Self-Organised Key Management for the Smart Grid

Foivos F. Demertzis[1], Georgios Karopoulos[2], Christos Xenakis[1], and Andrea Colarieti[3]

[1] University of Piraeus, Dept. of Digital Systems, Piraeus, Greece
{fdemertz,xenakis}@unipi.gr
[2] University of Athens, Dept. of Informatics and Telecommunications, Athens, Greece
gkarop@di.uoa.gr
[3] WEST Aquila S.r.l., L'Aquila, Italy
andrea.colarieti@westaquila.com

Abstract. As Smart Grid deployments emerge around the world, their protection against cyberattacks becomes more crucial. Before protective measures are put into place, one of the main factors to be considered is key management. Smart Grid poses special requirements compared to traditional networks; however, the review of previous work reveals that existing schemes are not complete. Here we propose a scalable and distributed key management scheme for the Smart Grid based on the Web-of-Trust concept. Our proposal is build on top of a Distributed Hash Table for efficient lookups of trust relationships. The target of this scheme is to create a key management system for the Smart Grid without the need of an always available Trusted Third Party. The underlying Distributed Hash Table can be further utilised as an infrastructure to build other Smart Grid services on top of it, like secure and/or anonymous aggregation, billing, etc.

Keywords: smart grid; security; key management; DHT; Chord

1 Introduction

In order to handle the power demand that is increasing in the last decades, Nation states turn to renewable sources to diversify their energy mix. Since the traditional power grid was not designed with the current situation in mind, it can neither cope with the efficient management of diverse energy sources nor respond effectively to events leading to blackouts; for these reasons, the Smart Grid is considered the next step in the power grid. Information and communication technology introduction to the traditional power networks will provide advantages like efficiency, increased reliability, resilience, distributed intelligence, and better control of demand response. The EU has plans to replace at least 80% of its electricity meters with smart ones by the year 2020[4]. According to a US report [1],

[4] http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters

the smart meter installations in the USA have reached 50 million of devices as of July 2014. Therefore, it is not long until large Smart Grid deployments will become true.

On the other hand, upgrading such a large and complex system, like the Smart Grid, could introduce new vulnerabilities and expose it to common cyberthreats, as have been described in relevant survey articles [23, 2, 28]. There are numerous possible attacks against the Smart Grid, for example attacks against the availability of the utility's control systems with varied consequences ranging from data theft to loss of human lives, against the smart meters leading to incorrect billing and personal data theft, and against the communication protocols that support the operation of the Smart Grid. Countermeasures to these attacks assume some sort of key management for supporting the cryptographic operations required for securing the Smart Grid and establishing trust relationships.

Before specifying a key management scheme that is appropriate for the Smart Grid, there are a few issues and trade-offs to be considered. These issues are mainly related to the type of cryptography, and the key provisioning system used. Typically, symmetric cryptography tends to be less computationally demanding, but more difficult in terms of key management than asymmetric; therefore, it is expected that it will be supported from Smart Grid devices. Regarding asymmetric cryptography, while appliances might have too limited computational resources for it, we argue that smart meters will be able to meet its demands. There are two alternatives here: either in software, using a crypto library, or in hardware, utilising a dedicated co-processor. Hence, we argue that smart meters will have the required capacity to implement both types of cryptography.

Key provisioning in the case of symmetric cryptography is difficult in comparison to digital certificates used in asymmetric cryptography. In the first case, each node needs to have a different secret key with every other node; in some implementations a single key is used throughout the networks, increasing the security risk substantially. Moreover, some kind of Key Distribution Center (KDC) should be employed, which creates a single point of failure, and should be online at all times; the latter is not always possible in the Smart Grid. On the other hand, digital certificates is a much more effective solution, and two alternatives exist: Public Key Infrastructures (PKIs) based on a Trusted Third Party (TTP), and Web-of-Trust which is a distributed solution. In the first case, however, usually a Certification Authority (CA) is needed, which has to be secured, creating a single point of failure; its operation introduces a significant amount of overhead as well. Moreover, PKIs are complex and might prove difficult to operate, especially for PKIs belonging to different organisations that need to interoperate. Another issue is checking the validity of a certificate which requires connectivity with the relevant server; intermittent communications as anticipated in Smart Grids will hinder key management operation. Also, trust management can be an issue when a single root CA is used; however, there are solutions to alleviate this problem by cross-signing other CAs or using bridge CAs. The Web-of-Trust concept offers a more distributed, self-organised, and scalable alternative for the

Smart Grid, which can manage trust relationships in a local level and operate even when a TTP is not always available.

