Secure Lossless Aggregation Over Fading and Shadowing Channels for Smart Grid M2M Networks

Andrea Bartoli, Juan Hernández-Serrano, Miguel Soriano, Mischa Dohler, *Senior Member, IEEE*, Apostolos Kountouris, and Dominique Barthel

***Abstract*—While security is generally perceived as an important constituent of communication systems, this paper offers a viable security-communication trade-off particularly tailored to smart grids. These systems, often composed of embedded nodes with highly constrained resources, require, e.g., metering data to be delivered efficiently while neither jeopardizing communication nor security. Data aggregation is a natural choice in such settings, where an additional challenge is to facilitate per-hop and end-to-end security as well as a mechanism to protect the valid nodes from exhaustion threats. The prime contribution of this paper is to include into the security design framework issues related to aggregation, wireless fading and shadowing channels, physical layer parameters (such as choice of modulation, packet length, channel coder), medium access control parameters (such as average number of transmissions), routing parameters (such as choice of route). Relying on analysis and corroborating simulations, unprecedented design guidelines are derived which determine the operational point beyond which aggregation is useful as well quantifying the superiority of our protocol enriched with a protection mechanism against nonintended packets (malicious or nonmalicious) w.r.t. nonaggregated and/or unsecured solutions.**

***Index Terms*—Communication system security, error correction, fading channels, smart grids.**

I. Introduction

EVER SINCE U.S. President Barack Obama's "National Broadband Plan" [1], smart grids have moved into the limelight. Smartness w.r.t. the current grid is achieved by many advanced time-critical automated and autonomous control features within interconnected macro as well as microgrids. Important constituents for such an automation are machine-to-machine (M2M) communication mechanisms, which seamlessly connect points of inference and control with a smart decision engine. A typical application is to use meters as points of inference, switches/fuses/valves as points of control and the the utility's control center as the decision point. Another important application is the monitoring of high-voltage masts from overheating of connection points as well as physical damage due to weather. We will subsequently concentrate on the smart metering application, understanding that all other applications obey the same or similar requirements.

Using an automated M2M systems has at national level the advantages that the efficiency and effectiveness of the grid are significantly increased; thus, dependency on foreign natural resources, waste, and usage at large is diminished. Advantages for resource suppliers, such as utility companies, are the ability of (near) real-time monitoring of the grid infrastructure and its load; thus, faults and outages can be detected and attended to with minimum delay, energy can be traded at different tariffs, etc. The end-user profits since an optimized and (nearly) instantaneous bill can be delivered, failures can be detected and handled remotely by the utility or the user him/herself, appliances are used when energy is cheapest, etc.

As outlined in [1], wireless communication systems play an integral role in accomplishing this vision. This is realized by the typically used communication architecture, where embedded radios are installed at each inference and control point; these communicate wirelessly between each other in a multihop fashion over a (typically) tree-like topology [2]; until a gateway is reached which could be a DSL line or a cellular interface.

Said architecture with underlying technical requirements on delay, autonomy, and security are facilitated by the emerging paradigm of M2M. Originated by a Swedish company Maingate in the late 1990s, it is currently being standardized within ETSI M2M [3], 3GPP [4], and IEEE 802.16p [5]. The envisaged architecture comprises M2M terminals and M2M gateways, all of which contain an embedded SIM card allowing connectivity to the cellular base station. The M2M gateway connects into a capillary network, which is composed of low-power, short-range embedded devices forming a local network. These embedded devices can rely on, e.g., IEEE 802.15.4x but also cellular device-to-device communication technologies [6].

These required wireless M2M constituents are becoming increasingly ubiquitous but suffer from some inherent shortcomings. Notably, the nodes are often limited in resources (e.g., power supply, memory, processing power); the spectrum they use to communicate is considered to be scarce; the wireless channel itself is a source of uncertainty which leads to packet errors and thus retransmissions; the wireless channel is broadcast by nature and thus prone to compromise in security. This

Manuscript received October 15, 2010; revised June 14, 2011; accepted June 14, 2011. Date of publication September 01, 2011; date of current version November 23, 2011. This work was supported in part by a France Telecom research contract on M2M security, the EU project ICT-258512 EXALTED, the Spanish Research Council Project TEC2008-06663-C03-01 and Spanish Ministry of Education and Science CONSOLIDER Project CSD2007-00004 (ARES). Paper no. TSG-00174-2010.

A. Bartoli, M. Soriano, and M. Dohler are with the Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), 08860 Castelldefels, Spain (e-mail: mischa.dohler@cttc.es).

J. Hernández-Serrano, and M. Soriano are with the Universitat Politècnica de Catalunya (UPC), 08034 Barcelona, Spain.

A. Kountouris, and D. Barthel are with the Orange, France Telecom, 38243 Meylan, France.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2011.2162431

advocates for a paradigm shift in designing wireless communication systems tailored to the needs of smart grids in that the system needs to be highly power efficient *and* very secure.

As for the utmost power efficiency, a first step is to use data aggregation at each multihop node, which aggregates the received packets from its leaf nodes prior to forwarding the aggregated packet to its parent node. Given that one of the core requirements of smart grid applications is to be able to obtain an exact reading from each node and also to be able to uniquely associate a node to the data, lossless aggregation must be used. Among the very few lossless techniques available, packet concatenation is a suitable solution which yields ease of use at notable performance gains. Lossless aggregation based on concatenation is particularly important when the communication infrastructure is to be shared among different inference applications, such as automated electricity, gas and water metering, third party services, etc., since messages pertaining to different applications need to be securely aggregated without loss. Aggregator nodes—instead of retransmitting the raw received data—thus forward the aggregated data by combining the packets (saving headers) or even removing redundant information.

As for security, not only does aggregation pose a particular challenge to securing the data but also is security of significant concern to various smart grid communities. Notably, ZigBee-type and many proprietary smart metering solutions are *not* at all or insufficiently secured and thus pose a serious threat to integrity and privacy. This has been recognized by various standardization bodies and, as of Q2 2011, the IETF ROLL, ETSI M2M, and Wavenis OSA [7] work on security mechanisms for said networks. These efforts largely rely on prior art dealing with end-to-end or hop-by-hop secure aggregation schemes.

In end-to-end encryption schemes [8]–[10], collected data is secured at the source and the keys to decrypt and check this data are only shared between the originator (mainly a metering node) and the base station or gateway. As a result, the challenge is how the intermediate nodes do aggregation on data they cannot decrypt. Aggregation on such solutions can be as simple as concatenation of encrypted data (saving packet headers) or more sophisticated provision of secure aggregation by using additive privacy homomorphism protocols [9]. However, with end-to-end encryption, the link layer is *not* protected at all and thus being accessible for an attacker. As a naive example, one could simply drain the radio by constantly sending packets which can only be identified as false once the entire reception and decryption has taken place.

Hop-by-hop aggregation protocols, such as [11]–[14], provide more efficient aggregation operations and protect the link layer and above. Nevertheless, since sensed data are revealed for the sake of aggregation at the aggregator nodes, hop-by-hop aggregation protocols are by design weaker in terms of confidentiality than end-to-end aggregation protocols. Combination of both protocols can be done under certain conditions and some proposals, such as [15] and [16], have already tackled this in parts.

Aggregating packets has also a profound impact onto various aspects of the wireless communication system. First, per-hop and end-to-end security mechanisms need to be redesigned. Second, next-hop communication and security overhead is saved when only one longer instead of several shorter packets is transmitted. Third, the packet error rate (PER) and thus the average number of retransmission of a longer packet are generally larger than of a shorter packet. To the best of the authors' knowledge, a joint trade-off of above security and communication paradigms has not been performed to date. That is, none of the prior art has designed a security framework which allows for aggregation *and* is also optimized for specific wireless channel conditions.

The aim of this paper is hence to propose and quantify the performance gain of a secure, lossless packet aggregation protocol operating over a lossy channel. To this end, the paper is structured as follows. In Section II, we propose a simple but viable aggregation protocol which is secure at PHY, hop-per-hop as well as end-to-end. In Section III, we quantify the average number of packet transmission as well as its outage probability in the presence of different channel coders and different fading and shadowing configurations. In Section IV, in order to justify the benefits of our protocol, we assess the overhead utilized and the energy consumption with and without a lossy channel of our protocol compared to traditional solutions or with solution without security requirements. In Section V, we position our protocol with respect to prior art and clearly highlight the differences between proposed solutions. In Section VI, we provide its characteristics within a taxonomy typically used in industrial designs. Finally, in Section VII, we conclude the paper.

II. Secure Lossless Aggregation Protocol

In this section we present a protocol for smart grid M2M networks that secures communications between a set of collector nodes or meters and their application server in an efficient and secure manner. The protocol is designed for a typical scenario depicted in Fig. 1 where some metering nodes collect data which is reported to a gateway or application server through an operator multihop network. As a result, four types of nodes compound the network: 1) metering nodes that actually infer the data; 2) aggregator nodes that collect data sensed by a set of metering nodes; 3) routers that provide the necessary infrastructure to facilitate communication between involved nodes (notice that aggregator nodes are also routers); and 4) the gateway itself.

The aim of the protocol is to provide end-to-end (between meters and gateway or beyond), hop-by-hop (within every link) as well as physical-layer (at received packet level) security while minimizing the traffic in the network and thus maximizing the overall life of involved nodes.

End-to-end security is achieved by means of a shared secret between every meter and the gateway; hop-by-hop security is done at MAC layer by means of pairwise keys between every network node and its one-hop neighbors; and physical layer security is facilitated by authenticating the physical layer preamble. Adding lossless aggregation to this extra security, allows further optimization of network resources and minimization of energy expenditures. As we will show later in Section IV, the proposed protocol not only avoids an extra cost for security but also reduces the overall cost of the process of sending the data. This is due to aggregation savings making up for or even exceeding the computational cost of the security operations.

