Layer-2 Security for PLC – a Comparison Between ITU-T G.9903 and IEEE 1901.2

Stefan G. Hoffmann
Institute of Computer Science
Hochschule Ruhr West
Bottrop, Germany
E-Mail: stefan.hoffmann@hs-ruhrwest.de

***Abstract*—This paper describes the layer-2-security functions of two narrow-band power line communication standards, namely ITU-T G.9903 and IEEE 1901.2. We describe how access control, authentication, confidentiality and integrity for network devices are achieved in both standards. We compare the approaches by using two practice-oriented installation scenarios and by evaluating the security methods.**

I. Introduction

A recommendation [1] on preparations for the roll-out of smart metering systems published by the European Commission in 2012 marks a turning point regarding protection of individual-related data in those kinds of systems. The recommendation states that data in smart metering systems is predominantly personal data that needs to be protected with "appropriate technical and legal solutions". Prior to 2012, the main argument for not considering smart metering data to be individual-related was that it only contains meter readings and meter numbers that would only become personal data with the later invoicing process.

In this publication, we focus on two international standards of narrow-band power line communications (NB-PLC), namely ITU-T G.9903 G3-PLC [2] and IEEE 1901.2 [3]. Cost-benefit analyses (e.g. [4]) showed that using PLC in smart metering systems is cost-efficient, which makes it an important technology in the context of smart grids. Both standards describe the physical (PHY) layer (layer 1) and the data link layer (layer 2) for NB-PLC. In particular, we evaluate the security functions on layer 2. The goal of these functions is to achieve certain security objectives for networks of PLC devices, namely access control, authentication, confidentiality and integrity on a low layer.

In order to evaluate the security from a practice-oriented point-of-view, we introduce two most-relevant installation scenarios that are motivated by the recently started smart meter roll-out.

The paper is organised as follows. In section II-A and II-B we describe the basic architectures and security methods of G.9903 and IEEE 1901.2. Section III introduces the installation scenarios that we use to compare the standards. Section IV provides a discussion on the security methods and on the advantages and disadvantages of the standards in the concrete scenarios.

II. ITU-T G.9903 G3-PLC and IEEE 1901.2

Both standards, ITU-T G.9903 G3-PLC [2] and IEEE 1901.2 [3], describe the two lowest layers (according to the OSI model) for orthogonal frequency division multiplexing (OFDM) NB-PLC, namely the physical layer and the data link layer. Figure 1 compares the particular layers that are covered by each of the standards.

In this paper we do not further examine the PHY layer. We focus on cryptographic methods to provide access control and authentication, and for communication with confidentiality and integrity.

As described in figure 1, both standards are using a MAC layer based on IEEE 802.15.4 [5]. G.9903 covers the complete data link layer including security functions, while IEEE 1901.2 only describes the MAC layer with MAC enhancements from IEEE 802.15.4e [6]. The security functions are utilized from higher sublayers.

An essential difference between the two standards is their routing method. ITU-T G.9903 provides the "Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation" (LOADng, described in G.9903 [2]) at the second layer ("mesh under"). IEEE 1901.2 supports the "Routing Protocol for Low power and Lossy Networks" (RPL) [7], which is a layer-3-routing protocol ("route over").

Both standards use 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) [8], a protocol to efficiently transmit IPv6 packets over networks based on IEEE 802.15.4. Basic tasks of 6LoWPAN are header compression, segmentation/reassembly, and the layer-2-routing protocol LOAD [9]. IEEE 1901.2 uses a MAC format that allows for sending packets which are large enough to reach the smallest possible maximum transmission unit (MTU) of IPv6 packets, which makes segmentation/reassembly needless. When using RPL, the LOAD protocol is not needed, so that IEEE 1901.2 only uses a (modified) version of the header compression in the 6LoWPAN layer.

IEEE-802.15.4-based personal area networks (PAN) contain a PAN coordinator that can be considered as a master node. We call all other nodes end devices (ED). In both standards, the Extensible Authentication Protocol (EAP) [10] is used to authenticate new devices in the PAN (IEEE 1901.2 uses it indirectly over a higher layer). EAP is a method that allows two parties for a mutual authentication. It supports various authentication methods, two of them are used in the standards

978-1-4673-6643-4/16/$31.00 ©2016 IEEE

and described in this paper.

