’s PoI. However, if it cannot entirely repair the PoI it will still repair elements that $LC$ provides and at least assists in the overall repair process of the outdated $Node$. In Section 6.2 we show that $LC$ can repair outdated PoIs with high probability, given appropriately chosen parameters.

6 Evaluation

In this section, we evaluate V’CER regarding multiple aspects. First, we evaluate its security, followed by an analysis on the success probabilities of the distributed repair approaches we introduced. Finally, we will consider V’CER’s performance regarding run-time overhead and large-scale networks.

6.1 Security

As V’CER provides the means to validate certificates, the adversary $Adv$ aims to convince $Nodes$ that (i) a revoked or forged certificate is valid, or (ii) a valid certificate is revoked. In the following, we will explore different strategies $Adv$ may use to achieve this goal and explain how V’CER prevents their success.

Manipulating Updates. To achieve either (i) or (ii), $Adv$ can try to counterfeit updates by disseminating a new $E$, that reflects the false state of the targeted certificate, i.e., a valid PoI. However, a false $E$ in $VF$ would also result in a different $A_r$. As $Aggr$ is signed by $CA$ via $A_r$, $Nodes$ with an up-to-date $Aggr$ will discard the counterfeit update as invalid.

Blocking Updates. $Adv$ can isolate a $Node$ preventing $CA$ updates to reach it or delay update messages such that they receive them after the validation. This way, a recently compromised certificate would still be validated regarding the outdated $VF$, making $Adv$ achieve (i). This requires $Adv$ to block any contact of the outdated $Node$ with up-to-date $Nodes$, to prevent them to update their $VF$. This gets increasingly more difficult with increased network connectivity and more opportunities to meet nodes. Nevertheless, as $CA$ regularly sends out an updated $Aggr$, even isolated $Nodes$ will eventually consider their current $VF$ to be outdated, and thus reject any PoIs. This limits the vulnerability window for $Adv$, similar to Certificate Revocation Lists (CRLs) or certificates with a limited lifetime, as considered in related works (cf. Section 9). However, we consider completely isolating $Nodes$ as non-trivial, and thus V’CER provides better security than schemes relying on a more centralized distribution of updates, as $Adv$ needs to prevent a $Node$ to communicate with more entities.

Denial-of-Service. Instead of preventing updates from reaching an individual $Node$, a powerful $Adv$ could also perform a DoS attack on the entire network to prevent it from receiving updates to achieve (i). Expecting a regular update of $Aggr$ by $CA$, all $Nodes$ will eventually consider their $VF$ to be stale. Again, the vulnerability window is similar to other revocation checks.

Destructive Repair. To achieve (ii), $Adv$ can target a $Node$ with an outdated PoI and send it false repair information to prevent it from obtaining a valid proof for its certificate after an applicable $CA$ update. As described in Section 5.4 an outdated $Node$ ensures the correctness of repair information regarding its up-to-date $VF$ before applying the repair. This way, any invalid repair information is detected. Further, meeting any benign $Nodes$ may result in a repaired PoI anyway and for $Adv$ to prevent this, requires it to isolate the $Node$. Finally, a $Node$ with an outdated PoI will give up on repairs eventually and request its valid PoI directly from $CA$.

6.2 Distributed Repair Analysis

In this section, we evaluate the effectiveness of distributed repair approaches. Note that the following results are for a single SMT; yet, $VF$ will consist of a tree per epoch. For example, assuming individual PoI updates are evenly distributed among all epochs, the number of total missed updates needs to be divided by the number of epochs. For this, we ran simulations on a pre-generated SMT with 100,000 random leaves and averaged the results over 10,000 runs.

Direct PoI Repair Analysis. We now present simulation results regarding the repair of an outdated PoI by using random up-to-date PoIs, as described in Section 5.4.1. From the perspective of an outdated $Node$, the key driver for success is the distance of the missed updated leaves from the $Node$’s own leaf in the SMT. The closer any missed updated leaf is, the fewer PoIs overall can help with the repair. The more updates are missed, the higher the probability that one of them is unfavorable for an outdated $Node$.

Figure 5 shows the simulation results for this strategy with an increasingly higher number of missed updates. first depicts the percentage of runs which failed to repair the outdated PoI on the first try and first 10 for the first ten tries. After trying 100 PoIs, the run gave up and consider the attempt failed. Thus, fails shows the percentage of runs that stopped after 100 tries. Finally, avg. try sketches the average number of PoIs it took to successfully repair the outdated PoI.