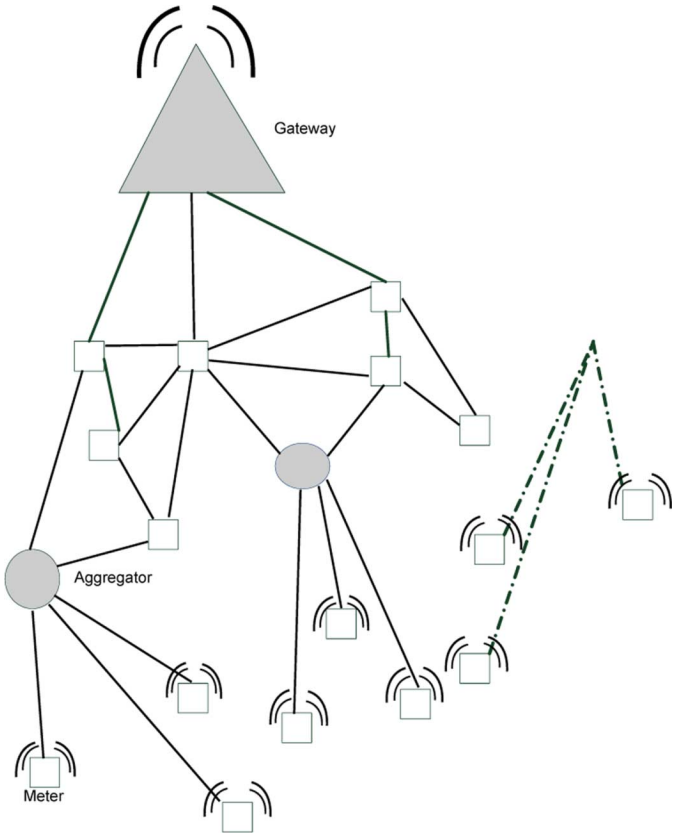


Fig. 1. Abstraction of the smart grid application scenario.

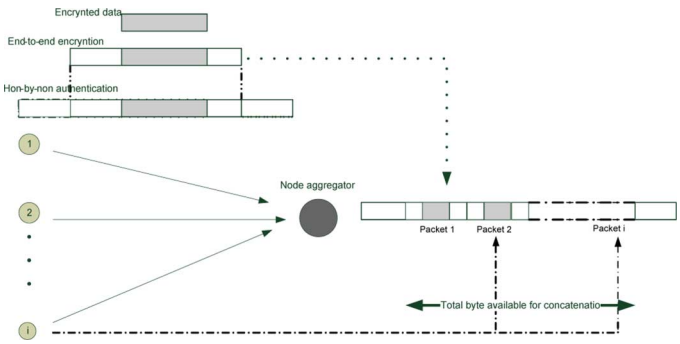


Fig. 2. The secure lossless aggregation process.

Subsequently, we outline the proposal of a complete security suite in form of end-to-end, hop-by-hop and PHY layer security and secured lossless aggregation, as well as needed key management. Later in the paper, when having dealt with the impact of the wireless channel, we will quantify the benefits of the proposed security suite in the context of the popular IEEE 802.15.4 standard.

A. End-to-End Security

The aim of end-to-end security is to protect the data from unauthorized eavesdropping (confidentiality); to allow the destination to check the integrity of the received data and its freshness; and to unequivocally identify the source of such data (authentication). End-to-end security is achieved here as follows.

The metering node creates a packet with the sensed data as shown in Fig. 2. The headers include the source of data (addressing field), destination (gateway), a timestamp, a key identifier, a security control, and the data length; the data is encrypted with the key shared with the gateway; and a *message integrity code* (MIC)[1] is appended. Consequently, end-to-end security, that is to say confidentiality, integrity, and authentication (CIA) and freshness (because of the timestamp), is provided between the meter and the gateway.

Compared to nonsecure protocols, the use of end-to-end security introduces some overhead (see OH_N in the implementation example in Fig. 6); however, on the other hand, it allows the gateway to unequivocally and securely identify the source of the data and to detect any modification of this data along its path to the gateway or beyond.

In a typical implementation, the overhead OH_N related to achieving end-to-end security is at least:

- An identifier of the key/s used for encrypting the data and creating the MIC. This identifier allows the gateway to find or derivate the keys for checking the MIC and decrypting the data. Once again, 1 byte should be enough in most cases.
- A security control that contains the security level and the key identifier mode.
- A timestamp in order to guarantee freshness of collected data (which will also be usually present in any nonsecure scenario). Its length will be related to the amount of sent/received packets per time interval. Usually the timestamp is just related to the frame counter, the key counter or both.
- The length of the encrypted data. The gateway will need this length in order to know how many bits to decrypt after this header. Typically the length is part of the frame control field.
- A MIC of the packet header and data. The MIC typically is 32, 64, or 128 bits long.

Emphasis of end-to-end security is on ensuring confidentiality while being able to confirm source authenticity and data integrity.

B. Hop-by-Hop Security

End-to-end security is checked at the final destination; however, before reaching the gateway or Internet destination, the packets must go through one or more wireless links that are by nature exposed to attackers. As a result, if no security is provided in order to restrict the access to the media, only the destination point will be able to detect altered, dropped or fake packets. This fact exposes the network to exhaustion attacks since those packets will waste precious energy at the intermediate nodes (routers). Consequently, hop-by-hop integrity, authentication, and freshness should also be provided at MAC layer.

From above reasoning, the protocol requires the use of timestamps and MICs also at MAC layer. Compared to nonsecure protocols, the use of hop-by-hop security introduces at least the following overhead:

- A timestamp (it is not related to the timestamp at network layer) in order to guarantee freshness. Once again,

[1]The acronym MIC (message integrity code) is used throughout this document instead of the more common MAC (message authentication code). The reason to do this is that we are also already using MAC for media access control.

the timestamp is often a frame counter, a key counter, or a combination of both.
- An identifier of the key used for creating the MIC. This identifier allows the next hop to find or derive the keys for checking the MIC. Once again, 1 byte is enough in most cases.
- A MIC of the frame header and payload. The MIC typically is 32, 64, or 128 bits long. Strictly speaking the frame integrity check sequence (commonly referred as frame check sequence—FCS) can be replaced by this MIC (for example when using TinyOS [17]), and thus the real overhead would be just the difference (if there is any) in size between the MIC and the check sentence.

Emphasis of hop-per-hop security is hence on source authenticity and data integrity.

C. Physical Layer Security

Packets being received can either be intended or not intended for the specific receiver. Typically, energy is spent in receiving the entire packet, performing the security checks on the entire packet, checking on intended destination; only then the packet is discarded. As we will show in Section IV, the energy spent on these to-be-discarded packets is not negligible. Therefore, we present here a physical authentication method that allows to discard a nonintended packet after reception of just the physical preamble and an added authentication preamble. Rejection of these packets leads to savings in unnecessary reception and processing of the remainder of the packet, but also improves the network protection against injection attacks, which pertain to an attacker injecting fake packets thus reducing lifetime of the network nodes or even exhaust them.

In the following we detail how to generate the authentication preamble, how to validate it, its security implications, the probability of out-of-sync and the time needed to compare all the K valid authentication preambles with the received one. For the sake of clarity we also provide Table I with the specific nomenclature for this section.

Concerning the generation of the authentication preamble, suppose a network node u that wants to send a packet to v that may itself be another network node or a group of nodes.

Let us denote ID_u and ID_v as unique identifiers of u and v respectively. Let us denote $\tau \in \mathbf{N}_0$ as a counter of the frames that u sends to v. Let us denote K_{u-v} as a groupwise key (key shared between a groups of nodes) or a pairwise key (link key between couples, of node) shared by u and v.

The authentication preamble $F_i^{u\to v}|_K$ for the ith message from u to v with shared secret K_{u-v} is defined as in (1), where H is a message authentication code or keyed hash function $H(m,k)$ of data m with key k. As clearly shown in Fig. 3, every new authentication preamble is a function of the previous one.

$$F_i^{u\to v}|_{K_{u-v}} = \begin{cases} H(\{ID_u, ID_v\}, K_{u-v}) & \texttt{if } i = 0 \\ H\left(F_{i-1}^{u\to v}|_{K_{u-v}}, K_{u-v}\right) & \texttt{otherwise.} \end{cases} \tag{1}$$

The recommended length of the authentication preamble is 32 or 64 bits since it provides a good trade-off between security and additionally transmitted bits [18]. Consequently, in a real implementation H would be a truncated cryptographic hash function, such as truncated HMAC, or a standard block cipher, like AES in CBC-MAC mode; the use of the latter is the most common

TABLE I
NOTATION

$\mathcal{A}$	Cost of generating an authentication preamble
$\mathcal{C}_l^K$	Cost of checking l bits against K chains of l bits
$\mathcal{E}$	Added cost per legitimate packet with physical authentication
$\mathcal{M}$	Storage cost when using physical authentication
$\mathcal{P}_{tx}$	Cost of processing a frame to be transmitted (besides authentication)
$\mathcal{P}_{rx}$	Cost of processing an incoming frame (besides authentication)
$\mathcal{R}_l$	Cost of receiving l bits
$\mathcal{T}_l$	Cost of transmitting l bits
$\mathcal{S}_{fake}$	Savings due to discarding a fake packet with physical authentication
$\mathcal{S}_{valid}$	Savings due to discarding valid non-intended packet with physical authentication
$\mathcal{T}$	Total savings per link in a given period with physical authentication
$\mathcal{N}$	Number of non-intended non-malicious packet received for neighbors
A	Length of the authentication preamble
K	Number of precomputed preambles. $K = N \cdot W$
L	Frame total length without authentication preamble
N	Number of the receiver's neighboring nodes
P	Length of the physical preamble
W	Preamble window. Number of precomputed authentication preambles per neighbor
p_K	Probability of finding a collision with K precomputed authentication preambles
ρ	Number of fake packets during the active interval
σ	Contents of the authentication preamble
$p_{r,t}$	Probability of the receiver r receives a message sent from the emitter t
Δt	Period of time equal a one rate
δ	Number of legitime packet received from a valid node

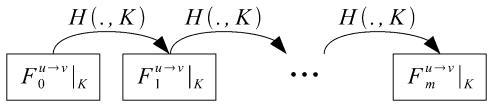


Fig. 3. Authentication preamble of the ith message from u to v.

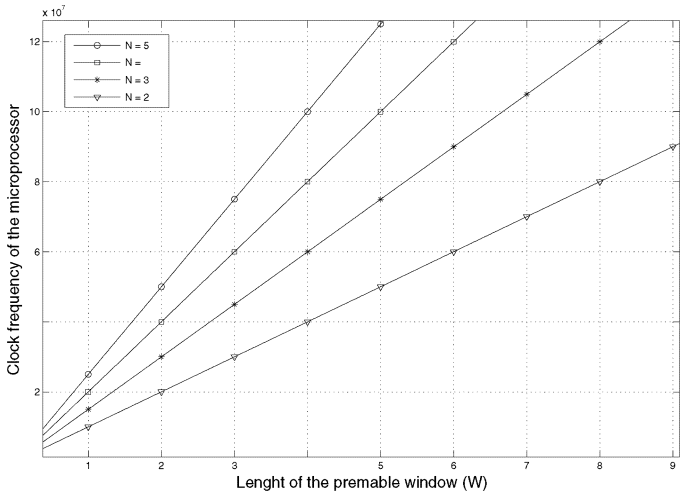


Fig. 4. Minimum clock frequency of the platform's microprocessor to ensure the proper functioning of the proposed authentication preamble with different values of W per neighbor.

choice when an embedded system needs to implement both encryption and hashing with minimal code size or hardware area while impacting efficiency and security [19].