A. G.9903

The G3-PLC standard was first published in 2009 by Maxim Integrated Products, Inc. as an open specification. The purpose was to meet smart grid requirements given by the Electricite Reseau Distribution France (ERDF). Later, the G3-PLC alliance was founded by the ERDF to maintain and enhance the standard. These efforts led to the publication of the G3-PLC specification by the ITU as the standard ITU-T G.9903 in December 2012 [2].

The standard defines the two lowest layers according to the OSI model (PHY and DLL layer) to enable IP-based communication over electrical grids.

1) Commissioning: G.9903 uses the LoWPAN Bootstrapping Protocol (LBP) [11], [12] to associate new end devices (ED) to a certain network. The PAN coordinator can be in a higher distance to the coordinator than 1-hop. In this context, the end device is called LoWPAN Bootstrapping Device (LBD). By using the LBP, the LBD is able to obtain necessary information to identify the correct PAN. The information is provided by the LoWPAN Bootstrapping Server (LBS), a functionality that is implemented by the PAN coordinator.

The LoWPAN Bootstrapping Agent (LBA) helps the LBD to communicate with an LBS. Before the LBD is a part of the network, it is only able to communicate with devices in a 1-hop distance. If the LBS is not reachable within this distance, the LBD needs to rely on an LBA. The LBA is an end device that is already member of the PAN and has already completed the bootstrapping process. Thus it is able to communicate with parties that are more than a 1-hop distance away (n-hop). Its task is to receive messages from the LBD and forward them to the LBS, and vice versa.

2) Access control and authentication: ITU-T G.9903 considers two architectures for authentication. First, the LBS can be connected over a wide area network (WAN) to an authentication server (AS) by e.g. the RADIUS protocol [13]. Second, the authentication function can be directly supported by the LBS, all authentication material needs to be loaded into the LBS device.

G.9903 recommends to use EAP with a pre-shared key [14] (EAP-PSK) for authentication. In order to use this method, every device that shall be part of the network needs to share a secret key with the AS. However, other EAP methods are not prohibited. EAP messages are embedded in the LBP on a lower layer. Figure 2 shows the layered communication between the devices within this approach.

The authentication is performed on a challenge-response principle. Both LBD and LBS send individual random numbers to each other. They compute Message Authentication Codes (cryptographic MACs) on the numbers and send the result back to the other party. Now they compute the cryptographic MAC on their own random numbers and check for equality with the received numbers.

By this means they can mutually authenticate by convincing each other that they share the same key. To perform this task, both parties need to exchange four messages in total.

3) Confidentiality and integrity: G.9903 provides cryptographic methods to achieve confidentiality and integrity on two different layers within layer 2.

On a higher layer, the EAP-PSK method provides a protected channel after authentication. Over this channel, both parties can securely communicate with each other. All messages are encrypted by using the Advanced Encryption Standard with a key size of 128 bits (AES-128). The encryption key is derived from the pre-shared key and a random number that is exchanged during the authentication process. The LBS establishes such a protected channel to each of the peer devices in the network.

On the lower MAC layer, the standard defines another sublayer of cryptographic protection defined by the method CCM*, a minor variation of CCM [15]. The MAC frames are encrypted and decrypted before and after every hop (except for some frames during the bootstrapping process). To enable this service, all nodes receive the same group master key, which is generated by the LBS and securely sent to every node by using the protected EAP-PSK channel.

Using encryption with a group key on this layer prohibits unauthenticated devices to access the network in order to perform malicious actions on lower layer processes. A device that is not part of the network does not know the group key and thus is not able to generate correct MAC frames.

B. IEEE 1901.2

The IEEE 1901.2 standard is an eventual outcome of the IEEE 1901.2 working group that was established in 2010 to develop a standard for NB-PLC. The standard was published in December 2013 after it was approved by the IEEE Standards Association.