Level-Cache Repair Analysis. From a theoretical perspective, each $LC$ divides each $E_r$ into $2^{clvl}$ parts. An outdated $Node$ should be able to successfully use an up-to-date $LC$ to repair its PoI, if no updates happened in the same part as its
We implemented a prototype of V’CER to evaluate run-time performance of all basic operations and distributed repair. The prototype is written in Python. While Python is not optimal in terms of performance on constrained devices, we believe that it suffices for a prototype. Further, we used Python’s `hashlib` for hash computations, which internally calls the OpenSSL native library [42]. Hash computations constitute the majority of computational overhead in V’CER. The prototype is available on GitHub3.

To show the feasibility for one of the most challenging constrained networks, satellite networks, we deployed the prototype on ESA’s OPS-SAT satellite, an in-orbit platform that is open for any party to register and upload experiments [19]. For this, we adjusted our prototype’s code to run as a NanoSat MO Framework app [23], a straightforward way to run code on OPS-SAT, as it provides crucial services, such as data encoding for transmissions. For this, we had to convert our prototype to Java, a requirement to use the MO Framework. The Java prototype uses the internal `BigInteger` class for the bit-operations and the internal `MessageDigest` class for the hash calculations. On the ground, we ran `CA` and deployed two additional devices, which were connected to ESA’s satellite dish via a SSH tunnel to transmit data from and to the satellite. OPS-SAT uses the S-Band frequencies as the main link for data communication, with up to 256 kbit/s for communication from the satellite and 1 Mbit/s to the satellite [19]. Due to OPS-SAT’s polar orbit and a single satellite dish in central Europe, a rough estimate for the amount of communication opportunities is less than 6 passes per day, each with less than 10 minutes of varying bandwidth capacity. This allowed us to successfully test V’CER’s feasibility on a deployed satellite with constrained communication, including revocation checks, uploading `CA` updates, and distributed repairs between devices.

In the following, we present performance measurements over 1000 executions for the most complex aspects of V’CER. We use SHA-256 as a hash algorithm and `secp256r1` ECDSA for signatures. OPS-SAT runs on a Altera Cyclone V SoC with 800MHz and 1GB of RAM, while on the ground one device runs on a Raspberry Pi 3B+ with 1.4 GHz and 4GB of RAM, the other on a Raspberry Pi Zero W with 1GHz and 512MB of RAM. Note that OPS-SAT also runs other crucial systems in parallel, such as the Attitude Determination and Control System (ADCS). Furthermore, while OPS-SAT is quite powerful compared to other deployed satellites, upcoming satellite hardware will be more powerful, e.g., see the DAHLIA project [14] or the RAD5500 [4]. Results in Table 1 indicate that even with a much weaker (in terms of performance and RAM) system the execution of the individual steps is still fast, keeping most execution times in the range of approximately less than 40ms. An exception is processing 20 update PoIs, which is quite a high number for a single epoch and expected to be rare. This makes V’CER practical even for low-power devices, and thus fulfills requirement R.4 for low-performance devices.

3https://github.com/vcer4pki/VCER
Table 1: Run-time measurements of V’CER, @A refers to the Raspberry Pi 3B+, @B refers to the Raspberry Pi Zero W, @C refers to the OPS-SAT satellite.

<table>
<thead>
<tr>
<th>Operation</th>
<th>@A [ms]</th>
<th>@B [ms]</th>
<th>@C [ms]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature check &amp; Aggr exchange</td>
<td>2.915</td>
<td>6.869</td>
<td>31.008</td>
</tr>
<tr>
<td>Pol authentication</td>
<td>3.776</td>
<td>19.847</td>
<td>228.083</td>
</tr>
<tr>
<td>Processing 20 update Pols</td>
<td>76.929</td>
<td>407.744</td>
<td>4544.915</td>
</tr>
<tr>
<td>Single Pol repair</td>
<td>7.574</td>
<td>39.377</td>
<td>452.260</td>
</tr>
<tr>
<td>LC (clvl = 7) repair</td>
<td>6.191</td>
<td>29.474</td>
<td>264.278</td>
</tr>
</tbody>
</table>

