GPRS Security for Smart Meters

Martin Gilje Jaatun, Inger Anne Tøndel, Geir M. Køien

GPRS Security for Smart Meters

Martin Gilje Jaatun[1], Inger Anne Tøndel[1], and Geir M. Køien[2]

[1] Department of Software Engineering, Safety and Security
SINTEF ICT
NO-7465 Trondheim, Norway
{martin.g.jaatun,inger.a.tondel}@sintef.no
http://www.sintef.no/ses

[2] Department of information- and communication technology (ICT)
Faculty of Engineering and Science
University of Agder
NO-4879 Grimstad, Norway
geir.m.koien@uia.no
http://www.uia.no/en

Abstract. Many Smart Grid installations rely on General Packet Radio Service (GPRS) for wireless communication in Advanced Metering Infrastructures (AMI). In this paper we describe security functions available in GPRS, explaining authentication and encryption options, and evaluate how suitable it is for use in a Smart Grid environment. We conclude that suitability of GPRS depends on the chosen authentication and encryption functions, and on selecting a reliable and trustworthy mobile network operator.

Keywords: Security, GPRS, Smartgrid, AMI, Smart Metering

1 Introduction

Smart Meters in an Advanced Metering Infrastructure (AMI) represent perhaps the most visible aspect of the Smart Grid [1]. Smart Meters are placed in every home, providing real-time two-way communication with the electricity provider, or Distribution Service Operator (DSO).

AMIs allow the automatic collection of power consumption data, and thereby more granular pricing schemes. However, AMIs also allow DSOs to have better overview of the current state of power delivery and increased opportunities for control. Smart meters can send status messages and alarms to the DSO, they may also have breaker functionality, allowing power to be turned off remotely. Furthermore, meters may be connected to equipment in the homes that allows automatic adjustment of power demand based on the current price level.

Smart Meters use a variety of communications means towards DSOs, but General Packet Radio Service (GPRS) is a popular choice in many rural settings [2]. GPRS was introduced as a faster data transfer service for GSM Mobile Stations, offering a packet-based data service according to the Internet Protocol (IP). It introduces a number of new network elements, most notably the Serving

GPRS Support Node (SGSN) which connects to the Mobile Station via the current active Base Transceiver Station (BTS), and the Gateway GPRS Support Node (GGSN) at the Mobile Station's home operator, which connects to the public internet. Using GPRS for AMI implies equipping smart meters with a UICC/USIM or SIM subscriber module, and a communication terminal that communicates by means of GPRS.

Security is important in AMI systems. Smart meters will need to communicate personal information; power delivery to meters can be remotely controlled; and status updates, software updates and configuration parameters can all be considered confidential. Thus, DSOs need to know how communication is secured. Security can be used as a differentiating factor when deciding on which communication technology to use. It is however likely that other considerations, such as the area of coverage of the telecommunication network and how densely the area is populated [3], will be given more weight. Still, knowledge of the protection offered by the alternative communication technologies is important to decide what additional security measures are needed. Only with such knowledge can DSOs end up with AMI solutions that are both cost-effective and offer adequate security.

This paper explains the security offered by GPRS, when used for AMI. Section 2 gives an overview of threats towards AMI systems to provide a basis for understanding the main security needs for AMI. Section 3 provides an overview of the security functionality of GPRS. Section 4 summarises the security offered by GPRS based on the security needs of AMI explained in Section 2 and provides recommendations for DSOs that plan on using GPRS for communication with their smart meters. Section 5 concludes the paper.