G3-PLC was used as a basis for the development of IEEE 1901.2. The IEEE 1901.2 standard defines methods for the PHY and MAC layer, but not for the complete data link layer. All security functions for this standard are provided by higher layers.

1) Access control and authentication: The security functions for network access control are based on IEEE 802.1X [16]. This standard defines the usage of EAP in general and leaves the choice of the concrete method open. The most popular EAP method however is EAP-TLS (Transport Layer Security) for authentication. EAP-TLS is a method that uses the messages of the TLS handshake protocol for mutual authentication. It is a certificate-based authentication method, i.e. both parties that intend to authenticate each other need to possess a certificate with their public key. A PKI (public-key infrastructure) is obligatory.

In IEEE 802.1X, an end device that wants to access the network is called “supplicant”. In order to access the network, it needs to authenticate itself to a party called “authenticator”. Before it is authenticated and registered in the PAN, the supplicant is not able to communicate with devices that are located on a higher distance than 1-hop. For such a case, all end devices are prescribed to implement a relay function to become an “authenticator relay”.

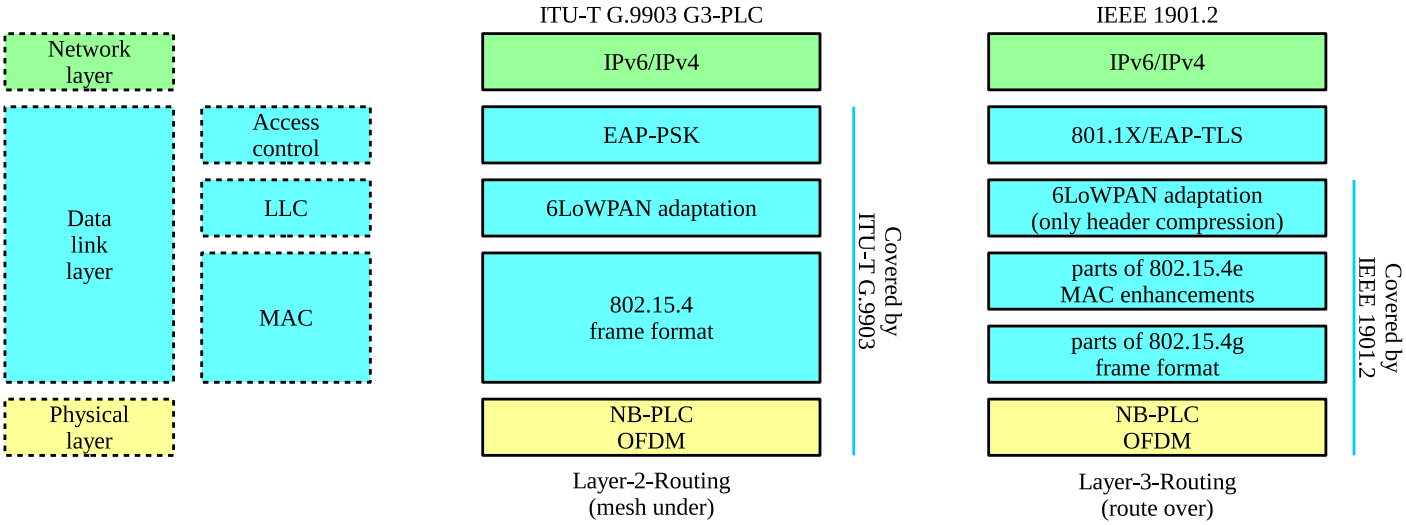

Fig. 1. Layer 1 and 2 of ITU-T G.9903 and IEEE 1901.2

If the authenticator is not in a 1-hop distance of the supplicant, at least one authenticator relay must be in 1-hop distance. The authenticator relay is responsible to send the EAP-TLS messages to the authenticator. As IEEE 1901.2 uses a layer-3-routing algorithm, the authenticator relay has to extract the EAP messages from the 802.15.4 messages sent by the supplicant. Next, it encapsulates them into UDP/IPv6 frames and sends them to the authenticator. EAP messages are transported by EAP over LAN (EAPOL) packet data units (PDU).