Taking into account the issues found in the Smart Grid [19] and the limitations imposed by the employed cryptography type and key provisioning method, the following key management requirements can be identified:

Resilient against well known attacks. Key management solutions are expected to take previously identified attacks and weaknesses into account, whether it is in the same or in similar systems, e.g., the Internet.

Holistic key management approach. The Smart Grid should be covered as a whole by the proposed key management schemes, rather than targeting subsystems of it.

Robust against key compromise. A key management scheme intended for the Smart Grid must provide an adequate level of protection for the keys. Equally important is to afford sufficient key diversity, so that compromise of a single device does not put in risk other devices or the network.

Distributed operation. It is expected that connectivity to central servers (like CAs) will not always be available in the Smart Grid, for reasons like natural disasters and outages. Moreover, the various systems and devices found in the Smart Grid are distributed in large geographical areas and need to face intermittent communications. In such cases, key management should be flexible and less centralised in order to increase availability of authentication and authorisation services.

Upgradeability. The cryptographic modules that support cryptographic operations need to be designed carefully so that they are upgradeable. This is required because Smart Grid devices will have an average lifetime of 20 years, which is much longer than usual IT systems.

Certificate revocation. When a certificate cannot be considered trustworthy or the private key has been compromised, then there must be a proper mechanism to revoke the certificate.

Scalability. A high degree of scalability is needed since Smart Grid deployments will comprise utilities with millions of customers; this will involve the management of tens of millions of credentials and keys.

Efficiency. The devices found in the Smart Grid tend to be constrained in terms of memory, processing power and storage; moreover, there are also limitations in bandwidth and connectivity availability. Therefore, proposed key management solutions should be efficient in memory, computation, storage, and communications.

As the interest on Smart Grid security is growing, one of the main challenges is the proposal of an appropriate key management scheme that can meet the security and network requirements of Smart Grids. However, already proposed key management schemes come with several limitations. According to [23], some of the existing key management schemes are for Supervisory Control And Data Acquisition (SCADA) systems. SCADA are decision making systems used to control and monitor physical processes remotely; they provide the connection between the cyber and the physical world and typically are closed and proprietary. While SCADA is considered a significant part of the Smart Grid, solutions targeting SCADA do not provide an adequate solution for the Smart Grid, since they only protect subsystems of the grid. We also show, in the related work section, that other solutions aiming at the Smart Grid as a whole are not appropriate as well, because they lack security, robustness, efficiency, and scalability. Hence, there is a considerable need for a key management solution that can meet Smart Grid's special requirements.

Here, we present a distributed and scalable authentication and key management scheme, namely Self-Organised key MAnagement for the Smart grid (SOMA-S), that can meet the special requirements that a Smart Grid has, compared to a typical communication network. Smart Grid will assume a mesh networking structure because of the advantages it can offer towards meeting Smart Grid's requirements, and mainly the high degree of reliability, self-configuring, and self-healing [27, 11]. Hence, schemes intended for mesh networks can be adapted to Smart Grids, taking into account their special requirements. We utilise our previous work, a scheme called Self-Organised Mesh Authentication (SOMA) [9, 10], which is a certificate-based authentication infrastructure that aims to create a large-scale secure authentication system for mesh networks without the need of a TTP. We adapt this framework to the Smart Grid context, so that it can fulfil the diverse requirements set by this type of networks. Compared to related work, our proposal follows a different approach by employing the Web-of-Trust concept found in Pretty Good Privacy (PGP) [5]; this allows our scheme to present a few advantages over existing schemes, like scalability and decentralisation.

In the next section we will examine related work and background on key management for the Smart Grid. Section 3 describes our key management system called SOMA-S. Next, Sect. 4 discusses security related issues, gives a critical overview of our proposal, and presents additional services that can be implemented for the Smart Grid, on top of the proposed infrastructure. Finally, Sect. 5 summarises important points and outlines the conclusions drawn.

2 Related Work

The first category of existing solutions focus on SCADA systems, which are decision making systems used to control and monitor physical processes remotely, and are considered a significant part of the Smart Grid. With the integration of the Smart Grid with existing SCADA systems, which have been employed since the '60s, the resulting system should have a unified key management scheme for the secure communication of all components among them. There are quite a few key management schemes designed especially for SCADA: [4, 8, 6, 17, 7, 12]; however, they are not adequate because they do not take into account the rest of the Smart Grid's components. An overview of each of these proposals is presented in [23].