6.3.2 Large-Scale Performance

To evaluate V’CER in terms of scalability, we implemented a large-scale network simulation in Python, directly leveraging the prototype described in Section 6.3.1, running on an Intel Xeon CPU E5-2650 v3 @ 2.30GHz with 10 cores and 256GB of memory. The simulation runs are executed with an increasing number of $\text{Nodes}$, from 10000 up to a million, over the course of 4 simulated weeks. In line with related work, we simulate the aspects that affect V’CER’s efficiency, i.e., communication overhead over the entire network. For instance, delays for individual communications between nodes will not significantly affect the system. As with the accompanying example in Section 5, we use the SHA256 hash function and secp256r1 ECDSA for signatures. Further, $\mathcal{VF}$ is split into 52 epochs, representing 52 weeks of a lifetime of one year per certificate, and 7 parities consisting of 2 Bytes for each $\mathcal{A}$.

Each simulated week, an epoch change occurs, which executes the forest prune (cf. Section 5.1) and issues $0.1\%$ new certificates ($\sim5\%$ yearly). On each day in the simulation, $0.028\%$ of the active certificates are revoked ($\sim10\%$ yearly), which are re-issued the next day in the newest epoch. For example, as IoT devices are notorious for having security bugs, we assume a relatively large share of yearly revocations. Our share of revocations is based on the estimate of certificates affected by the Heartbleed bug in the Internet [35], one of the biggest recorded revocation events. Splitting the yearly revocations in days is in-line with related work [46], as even in the case of Heartbleed, revocations occurred gradually [35].

Every time $\mathcal{CA}$ distributes an update, a random share of $\text{Nodes}$ do not receive the update, i.e., become outdated. We simulated different missing shares of $10\%$, $30\%$, and $50\%$ in separate runs. $10\%$ of $\text{Nodes}$ are cachers that additionally store a $\text{LC}$ with $\text{clvl} = 7$; yet, also can miss updates. For outdated $\text{Nodes}$ to repair their own validation information, each Node encounters 5 random $\text{Nodes}$ each hour. During those encounters, both $\text{Nodes}$ exchange $\text{Aggr}$, update their $\mathcal{VF}$ if applicable as well as notice outdated validation information, and if only one Node is outdated try the distributed repair. After an outdated Node has met 30 up-to-date $\text{Nodes}$ and was not able to repair its validation information, it will give up and request it directly from $\mathcal{CA}$.

Figure 7 shows the measurements of two failure percent-ages. The failed repairs shows the share of outdated $\text{Nodes}$, which were not able to distributively repair their validation information and instead, required a direct request to $\mathcal{CA}$. Even in the drastic case of $50\%$ $\text{Nodes}$ missing updates with 1 million $\text{Nodes}$ total, more than $93\%$ of the outdated $\text{Nodes}$ are able to collaboratively repair their PoI. Therefore, V’CER fulfills requirement R.1 and R.5 for a $\mathcal{Node}$’s own validation proof. Outdated $\text{Nodes}$ need to meet $8.9$, $9.3$, and $10.1$ up-to-date $\text{Nodes}$ on average until the distributed repair is successful. For $10\%$, $30\%$, and $50\%$ of $\text{Nodes}$ missing updates respectively. Assuming only one of the two $\text{Nodes}$ in an encounter needs an up-to-date PoI, e.g., to establish a secure channel without mutual authentication, we also measured the percentage of encounters in which both $\text{Nodes}$ are outdated. With 1 million $\text{Nodes}$ and 50% $\text{Nodes}$ missing updates, there are less than 5% of encounters, in which both do not have an up-to-date PoI.

Figure 8 depicts three key communication overhead measurements. The graphs for nodes weekly exchange represents the average amount of exchanged Kilobytes directly between $\text{Nodes}$, per node per week. This includes the $\text{Aggr}$ exchange, $\mathcal{VF}$ repair, and distributed repair of outdated Pols. With 1 mil-
lion \textit{Nodes} and 10\% of \textit{Nodes} missing updates, \textit{Nodes} directly exchange 27.2KB per week and 81.6KB with 50\%. The CA update size is the average update size sent out daily by CA. This contains both the revocations as well as the re-issuance the day after revocation (0.056\% of total number of \textit{Nodes}). This metric is independent of the missing share and for 1 million \textit{Nodes}, the daily CA update is 179.3KB on average. Finally, the epoch change size shows the size of the weekly update sent out by CA. Independent of the missing share as well, the epoch change is 629.8KB. Note, as mentioned in Section 5.2, that the epoch change update does not need to be distributed to all of the network and only needs to be sent to \textit{Nodes} affected by epoch change.