The authenticator must also be able to receive EAP messages within 802.15.4 messages, because it might be in 1-hop distance from the supplicant.

Similar to G.9903, the authenticator can either be connected to an authentication server over WAN or implement the authentication function itself. Figure 3 shows the basic layered communication between the devices.

2) Confidentiality and integrity: As described, G.9903 offers confidentiality and integrity by cryptographic encryption on two different layers. In contrary to EAP-PSK, the EAP-TLS method does not define a protected channel that can be used for encrypted communication after the authentication. However, IEEE 802.15.4 defines cryptographic frame protection based on the CCM* encryption mode. It can be established both between two devices (using a "link key") and/or within a group of devices ("group key"). This allows for establishing a similar approach of confidentiality protection as in G.9903 (see section II-A).

III. Scenarios

In order to compare both standards, we introduce two contrary practice-oriented installation scenarios for PLC networks. The first scenario represents a huge network that arises due to an area-wide spreaded roll-out of smart metering devices with a large amount of end devices. The second scenario focuses on smaller networks with just a few devices for isolated applications, i.e. with no direct access to the WAN. Such a scenario can also be effectuated by the smart meter roll-out.

A. Scenario L (large): wide-spreaded rollout

Recently, an area-wide rollout of smart metering devices and systems was initiated in European countries. As a consequence, one can expect an increasing (and eventually huge) amount of smart metering devices in participating countries. The number of metering devices behind a substation can typically be up to 1000. Assuming an amount of 500 substations, we have a realistic expected amount of up to 500 000 PLC devices in a network if all meters implement PLC functionality. This scenario thus represents a situation of a network in which an extremely high amount of devices have to be handled and maintained.

B. Scenario S (small): small networks for isolated applications

For this scenario we consider the meters of a multi-apartment house that are connected in a network that is isolated from a public network by using a firewall located in a gateway (e.g. the German Smart Meter Gateway [17]). The meters are not necessarily located near the physical location of the gateway. Typically, each meter is located within an apartment it belongs to. In this case it is very useful to utilize PLC to connect the meters to the gateway. This scenario represents a network with a manageable amount of devices within a protected and isolated environment.

IV. Discussion

A. Scenarios

In scenario S we consider a network with a small amount of peers. The network is isolated from the WAN, which means that we are not able to use a remote authentication server. Instead, a device within the network needs to implement the authentication function. The authentication material (like keys) must be loaded into the device. A reasonable choice is the gateway that might also play the role of the LBS (ITU-T G.9903) or authenticator respectively (IEEE 1901.2).

IEEE 1901.2 uses IEEE 802.1X for security, in which context the use of the certain EAP method is not defined, but