Various solutions have proved to be insecure and susceptible to different attacks. In [24], a novel key management scheme for Smart Grids is proposed, combining public and symmetric key cryptography; the used techniques are elliptic curve and the Needham-Schroeder authentication protocol. The authors of [25], however, prove that it is susceptible to man-in-the-middle attacks and propose their own scheme. The latter is a symmetric key distribution scheme utilising an online TTP with precomputed responses, which can be operated as an LDAP server and replicated with low cost. This scheme was also found to be vulnerable to an impersonation attack [20].

One of the easiest, yet insecure, key management methods is sharing a single symmetric key among many or even all parties. In fact, according to [19], there exist deployed systems that use the same symmetric key among all their meters. The main issue with this method is that if one node is compromised, then the whole network is at risk.

In the pursuit of efficiency, several researchers have proposed key management schemes based on shared secret keys. The scheme proposed in [13] introduces an efficient and scalable key management protocol for secure unicast, multicast, and broadcast communications in Smart Grids; its operation is based on a binary tree to manage secret keys shared among entities. This proposal does not scale well, since it requires substantial manual work in order to create the binary tree and transmit it together with the secret values to every node; moreover, as nodes join or leave the network, the whole network should update the broadcast keys. Another scheme based on shared secrets is [16], which can also support unicast, multicast and broadcast communications. The Smart Grid is divided into two levels, based on the computational resources of its devices, and each level has its own key management system. The nodes follow a binary tree arrangement and the secret key of a parent node is the hash of its children keys. The Dynamic Key Management Scheme (DKMS) [26] uses symmetric keys with frequent key updates among the nodes comprising the Smart Grid. When a node A joins the grid, a key is installed manually between node A and a bootstrapping node B. To communicate with a third node C, node A has to negotiate a new key with C using the association it has with node B. All the methods presented in this paragraph have the same issue: every node has to maintain one key for each secure connection to another node. This hinders scalability, since it involves high efforts for key management, renewal, and distribution.

Another category of key management schemes utilises ID-based cryptography. In [15], a key management scheme for Advanced Metering Infrastructure (AMI) is proposed, which is based on a key tree structure. However, the authors of [22] found that it is susceptible to de-synchronisation attacks, while it lacks scalability due to inefficient key management. For this reason, they proposed Scalable Key Management (SKM), which utilises ID-based encryption and a key graph technique for efficient multicast key management. The authors in [18] propose a key management solution occupying a CA that resides in the utility network. They use secret values shared between the CA and the smart meters together with an ID-based cryptography model. The main drawback of the above solutions, as with all ID-based systems, is that the Private Key Generator (PKG) should always be online and available; moreover, since the PKG holds the private keys of all nodes, it can be a single point of failure.

Wide-area measurement system key management (WAKE) [14] is a solution based on traditional hierarchical PKI architecture. Each participating node has a X.509 certificate and the root CA is the grid operator. Secure channels between devices are established using the Diffie-Hellman key establishment protocol. The hierarchical PKI architecture is not well suited for the Smart Grid, as stated in [3], since it does not meet the high availability requirement, because the root CA tends to be a single point of failure.

Summing up, we showed that each proposed solution presents one or more of the following limitations: (a) partial coverage of the Smart Grid, (b) vulnerability against well known attacks, (c) secret key re-use, (d) poor scalability, (e) contain a single point of failure, and (f) require high availability. On the other hand, as we will show in the following sections, SOMA-S addresses the aforementioned limitations by following a different approach, i.e. the Web-of-Trust concept. At the same time, it meets the key management requirements stressed in Sec. 1.

3 SOMA-S

3.1 Functional Components

The components that comprise a basic Smart Grid infrastructure are presented in Fig. 1; particular focus has been given to the communication links between elements rather than power delivery. Here we deliberately omit communication technologies among nodes which range from ZigBee, to WiFI, cellular, satellite, powerline communications, etc.