Concerning the validation of the authentication preamble, let us suppose that an emitter u sends a packet to a receiver v. The authentication preamble is denoted as σ. Verification of σ by v is a deterministic process: v calculates the potential authentication preamble using the common attributes $\sigma' = F_{\tau}^{u \to v}|_{K_{u-v}}$, and checks it against the received σ; if the two are the same, authentication succeeds, otherwise it fails.

In order to increase the speed of checking,[2] every node may precompute the potential σ' values of every incoming packet from any of its N neighboring nodes. Consequently, assuming an initial value of $\tau = 1$ for every neighboring node, at a first stage every node precomputes values of σ' with $\tau \in [1, W]$ for every neighboring node or potential emitter. Then, every node stores $K = N \cdot W$ potential future values of σ'. The use of the preamble window W prevents an out-of-sync risk due to a packet loss; only if the W precomputed values of σ' for a given emitter are lost, the emitter will get into an out-of-sync state and its future packet will be rejected. Therefore, the value of W should be closely related to the channel error rate; the higher the error rate, the larger W.

When the authentication preamble σ of a packet is received, since the MAC destination is not know until reception of the MAC frame, it is compared with the K precomputed values of σ'; if some σ' matches the received σ, all previous σ' values from the same emitter are removed, and new potential values of σ' are precomputed in order to restore the W values for every neighboring node.

To corroborate the strength of our proposed PHY layer security scheme, we subsequently perform some security analysis. For this analysis, we will assume that the output of function H cannot be predicted; for security analysis regarding the election of H, we refer the reader to [20] and [21]. The probability for an attacker to generate a valid authentication preamble for impersonating a valid emitter for a given receiver can be expressed as in (2) with A being the length of the authentication preamble and K the number of precomputed authentication preambles.

$$p_K^i = 1 - (1 - (1/2^A))^K. \tag{2}$$

Notice that finding a collision leads a packet to bypass physical authentication, but it has still to be a valid packet at higher layers. This fact minimizes the effect of security invasion or bypassing authentication at large. Moreover, once a collision (in the security sense) is found, it is only valid once and thus it cannot be replayed for exhaustion attacks.

Implementing the proposed authentication preamble mechanism, the communications between motes, are possible only if the devices are synchronized. In order to avoid the effect of possible losses in the synchronization, a long enough window of precomputed authentication preambles is used. In this section, we analyze those situations where the motes are not able to communicate, defining $p_{\mathrm{out-of-synch}}$, the probability of out-of-synch. There are two possible cases that can produce this problem.

The first situation is produced when a valid fake authentication preamble is received. In this case, the valid fake authentication preamble will desynchronize the receiver and the emitter of which corresponds the valid authentication preamble falsified. This leads to a denial-of-service attack. Therefore, this requires a cross-layer mechanism allowing to update τ and the correct value of the authentication preamble for a given emitter from above layers; once the packet that had bypass the physical authentication is detected to be a fake, τ and the authentication preamble value should be updated to its old values.

The second situation occurs when a couple of motes try to exchange messages but no one of the W consecutive packets sent from the emitter arrive to its destination. In this case the nodes will be desynchronized because the new authentication preamble used by the sender is not precomputed by the receiver. Defining the bit error probability (BEP) as the average bit error probability (to be quantified in more detail in the subsequent section), $p_{\mathrm{out-of-synch}}$ can be roughly calculated as

$$p_{\mathrm{out-of-synch}} = (1 - (1 - \mathrm{BEP})^A)^W. \tag{3}$$

Utilizing the BEP given in (8), a typical SNR value in a wireless channel of 5 dB [22], $A = 32$ bits, and $W = 5$ leads to $p_{\mathrm{out-of-synch}} = 10^{-12}$, i.e., a very rare event.

In order to save the emitter's energy, this situation could be mitigated implementing a security system that provides special messages when pairs of nodes are not able to communicate for a consecutive $W\ \Delta t$ time. In low rate networks, the receiver expects a legitime message every Δt; therefore, if after $(W + 1)\ \Delta t$, there is still no communication, the supposed receiver will start a new "registration process" to resynchronize with the emitter. This process permits reliable communication and safeguard the network against the waste of energy.

Finally, we demonstrate that the comparison between σ and all the K valid authentication preambles is practically feasible. The proposed mechanism is clearly only useful if the comparison is finished before the reception of the next byte after the physical authentication preamble field. In our analysis, we will use some typical parameters of the most usual platforms used with the IEEE 802.15.4 standard. It supports a maximum data rate of 250 KBps when operated in the 2.4 GHz ISM band. This means that the platforms are able to receive a byte every 4 μs $(1/(250 \cdot 10^3) = 4\ \mu\mathrm{s})$.

We essentially wish to define the relationship between the minimum clock frequency of the microprocessor and the length of the window preamble. To this end, we calculate the number of operations for every received byte that each platform needs to compute in order to load the precomputed values and compare them with σ. For example, Atmel ATmega 128L [23] needs: 2 cycles/byte to "load," 1 cycle/byte to "subscript," and 2 cycles/byte to "brunch if equal." That said, the total time to compare all the possible valid authentication preambles (K) is given as

$$T = K \cdot ((A \cdot \mathrm{cyclos})/f_{\mathrm{microprocessor}}). \tag{4}$$

[2]Note that computing F could be slower than receiving the rest of the frame thus making the physical authentication useless.

In this way we can calculate the threshold value for W as

$$W = (2 \cdot 10^{-7} \cdot f_{\text{micorprocessor}})/N. \quad (5)$$

Equation (5) shows that with, e.g., $N = 5$ the proposed authentication preamble must run on platforms with a microprocessor that works at at least 25 MHz (clock frequency rate).

D. Key Management

End-to-end security, hop-by-hop security, and physical authentication make use of at least the following keys:

- End-to-end security: a shared key between every meter and the application server.
- Hop-by-hop security: pairwise keys shared between every node and its neighbor nodes.
- Physical authentication: a groupwise key shared by all the smart grid nodes.

All these keys should be periodically updated in order to increase the difficulty of cryptanalysis and whenever any of them has been compromised. How to update and distribute the keys is what is referred to as key management.

Key management starts with the identification of ownership and responsibilities. From the three above, the first is clearly in the realms of the application, commonly a customer of the network operator who offers services from the metering data, while the other two are responsibility of the network operator.

Key management of end-to-end security is the easiest to achieve since it just relies on shared pairwise keys between the meters and the customer application server. This is a high resilience scheme, since when a meter is compromised, its key is rejected and it does not affect the rest of the nodes. The customer in any case is in charge of at least use short-term pairwise keys derived from the long-term ones in order to make the cryptanalysis more difficult.

An operator trusted third party should be used to securely negotiate the neighbor pairwise keys just after the network deployment. This approach, which is widely accepted, was first implemented in SPINS [24] and, with minor adaptations, is suitable in any environment. The negotiation system and periodicity is typically part of the operator security policies.

Another operator trusted third party, or just the same as before, is in charge of distributing the group key for the physical authentication and securely updating it whenever a node is compromised or whenever the updating policy determines it. Within the simplest approach, the trusted third party delivers updated keys through individual secure channels with every node [25] and thus every smart grid node should also store a pairwise key with the operator trusted third party. However, many other proposals with better efficiency for large groups (most of the deriving from [26], [27]) have been appeared during the last ten years and may be used by the operator.

E. Secure Lossless Aggregation

Since the collected/sensed data normally contains just a few bits of metering information, the payload of packets between meters and their aggregator node is usually far from its maximum allowed or its optimal size. As a result, within the security framework described above, we propose to concatenate several legitimate packets into a single one at the aggregator node. This concatenation or lossless aggregation reduces unnecessary overhead (headers and MICs), and thus aids in compensating for the overhead induced by hop-per-hop and end-to-end security. The proposed aggregation process is illustrated in Fig. 2 and its execution is detailed in Algorithm 1.

Algorithm 1 Secure lossless aggregation (at every aggregator node).

```
osize = 0
opacket_id = 0
createOutputPacket( opacket_id )
for every input packet do
  if checkMIC() == TRUE then
    mac_data = getPacketMacData()
    if osize + sizeOf(mac_data)>P'_a then
      createMIC( opacket_id )
      sendPacket( opacket_id )
      opacket_id = opacket_id + 1;
      createOutputPacket( opacket_id )
      osize = 0
    end if
    aggregateInputPacketPayloadIntoOutputPacket(
    mac_data, opacket_id)
    osize = osize + sizeOf(mac_data)
    if last received packet OR timeout then
      createMIC( opacket_id )
      sendPacket( opacket_id )
    end if
  end if
end for
```

From the aggregator node to the gateway, the intermediate nodes have only to check the MAC integrity/authentication of every received packet, and forward the packet with a new MIC and updated headers. Integrity, authentication, and freshness at MAC layers are therefore checked at every hop. The resulting packets at the aggregator will be made of the following fields:

- MAC header: that also includes the key identifier used for hop-by-hop security and timestamp.
- for $i = 1$ until $i = n$ with n the number of aggregated input packets at every output packet.
  - — Network header of the ith meter's packet.
  - — Encrypted data of the ith meter's packet.
  - — MIC of the ith meter's packet.
- MAC MIC.

Summarizing, the aggregator receives the packets, checks their MAC layer MICs, concatenates the payloads of as many MAC layer received packets as it can into one MAC layer payload of every output packet, calculates the MAC layer MIC of the output packet and sends the resulting packet to the next hop.

In summary, we have proposed here a complete security suite which joins prior art in end-to-end security, prior art in hop-per-hop security and an innovative PHY layer security approach with a novel aggregation mechanism which does not jeopardize any of the invoked security mechanisms. To evaluate the effectiveness of this suite, we first need to understand the impact of the wireless communication channel, which is dealt with in the following section.

III. Embedded Communication Protocols

This section is dedicated to the quantification of the impact of the lossy wireless channel onto the performance of the embedded M2M secure protocol suite using specific physical (PHY), medium access control (MAC), and networking (NTW) layers. Notably, we quantify the average energy needed to delivery a message from a given source node via multiple relaying nodes to the sink node (gateway). Core to this calculus is a rigorous quantification of the average number of transmissions at each hop. We thus first briefly discuss the properties of wireless channels typically encountered in M2M settings. We then derive the packet error rate at PHY, which is expressed as a general function of the used modulation and coding scheme, packet length, and channel conditions. Thereupon we derive the average number of transmissions at MAC, which is expressed as a function of the previously derived packet error rate. We finally derive obtain the optimal routing path, which is obtained as a function of the average number of transmissions previously derived. A complete framework taking all these factors into account is, in fact, unprecedented and allows us to correctly configure the M2M system.