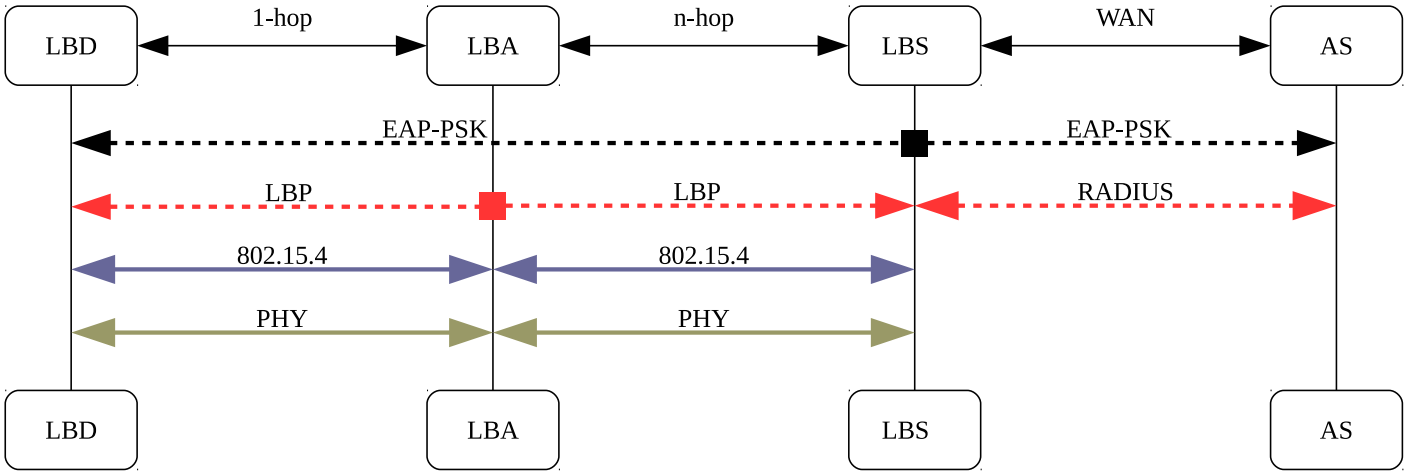

Fig. 2. Layered communication in G3-PLC commissioning

EAP-TLS is the de-facto standard. ITU-T G.9903 recommends the use of EAP-PSK, which has the advantages of simplicity and efficiency especially in this scenario. Less messages need to be exchanged between supplicant and authenticator in order to achieve network authentication.

However, a disadvantage comes from the maintenance procedure. It is strongly recommended to exchange (and thus renew) keying material after a certain time period (see e.g.[18]), which also holds for the PSK. Each key update in a single ED requires securely communicating the key to the authenticator.

This disadvantage is reduced when using the certificate-based EAP-TLS from IEEE 1901.2. Each device has its asymmetric key pair with certificate. Updating an asymmetric key pair (including the certificate) only affects the ED itself, which makes the process less complex than the EAP-PSK update process.

In scenario L, due to the high amount of peers it is practically infeasible to use EAP-PSK if a central remote server shall be used. The symmetric keys of all end devices in the network would have to be loaded into the server. Instead, the authentication server functionality needs to be distributed over several devices in a decentralised manner, which is allowed by both standards.

A centralised authentication server can thus only be used in the IEEE 1901.2 standard if the recommendation of G.9903 shall not be contradicted. The network has access to the public network, the authentication server function can be implemented by a remote server that has to be part of the PKI.

B. EAP-PSK vs. EAP-TLS

As described in section II, EAP-PSK is finished after four messages exchanged between the parties (in case of successful authentication).

When using EAP-TLS, the two parties do not need to share a secret key before. Instead, each party needs to be part of a PKI and possess an asymmetric key pair with a certificate. EAP-TLS is based on the TLS handshake protocol. In the successful case, both parties exchange nine messages including certificates and random numbers. Afterwards they are mutually authenticated and share a common secret key.

The latest version of the EAP-TLS description [19] states that it is not mandatory for the usage to support all TLS ciphersuites listed in TLS 1.1 [20], which is not the latest version of TLS. Four ciphersuites shall be supported. One of them uses the Message-Digest Algorithm 5 (MD5) as a cryptographic Hash function, which is considered to be broken [21], [22]. When implementing EAP-TLS, it should be ensured that the usage of weak ciphersuites is avoided [23].

A formal correctness proof for EAP-TLS was given in [24]. The proof is based on Protocol Composition Logic (PCL), a “logic for proving security properties of network protocols” [25].

C. CCM

The security of CCM was proven under the assumption that the underlying block cipher is secure [26]. Both standards use AES, which can be considered to be secure [27]. In combination, CCM can be considered to be a secure encryption mode.

CCM* is a small variation that includes the complete functionality of CCM and additionally supports use cases where only encryption is required.

D. Inaccurate standard definition

Both standards provide a rather high margin for implementation of devices according to the standard definition. There is no basis for certifyability like a protection profile which usually provides implementation instructions in much greater detail.

Such a high implementation margin might not only lead to incompatibility (and a lack of interoperability) of devices manufactured by different companies. It can also lead to strong security weaknesses. For example, there are no concrete instructions given on the source of randomness to be used, although the usage of a strong cryptographic random number generator is an important requirement for cryptographic methods.