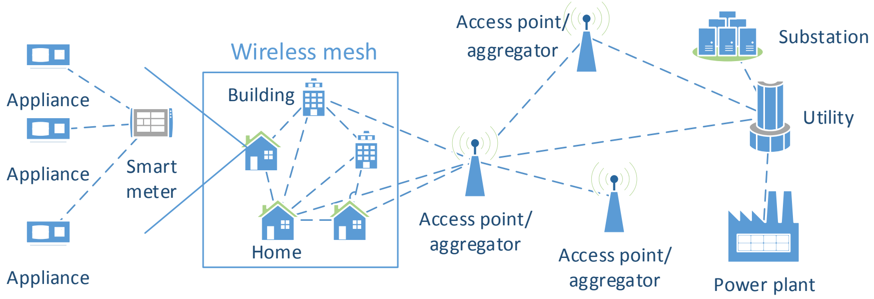

Fig. 1. Functional components of a Smart Grid

One of the basic nodes of the Smart Grid is the utility company that provides power to its customers. Here we depict a single company, but normally a Smart

Grid will comprise more than one. Power generation and distribution installations do not directly communicate with the end customer, but with the utility instead. Aggregator nodes reside in between the utility and the end customers and their main purpose is to aggregate smart meter readings and forward the results towards the utility. They are considered more powerful nodes than smart meters, thus they can support more computationally intensive operations than smart meters. In each home or building there are one or more smart meters, connected in a mesh network.

3.2 Architecture

Figure 2 presents our proposal together with the Smart Grid architecture. The lowest level depicts the power delivery network over which the utility company delivers power to its customers. Above this, the ICT level resides, allowing bi-directional communications among Smart Grid elements. To support the operations of SOMA-S, we have two logical layers comprising the overlay on top of the ICT level, which we will present in the following paragraphs in more detail.

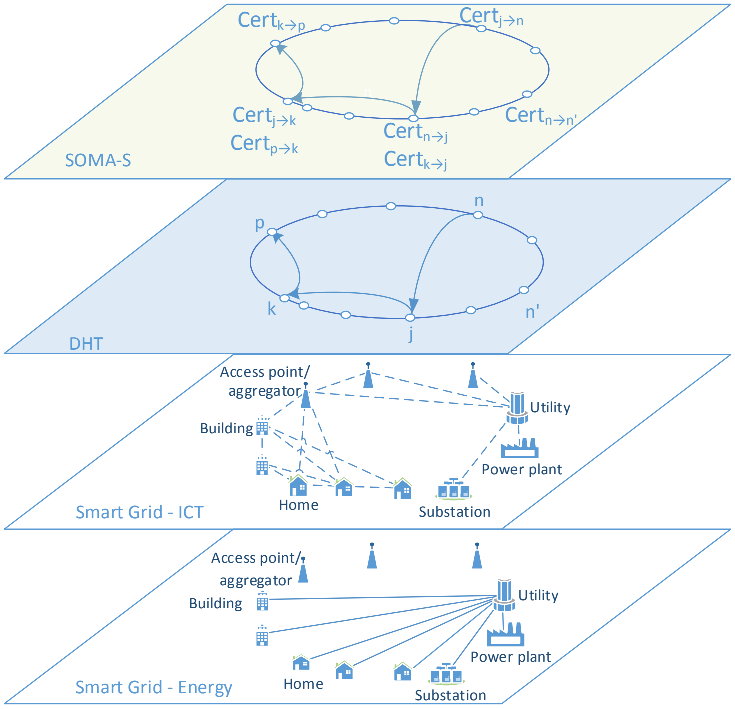

Fig. 2. DHT and SOMA-S over Smart Grid

The overlay layer, over which SOMA-S is built, provides a generic Distributed Hash Table (DHT) functionality. On a DHT we can normally store (key,value) pairs, as in every other locally stored hash table, and retrieve the value back based on the key. Our scheme is based on Stoica's Chord [21], where nodes are placed as IDs occupying a circular identifier space; in our case, every node of the Smart Grid is represented as a node of the Chord ring. Chord is scalable and efficient, taking O(log N) communication hops and keeping O(log N) state per node, where N is the total number of nodes in the system; moreover, it is robust on node joins and failures. The overlay can support on top of it diverse applications that require efficient lookup services, like authentication with SOMA-S; other services that could benefit from the overlay include billing, and secure aggregation.

In the case of SOMA-S, the overlay key of a node n is ID_n and will be derived by hashing the concatenation of its public key and a device identifier of the node $ID_n = h(Pk_n + ID_{device})$. This concatenation ensures that ID_n will be unique even when the device identifiers are not. The digital certificates, where used, follow the OpenPGP Message Format [5] or any compliant format. The overlay structure forms the framework for the transitive trust relationships and each node exchanges certificates with the nodes that is directly responsible for routing. When a node requests a chain of certificates to another node, following the overlay routing, will result to an efficient trust path discovery.