A. Wireless Channel

The wireless channel is generally impaired by pathloss, shadowing, and fading. The presence and interaction of these three phenomena influences the signal-to-noise (SNR) ratio and has thus a profound impact on the PHY and MAC layer performances of the M2M system at large.

The underlying processes of these phenomena are well known, and we will only state the distributions needed for subsequent calculus. Notably, the distribution of shadowing is typically assumed lognormal

$$p_s(\overline{\gamma}|\mu_{\mathrm{dB}},\sigma_{\mathrm{dB}}) = \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{dB}}}\frac{10}{\ln 10}\frac{1}{\overline{\gamma}}e^{-\left(\frac{10\log_{10}\overline{\gamma}-\mu_{\mathrm{dB}}}{\sqrt{2}\sigma_{\mathrm{dB}}}\right)^2}. \tag{6}$$

where σ_{dB} is the standard deviation (not variance) of the shadowing process in dB (not linear scale), and μ_{dB} is its mean which typically reflects the pathloss and thus relates to the SNR. Due to the fixed positions of the meters, we will subsequently assume that the shadowing process is static or very slowly varying in time but variable in space.

As for fading, indoor and many low-height transceiver measurements have shown that the Nakagami distribution is the most suitable modeling assumption, which occurs if a bunch of impinging waves phase-aligns. The PDF of the received power is gamma distributed and given as

$$p_\gamma(\gamma|\overline{\gamma}) = \frac{m^m(\gamma)^{m-1}}{(\overline{\gamma})^m\Gamma(m)}\exp\left(-\frac{m\gamma}{\overline{\gamma}}\right), \tag{7}$$

where $\Gamma(\cdot)$ is the complete Gamma function and m is the Nakagami fading factor. The spatial and temporal dynamics of fading heavily depend on the operating conditions, as will be explained below.

B. PHY Layer

The aim of the physical (PHY) layer is to ensure that data is reliably delivered point-to-point. The core functionalities of the PHY layer of a capillary M2M radio at the transmitter are channel encoding of the bit stream and modulation of the bit stream to a symbol stream which form the over-the-air packet. At the receiver, the PHY layer is responsible for detecting the symbols, demodulating, and decoding. Subsequent analysis hence pertains to average bit error rates at the input of the channel decoder and thus resulting packet error rates at the output of the decoder.

AWGN BER: The average bit error rates over nonfaded additive white Gaussian noise (AWGN) channels for arbitrary quadrature amplitude modulation (QAM) and phase shift keying (PSK) is difficult to obtain in closed form. However, such a channel may occur in smart grid settings where the random fading realizations are assumed to be constant over the packet length or even over a very long duration. Note further that both QAM and PSK modulations are indeed used in capillary M2M solutions: QAM offers a higher spectral throughput and is used in advanced embedded radios; and PSK offers a constant envelope and thus cheaper power amplifiers and is throughout traditional embedded radios. To obtain a closed form expression for the average bit error probability (BEP), it is typically assumed that the system operates at sufficiently large signal-to-noise (SNR) values and uses Gray coding, yielding one symbol error to cause approximately one bit error. The BEP is then approximated by [28]

$$\mathrm{BEP}_{\mathrm{AWGN}}(\gamma) \approx a\cdot Q(\sqrt{b\gamma}), \tag{8}$$

where γ is the SNR and $Q(x)$ the Q-function. The constants a and b depend on the choice of modulation and modulation order M, i.e., $a = 4/\log_2 M(1-1/\sqrt{(M)})$, $b = 3/(M-1)$ for M-QAM and $a = 2/\max(\log_2 M, 2)$, $b = 2\sin^2(\pi/M)$ for M-PSK.

Fading BER: The average BEP over Nakagami-m wireless fading channels for arbitrary QAM and PSK constellations is also difficult to obtain in closed form. However, assuming again sufficiently large SNRs and Gray coding, these can be approximated as [29]

$$\mathrm{BEP}_{\mathrm{Nakagami}}(\overline{\gamma}) \approx \alpha\cdot\left(\frac{m}{m+\beta\overline{\gamma}}\right)^m \times {}_2F_1\left(m,\frac{1}{2};m+1;\frac{m}{m+\beta\overline{\gamma}}\right), \tag{9}$$

TABLE II
PARAMETERS FOR TYPICAL BLOCK CODES

Code	J	k	$d_{\min}$	coding rate	t
Hamming	7	4	3	0.57	1
Golay	23	12	7	0.52	3

TABLE III
PARAMETERIZATIONS OF TYPICAL CONVOLUTIONAL ENCODERS

K	R_c	T	d_{min}	$a_{d_{min}}$	asymptotic WEP
4	1/2	1	6	1	$10N\mathrm{BEP}^3$
7	1/2	1	10	11	$1386N\mathrm{BEP}^5$

where $\overline{\gamma}$ is the average SNR and ${}_2F_1(x,y;c;u)$ is the Gauss hypergeometric function with 2 parameters of type 1 and 1 parameter of type 2 ([30], Sec. 9.14.1)). The constants α and β depend on the choice of modulation and modulation order M, i.e., $\alpha = 2(1-1/\sqrt{(}M))/(\sqrt{\pi}\log_2 M)\cdot\Gamma(m+1/2)/\Gamma(m+1)$, $\beta = 3/2/(M-1)$ for M-QAM and $\alpha = 1/\sqrt{\pi}/\max(\log_2 M, 2)\cdot\Gamma(m+1/2)/\Gamma(m+1)$, $\beta = \sin^2(\pi/M)$ for M-PSK.

Block Channel Code: That erroneous bit stream is fed into the channel decoder, which can either be of convolutional or block type. Note that both channel coding methods are indeed in use today by advanced embedded metering radios, such as provided by [2]. The error performance of channel coders is evaluated by means of the average word error probability (WEP), which quantifies the probability that a codeword is erroneous. For block coding, this probability can be approximated by [28], [31]

$$\mathrm{WEP}_{\mathrm{block}}(\overline{\gamma}) \approx \sum_{j=t+1}^{J} \binom{J}{j} \mathrm{BEP}^j (1-\mathrm{BEP})^{J-j}, \quad (10)$$

where J is the word length in bits, t the number of errors which can be corrected by the code, BEP the uncoded bit error probability of the channel taking any form given above. Even though (10) only holds rigorously if all bit errors in the codeword are independent, [31] has shown that the approximation is sufficiently tight even for large modulation orders and a wide range of fading conditions. The parameters J, t are summarized in Table II for some typical block codes. Several other important parameters are also stated in Table II: $d_{\min}$ is the minimal Hamming distance of the code and k is the uncoded number of information bits in the code word. This allows us to obtain the average packet error probability (PEP) as

$$\mathrm{PEP}_{\mathrm{block}}(\overline{\gamma}) \approx 1-(1-\mathrm{WEP}_{\mathrm{block}}(\overline{\gamma}))^{N/k}, \quad (11)$$

where N is the total number of bits per packet and k the number of bits per block code word. This is only an approximation, albeit tight [31], because at higher order modulations the codewords are not strictly speaking independent.

Convolutional Channel Code: For convolutional codes, the average WEP can be approximated by [31], [32]

$$\mathrm{WEP}_{\mathrm{conv}}(\overline{\gamma}) \approx N\cdot\frac{1}{2T} a_{d_{\min}} \binom{d_{\min}}{\frac{d_{\min}}{2}} \mathrm{BEP}^{\frac{d_{\min}}{2}} \quad (12)$$

where $a_{d_{\min}}$ is the number of paths with the minimal distance $d_{\min}$, and T the puncturing period. Above (12) only holds for $d_{\min}$ even which holds for typically used convolutional coder; for the general case, consult [32]. Table III summarizes the parameterization of typically used convolutional codes without puncturing, i.e., $T=1$. Finally, since convolutional decoding is typically done over the entire packet, the PEP is equal to the WEP

$$\mathrm{PEP}_{\mathrm{conv}}(\overline{\gamma}) = \mathrm{WEP}_{\mathrm{conv}}(\overline{\gamma}). \quad (13)$$

C. MAC Layer

The role of the MAC layer is to handle contention between potentially interfering links, assigning resources to a given link and also handle retransmissions in case the first transmission attempt fails. Since the amount of MAC protocols for capillary systems is extremely large [33], we will not focus on a specific contention-based or contention-free realization but rather assume that a specific link between transmitter and receiver is already established. Furthermore, since resource allocation in the context of embedded systems essentially reduces to power control, we will also not further take this into account. Retransmissions, however, are explicitly considered as they are quintessential in ensuring reliable links. Following the notation of [34], $\overline{N}_{\mathrm{tx}}$ denotes the average number of transmissions needed to ensure a successful reception and is given by $\overline{N}_{\mathrm{tx}} = \sum_{n=1}^{\infty} n(1-\mathrm{PEP}_{\mathrm{data}})(1-\mathrm{PEP}_{\mathrm{ack}})(\mathrm{PEP}_{\mathrm{data}}\mathrm{PEP}_{\mathrm{ack}})^{n-1} = 1/((1-\mathrm{PEP}_{\mathrm{data}})(1-\mathrm{PEP}_{\mathrm{ack}}))$, where n is the number of transmissions, $\mathrm{PEP}_{\mathrm{data}}$ and $\mathrm{PEP}_{\mathrm{ack}}$ are the PEP of data and acknowledgement (ACK) packets, respectively. In the acknowledgment process, it is assumed that an ACK packet can be successfully transmitted in a single attempt. This is based on the fact that ACK packets are much smaller and thus much likelier to go through, and on temporal channel correlation which ensures that, if the data packet experienced a good channel, the return path experiences the same beneficial channel conditions. We can therefore assume that $\mathrm{PEP}_{\mathrm{ack}} \approx 1$, yielding

$$\overline{N}_{\mathrm{tx}}(\overline{\gamma}) \approx \frac{1}{1-\mathrm{PEP}_{\mathrm{data}}(\overline{\gamma})}. \quad (14)$$

To characterize the average number of retransmissions, we will subsequently distinguish three wireless operating conditions, i.e.,

1) fast fading where the Nakagami-m channel varies from symbol to symbol (ergodic over packet);
2) block fading where the channel remains constant over a packet but changes from packet to packet (ergodic over retransmission window); and
3) static fading where the channel remains constant over time but varies in space (nonergodic).

For all three channel conditions, we assume that a static shadowing process is observed, i.e., shadowing remains constant over time but varies in space (nonergodic). Ergodicity implies that averages can be invoked, whereas nonergodic conditions

require outages to be invoked since the averages simply have no meaning [35].