7 Discussion

This section discusses various practical aspects of V’CER.

PKI integration. Since V’CER only deals with certificate validation, it needs a Public Key Infrastructure (PKI) as the basis for deployment. To the best of our knowledge, V’CER can be used alongside any PKI scheme, similar to OCSP Stapling, by having the prover provide validation evidence (see Section 8). Ideally, the authentication PoI is directly sent along with the certificate during the handshake protocol to reduce communication overhead. Furthermore, to allow audit of individual changes, CA can keep a log of all individual operations, such as revocation of a certificate. External observers need only to store the resulting \textit{Aggr} for each CA update, allowing them to verify CA logs after the fact.

Multiple Certificate Authorities. While we assume a single Certificate Authority (CA) throughout the paper, in some real-world use-cases there multiple CAs can be involved. This can be accommodated by employing a committee that acts as a single CA via consensus among the members, for all operations. For example, a signature scheme to allow for such a strategy are BLS signatures [9], which can model the necessary threshold-based signatures to create \textit{A}, verifiable by \textit{Nodes}. Alternatively, each member can maintain its own \textit{VF} and be responsible for certifying their distinct group of nodes in the network. In such a case, a node from one vendor can simply collect and keep the most recent \textit{VF} of other vendors to authenticate their nodes. \textit{Nodes} would only have to deal with PoI updates regarding their vendor’s \textit{VF}, while only keeping the other \textit{VF} up-to-date.

Caching Certificates. If a \textit{Node} regularly communicates with another \textit{Node}, the other \textit{Node}’s certificate and PoI can be cached to avoid subsequent redundant checks. A \textit{Node} can keep cached PoIs up-to-date, just like it does for its own PoI. This way, there is a good chance that cached certificates are ready for use, even after many updates. If any cached PoIs get revoked, they can be discarded. Furthermore, since a \textit{Node} can provide many up-to-date PoIs to an outdated node, this strategy can vastly improve the direct PoI repair approach, as discussed in Section 5.4.1).

Dynamic Cache Sizes. While we assumed uniform use of \textit{LC}, i.e., all cacher \textit{Nodes} use the same \textit{clvl} across all epochs in \textit{VF}, it may be advantageous in some scenarios to use a dynamic cache size. On the one hand, cacher \textit{Nodes} with bigger storage can also keep bigger caches, allowing them to succeed more often when executing distributed repairs. On the other hand, the same cacher may use different cache sizes for different epochs. For example, if most updates are expected within newer epochs, a cacher can use a bigger cache for these than for almost expired epochs. Note, a bigger \textit{LC} can easily construct a smaller one, e.g., when transitioning to a smaller cache on an epoch change.

8 Comparison to OCSP and CRL schemes

This section focuses on comparing V’CER to the most commonly found types of schemes found in the revocation space, Online Certificate Status Protocol (OCSP), CRLs, and variants that improve on CRLs.

OCSP Stapling. In OCSP, the verifier of a certificate directly requests a confirmation from CA that the certificate is not revoked. Due to the on-demand nature of OCSP, it is not directly applicable to our system model (cf. Section 3), as it requires a fast and reliable connection to CA to properly function. Nevertheless, there is also OCSP Stapling. Here, the proving party requests the OCSP for its own certificate, stores it, and directly delivers it to the verifier. Each OCSP has a validity period that enforces a fresh OCSP eventually. A single OCSP request is around 4KB in size [35]. However, if we assume the same validity period as in our accompanying example of a single day, this means all \textit{Nodes} in the network each needs to request a new OCSP daily. For example, even with 100000 \textit{Nodes}, this would already amount to around 390MB of communication overhead across the network, compared to our 18.4KB via the universal CA update.