All the nodes of the Smart Grid (even from different utility companies) are put onto one SOMA-S ring so as to minimize the complexity of the system. An alternative solution would be to have one ring for each utility and an overlay ring for inter-utility communications. While this might improve efficiency (since most searches will be intra-utility), it increases complexity as well. The optimal trade-off between complexity and efficiency, and the decision to use one or more SOMA-S rings, remains to be seen and we leave it as future work.

3.3 Operation

Initially, node n has to generate an ID_n to connect to the overlay. As a first step, n receives or generates a public/secret key pair Pk_n/Sk_n; then, it receives a certificate $Cert_n$ signed by another node that acts as an introducer to the SOMA-S ring. The introducer could be the utility network or another "empowered" node of the Smart Grid acting on a local level, e.g., an aggregator. There are three ways to load these credentials, i.e. the key pair and the certificate, to each node: (a) they can be received through physical contact or other direct channels, (b) generated from the node, or (c) loaded to the node from the utility operator before deployment. To join the SOMA-S ring, node n can use ID_n to connect to the overlay.

Following the ID_n generation, node n needs to set-up a finger table [21], which is a list of pointers to node IDs in the overlay. Instead of holding a single pointer to the next node, $n.finger = ID_{next\_node}$, a list of m nodes is maintained, *n.finger(m)*, with their logical inter-node distance increasing exponentially, providing the efficient look up mechanism. Every entry in the table will be associated with an IP address; moreover, as n establishes trust relationships with other nodes from its finger table, it adds the corresponding certificate to this table entry as following. Node n can use its certificate to introduce itself to an "empowered" node *n'* residing in its finger table, which also holds a certificate signed by the utility. Next, *n'* will check the authenticity of key Pk_n, and sign it; similarly, n will sign the authenticity of $Pk_{n'}$. Following the PGP Web-of-Trust, *n'* will put in its keyring the certificate $Cert_{n \rightarrow n'}$; additionally, n will hold $Cert_{n' \rightarrow n}$ in its keyring. After the bootstrapping phase, Pk_n is signed by other nodes as well, using n's Web-of-Trust. This will lead node n to set-up an authentication aware finger table. This way, n can be authenticated later, even if some of the signing nodes have been withdrawn or their certificates revoked, using signatures that are still valid. Regarding performance, SOMA-S is based on the Chord protocol, hence it follows its mathematical properties; therefore, a node would be able to find a chain of certificates in O(log N) time and in O(log N) number of certificates for any trust path given.

An example operation of SOMA-S is shown in Fig. 2. When node n wants to authenticate with p, it must have a trust chain to p. If p is already in the trust path of n, then they can communicate directly. Otherwise, node n has to follow the look-up methods provided by SOMA-S as following. Node n communicates with the closest node to p with which it has a mutual trust relationship, i.e. node j; that is the closest node to p in n's finger table, or p is an introducer for n. Node j does the same and ends up communicating with node k. Finally, k communicates with p completing the authentication between n and p. Details on joining the ring, stabilisation, and lookup procedures can be found in [10].

To further protect the Smart Grid from misbehaving nodes, we can use a reputation framework to include ratings from all the experiences between principals, in addition to the above certificate path-building method. On every transaction between a node and a finger, an outcome will be recorded and its reputation score calculated. We do not wish to claim specific parameter values as accurate ratings other than the positive and negative outcomes between events. For instance, supposing a node j was malicious and was misbehaving in routing, node n could undershoot in its finger table and therefore avoiding the problematic node as if it was faulty. After a while, intentional routing misbehaviour by specific nodes would be represented in the rest ring effectively, skipping it in their finger tables. This approach results in a reputation based path ranking that is similar to the discrete ranking of PGP Web-of-Trust [5], but also allowing for further flexibility and extensibility, and more complex representation of social interactions and structures.

Regarding certificate revocation, in a large system like the Smart Grid, a typical Certificate Revocation List (CLR) can become very lengthy creating efficiency issues. To solve this, administrators set short validity periods to certificates so that, when a previously revoked certificate expires, it is removed from the CRL. However, this creates higher operational overhead, especially when a large number of certificates needs to be frequently re-issued.

In SOMA-S a node can explicitly revoke its certificate by using a revocation certificate as described in OpenPGP [5]. The node that revoked its certificate does not need to send the revocation request certificate to all the nodes in SOMA-S, but only to its predecessor, and exchange it through Chord's stabilisation protocol with all the nodes that update their finger table to the node itself. When a node requires to check if a certificate is currently revoked, it only needs to proceed with the normal lookup operation.