Fast Fading and Shadowing: In the first case, we observe that the BEPs are obtained from (9). We first deal with block coding, where we insert (9) into (10), the thus resulting expression into (11), and the finally resulting expression into (14). Unfortunately, this leads to a fairly intricate expression which does not lend itself to closed-form analysis. We thus invoke two further approximations, where the first one,

$$ {}_2F_1\left(m, \frac{1}{2}; m+1; \frac{m}{m+\beta\overline{\gamma}}\right) \approx 1, \tag{15}$$

is due to the fact that the hypergeometric function converges to unity for large $\overline{\gamma}$; and the second one,

$$ \mathrm{WEP}_{\mathrm{block}}(\overline{\gamma}) \approx c \cdot \mathrm{BEP}^{t+1}, \tag{16}$$

with $c = 1/((t+1)B(t+1, J-t))$ and $B(x,y)$ being the Beta function, is mainly due to the fact that the binomial sum in (10) can be expressed in closed form by a hypergeometric function, to which we apply the Laplace approximation and neglect again the terms which converge towards unity. The average number of transmissions under fast Nakagami-m fading conditions with block channel coder can thus be expressed as

$$ \overline{N}_{\mathrm{tx}}(\overline{\gamma}) \approx \left(1 - c \cdot \left(\alpha\left(\frac{m}{m+\beta\overline{\gamma}}\right)^m\right)^{t+1}\right)^{-N/k}. \tag{17}$$

The characterization of shadowing requires the concept of outage to be applied to the average number of retransmissions. Notably, we define the average transmission outage (ATO) as the probability that the average number of transmissions $\overline{N}_{\mathrm{tx}}$ exceeds a given threshold $\overline{N}^*_{\mathrm{tx}}$, i.e.,

$$ \mathrm{ATO} = \mathrm{Prob}(\overline{N}_{\mathrm{tx}} \geq \overline{N}^*_{\mathrm{tx}}). \tag{18}$$

As per our system assumptions, the the average number of transmissions is a nonincreasing function in $\overline{\gamma}$, hence (18) can be shown to be equivalent to

$$ \mathrm{ATO}(\mu_{\mathrm{dB}}, \sigma_{\mathrm{dB}}) = \int_0^{\overline{\gamma}^*} p_s(\xi|\mu_{\mathrm{dB}}, \sigma_{\mathrm{dB}}) d\xi, \tag{19}$$

where $\overline{\gamma}^* = f(\overline{N}^*_{\mathrm{tx}})$ is the required SNR to reach the target average number of transmissions $\overline{N}^*_{\mathrm{tx}}$. Assuming the lognormal shadowing distribution of (6), it can be calculated in closed form as

$$ \mathrm{ATO}(\mu_{\mathrm{dB}}, \sigma_{\mathrm{dB}}) = Q\left(\frac{\mu_{\mathrm{dB}} - 10\log_{10}\overline{\gamma}^*}{\sigma_{\mathrm{dB}}}\right), \tag{20}$$

where $Q(x)$ is the Gaussian Q-Function and, following from (17),

$$ \overline{\gamma}^* \approx \frac{m}{\beta}\left[\left(\frac{1-(\overline{N}^*_{\mathrm{tx}})^{-\frac{k}{N}}}{c \cdot \alpha^{t+1}}\right)^{-\frac{1}{m(t+1)}} - 1\right]. \tag{21}$$

The behavior of the outage probability ATO of the average number of transmissions $\overline{N}_{\mathrm{tx}}$ is exemplified in Fig. 5 assuming QPSK modulation, a Nakagami fading channel with $m = 2$,

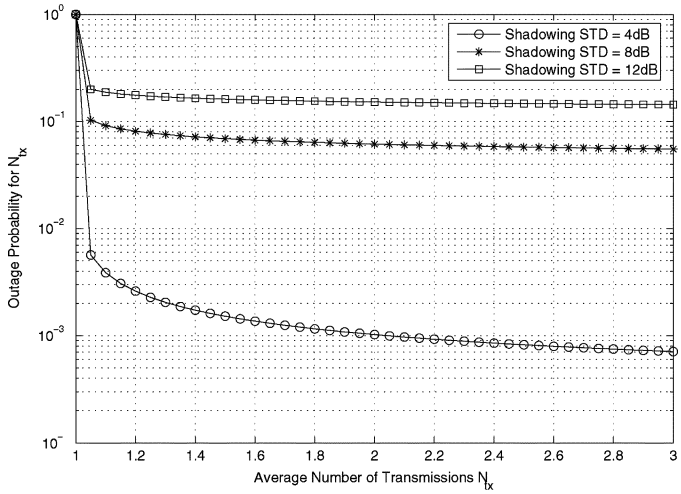


Fig. 5. Outage probability of the average number of transmissions parameterized on various shadowing channels; furthermore $\mu_{\mathrm{dB}} = 20$, $t = 3$, $k = 12$, $J = 23$, $N = 8 \cdot 127$, $m = 2$, and QPSK modulation.

various realizations of the shadowing channel $\sigma_{\mathrm{dB}} = \{4, 8, 12\}$ dB, a received SNR which yields $\mu_{\mathrm{dB}} = 20$ dB, a Golay block code with $t = 3$, $k = 12$, $J = 23$, and a packet length of $N = 8 \cdot 127$ bits. For instance, for a weak shadowing of $\sigma_{\mathrm{dB}} = 4$ dB, an average of 2 transmissions is required to guarantee .1% outage and thus 99.9% reliability of the entire smart grid region. We also observe that shadowing has a profound impact in that a stronger shadowing does not allow one to meet an outage requirement of .1%. The impact of channel coder, choice of modulation, packet length, fading strength, etc., is highly nonlinear but not depicted further here.

The above expressions allow an M2M service provider to estimate the coverage area. Notably, given a shadowing standard deviation σ_{dB} for the considered environment, a given required outage level ATO^* and the tolerated average number of transmissions $\overline{N}^*_{\mathrm{tx}}$, one can obtain the needed μ_{dB} as

$$ \mu_{\mathrm{dB}} = \sqrt{2}\sigma_{\mathrm{dB}}\mathrm{erf}^{-1}(1 - \mathrm{ATO}^*) + 10\log_{10}\overline{\gamma}^*, \tag{22}$$

where $\mathrm{erf}^{-1}(x)$ is given in (23) on the next page [36]. From above μ_{dB}, one can obtain the average communication distance with a given transmission power, receiver noise power density and communication bandwidth. Similarly, if the required distance is given, one can estimate $\overline{N}^*_{\mathrm{tx}}$ which impacts, e.g., reservation protocols. See (23) at the bottom of the next page.

As for the use of convolutional channel coder, one can follow a similar procedure as above to derive the average number of transmissions under fast Nakagami-m fading conditions, i.e.,

$$ \overline{N}_{\mathrm{tx}}(\overline{\gamma}) \approx \frac{1}{1 - N\frac{a_{d_{\min}}}{2T}\left(\frac{d_{\min}}{\frac{d_{\min}}{2}}\right)\alpha^{d_{\min}/2} \cdot \left(\frac{m}{m+\beta\overline{\gamma}}\right)^{md_{\min}/2}}, \tag{24}$$

and its ATO threshold value as

$$ \overline{\gamma}^* \approx \frac{m}{\beta}\left[\left(\frac{2T(1-1/\overline{N}_{\mathrm{tx}})}{a_{d_{\min}}\left(\frac{d_{\min}}{\frac{d_{\min}}{2}}\right)\alpha^{d_{\min}/2}}\right)^{-2/(md_{\min})}\right], \tag{25}$$

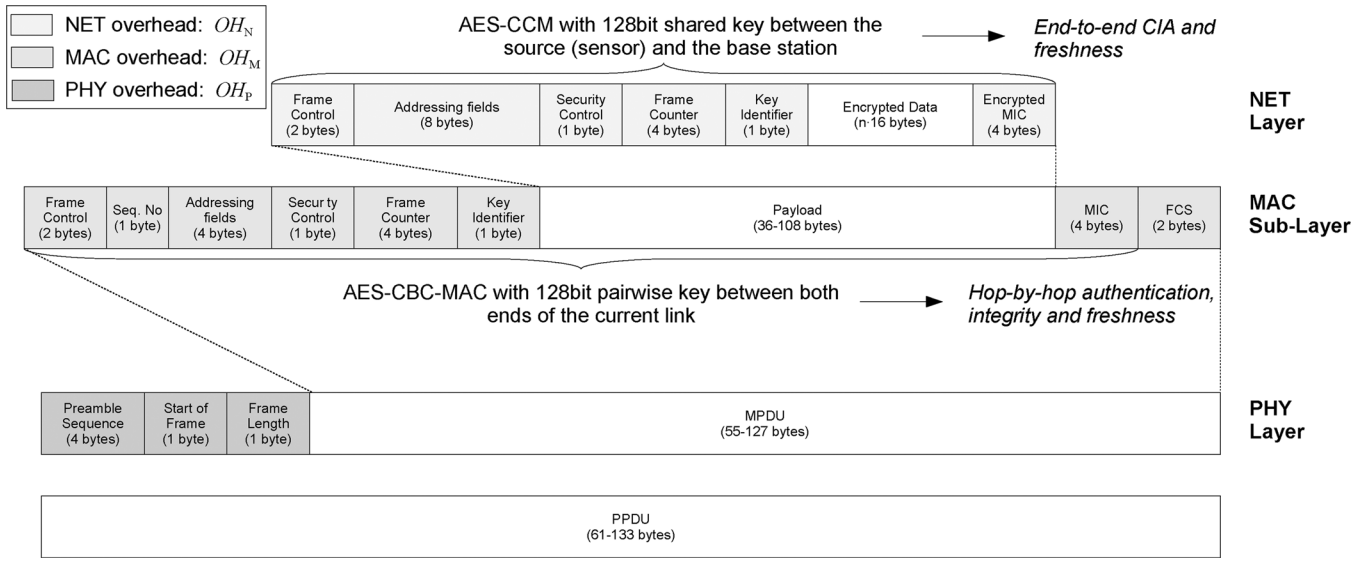


Fig. 6. The proposed aggregation packet format.

from which the spatial outage and related quantities can be calculated using (20).