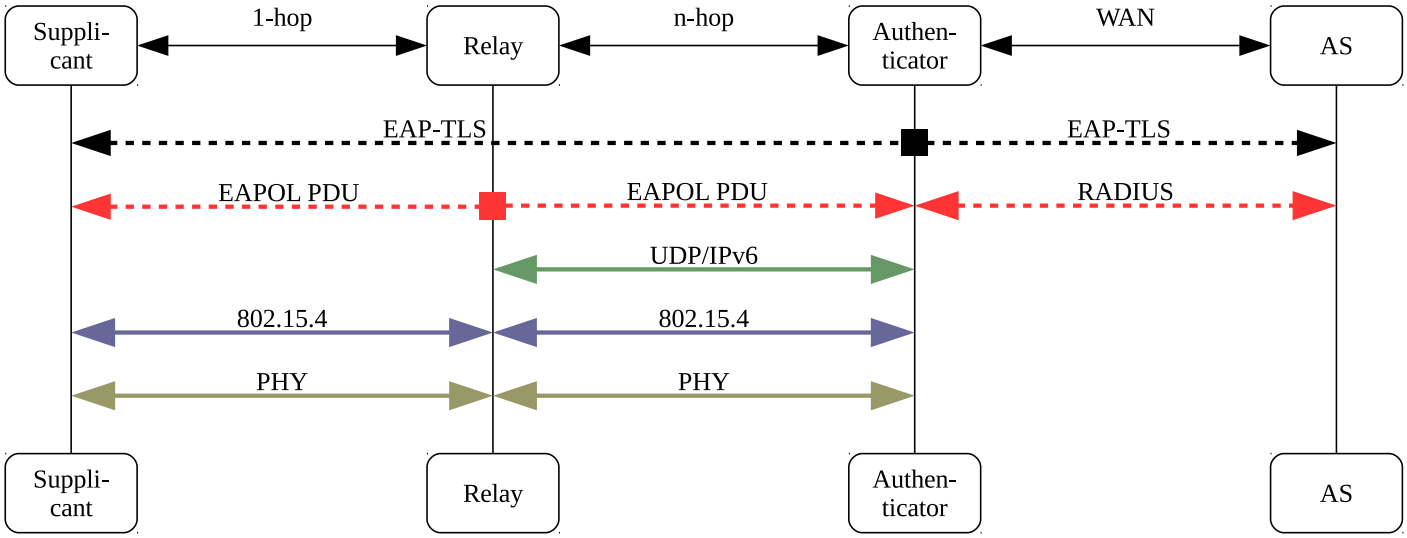

Fig. 3. Layered communication in 1901.2 commissioning

A protection profile is eligible for both standards, not only from a security point-of-view. Such a profile collects and analyses all imaginable adversaries and threats for the system. It covers them by providing detailed cryptographic requirements. By this means it provides a basis for certifyability (e.g. to Common Criteria).

V. Conclusion

According to our description in section II, the two compared standards ITU-T G.9903 and IEEE 1901.2 have certain differences of which the different routing mechanisms is probably one of the most significant. Although the approaches' differences appear to be rather significant at first view, the two contrary installation scenarios can be realised with a similar level of efficiency and security with both standards.

The basic difference between the standards (from a security point-of-view) can be reduced to the choice of the EAP method, which is (disregarding from certain recommendations) free for both standards.

Choosing EAP-PSK is useful for reasons of efficiency and simplicity, but gets hard to manage and maintain with an increasing amount of devices in the network. Huge networks cannot be covered by this method, at least not with a central authentification authority.

The method EAP-TLS is more complex and thus has (by complexity) more potential for security problems. The latest description of EAP-TLS prescribes the support of a certain set of ciphersuites. One of these suites can be considered to be weak, so that negotiating this ciphersuite can be one of these security gaps.

Both standards also implement measures against replay and denial-of-service attacks. They use similar kinds of encryption modes on a lower layer than EAP. A device must first be authenticated to get the secret group key of the network.

References

[1] "COMMISSION RECOMMENDATION of 9.3.2012 on preparations for the roll-out of smart metering systems," http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32012H0148, The European Commission, March 2012.

[2] "G9903: Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks," ITU-T, 2 2014.