Traditional CRLs. With the CRL approach, \textit{Nodes} need to maintain and store the entire CRL. However, these lists can grow very large. For example, in the Internet the CRLs size for the median certificate is 51KB, ranging up to 76MB for a single CRL [35]. Yet, even assuming an optimal CRL, i.e., storing only strictly necessary entries, would already require over 3.6MB of storage to cover for the whole year with 1 million \textit{Nodes} (as in our evaluation)—assuming an average of 38 Bytes per entry [35]. In contrast, \textit{Nodes} in V’CER only need to store ~3KB to achieve the same.
**Enhanced CRLs.** While traditional CRLs can be very large, there are numerous works to significantly reduce the storage and update overhead. To the best of our knowledge, the most notable works in this space recently are CRLlite [32] and Let’s Revoke [46]. Both aim to reduce storage and update sizes of revocation information for the Internet. CRLlite uses a cascade of decreasingly smaller bloom filters to aggregate revocation information. For 1 million certificates, this requires ~112.5KB of storage [32]. Delta updates model the difference between the old and the new bloom filters on all levels, which can be applied in a XOR-like fashion. Modeling a change of 0.056% in the contained certificates, e.g., on daily revocations plus re-issuance (as in our evaluation), requires around 10% to 50% of the original filter size (according to the measurements presented in Figure 6 in [32]). Let’s Revoke [46] uses a bitvector per expiration day per CA, which flags if consecutively numbered certificates have been revoked. As these bitvectors are expected to have many zeroes, they can further be compressed to save storage space. With 1 million certificates and 10% of them revoked, this requires ~70KB of storage (~125KB when not compressed) [46]. For delta updates, bitvectors are constructed that can be applied to the original bitvectors via simple bit operations. A compressed update modeling 0.056% of certificate changes is ~2KB in size [46]. Note, these schemes are specifically designed for the Web’s PKI and are not concerned with constrained networks.

Both approaches require nodes that missed updates to directly contact any authority or their delegates (e.g., aggregators in [32]) to keep up-to-date. In this case, outdated nodes need to individually request the specific range of updates they missed. On the one hand, this requires careful placement of delegates regarding the targeted topology to ensure coverage, which is difficult in many constrained networks, e.g., due to the nature of a dynamic topology. On the other hand, all affected nodes would need to individually request missed updates. For example, a 2KB delta update in Let’s Revoke [46] for 1 million nodes with 10% of nodes missing a single update would surmount to 195MB of communication overhead across the network.

In contrast, V’CER only requires less than 3KB of storage on each node and uses universal updates that can be applied at any time, e.g., even though a node missed an update, it may receive a subsequent update in the meantime, which may repair its proof without further requests. Nodes in V’CER can also help each other to distributively repair their proof, eliminating the need for individual requests to the CA for the principal share of nodes (as shown in Section 6.3.2). Further, even if the distributed repair fails for nodes, with the up-to-date and quickly disseminated PoI they can still correctly validate other certificates. Finally, when nodes do need to request their fresh PoI from the CA, it only requires less than 1KB of communication overhead each.

**9 Related Work**

In the following, we will examine the related work in the field of certificate validation. Aside the ones mentioned throughout this section, there are also works that focus on constructing PKIs for Internet of Things (IoT); yet, for revocation checks, they rely on CRLs [50], on-demand checks [24] that we both discussed in Section 8, or are blockchain-based [28, 45], which we examine later in this section. Otherwise, recent works are dominated by observer-based approaches among CAs, end-user-based approaches, or blockchain-based approaches. Finally, we compare preceding works focusing on efficient validation for untrusted validation directories with V’CER.

**Observer-based approaches.** These works focus on restricting maliciously acting CAs by monitoring them for suspicious behavior. Most prominent in this area is Certificate Transparency (CT) [33], already adopted by many CAs and browsers for the Internet. In this approach, an append-only Merkle Tree is used to log all issued certificates by a CA as hash leaves. On issuing, the CA publishes the new certificates along with a consistency proof, which proves that the previous Merkle Tree is contained in the now extended tree. Observers, such as other CAs, check if the new certificates contain any unjustly issued ones, e.g., for domains that the issuing CA is not responsible for. The consistency proof ensures all certificates were published and correctly appended to the CA’s Merkle Tree. On the end-user side, aside from validating the certificate directly with the issuing CA, the client additionally requests the PoI of the certificate from multiple observers. Falsely issued certificates then become apparent; yet, this does not cover revocations. An informal report by Laurie and Kasper hints at extending CT with Sparse Merkle Trees to provide Revocation Transparency [34].