4 Discussion

In this section we discuss several issues related to our scheme. First, we provide a security analysis by employing a few representative attack scenarios; for each case we study the actions taken by our proposal. Next, we review the key management requirements of Smart Grids and check on which degree SOMA-S fulfils them. Finally, we present alternative services that can be offered on top of the DHT infrastructure supporting SOMA-S.

4.1 Security Analysis

In this section we analyse the possible attack scenarios derived from the characteristics of our architecture and the desirable system properties. Attacks range from the certificate exchange mechanism, the control and use of key material and, finally, the overlay routing itself.

Node Join. A malicious party could try to implant a fake node that it controls to the SOMA-S ring. However, bootstrapping of new nodes is controlled by the utility (or delegates like aggregators) so that not even a large number of colluding malicious nodes could successfully introduce this new node to the Smart Grid.

Utility Certificate Revocation. An issue that could probably arise is what happens when the utility certificate is revoked. If the node has not already bootstrapped to the network, then it needs to acquire a new certificate signed using the new utility certificate. If the node has already bootstrapped to the network, then no action is needed; the utility certificate is used for bootstrapping only, and the node's certificate will have been signed by other nodes and considered valid until expired or revoked.

Certificate Chain. A node wanting to find a certificate chain to another node, needs to authenticate first a chain of intermediate nodes. These intermediate nodes have valid IDs and the digital certificates provide authentication and non-repudiation for each node in the certificate path. The consistent hashing is a pre-image resistant mechanism between the IP and logical address which, provides a simple defence against impersonation and Sibyl attacks. If one of the nodes misbehaves or simply creates multiple identities, it will be trivially detected, since the certificates are bound to its device identifier. Therefore, this node can simply be ignored and move on the previous node preceding the target node in the finger table. As long as a single node in the finger table follows the protocol, the authentication can proceed. Moreover, with our reputation extension we can have a threshold for misbehaviour tolerance. After this threshold a malicious node can be blacklisted or be dealt accordingly to predefined rules.

Denial of Service. If a node joins a SOMA-S ring, where the majority of the nodes are malicious, then its identity even though could not be forged, the authentication service for that node could be potentially disrupted through Denial of Service (DoS). Against DoS attacks, SOMA-S is resilient by using ratings and hashing. With ratings as a defence mechanism, peers can blacklist and exclude malicious nodes that sent fraudulent messages after a threshold, since their identities are detectable. In combination to reputation, consistent hashing is used to distribute the logical identities of the nodes. Therefore, malicious peers would require a large majority to eclipse a node (cut off his ingoing and outgoing links). This is due to the fact that the IDs are mapped using consistent hashing, where the standard hardness assumptions for the chosen hash function apply.

Credential Exchange. An attack directly on the certificate exchange is thwarted by the use of nonces and timestamps, which ensure freshness, and prevent man-in-the-middle attacks. Additionally, the inclusion of origin and target data safeguards against certificate hijacking and all forms of impersonation.

Overlay attack. Attacks on the routing protocol, itself, can be hard to avoid if the majority of nodes are malicious. Even though impersonation is averted through the logical-IP address relationship of the public key certificates, a DoS attack could potentially disrupt the overlay as a whole. In such a case, our reputation model provides the necessary insight to marginalise or expel malicious nodes. Attacks on the network infrastructure itself could include churn attacks and potential network failures from the malicious nodes. Against such attacks, SOMA-S is resilient by requiring at least one correct node in the finger table for correct routing. In addition, instead of using a single successor, employing successor lists will provide additional routes and mitigate the effects of overlay attacks.

4.2 Critical Appraisal

In this section, we reconsider the key management requirements presented in Sect. 1 and discuss on which degree SOMA-S fulfils them.

First of all, our scheme is based on the well known PGP Web-of-Trust and asymmetric cryptography operations, so that it can be considered *resilient against well known attacks*, at least to the extent these two building blocks can be considered resilient.

SOMA-S also provides *full coverage to the Smart Grid* since all its nodes are added to the ring.

Regarding *robustness against key compromise*, while the adequate protection of keys is highly dependent on the implementation, key diversity can be supported by using key derivation techniques based on the public/private key pair of each node. Thus, we argue that this requirement is partially met, but SOMA-S provides all the necessary elements to fully achieve this target.