2 Background

The increased connectivity and the new trust models that come with the introduction of AMI lead to new threats and a pressing need for DSOs to deal with information security and consumer privacy. The context in which we are considering GPRS communication is illustrated in Fig. 1. Tøndel et al. [1] identified threats towards AMI systems on the interface between a smart meter and the Head End System (HES) at the DSO. Threats include the following (threats are numbered in the same way as in the paper by Tøndel et al.):

- Fake identities: Someone takes the identity of a meter (T2) or the identity of the HES (T1)
- Tamper with communication: Someone tampers with the communication sent between the HES and meters (T5)
- Repudiation: Meter denies receiving a message (T10) or the sending of a message (T11)
- Eavesdropping: Someone eavesdrops on communication between a meter and the HES (T13)
- Denial of service: Communication is hampered due to a denial of service attack on the HES (T18), an attack on one or more meters (T19) or a failure on the communication link (T20)

For DSOs it is important to understand the extent to which GPRS and other candidate communication technologies are vulnerable to such attacks or help prevent failures of the above listed types. Also it is important to become aware of the configuration choices available that can increase or lower the achieved level of security.

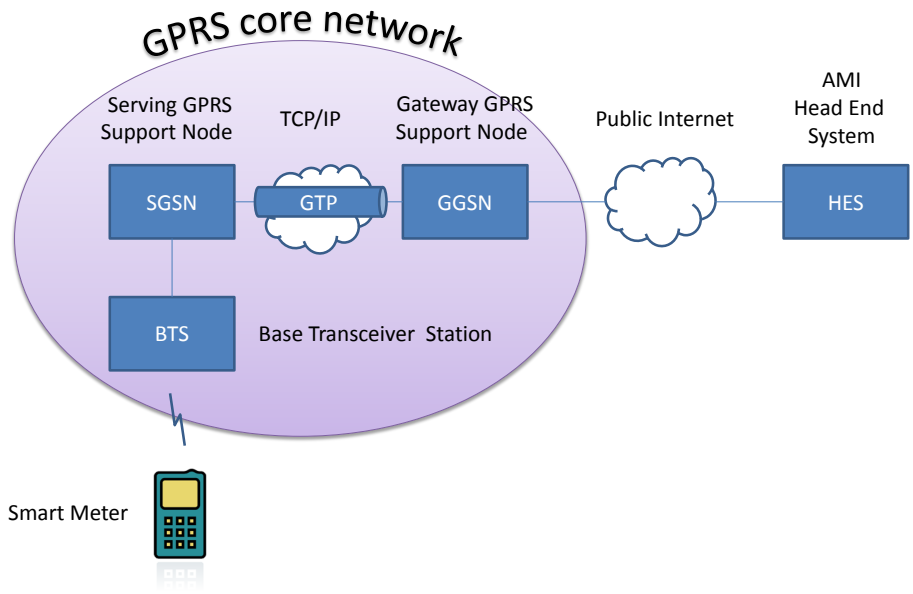

Fig. 1. GPRS communication for AMI

The ability to use fake identities is related to the authentication functionality of GPRS. The feasibility of eavesdropping and tampering is dependent on the degree of protection of the communication. The risk of repudiation problems are dependent on the degree to which actions can be proved. The risk of denial of service has to do with the capacity of the communication media and the equipment, as well as its robustness. In the following, we will describe available security mechanisms in GPRS in order to evaluate how these threats are handled.

3 GPRS Security Functions

GPRS offers security functionality on the interface between the mobile terminal and the GPRS core network. This section describes that functionality, including security functionality that can be achieved by use of UICC/USIM instead of SIM. It also provides a brief introduction to security in the GPRS core network,

and means to protect information when sent from GPRS core to the DSO via the public internet.

3.1 Authentication and key agreement

In GPRS, mobile users are authenticated towards the network. The native 2G authentication and key agreement (AKA) protocol used in the packet-switched GPRS system is the same as the one used in the circuit-switched GSM system, but the challenge-response is performed by the Serving GPRS Support Node (SGSN) rather than the Visitor Location Register/Mobile Switching Center (VLR/MSC). We use the name VLR/SGSN to denote cases where there is no distinction between the GSM and GPRS cases. The authentication protocol is known as GSM-AKA, using the interface[3] functions A3 and A8 (TS 43.020 [4]). The actual implementation is operator dependent, but the GSM Association have several example algorithms available.