Enhanced Certificate Transparency [43] aims to extend the CT approach to also handle revocations efficiently. The authors argue that search in the Revocation Transparency proposal [34] remains linear in the number of issued certificates. Aside an append-only Merkle Tree as in CT, the paper introduces an additional tree that is ordered by the subject identities, allowing for logarithmic look-up of revocations. Nevertheless, to ensure consistency, each observer still needs to verify all certificates published and their inclusion into the respective trees. The paper mentions its approach can be extended in a distributed manner, so users require less trust into the CAs. However, this would require random monitoring of CAs by all users as well as gossiping the observed information to identify inconsistencies. Further work focuses on improving resilience of these approaches against colluding CAs, such as AKI [30] or ARPKI [5].

While these observer-based approaches use similar cryptographic structures to V’CER, i.e., hash trees and PoIs, they aim at the orthogonal goal of limiting malicious behavior of CAs by giving them the means to efficiently monitor each
other. V’CER, on the other hand, provides efficient certificate validation for end users among each other. Further, V’CER is not reliant on having reliable connectivity to trusted parties for validation.

**End-user-based approaches.** These approaches aim to modify the observer-based schemes to allow end-users to monitor for inconsistencies regarding their certificates themselves. In CONIKS [37], a Prefix Merkle Tree is used, along with randomly generated user IDs, to protect the privacy of users. Here, all users need to constantly check all issuing parties for certificates of their own domain, to recognize abuse. When the issuing CA updates its tree in any way, it also needs to re-issue all of its users’ PoIs so they are correct with respect to the new tree root. Revocation is handled by on-demand requests to the respective CA. DTKI [53] aims to provide users full data ownership for their certificates by introducing a Merkle Tree log per individual domain. Each log is maintained in a decentralized database, based on consensus of multiple independent entities. Users need to gossip all tree roots among each other to prevent problems on network partitioning. Additionally, DTKI revocation is also done with on-demand requests.

These approaches provide users capabilities to monitor their own domains. However, they are very communication heavy and rely on on-demand requests to check for revocation, making them unsuitable for constrained networks. In contrast, V’CER requires minimal communication by only distributing a number of hashes, i.e., \( \varphi \). Further, it allows nodes to collaboratively repair their individual validation proof, mostly without the need to contact any authorities.

**Blockchain-based approaches.** The works in this area aim to shift trust from the CAs to the blockchain. One of the first proposals in this area is Certcoin [21], which builds a decentralized PKI based on Namecoin [29]. The idea is to simply store all certificate updates, including revocation, on the blockchain. A certificate owner may send the PoI for the block containing the certificate for validation, similar to Bitcoin’s Simplified Payment Verification [6]. This requires a user to monitor and store all block headers, instead of the full blockchain. Analogously, Blockstack [1] directly builds on Bitcoin for improved security and separates different abstraction layers for simplified access. For certificate validation, a user contacts multiple full nodes (i.e., storing the entire blockchain) and checks if the responses are consistent with each other. EthIKS [10] simply puts CONIKS [37] on top of Ethereum [11] and uses smart contracts for global monitoring and validation of certificates.

All these approaches share the notion of having, at least indirect, access to the blockchain. This is difficult to guarantee in constrained networks or requires significant storage overhead on limited devices. On the contrary, V’CER only requires minimal storage overhead, without the need to be constantly connected to any specific nodes.

**PKI for dynamic networks.** There are approaches specifically aiming to construct PKIs for constrained networks. There are many works focusing on Mobile Ad-Hoc Networks [12,36,51,52] and Delay-Tolerant Networks [15,17,41]. Note, the latter is considered the state of the art for satellite networks. They generally aim to distribute the role of the CA among the network of nodes. This usually requires a lot of coordination between all nodes. However, the key aspect in the context of this work is how revocation is handled. For this, the approaches either rely on traditional CRLs [51,52], individual revocation information aggregated by exchanging them among the network [12,15,36], or by simply limiting the lifetime of certificates [12,41].

To the best of our knowledge, all schemes in these areas either share similar problems of CRLs, require communication heavy coordination between nodes, or introduce an additional vulnerability window. In V’CER the vulnerability window can be kept to a minimum, as it relies on distributing only \( \varphi \). Otherwise, it minimizes the communication overhead required, making it well suited for constrained networks.