SOMA-S can support *distributed operation* of its nodes given that, after the bootstrapping phase, its operation is based on a Web-of-Trust and no central TTP is needed. Hence, it shows high availability even over intermittent connections or no connectivity at all with the central utility servers.

Smart Grid devices are expected to have a long lifetime, in the order of 20 years. SOMA-S fulfils *upgradeability* since its distributed nature allows digital certificates to be easily and inexpensively updated with longer key sizes.

The requirement of *certificate revocation* is covered as well, since it is a procedure provided by SOMA-S. Moreover, it is implemented in a distributed manner without the administrative burden imposed by CRLs or having availability requirements like Online Certificate Status Protocol (OCSP) based methods.

Regarding the *scalability* requirement, we argue that SOMA-S can support large numbers of devices since after bootstrapping, where the utility is involved, it is completely decentralised and there is low administrative cost.

Efficiency is highly related to the hardware that will be used. Even though SOMA-S utilizes digital certificates and asymmetric cryptography, there are ways to mitigate the performance penalty by using session keys based on these certificates.

4.3 Smart Grid Services

The overlay described previously is only used as a meta-structure providing a key management service among the Smart Grid nodes. A possible extension to our proposal would be to leverage the DHT to allow diverse and powerful services in the Smart Grid. The DHT will provide an efficient indirection layer, with the services being implemented on top of the overlay. These services will be implemented by the utility companies themselves to overcome the usual point-to-point limitations of the traditional approaches, providing robust services for data aggregation, demand-side-management, privacy protection, advanced policies for billing, two-way consumer-producer services, etc.

5 Conclusions

Due to Smart Grid's special characteristics and requirements, existing key management solutions cannot be applied as is; moreover, as we showed, existing proposals leave space for further improvements. This paper has proposed a distributed and scalable key management system for the Smart Grid without the need of a TTP with high availability. Its operation is based on a DHT for efficient discovery of trust relationships among the Smart Grid nodes. Having the utility take part during the bootstrapping phase, we ensure that it will be difficult for malicious nodes to join the Smart Grid. After this phase, trust policy is more decentralised and flexible in order to promote scalability and resilience.

In our case, the overlay is used as a meta-structure to infer trust relationships and not as the means to provide distributed directory storage. The same overlay, however, could be utilised as an infrastructure to provide other Smart Grid related services, like secure aggregation, and billing. Our future work includes a more detailed definition of the underlying overlay infrastructure, together with the description of additional services for the Smart Grid on top of it.

Acknowledgement

This research has been funded by the European Commission as part of the SMART-NRG project (FP7-PEOPLE-2013-IAPP Grant number 612294).

References

1. Utility-scale smart meter deployments: Building block of the evolving power grid. Tech. rep., The Edison foundation (September 2014)
2. Aloul, F., Al-Ali, A., Al-Dalky, R., Al-Mardini, M., El-Hajj, W.: Smart grid security: Threats, vulnerabilities and solutions. International Journal of Smart Grid and Clean Energy 1(1), 1–6 (2012), https://dx.doi.org/10.12720/sgce.1.1.1-6
3. Baumeister, T.: Adapting PKI for the smart grid. In: Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on. pp. 249–254 (Oct 2011)
4. Beaver, C., Gallup, D., Neumann, W., Torgerson, M.: Key management for SCADA. Cryptog. Information Sys. Security Dept., Sandia Nat. Labs, Tech. Rep. SAND2001-3252 (2002)
5. Callas, J., Donnerhacke, L., Finney, H., Shaw, D., Thayer, R.: OpenPGP Message Format. RFC 4880 (Proposed Standard) (Nov 2007), http://www.ietf.org/rfc/rfc4880.txt, updated by RFC 5581
6. Choi, D., Kim, H., Won, D., Kim, S.: Advanced key-management architecture for secure SCADA communications. Power Delivery, IEEE Transactions on 24(3), 1154–1163 (2009)
7. Choi, D., Lee, S., Won, D., Kim, S.: Efficient secure group communications for SCADA. Power Delivery, IEEE Transactions on 25(2), 714–722 (2010)
8. Dawson, R., Boyd, C., Dawson, E., Nieto, J.M.G.: SKMA: a key management architecture for SCADA systems. In: Proceedings of the 2006 Australasian workshops on Grid computing and e-research-Volume 54. pp. 183–192. Australian Computer Society, Inc. (2006)
9. Demertzis, F., Xenakis, C.: SOMA: Self-Organised Mesh Authentication. In: Public Key Infrastructures, Services and Applications, Lecture Notes in Computer Science, vol. 6711, pp. 31–44. Springer Berlin Heidelberg (2011), http://dx.doi.org/10.1007/978-3-642-22633-5_3
10. Demertzis, F.F., Xenakis, C.: SOMA-E: Self-organized mesh authentication-extended. Mathematical and Computer Modelling 57(7-8), 1606–1616 (2013)
11. Gharavi, H., Hu, B.: Multigate communication network for smart grid. Proceedings of the IEEE 99(6), 1028–1045 (June 2011)