The GSM-AKA protocol is a two-stage protocol, as illustrated in Fig. 2:

- Request from VLR/SGSN to HLR/SGSN and forwarding of triplet (authentication set) from HLR/AuC to the VLR/SGSN (steps ① and ②)
- Network-initiated challenge-response (VLR/SGSN - SIM) (steps ③ and ④)

Table 1. Elements used in the GSM-AKA Authentication and Key Agreement protocol

K_c	Secret calculated by SIM and HLR/AuC, sent to VLR/SGSN
K_i	Secret key shared between SIM and AuC
RAND	Random challenge selected by VLR/SGSN
RES	Result of challenge calculated by SIM and sent to VLR/SGSN
XRES	Expected result of challenge calculated by HLR/AuC, sent to VLR/SGSN

The tamper resistant SIM card includes the permanent subscriber identity (International Mobile Subscriber Identity – IMSI), the per-subscriber authentication secret K_i and the AKA algorithms (A3/A8). The IMSI and K_i are one-to-one associated, and the K_i is a pre-shared secret. The IMSI will be known to multiple nodes and networks, but the K_i is only known to the SIM and the HLR/AuC.

The HLR/AuC will produce triplets $(RAND, SRES, K_C)$ and forward these to the VLR/SGSN upon request. The $RAND$ is 128-bit wide and is the (pseudo) random challenge while the 32-bit $SRES$ is the signed response. The A3/A8 are

[3] The various Ax, fy functions defined in GSM and UMTS (A3, A5, f1, f2, ...) are only standardised at the interface level; i.e., expected input and output is defined, but the actual implementation is left to each operator. However, many operators employ one of the example implementations documented by The GSM Association and 3GPP, as explained later in this paper.

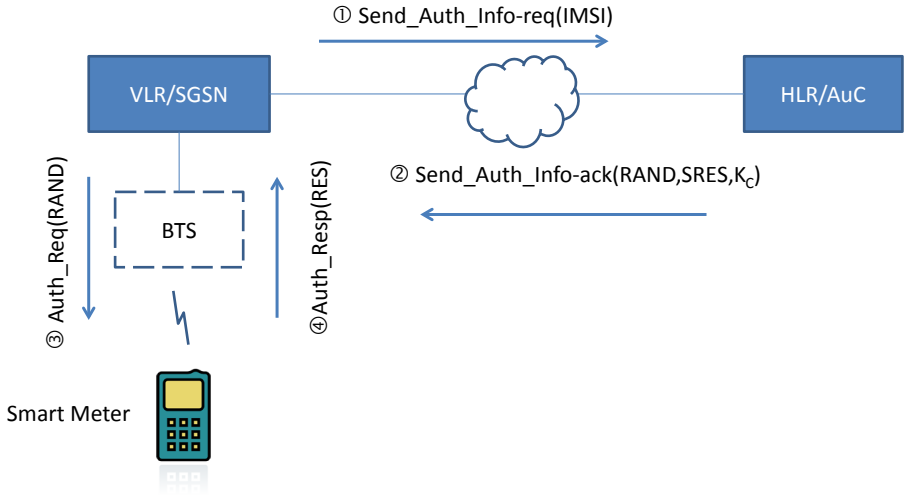

Fig. 2. The GSM-AKA Authentication and Key Agreement protocol

one-way functions (Fig. 3), ideally making it computationally infeasible for an intruder to determine the K_i and the K_C upon witnessing the plaintext exchange of the challenge-response procedure[4]. The VLR/SGSN receives the triplet and challenges the SIM by forwarding the $RAND$. The SIM will compute the $SRES$ and K_C, and the $SRES$ will be forwarded as the response to the VLR/SGSN. The encryption key will be forwarded to the MS from the SIM upon request. Provided that the $SRES$ from the HLR/AuC matches the result from the SIM, the authentication is considered successful. The outcome also includes the SIM and the VLR/SGSN sharing the K_C encryption key. The ciphering key used is the 64-bit K_C key for both GSM and GPRS.