[3] "IEEE Standard for Low-Frequency (less than 500kHz) Narrowband Power Line Communications for Smart Grid Applications," IEEE Standards Association, 10 2013.

[4] "Studie zur Analyse der Kosten-Nutzen einer sterreichweiten Einfhrung von Smart Metering," http://www.e-control.at/documents/20903/-/-/b68eb019-b6bf-444d-b4fb-95f3d05727ca, PricewaterhouseCoopers Austria, Juni 2010.

[5] "802.15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE Standards Association, 2011.

[6] "802.15.4e: Low-Rate Wireless Personal Area Networks (LR-WPANs) (MAC sublayer)," IEEE Standards Association, 2012.

[7] "RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," 3 2012.

[8] "RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks," 9 2007.

[9] K. Kim, S. D. Park, G. Montenegro, S. Yoo, and N. Kushalnagar, "6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD)," 6 2007, http://tools.ietf.org/html/draft-daniel-6lowpan-load-adhoc-routing-03.

[10] "RFC 3748: Extensible Authentication Protocol (EAP)," 6 2004.

[11] "Commissioning in 6LoWPAN," 7 2008.

[12] H. Cha, K.-H. Kim, and S. Yoo, "LBP: A Secure and Efficient Network Bootstrapping Protocol for 6LoWPAN," in *Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication*, ser. ICUIMC '11. New York, NY, USA: ACM, 2011, pp. 54:1–54:8. [Online]. Available: http://doi.acm.org/10.1145/1968613.1968679

[13] "RFC 2865: Remote Authentication Dial In User Service (RADIUS)," 6 2000.

[14] "RFC 4764: The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method," 1 2007.

[15] "RFC 3610: Counter with CBC-MAC (CCM)," 9 2003.

[16] "802.1X: Port-Based Network Access Control," IEEE Standards Association, 2010.

[17] "Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)," Bundesamt für Sicherheit in der Informationstechnik, 2014, version 1.3.

[18] E. B. Barker, "Sp 800-57. recommendation for key management, part 1: General (revision 4)," National Institute of Standards & Technology, Gaithersburg, MD, United States, 1 2016.

[19] "RFC 5216: The EAP-TLS Authentication Protocol," 3 2008.

[20] "RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1," 4 2006.

[21] X. Wang, D. Feng, X. Lai, and H. Yu, "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD," Cryptology ePrint Archive, Report 2004/199, 2004, http://eprint.iacr.org/.

[22] A. A. Kuznetsov, "An algorithm for MD5 single-block collision attack using high-performance computing cluster," Cryptology ePrint Archive, Report 2014/871, 2014, http://eprint.iacr.org/.

[23] I. Muscat, "Recommendations for TLS/SSL Cipher Hardening," https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/, October 2014.

[24] C. He, M. Sundararajan, A. Datta, A. Derek, and J. C. Mitchell, "A Modular Correctness Proof of IEEE 802.11I and TLS," in *Proceedings of the 12th ACM Conference on Computer and Communications Security*, ser. CCS '05. New York, NY, USA: ACM, 2005, pp. 2–15. [Online]. Available: http://doi.acm.org/10.1145/1102120.1102124

[25] A. Datta, A. Derek, J. C. Mitchell, and A. Roy, "Protocol Composition Logic (PCL)," *Electronic Notes in Theoretical Computer Science*, vol. 172, pp. 311 – 358, 2007, computation, Meaning, and Logic: Articles dedicated to Gordon Plotkin. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1571066107000849

[26] J. Jonsson, "On the Security of CTR + CBC-MAC," in *Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography*, ser. SAC '02. London, UK, UK: Springer-Verlag, 2003, pp. 76–93. [Online]. Available: http://dl.acm.org/citation.cfm?id=646558.694897

[27] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique Cryptanalysis of the Full AES," in *Advances in Cryptology ASIACRYPT 2011*, ser. Lecture Notes in Computer Science, D. Lee and X. Wang, Eds. Springer Berlin Heidelberg, 2011, vol. 7073, pp. 344–371. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-25385-0_19