**Efficient Validation Directories.** There have been several works aiming to provide efficient certificate validation [18,22,31,39,40]. They use authenticated data structures providing efficient validation proofs, to allow the use of untrusted directories capable of answering validation requests, while removing the need for distributing entire CRLs. The reduced communication overhead enables shorter validity periods of revocation information, e.g., daily or even hourly. The data structures are either based on trees for revocation [31,40], trees covering both revocation and validation [22], hash-chains containing all validity periods [39], or a combination of both hash-chains and trees [18].

These approaches aim at supplying directories with fresh validation information by regular updates from the CAs, e.g., by distributing tree updates [22,31,40]. In contrast, V’CER supplies all nodes with fresh validation information by only distributing \( \varphi \). Nodes can additionally collaborate without any special directories to keep their proofs up-to-date.

**10 Conclusion**

In this work, we presented V’CER, a novel certificate validation scheme, which is designed to work in a distributed and efficient manner. V’CER can be used to augment any PKI scheme, enabling it to work even in constrained networks. This is achieved by introducing data structures and operations that allow for fast dissemination of validation information as well as a collaborative way for nodes to keep up-to-date. We have demonstrated the efficacy and efficiency of V’CER with large-scale simulations modeling a constrained network.
Acknowledgments

The authors of the Technical University of Darmstadt were supported by the European Space Operations Centre with the Networking/Partnering Initiative and the European Union’s Horizon 2020 Research and Innovation program under Grant Agreement No. 952697 (ASSURED). Gene Tsudik’s work was supported in part by NSF awards SATC-1956393 and CICI-1840197, as well as a subcontract from Peraton Labs.

References


A.2 CA Operations

This section describes how V’CER does basic operations. We use an incremental approach using the Look-Up-Table.

A.2.1 Add Leaf to SMT

This operation is executed by the CA and adds one leaf hash to an epoch tree while updating the LUT for subsequent operations. Figure 1 (b) illustrates how it works for \( c_1 \). Starting from the leaf, the operation will go up the tree, look-up the respective neighbor in the LUT (see green nodes), calculate and set the intermediate nodes along the leaf’s path in the LUT (see green line), and repeat this process until reaching the root. For the initial epoch tree construction or processing multiple updates, this operation is called multiple times individually for each leaf.

Algorithm 4 describes the operation in detail. First, it sets the hash to be added on the respective leaf position in line 1. It traverses the tree from bottom to top, i.e., starting at the right-most bit in the leaf going successively left. In line 4 we construct the position of the neighbor at the current depth by flipping the bit representing this depth. Depending on which side the leaf and neighbor is, in lines 5 to 10, we look-up the left and right hash to concatenate them in correct order, hash them, and set the result at the respective position in the LUT (line 11). This process will be repeated for all depths until the root is reached. For revocation, the same operation is used regarding the leaf to be removed, except in line 1 we set the leaf to \( \emptyset \) instead.

---

Table 2: Variables and operation definitions.

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( LUT )</td>
<td>Look-Up-Table storing hashes of all non-empty branches and leaves of SMT</td>
</tr>
<tr>
<td>(</td>
<td>l</td>
</tr>
<tr>
<td>( l[l] )</td>
<td>Number of elements in list ( l )</td>
</tr>
<tr>
<td>( LC )</td>
<td>Level-Cache-List sorted by position of the cache elements in SMT</td>
</tr>
<tr>
<td>( clvl )</td>
<td>Depth of ( LC )</td>
</tr>
</tbody>
</table>

---

Algorithm 4: Add Leaf to SMT Operation

1. Set hash to be added on the respective leaf position.
2. Traverse the tree from bottom to top.
3. For each depth, calculate the position of the neighbor.
4. Look-up the left and right hash into the cache.
5. Concatenate the hashes in correct order.
6. Hash the concatenated result.
7. Set the result at the respective position in the LUT.
Algorithm 4 add_leaf function for adding a new leaf hash and recalculating the tree while updating the LUT