It should be noted that there exist some rather weak A3/A8 implementations, and specifically the original "example" algorithm known as COMP128 (completely broken [5, 6]). Also note that GSM-AKA only generates a 64-bit session key, which clearly is not future proof considering the continual improvements in processing speeds for exhaustive key search applications. For standard GSM-AKA, we recommend the use of the GSM-Milenage [7] implementation, which uses the UMTS Milenage AKA functions and a set of conversion functions to implement the A3/A8 functions.

[4] Note that it must be computationally infeasible to recover K_i also when the attacker can observe a large number of challenge-response exchanges, ideally also for chosen-plaintext attacks. Even if an attacker should have access to the full triplet (including $SRES$ and K_c) it should not be possible to recover K_i.

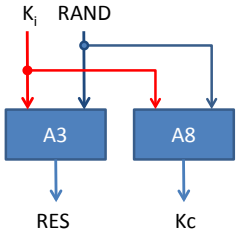

Fig. 3. Using the GSM A3/A8 functions to perform GSM-AKA calculations

3.2 UMTS Authentication and Key Agreement

It is possible to run the UMTS Authentication and Key Agreement (UMTS-AKA) [8, 9] protocol over the "GSM Edge Radio Access Network" (GERAN) if the subscriber has a UICC/USIM module instead of the old GSM SIM. The UMTS AKA protocol is defined in 3GPP TS 33.102 [10] and the functions are shown in Fig. 4. All the interface functions f1-f5 take the secret key K and a random challenge RAND as input, while f1 also takes a sequence number SQN and an Authentication Management Field AMF as input. The functions produce the following outputs:

MAC-A Message Authentication Code
XRES Expected challenge result
CK Cipher Key for subsequent message encryption
IK Integrity Key
AK Anonymity Key (for obfuscating the sequence number in case this exposes the identity of the client)

These values are computed by the Authentication Center (AuC), and further

$$\text{AUTN} = \text{SQN} \oplus \text{AK}||\text{AMF}||\text{MAC-A}$$

$$\text{AV} = \text{RAND}||\text{XRES}||\text{CK}||\text{IK}||\text{AUTN}$$

The Authentication Vector (AV) can be considered the UMTS equivalent to the GSM triplet. See Table 2 for a complete overview of the elements used in UMTS-AKA.

The Authentication Vector (AV) is roughly equivalent to the GSM triplet. The AK is used to mask the sequence number. The challenge from the SGSN includes the (RAND,AUTN) tuple. The UICC/USIM runs the calculations depicted in Fig. 4, and returns the result of f2 (RES). The SGSN compares the RES from the MS with the XRES from the AV, and if they match, the MS is authenticated.

Table 2. Elements used in the UMTS-AKA protocol

Acronym	**Explanation**
AK	48 bit Anonymity Key
AMF	16 bit Authentication Management Field
AUTN	Authentication values computed by AuC
AV	Authentication vector computed by AuC, sent to SGSN (equivalent to the GSM triplet)
CK	128 bit Cipher key, for encryption of data (confidentiality key)
IK	128 bit Integrity key
K	128 bit Secret key pre-shared between USIM and AuC
MAC-A	64 bit Message Authentication Code, "signature" to authenticate the challenge
RAND	128 bit Random challenge selected by VLR/SGSN
RES	32-128 bit Result of challenge calculated by USIM and sent to SGSN (default 64 bit)
SQN	48 bit Sequence Number
XRES	32-128 bit Expected result of challenge calculated by AuC, sent to SGSN (default 64 bit)