Block Fading and Shadowing: In the second case, we observe that the BEPs are obtained from (8). We first deal with block coding, where we now insert (8) into (16), integrate over the fading distribution, the thus resulting expression into (11), and the finally resulting expression into (14). Thereupon, the invert the expression w.r.t. $\overline{\gamma}$ to be able to obtain the ATO under shadowing conditions. Following the same procedure as above, the average number of transmissions under block Nakagami-m fading conditions with block channel coder can be derived as

$$\overline{N}_{\rm tx}(\overline{\gamma}) \approx \left[1 - A \cdot \frac{\Gamma\left(m - \frac{t+1}{2}\right)}{\overline{\gamma}^m \left(\frac{t+1}{2} b + \frac{m}{\overline{\gamma}}\right)^{m-(t+1)/2}}\right]^{-1}, \tag{26}$$

where $A = c \cdot d \cdot N \cdot a^{t+1}/(2\pi b)^{(t+1)/2}/k$ and $d = m^m/\Gamma(m)$, and its ATO threshold value as

$$\overline{\gamma}^* \approx \sqrt[m]{\frac{A \cdot \Gamma\left(m - \frac{t+1}{2}\right)}{\left(1 - \overline{N}_{\rm tx}^{-1}\right)\left(\frac{t+1}{2} b\right)^{m-(t+1)/2}}}, \tag{27}$$

from which the spatial outage can be calculated using (20). Similarly, the average number of transmissions under block Nakagami-m fading conditions with convolutional channel coder can be derived as

$$\overline{N}_{\rm tx}(\overline{\gamma}) \approx \left[1 - B \cdot \frac{\Gamma\left(m - \frac{d_{\min}}{4}\right)}{\overline{\gamma}^m \left(\frac{d_{\min}}{4} b + \frac{m}{\overline{\gamma}}\right)^{m-d_{\min}/4}}\right]^{-1}, \tag{28}$$

where $B = a \cdot d \cdot N \cdot (1)/(2T) a_{d_{\min}} \binom{d_{\min}}{(d_{\min})/(2)} / (2\pi b)^{d_{\min}/4}$, and its ATO threshold value as

$$\overline{\gamma}^* \approx \sqrt{[m]} \frac{B \cdot \Gamma\left(m - \frac{d_{\min}}{4}\right)}{\left(1 - \overline{N}_{\rm tx}^{-1}\right)\left(\frac{d_{\min}}{4} b\right)^{m-d_{\min}/4}}, \tag{29}$$

from which the spatial outage can be calculated using (20).

Static Fading and Shadowing: Finally, in the third case, we observe that the BEPs are obtained from (8). We first deal with block coding, where we insert (8) again into (16), the thus resulting expression into (11), and the finally resulting expression into (14). Thereupon, the invert the expression w.r.t. $\overline{\gamma}$ to be able to obtain the ATO under shadowing conditions. Following the same procedure as above, the average number of transmissions for a given joint Nakagami-m and shadowing realization with block channel coder can be derived as

$$\overline{N}_{\rm tx}(\gamma) \approx [1 - c \cdot Q(\sqrt{b\gamma})]^{-N/k} \tag{30}$$

$$\operatorname{erf}^{-1}(x) \approx \frac{x}{|x|} \sqrt{\sqrt{\left(\frac{2}{\pi a} + \frac{\ln(1-x^2)}{2}\right)^2 - \frac{\ln(1-x^2)}{a}} - \left(\frac{2}{\pi a} + \frac{\ln(1-x^2)}{2}\right)}$$
$$a = \frac{8(\pi - 3)}{3\pi(4 - \pi)} \approx 0.140012. \tag{23}$$

and its ATO threshold value as

$$\gamma^* \approx \frac{2}{b}\left(\mathrm{erf}^{-1}\left[1-\sqrt{[t+1]}\frac{1-\overline{N}_{\mathrm{tx}}^{-k/N}}{c\cdot(a/2)^{t+1}}\right]\right)^2. \quad (31)$$

The spatial outage *cannot* be calculated using (20) since the joint fading and shadowing process is not Gaussian anymore. To obtain the outage on the average number of transmissions, we utilize the derivation of the cumulative distribution function (CDF) of the joint process [37], i.e.,

$$\mathrm{ATO}(\mu_{\mathrm{dB}},\sigma_{\mathrm{dB}}) = D\sum_{i=1}^{M}\frac{a_i}{b_i^m}\gamma(m,b_i\gamma^*), \quad (32)$$

where $\gamma(x,y)$ is the lower incomplete Gamma function, $D = 1/2\sqrt{\pi}\sum_{i=1}^{M} w_i$, $a_i = 2m^m w_i e^{-m(\sqrt{2}\sigma_{\mathrm{dB}}t_i+\mu_{\mathrm{dB}})}/\sqrt{\pi}\Gamma(m)$, $b_i = me^{-(\sqrt{2}\sigma_{\mathrm{dB}}t_i+\mu_{\mathrm{dB}})}$, and t_i and w_i are abscissas and weight factors of the Gaussian-Hermite integration which are available for different M values in ([38], Table (25.10)).

The average number of transmissions and its ATO threshold value for a fixed joint fading and shadowing realization with convolutional channel coder can be derived following exactly the same procedure above and thus omitted here.

D. NTW Layer

The role of the NTW layer is to chose the best route for a packet to reach its destination. Different routing protocols have been put forward to date, which are generally classified into proactive and reactive routing protocols. The former establishes an optimum routing path between any source and its sink(s), independent whether a packet needs to be sent; the latter only does so when a packet is to be sent. Proactive routing protocols are very energy consuming since routes need to be updated continuously, at the advantage of always having an up-to-date route. Reactive routing protocols may chose a suboptimal path or take a while to establish a good path, at the advantage of being significantly more energy efficient. Due to the stringent energy constraints of embedded M2M systems, the latter is typically the choice of design.

To this end, the IETF ROLL group has designed a routing protocol for precisely this type of networks where nodes have limited resources and operate over lossy channels. The protocol design can be found under [39] and the quantification of its benefits under [40]. The core of the protocol is the metric deciding on the choice of the actual route w.r.t. all possible routes available. Due to the distributed nature of the embedded system without central control, this decision is done locally where a transmitter chooses its target receiver (from all possible receivers) as the one which possesses minimum rank and costs least to communicate to. The latter, i.e., the transmission cost, is referred to as **ETX** and reflects the energy cost to transmit a packet over a given link. This energy cost is directly proportional to the average number of transmissions $\overline{N}_{\mathrm{tx}}$ which has previously been derived. The former, i.e., the rank, is essentially the aggregated number of transmissions between the given node and the sink, and thus reflects the "distance" of the node to the sink including the channel conditions and choice of technology on the way.

Therefore, without going into the details of the actual protocol design, the best route from all available routes is the one which exhibits the minimum aggregated number of transmissions. The protocol of IETF ROLL is designed such that said path is found iteratively by updating the rank (through the **ETX**s) at specific times, stipulated by the trickle timer. We will subsequently assume that such path is established.

IV. Protocol Analysis and Optimization

In the following we present a thorough evaluation of our introduced protocol suite. The aim is to show its goodness in terms of energy consumption apart from its previously stated security characteristics. To be more realistic, we have applied it to IEEE 802.15.4, which is the most extended wireless communications technology for remote metering to-date. It is understood, however, that the analysis is equally applicable to emerging IEEE 802.15.4g as well as a large set of proprietary networks. Regarding the secure aggregation protocol, we thus first describe the actual frame structure in more details, after which we quantify the performance and energy benefits of the aggregated solution assuming a lossless channel first and extending it then to lossy channels. Regarding the authentication preamble, we present the energy savings in lossless channel, underlining in which cases it is really useful. Finally, the total energy savings for the involved nodes is quantified.

A. Frame Structure

We define subsequently a complete frame structure that allows both hop-by-hop and end-to-end security based on the IEEE 802.15.4 frame format [41]. Since the PHY layer security approach does not impact the secure aggregation process, it is handled separately thereafter.

At the PHY layer, we have assumed that we are operating, for the sake of simplicity, at the 868–868.6 MHz or 902–928 MHz frequency bands with binary phase-shift keying modulation. These options lead to a PHY preamble of 4 bytes and a start of frame delimiter (SFD) of 1 byte [41]. Then, the standard PHY header is applied (1 byte more). Consequently, and assuming BPSK, the resulting frame structure in bytes is shown in Fig. 6.

At MAC layer, we use short addressing (2 bytes per address) since we can assume that a given node will not have more than 2^{16} one-hop neighbors. Further, we apply the standard IEEE 802.15.4 security headers in order to generate a MIC with Advanced Encryption Standard (AES) in Cipher Block Chaining Message Authentication Code (CBC-MAC) mode with a 128 bit pairwise key between both ends of the current link. Since the MIC is applied to the MAC header as well as the MAC payload, it guarantees: 1) *authentication*, since the receiving node can certify the transmitting node MAC address; 2) *integrity*, since the link layer frame contents cannot be modified without being detected (with a high probability); and 3) *freshness*, since the receiving node can verify sequence number and frame counter fields in order to discard old or replayed packets.

Above MAC layer, that we will call for simplicity NET layer, we have assumed standard addressing (4 bytes per address) thus supporting standard network protocols such as the Internet Protocol (IP). Moreover, we define the use of AES in Counter

TABLE IV
COST OF TRANSMISSION AND RECEPTION

Fields	Value
Effective data rate (ϱ)	12.4kbps
Energy to transmit (ϵ_{tx})	59.2uJ/byte
Energy to receive (ϵ_{rx})	28.6uJ/byte
ATmega 128L active mode	13.8mW
ATmega 128L power down mode	0.0075mW
ATmega 128L MIPS/Watt	289 MIPS/W
$\mathcal{C}_A^K$ in ATmega 128L	K * 0.07 uJ

TABLE V
COST OF SECURITY OPERATIONS

Algorithm	Value
AES-128 Enc Φ_{enc}	1.62uJ/byte
AES-128 Dec Φ_{dec}	2.49uJ/byte
SHA-1 η	5.9uJ/byte

with CBC-MAC (CCM) mode with 128 bit shared key between the source (meter) and the gateway for end-to-end security. AES-CCM provides: 1) *confidentiality*, since the metered data is encrypted; 2) *integrity*, since the entire NET packet can be verified with the provided MIC; *authentication*, since it allows to verify the original source of data; and *freshness* since a frame counter or timestamp is also provided at this level. Because of the use of AES-CCM, the payload length is a multiple of the key length, i.e., 16 bytes; therefore, padding is applied whenever necessary.

B. Energy Cost

In order to conduct a realistic analysis, we use the Berkeley/Crossbow motes platform on the Mica2dots [42] which is a popular platform for WSN research. The major energy consumers on these sensor devices are the Atmel ATmega128L 8-bit microcontroller and the Chipcon CC1000 low-power wireless transceiver. The Atmega128L runs at a clock frequency of 4 MHz.

Our analysis is based on [42], which has approximated the energy consumption for individual cryptographic algorithms and other activities such as data transmission by measuring the current drawn from the power supply. A more accurate approach using an oscilloscope and a sense resistor, conducted from the same authors, showed the error to be less than 5%. Table IV presents the characteristic data for the Mica2dot platform. It is interesting to note that the power required to transmit 1 bit is equivalent to roughly 2090 clock cycles of execution on the microcontroller alone.