Input: leaf_hash, LUT
Output: \( E_i, LUT \)
1: \( LUT[leaf\_hash, i\] \leftarrow leaf\_hash \\
2: for i \leftarrow 0 to \|i\| do \\
3: neighbor \leftarrow leaf\_hash \\
4: neighbor[i] \leftarrow \sim neighbor[i], i \end{cases} \\
5: if leaf\_hash[i] = True then \\
6: left\_hash \leftarrow LUT[neighbor, (\|il\| - i)] \\
7: right\_hash \leftarrow LUT[leaf\_hash, (\|il\| - i)] \\
8: else \\
9: left\_hash \leftarrow LUT[leaf\_hash, (\|il\| - i)] \\
10: right\_hash \leftarrow LUT[neighbor, (\|il\| - i)] \\
11: LUT[leaf\_hash, (\|il\| - i)] \leftarrow H(left\_hash || right\_hash) \\
12: return LUT[\varnothing, 0], LUT

A.2.2 PoI Construction

This operation is executed by the CA to construct a PoI for the given leaf hash. The LUT, populated by the add_leaf operation, is used for the PoI construction. Only necessary hashes will be put in the PoI by excluding empty hashes. However, this additionally requires a \(|\|il\|\)-bit sized path bitmap for verification, to know which depth each element in the PoI represents.

Algorithm 5 calc_poi function for calculating the proof of inclusion for a leaf

Input: leaf_hash, LUT
Output: path, path_bitmap
1: \( path[i] \leftarrow \varnothing \\
2: path\_bitmap \leftarrow 0 \\
3: for i \leftarrow 0 to \|i\| do \\
4: neighbor \leftarrow leaf\_hash \\
5: neighbor[i] \leftarrow \sim neighbor[i], i \end{cases} \\
6: neighbor\_hash \leftarrow LUT[neighbor, (\|il\| - i)] \\
7: if neighbor\_hash = \varnothing then \\
8: path\_bitmap[i] \leftarrow True \\
9: path.append(neighbor\_hash) \\
10: return path, path\_bitmap

The operation is shown in Algorithm 5. It works similar to add_leaf, by starting from the bottom of the tree and working its way up. For each depth, the neighbor position for the given leaf is calculated and looked-up in line 6. If the looked-up hash is not empty, it will be appended to the PoI and the bit at the current depth is set in the path bitmap. For a revoked leaf the operation does not require any changes.

A.2.3 PoI Verification

For this operation, we calculate the root resulting from a PoI. Given the leaf to be verified, its PoI, and respective path bitmap, the operation can be executed by anyone. If this root matches the expected epoch root, the certificate represented by the leaf is valid. Per default, the operation will calculate the root, yet, an optional parameter can be passed to stop at the specified depth-level.

Algorithm 6 calc_path_root function for calculating the root of a proof of inclusion, optionally only until a given depth

Input: leaf_hash, path, path_bitmap, [lvl] \leftarrow 0 \\
Output: root_hash
1: result \leftarrow leaf\_hash \\
2: for i \leftarrow 0 to (\|il\| - lvl) do \\
3: if path\_bitmap[i] = True then \\
4: neighbor \leftarrow path[0] \\
5: path.popfront() \\
6: else \\
7: neighbor \leftarrow \varnothing \\
8: if leaf\_hash[i] = True then \\
9: result \leftarrow H(neighbor || result) \\
10: else \\
11: result \leftarrow H(result || neighbor) \\
12: return result

Algorithm 6 gives a detailed description of the operation. The algorithm starts by setting the given leaf in the result variable and then works its way up the tree from the bottom. In the lines 3 to 7 it checks if there is an element in the given PoI for the current depth and if so, it extracts this PoI element. Otherwise, an empty hash is assumed instead. Then both hashes are hashed together in the respective order and set to the result variable. This process is repeated for all depths until we reach the root, or the given depth level, if specified.

A.2.4 Level-Cache Construction

The construction of a LC by the CA is shown in Algorithm 7. Note that the elements of LC are sorted left-to-right by their position in the epoch tree. Thus, we can simply go through all positions in the LC, bit-shift it to the very left regarding the digest size, and use this to simply look-up the value at the depth clvl. The CA can repeat this for all epochs and then distribute the resulting LC. If some Nodes missed this distribution, Nodes that received the LC may share it with others, or construct LCs with a smaller clvl if requested.

Algorithm 7 construct_lvl_cache for constructing a level-cache with a specified depth

Input: clvl, LUT
Output: LC
1: LC[i] \leftarrow \varnothing \\
2: for i \leftarrow 0 to 2^{clvl} do \\
3: position \leftarrow i \ll ((\|il\| - clvl)) \\
4: LC.append(LUT[position, clvl]) \\
5: return LC