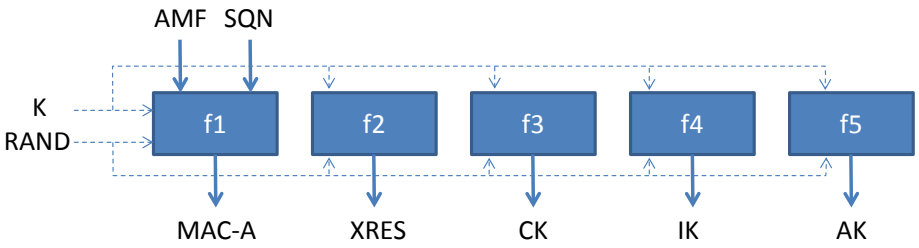

Fig. 4. UMTS Authentication and Key Agreement (AKA) functions

3GPP has provided the Milenage algorithm set [11] as an example implementation of the f1-f5 functions. The Milenage algorithm set includes a cryptographic core, Rijndael (i.e., the algorithm implementing the Advanced Encryption Standard (AES)), and a set of constants and parameters to produce independent output from all the UMTS AKA functions.

3.3 GPRS Encryption

With GPRS, the data and signaling traffic is encrypted over the wireless interface and all the way from the mobile station to the GPRS core. The ciphering algorithms used in GPRS are known as the GEA family of algorithms (GEA, GEA2, GEA3, GEA4). The GEA interface is defined in TS 41.061 [12]. We note again that in 2G GPRS, the ciphering terminates in the core network (CN) in the SGSN, while in GSM the ciphering terminates in the BTS. The GSM equivalent ciphering algorithms are known as the A5 family of algorithms (A5/1, A5/2, A5/3, A5/4), where the A5/2 algorithm has been deprecated and where the A5/1 algorithm is now showing its age. The ciphering key used is the 64-bit K_C key for both GSM and GPRS, with the exception of GEA4 (and A5/4), which uses a 128 bit key.

The original GPRS algorithms (GEA and GEA2) are 64-bit designs and they are in fact similar, but the GEA algorithm is modified to only use 54 significant bits. This dates back to cold war export regulations, and the relaxation of export conditions allowed the GEA2 algorithm to regain the 10 lost bits.

The GEA3 algorithm is defined by the Keystream Generator Core (KGCORE) block cipher mode of operation, which in turn uses the the KASUMI[5] block cipher. The KGCORE primitive is based on a 128-bit key internally, and the interface achieves this by using the K_C key twice. GPRS can also use the GEA4 encryption algorithm with a 128 bit key called K_{C128}. GEA4 also uses KGCORE, but there the K_{C128} key is used directly. In order to use GEA4 (or A5/4 in GSM) the subscriber must use a UICC/USIM and run the UMTS AKA protocol.

We note that while a 3G/UMTS identity module (UICC/USIM) may be used in a 2G device (GSM/GPRS), the cipher function must inevitably be compatible with the over-the-air interface. This means that the UMTS key pair (CK,IK) must be converted into the the 64-bit K_C key (or the 128 bit K_{C128} key for GEA4).

The selection of encryption algorithm takes place by the mobile station indicating which version(s) of GEA it supports, and then the SGSN decides which version will be used [13]. If they do not support a common algorithm, the connection may be released. It is also an option that the SGSN decides on not encrypting the data.

[5] Despite appearances, KASUMI is a proper noun ("mist" in Japanese), not an acronym.

There are no built-in security functions in GPRS that offer confidentiality or integrity protection beyond the SGSN[6]; specifically, all data sent on the public internet interface (Gi) from the GGSN is sent in plaintext. In fact, integrity protection is not provided at at all for GERAN. However, it is possible to configure so-called access point names (APNs) at the GGSN, and it is possible to use this mechanism to set up a VPN tunnel from the G_i-interface to an external network. To some extent such solutions[7] are already in commercial use.

3.4 Core Network Protection

The access security in GPRS terminates at the SGSN. Data traffic is forwarded between the SGSN and the GGSN by means of the GPRS Tunneling Protocol (GTP). There are various versions of GTP and there is a distinction between user plane (GTP-U) and control plane (GTP-C). Whereas the access may be by means of GERAN, the core network may still be 3G or 4G compliant. The GTP protocol (any version) does not by itself provide any security. There is not a strict requirement in 3GPP to cryptographically protect the GTP protocol, but it certainly is recommended [10]. Specifically, the 3GPP have profiled IPsec for use within 3GPP systems (TS 33.210 [14]) in what is known as the Network Domain Security (NDS) area. The NDS/IP [14] was originally developed for inter-operator use, but it increasingly being used for all IP-based interfaces in 3GPP system. We strongly recommend that NDS/IP be used for protection of GTP.