The cost of receiving one byte (28.6 μJ) is roughly half of that required to transmit a byte (59.2 μJ). During transmission and reception, the microcontroller is powered by the wireless transceiver. We used different packet sizes, but for example a packet of 61 bytes costs $61{*}28.6\,\mu\text{J} = 1.7446$ mJ to receive and $61 * 59.2\ \mu\text{J} = 3.6112$ mJ to transmit. In addition, we chose to focus on AES with 128-bit keys for data encryption/decryption [42] and SHA-1 for hashing; see Table V.

We thus observe that transmission and reception energy costs are within the same order of magnitude. Furthermore, the energy consumption of security operations is by an order of magnitude lower than the communication costs. We will therefore subsequently neglect the security energy cost and assume that transmission and reception cost the same amount of energy. The spent energy is thus directly proportional to the number of bits sent, which will be our metric of choice when quantifying gains.

C. Per-Aggregator Byte Savings Over Lossless Channels

As depicted in Fig. 6, the minimum payload at MAC layer is 36 bytes and the maximum is 108 bytes. That is to say, a maximum of 3 packets can be aggregated at MAC layer into one packet ($3 \cdot 36$ bytes $= 108$ bytes).

We next assume a varying number of meters N attached to a given aggregator and two possible lengths of collected data, 16 and 32 bytes (multiples of 128 bits as previously stated). As a result, since the total overhead (see Fig. 6) is $\text{OH}_N + \text{OH}_M + \text{OH}_P = 20 + 19 + 6 = 45$ bytes, the size of the PHY packets generated by the meters P_m is either 61 or 77 bytes. Considering that the aggregator concatenates network packets and that the maximum PHY packet size is P_a, then the maximum number of aggregated packets at the output frame is $A = \lceil (P_a - \text{OH}_P - \text{OH}_M)/(P_m - \text{OH}_P - \text{OH}_N) \rceil$ and the total amount of packets at the aggregator output is $O = \lceil N/A \rceil$.

From the above reasoning, assuming an error-free lossless channel, the total amount of bytes at the output of the aggregator with and without aggregation as well as the Δ in bytes are respectively obtained as per the below expressions.

$$B_{\text{agg}} = N \cdot (P_m - \text{OH}_P - \text{OH}_M) + O \cdot (\text{OH}_P + \text{OH}_M)$$
$$B_{\overline{\text{agg}}} = N \cdot P_m$$
$$\Delta = B_{\overline{\text{agg}}} - B_{\text{agg}} = (N - O) \cdot (\text{OH}_P + \text{OH}_M).$$

Fig. 7 presents the percentage of saving $(\Delta)/(B_{\overline{\text{agg}}}) \cdot 100\%$ in bytes transmitted at the aggregator node when using lossless aggregation on a perfect and lossless communication channel. Fig. 7 clearly shows how the aggregation efficiency grows when the length of the collected data decreases. Since typically collected data in smart grid metering applications are just a few bits long, we can save up to a 27% of the bits transmitted at the output of the aggregator, a gain which is further pronounced if multiple hops are present. This gain in overhead translates directly in energy gains since the energy needed to accomplish proposed security is by orders of magnitude lower than the communication energy (Tables IV and V).

D. Performance Optimization Over Lossy Channel

We now utilize the analytical body derived in Section III and apply it to the performance analysis and optimization of the secure aggregation protocol. We will subsequently only consider the case of fast fading with shadowing and block channel coder; the analysis and insights for the other cases are very similar and thus omitted here. With the mathematical body and set of protocols at hand, various issues pertaining to energy efficiency can be looked at. We will subsequently concentrate on two issues, notably the optimal hop-per-hop packet length and the best end-to-end aggregation strategy.

As for the optimal hop-per-hop packet length, we observe that having longer packets allows us to send more data at the caveat that packets are more likely corrupted due to noise, fading, and shadowing. There is hence a clear trade-off in terms of energy efficiency, which is defined as the number of useful data bits

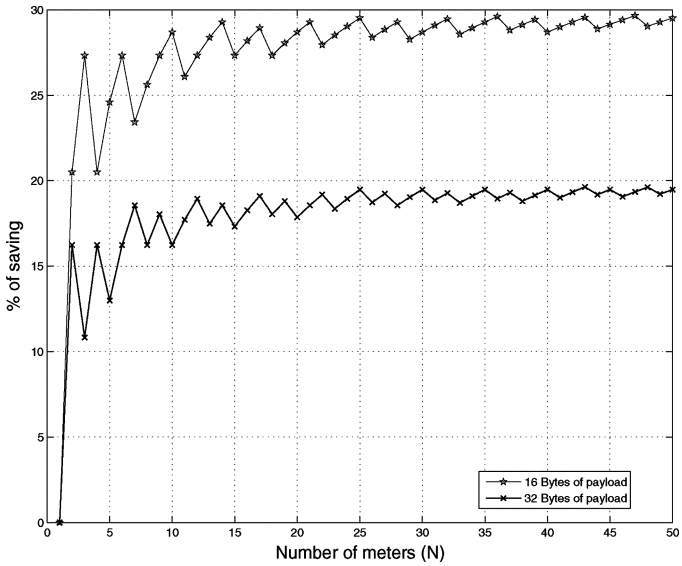


Fig. 7. Percentage of transmitted bytes and thus energy saved when using lossless aggregation.

N sent over the average energy spent in sending this amount of data, i.e.,

$$\eta = \frac{\epsilon' N}{\epsilon'(N+\mathrm{OH})\overline{N}_{\mathrm{tx}}(N+\mathrm{OH})}, \tag{33}$$

where $\epsilon' = \epsilon/8$ is the energy spent per bit and OH is the overhead discussed before. Using (17) and differentiating w.r.t. the packet length N, we obtain the optimal packet length which allows us to send a given amount of information with least energy

$$N_{\mathrm{opt}} = -\frac{\mathrm{OH}}{2} + \sqrt{\left(\frac{\mathrm{OH}}{2}\right)^2 - \frac{\mathrm{OH}}{\ln F}}, \tag{34}$$

where $F = \sqrt[k]{1 - c \cdot (\alpha((m)/(m+\beta\overline{\gamma}))^m)^{t+1}}$. Since in embedded systems the channel quality $\overline{\gamma}$ can typically be known at the transmitter, each transmitting node could modulate its packet length to improve energy efficiency. If each node along the routing path performs this operation, energy expenditure will be minimal. For instance, assuming a shadowing of $\sigma_{\mathrm{dB}} = 4$ dB, a dynamic packet length yields about 15% energy gains over a static packet length of 127 bytes.

The motivation for designing optimal end-to-end aggregation strategies is to find the aggregation threshold beyond which an aggregated packet requires more energy to deliver the information than the separate nonaggregated packets. It is thus a more holistic approach w.r.t. above per-hop strategy and also avoids bottlenecks which may arise with above strategy if one particular link is very poor. To conduct the analysis, we assume a multihop network of H hops where the first hop is formed by K nodes communicating with one parent node, which in turn communicates with its parent nodes, etc., until the gateway is reached after H. To not unnecessarily cluttering the analysis, we assume here a fixed packet length N. The energy difference between the aggregated and nonaggregated cases appear after the aggregation node; we will thus not consider the energy spent in the first hop. In the nonaggregated case, the energy spent to

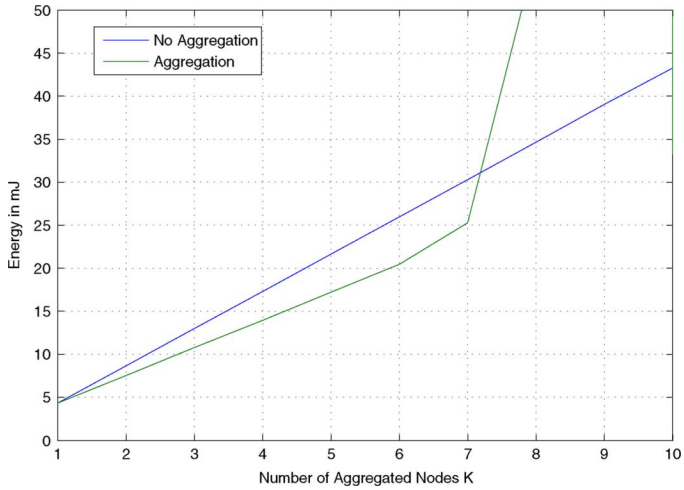


Fig. 8. Energy of aggregated versus nonaggregated scheme over a 5-hop network and prior discussed operating conditions.

sent the K packets of length N with overhead OH from the first parent node to the sink is

$$\begin{aligned} E_{\mathrm{agg}} &= \epsilon' \sum_{j=2}^{H} K \cdot (\mathrm{OH}+N) \cdot \overline{N}_{\mathrm{tx}}(\mathrm{OH}+N) \\ &= \epsilon' \sum_{j=2}^{H} K \cdot (\mathrm{OH}+N) \cdot G(\overline{\gamma}_j)^{\mathrm{OH}+N}, \end{aligned} \tag{35}$$

where $G(\overline{\gamma}_j) = (1 - c \cdot (\alpha((m)/(m+\beta\overline{\gamma}_j))^m)^{t+1})^{-1/k}$. In the aggregated case, the energy can be calculated as

$$E_{\mathrm{agg}} = \epsilon' \sum_{j=2}^{H} (\mathrm{OH} + K \cdot N) \cdot G(\overline{\gamma}_j)^{\mathrm{OH}+K \cdot N}. \tag{36}$$

The aggregation threshold occurs when aggregating data from K_{th} nodes into a single packet becomes energy inefficient, i.e., $E_{\mathrm{agg}} \leq E_{\not{\mathrm{agg}}}$, simply because the resulting packet is too long and thus requires too many retransmissions. To obtain the aggregation threshold K_{th} requires above highly nonlinear equations to be equated and solved w.r.t. K, requiring numerical tools. However, assuming that $K_{\mathrm{th}} \cdot N$ is sufficiently large which allows us to invoke some limiting properties of generalized means with exponent $N_{\mathrm{th}} \cdot K$, yields an approximate closed-form solution as

$$K_{\mathrm{th}} \approx \frac{\log \sum_{j=2}^{H} (1 + \mathrm{OH}/N) \cdot G(\overline{\gamma}_j)^{\mathrm{OH}+N} - \log(H-1)}{N \cdot \log \max_j \{G(\overline{\gamma}_j)\}}. \tag{37}$$

Various performance dependencies can be deduced from above analysis, where, e.g., Fig. 8 illustrates the energy gains of the aggregated solution until the breakpoint beyond which aggregation is detrimental.

Above analysis hence facilitated the understanding, quantification, and optimization of secure aggregation protocols.

E. Performance Evaluation of Physical Authentication

In this section, we quantify memory storage and energy saving when using physical layer authentication. The target is

to show under which conditions savings make up for the added cost.