12. He, W., Huang, Y., Sathyam, R., Nahrstedt, K., Lee, W.C.: SMOCK: a scalable method of cryptographic key management for mission-critical wireless ad-hoc networks. Information Forensics and Security, IEEE Transactions on 4(1), 140–150 (2009)
13. Kim, J.Y., Choi, H.K.: An efficient and versatile key management protocol for secure smart grid communications. In: Wireless Communications and Networking Conference (WCNC), 2012 IEEE. pp. 1823–1828. IEEE (2012)
14. Law, Y.W., Palaniswami, M., Kounga, G., Lo, A.: WAKE: Key management scheme for wide-area measurement systems in smart grid. Communications Magazine, IEEE 51(1), 34–41 (2013)
15. Liu, N., Chen, J., Zhu, L., Zhang, J., He, Y.: A key management scheme for secure communications of advanced metering infrastructure in smart grid. Industrial Electronics, IEEE Transactions on 60(10), 4746–4756 (Oct 2013)
16. Long, X., Tipper, D., Qian, Y.: An advanced key management scheme for secure smart grid communications. In: Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on. pp. 504–509 (Oct 2013)
17. Mittra, S.: Iolus: A framework for scalable secure multicasting. In: ACM SIGCOMM Computer Communication Review. vol. 27, pp. 277–288. ACM (1997)
18. Nicanfar, H., Jokar, P., Leung, V.: Smart grid authentication and key management for unicast and multicast communications. In: Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES. pp. 1–8 (Nov 2011)
19. NIST: Guidelines for smart grid cybersecurity: Vol. 1 - smart grid cybersecurity strategy, architecture, and high-level requirements vol. 2 - privacy and the smart grid vol. 3 - supportive analyses and references. Tech. rep., NIST (2014), dOI: 10.6028/NIST.IR.7628r1
20. Park, J.H., Kim, M., Kwon, D.: Security weakness in the smart grid key distribution scheme proposed by Xia and Wang. Smart Grid, IEEE Transactions on 4(3), 1613–1614 (Sept 2013)
21. Stoica, I., Morris, R., Karger, D., Kaashoek, M.F., Balakrishnan, H.: Chord: A scalable peer-to-peer lookup service for internet applications. ACM SIGCOMM Computer Communication Review 31(4), 149–160 (2001)
22. Wan, Z., Wang, G., Yang, Y., Shi, S.: SKM: Scalable key management for advanced metering infrastructure in smart grids. Industrial Electronics, IEEE Transactions on 61(12), 7055–7066 (Dec 2014)
23. Wang, W., Lu, Z.: Cyber security in the smart grid: Survey and challenges. Computer Networks 57(5), 1344 – 1371 (2013), http://www.sciencedirect.com/science/article/pii/S1389128613000042
24. Wu, D., Zhou, C.: Fault-tolerant and scalable key management for smart grid. IEEE Transactions on Smart Grid 2(2), 375–381 (2011), http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5743049
25. Xia, J., Wang, Y.: Secure key distribution for the smart grid. Smart Grid, IEEE Transactions on 3(3), 1437–1443 (Sept 2012)
26. Xiao, S., Gong, W., Towsley, D.: Dynamic key management in a smart grid. In: Dynamic Secrets in Communication Security, pp. 55–68. Springer New York (2014), http://dx.doi.org/10.1007/978-1-4614-7831-7_5
27. Xu, Y., Wang, W.: Wireless mesh network in smart grid: Modeling and analysis for time critical communications. Wireless Communications, IEEE Transactions on 12(7), 3360–3371 (July 2013)
28. Yan, Y., Qian, Y., Sharif, H., Tipper, D.: A survey on cyber security for smart grid communications. Communications Surveys Tutorials, IEEE 14(4), 998–1010 (Fourth 2012)