3.5 GPRS Closed User Groups

It is possible to set up closed user groups in the cellular networks [15], but as there is no appreciable security provided this can at best serve as a defence-in-depth measure. Furthermore, the service is really tailored for circuit-switched calls and is therefore largely irrelevant.

4 Discussion

In Section 2, we listed a set of risks relevant to the communication between a smart meter and the HES at DSOs. On this interface we claimed that DSOs need to be aware of the availability and strength of authentication mechanisms, the extent to which communication is protected, the degree to which actions can be proved, and the capacity and robustness of the communication media and the equipment used. In this section we sum up what support GPRS offers in this respect. We also identify technology and configuration choices that DSOs should

[6] However, as will be described below, from SGSN to GGSN data is sent over GTP, which may offer additional protection options.

[7] See for instance `http://www.telenorfusion.no/makeit/communicationapis/mobiledataaccess/mdatechnicaldetails.jsp`

make in order to improve the security of a GPRS communication solution used for AMI. The findings are summarised in Table 3.

Authentication of smart meter terminals to the communication network is performed by GPRS. The strength of this authentication is dependent on the authentication mechanism used, where the main alternatives, as explained above, are GSM-AKA and UMTS-AKA. Implementations of GSM-AKA algorithms (A3/A8) are operator dependent, and it should be noted that some of the available implementations are rather weak. Using the GSM-Milenage implementations of the A3 and A8 algorithms is thus recommended. For DSOs, the strength of the algorithm employed could be used as a differentiating factor among GPRS providers. DSOs should however consider equipping new smart meters with UICC/USIM. This will allow using UMTS-AKA for authentication, and also allow for additional security improvements over the use of SIM.

In GPRS, there is no mechanism for authenticating the communication network to the smart meter. This implies that it is possible to trick the meter into using a fake base transceiver station. According to Mitchell [16], it is no longer unfeasible for attackers with modest budgets to acquire a fake base transceiver station, and indeed news reports stated three years ago that a fake GSM base station could be built for as little as £1000 [17] - this sum is likely to be even lower today. However, if a meter is equipped with a UICC/USIM, two-way authentication can be performed (through the use of the MAC-A "signature" to verify the authentication challenge), and the fake base transceiver station threat is effectively mitigated.

GPRS communication that is sent on the wireless link is encrypted, but the encryption terminates in the core network. The strength of the encryption is dependent on the algorithm used, and it is also possible for the SGSN to specify that the traffic shall not be encrypted. Standard GPRS with a traditional GSM SIM can only support 64-bit encryption, making GEA, GEA2 and GEA3 the available algorithms. With a USIM, GEA4 is also an option. We recommend that smart meters use GEA3 or above for encryption. The smart meters thus need to support one of these algorithms, and only advertise these during authentication. The SGSN also needs to support the algorithm, but as smart meters are not likely to move around, the support of one of these algorithms can be checked beforehand when selecting an operator. In other words, it is unlikely that a smart meter would need conventional roaming capability at all, always only connecting directly to the home mobile network operator. However, it should be pointed out that availability considerations might dictate that a smart meter should be able to use alternative providers if the home network provider is unavailable [2].

Generally, there is no default security in the protocols used in the GPRS core network. Operators may however choose to implement NDS/IP for protection of the GTP traffic; this is something we would recommend. DSOs should consider the trustworthiness and competence of the operator, as the operator's perimeter protection as well as its staff and internal routines are essential for the security of the communication. Selection of an operator implies that the DSO has to trust that operator's internal network.

Table 3. AMI threats evaluated based on using GPRS communication

Description	**Threat#**	**Evaluation**
Fake identities		
Fake HES	T1	GPRS with normal SIM will not prevent fake base transceiver stations (SGSN), and thus no protection against a fake HES. GPRS with UICC/USIM can perform mutual authentication toward a base transceiver station, and prevent introduction of fake HES in GPRS scope (but additional protection may be needed beyond the GGSN)
Fake meter	T2	GPRS authentication mechanisms will prevent fake meters from connecting to the network
Tamper with communication		
	T5	GPRS offers reasonable protection against tampering with GEA3 encryption (GEA4 offers good protection) (but additional protection may be needed beyond the GGSN)
Repudiation		
Reception	T10	GPRS offers no non-repudiation mechanisms
Sending	T11	GPRS offers no non-repudiation mechanisms
Eavesdropping		
	T13	GPRS offers reasonable protection against eavesdropping with GEA3 encryption (GEA4 offers good protection) (but additional protection may be needed beyond the GGSN)
Denial of service		
Attack on HES	T18	GPRS authentication mechanisms will prevent fake meters or other nodes from connecting with the HES
Attack on meter	T19	GPRS with normal SIM will not prevent fake base transceiver stations, which could be used to tie up a meter indefinitely. GPRS with UICC/USIM can perform mutual authentication of base transceiver station, ensuring that fake base transceiver stations are dropped immediately
Failure of communication link	T20	GPRS has no special protection against jamming, but neither does most commercially available wireless technology

From the GPRS core network the communication is sent unencrypted on the Internet on its way to the HES, unless additional protection measures are applied. Operators often offer VPN solutions, so that communication is sent in a secured tunnel from the GPRS core network to the network of the DSO. If the operator offers such solutions, we recommend that DSOs use them in order to protect the data sent to and from the smart meters.

Note that GPRS offers no mechanisms to prove actions (i.e, there is no non-repudiation functionality). If this is needed, then mechanisms must be added on top of GPRS. There is also no specific protection against denial of service attacks, and a fake base transceiver station could potentially effect a denial-of-service attack against a meter by tying it up indefinitely (this attack can be prevented by using UICC/USIM instead of SIM). Using wireless protocols is always challenging with respect to denial of service, as wireless media can easily be jammed. That being said, we are not aware of any particular weaknesses (compared to similar wireless technologies) in the GPRS technology when it comes to capacity and robustness of the communication media and equipment used. This may however depend on the operator.

As AMI systems will need to communicate confidential information; such as detailed meter consumption, configuration changes, software updates, and breaker commands; protection of the communication is essential. It is however important to note that AMI protection is not solely dependent on the security of the communication protocols. If GPRS is not able to offer strong enough protection, then additional security can be added on the application layer. This includes encryption, integrity protection and non-repudiation mechanisms. For DSOs that utilise several different technologies for meter communication, such application layer protection may be needed anyway because of different levels of security in the communication technologies used. It is however important that DSOs are aware of the protection offered, so that they can end up with a solution that is cost-effective while still offering adequate security.

5 Conclusion and Further Work

This paper has provided an overview of the security of GPRS related to its use for AMI. From a security point of view, we recommend the use of UICC/USIM instead of the SIM as this offers stronger and more extensive authentication and encryption. If using SIM, we recommend the use of the GEA3 encryption algorithm. We also recommend that DSOs use security and trustworthiness as a differentiating factor when choosing among mobile network operators.

There may be a need for security on top of GPRS. In particular, the communication between the GPRS core network and the DSO needs to be protected, either by using a VPN solution offered by the operator, or by implementing additional security functionality in higher layers. In a longer term perspective, additional security mechanisms may also contribute to future-proofing smart grid communication solutions that are likely to have a longer life span than

their mobile telephony counterparts. Mobile communications technologies are constantly evolving, and it remains to be seen how e.g. LTE will influence AMI.

Acknowledgment

The research reported in this paper has been supported by the Telenor-SINTEF collaboration project, Smart Grid initiative.

Abbreviations

The world of mobile communications is drenched in three- and four-letter abbreviations and acronyms. To ease the reader's burden, we provide a list of the abbreviations used in this document here.

3GPP 3rd Generation Partnership Project
AKA Authentication and Key Agreement
APN Access Point Name
AuC Authentication Centre
AUTN AUThenticatioN value
BTS Base Transceiver Station (known as the Base Station in GSM)
GEA GPRS Encryption Algorithm (1-4)
GERAN GSM EDGE Radio Access Network
GGSN Gateway GPRS Support Node
GPRS General Packet Radio System
GSM Global System for Mobile Communications, originally Groupe Spécial Mobile
GTP GPRS Tunneling Protocol
HES Head End System
HLR Home Location Register
IMSI International Mobile Subscriber Identity
KGCORE Keystream Generator Core
LTE Long-term Evolution (also known as 4G LTE)
MS Mobile Station (Mobile telephone handset, or – in our case – a stationary Smart Meter)
MSC Mobile Switching Center
NDS Network Domain Security
SIM Subscriber Identity Module
SGSN Serving GPRS Support Node
TS Technical Specification
UICC Universal Integrated Circuit Card
UMTS Universal Mobile Telephone System
USIM Universal Subscriber Identity Module
VLR Visitor Location Register

References

1. Tøndel, I.A., Jaatun, M.G., Line, M.B.: Threat Modeling of AMI. In: "Proceedings of the 7th International Conference on Critical Information Infrastructures Security (CRITIS 2012)". (2012)
2. Telenor: Smart metering white paper – Best practices recommendation by Telenor Connexion (2013)
3. Gungor, V., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., Hancke, G.: Smart grid and smart homes: Key players and pilot projects. Industrial Electronics Magazine, IEEE **6**(4) (2012) 18–34
4. 3GPP: 3rd Generation Partnership Project; Technical Specification Group Services and system Aspects; Security related network functions (Release 12) (2013) 3GPP TS 43.020 V12.0.0.
5. SDA: Smartcard Developer Association Clones Digital GSM Cellphones (1998) http://www.isaac.cs.berkeley.edu/isaac/gsm-press.html.
6. Rao, J., Rohatgi, P., Scherzer, H., Tinguely, S.: Partitioning attacks: or how to rapidly clone some gsm cards. In: Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on. (2002) 31–41
7. 3GPP: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the GSM-MILENAGE Algorithms: An example algorithm set for the GSM authentication and key generation functions A3 and A8 (Release 8) (2008) 3GPP TS 55.205 V8.0.0.
8. Køien, G.M.: An introduction to access security in UMTS. Wireless Communications, IEEE **11**(1) (2004) 8–18
9. Niemi, V., Nyberg, K.: UMTS security. John Wiley & Sons (2003)
10. 3GPP: Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 11) (2012) 3GPP TS 33.102 V11.0.0.
11. 3GPP: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General (Release 1999) (2001) 3GPP TS 35.205 V3.0.0.
12. 3GPP: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements (Release 4) (2002) 3GPP TS 41.061 V4.0.0.
13. Xenakis, C.: Security measures and weaknesses of the gprs security architecture. International Journal of Network Security **6**(2) (2008) 158–169
14. 3GPP: Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Network Domain Security (NDS); IP network layer security (Release 12) (2012) 3GPP TS 33.210 V12.0.0.
15. 3GPP: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Closed User Group (CUG) Supplementary Services - Stage 1 (Release 9) (2009) 3GPP TS 22.085 V9.0.0.
16. Mitchell, C.J.: The security of the GSM air interface protocol (2001) http://www.ma.rhul.ac.uk/static/techrep/2001/RHUL-MA-2001-3.pdf.
17. Stanley, N.: Mobile Phone Hacking for £1000. ComputerWeekly (2010) http://www.computerweekly.com/blogs/Bloor-on-IT-security/2010/04/mobile-phone-hacking-for-1000.html.