The cost of physical authentication in terms of memory storage are mainly related to the number of potential emitters N in the vicinity and the authentication preamble W as well as the necessary keying material (all the pairwise keys). As a result the memory costs $\mathcal{M}$ can be expressed through l, the length of the pairwise keys. As an example, for a common smart grid scenario with five neighbors, an authentication preamble of 32 bits, pairwise keys of 128 bits, and a window preamble of 10 precomputed preambles, the necessary storage costs are just $5 \cdot (128 + 10 \cdot 32) = 280$ bytes.

$$\mathcal{M} = N \cdot (l + W \cdot A). \tag{38}$$

However, in the second part of this section, we define the energy savings adopting the notation in Table I and under the following assumptions:

- The victim is part of a low rate network and sends one packet every fixed period, $\delta = 1$.
- Every node within the victim vicinity has the same packet rate.
- The attacker has no knowledge of the keying material but tries to inject valid packets. Thus, she randomly chooses a different authentication preamble for every fake packet generated.

Using physical authentication, a receiver can realize that a given packet is nonintended to itself while receiving the authentication preamble thus saving itself to receive the rest of the packet. But, on the contrary, it has an added cost for both the transmitter and the receiver: the former will have to compute the authentication preamble and send it in a larger frame; and the latter will have to receive also such authentication preamble and check it against the K precomputed ones before discarding it.

The added cost because of the use of physical authentication relies on the transmission and the reception of the authentication preamble bits A, and, in the case of the emitter, to create the authentication preamble of the packet and, in the case of the receiver, to precompute another authentication preamble for the same source in order to keep K preambles for that source in memory. Thus, the added cost $\mathcal{E}$ per legitimate packet with physical authentication can be expressed as in (39).

$$\mathcal{E} = \mathcal{T}_A + \mathcal{R}_A + 2 \cdot \mathcal{A} + \mathcal{C}_A^K. \tag{39}$$

The savings in energy due to the use of physical authentication in a given link for a given nonintended nonmalicious packet are as in (40).

$$\mathscr{S}_{\text{valid}} = \mathcal{R}_L - \mathcal{R}_{P+A} - \mathcal{C}_A^K. \tag{40}$$

However, if the packet comes from an attacker, there is a probability that the fake authentication preamble matches one of the precomputed ones, thus having the receiver receive the whole packet (including the authentication preamble) before it can be discarded at higher layers. Therefore, the savings in energy $\mathscr{S}$ due to the use of physical authentication in a given link for a fake packet are as in (41) with p_K as in (2) being the probability of finding a collision (in the security sense) with one of the K precomputed authentication preambles.

$$\mathscr{S}_{\text{fake}} = (1 - p_K)\left(\mathcal{R}_L - \mathcal{R}_{P+A} - \mathcal{C}_A^K\right) + p_K\left(-\mathcal{R}_A - \mathcal{C}_A^K\right). \tag{41}$$

Assuming that every node in a vicinity sends one packet per period with a relative rate of fake packets per period ρ, and that every destination is not equally probable, we can evaluate the savings per period at a given link as in (42) with $N_{\text{tx}}(m, \gamma)$ the average number of transmissions per packet of length m and SNR γ derived as in (21), and $p_{r,t}$ the probability of the receiver t receives a nonintended nonmalicious packet sent from the transmitter mote t.

$$\mathscr{T} = \rho \cdot \mathscr{S}_{\text{fake}} + \left(\sum_{r=1}^{N} p_{r,t} \cdot \mathscr{N} \cdot \mathscr{S}_{\text{valid}} - \mathcal{E} \cdot \delta\right) \cdot \frac{N_{\text{tx}}(L, \gamma)}{N_{\text{tx}}(L + A, \gamma).} \tag{42}$$

Alternatively, assuming that every destination is equally probable, (42) can be defined as

$$\mathscr{T} = \rho \cdot \mathscr{S}_{\text{fake}} + \left(\mathscr{N} \cdot \mathscr{S}_{\text{valid}} - \mathcal{E} \cdot \delta\right) \cdot \frac{N_{\text{tx}}(L, \gamma)}{N_{\text{tx}}(L + A, \gamma)}. \tag{43}$$

The above (43) takes into account the intended malicious packets that are threats jeopardizing device and/or link availability $(\rho \cdot \mathscr{S}_{fake})$ and the nonintended nonmalicious packets, typically originating from transmitting nodes in the one-hop neighborhood of the receiving node $(N \cdot \mathscr{S}_{\text{valid}})$. In addition, it shows that the proposed solution is not only robust against attacks but also minimizes overhearing (the process of a node listening to its neighbors just to figure out that the packet received was for somebody else).

Table VII reflects the impact of the energy savings, expressed by (43), when different exhaustion attacks and nonintended nonmalicious packets are received, with and without the proposed authentication preamble. Here, for typical smart grid scenario, we fixed the number of neighbors to $N = 5$, the number of legitime packet received in Δt to $\delta = 1$, the length of the Physical Authentication preamble to $A = 32$ bits and the length of the received packets. Regarding the packet size, we chose 101 bytes ($L + A = 97 + 4$ bytes), because it is the aggregation result of two typical packets of 61 bytes, as presented in Table VI, aggregated with our proposed Lossless Data Aggregation protocol. The contribution of this table is two-fold: first, it permits to identify that, in order to respect the threshold presented in Section II.C, the probability of collision is very low also for the maximum value of K, so the preamble window length (W) does not influence the energy savings in Δt; and, second, it permits to quantify the energy savings in typical situations for low rate low power networks.

The table row entries are as follows: when only a legitime message is received from the receiver mote (rows 1 and 2), when the receiver node tries to receive nonintended messages sent from the one-hop neighborhood (rows 3 and 4), when only an exhaustion threat is launched against the receiver (rows 5

TABLE VI
COMPARISON OF BYTES TRANSMITTED BY THE AGGREGATOR NODE WITH AND WITHOUT AGGREGATION

N	collected data (bytes)	P_m (bytes)	$bytes_{na}$	$bytes_a$	Δ (bytes)	Δ (%)
2	16	61	122	97 ($O=1$)	25	20.49%
3	16	61	183	133 ($O=1$)	50	27.32%
19	16	61	1159	859 ($O=7$)	300	25.88%
31	16	61	1891	1391 ($O=11$)	500	26.44%
53	16	61	3233	2358 ($O=18$)	875	27.06%
97	16	61	5917	4353 ($O=33$)	1564	26.43%
2	32	77	154	129 ($O=1$)	25	16.23%
3	32	77	231	206 ($O=2$)	25	10.82%
19	32	77	1463	1238 ($O=10$)	225	15.37%
31	32	77	2387	2012 ($O=16$)	375	15.71%
53	32	77	4081	3431 ($O=27$)	650	15.92%
97	32	77	7469	6269 ($O=49$)	1200	16.06%

TABLE VII
COMPARISON OF ENERGY SAVINGS BY THE RECEIVED MOTE WITH AND WITHOUT PHYSICAL AUTHENTICATION MECHANISM

$N*W=K$	$\mathcal{N}$	ρ	$L+A$ (Bytes)	ΔE (uJ)	ΔE (%)
5*5 = 25	0	0	97 + 4 = 101	-363	-13.1%
5*100 = 500	0	0	97 + 4 = 101	-363	-13-1%
5*5 = 25	5	0	97 + 4 = 101	12364	445.7%
5*100 = 500	5	0	97 + 4 = 101	12364	445.7%
5*5 = 25	0	1000	97 + 4 = 101	2545000	91739.5%
5*100 = 500	0	1000	97 + 4 = 101	2545000	91739.5%
5*5 = 25	5	1000	97 + 4 = 101	2557800	92198.2%
5*100 = 500	5	1000	97 + 4 = 101	2557800	92198.2%

and 6) and finally when nonintended nonmalicious and malicious packets are received from the receiver mote (rows 8 and 9). Since it is very unlikely that a valid node does not try to receive a nonintended nonmalicious packet and since the real savings for the whole network grows linearly with the number of motes considered and with the number of nonintended nonmalicious and malicious packets received, this justify even more the use of our PHY layer authentication preamble. The only case when the proposed method is not recommended is when none of the nonintended messages is received; this situation however is very improbable.

As per Table VII, the probability of a successful attack due to a collision of an invalid authentication preamble with a valid one, does not have a great impact onto energy savings. Furthermore, assuming links with acceptable SNR level (typically larger than 5 dB [22]) having approximately the same PER for packets of length $L+4$ bytes as for packets of length L, the savings per packet is given in (44), where we underline that it manly depends on the number of nonintended packets $(\rho+\mathcal{N})$ received in Δt without distinction between nonmalicious and malicious packets.

$$\mathcal{T} = (\rho+\mathcal{N})\mathcal{S}_{valid} - (\mathcal{E}\cdot\delta). \tag{44}$$

Figs. 9 and 10 show the energy savings every Δt defined in (44), where the nonintended packets, the sum between nonintended nonmalicious, $\mathcal{N}$, and malicious packets, ρ, is variable. For completeness, in this case, we take into account received packets 133 Bytes long (considering also the authentication preamble mechanism, $L+A=129+4=133$ Bytes). This packet size, as presented in Table VI, is the aggregation result of two typical packets of 77 Bytes, and aggregated with our Lossless Data Aggregation protocol. As expected, these figures show that the energy savings increases linearly with the number of nonintended

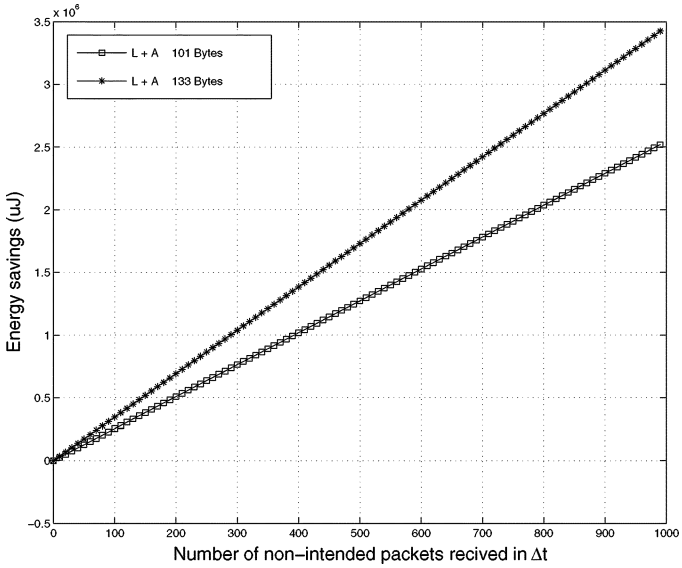


Fig. 9. Energy savings when a variable number of nonintended messages are received from the receiver.

malicious and nonmalicious messages and the proposed mechanism is not recommended when no one of them is received in Δt. In this case, the extra cost of the proposed method is presented in (39).

We conclude affirming that, when our motes receive nonintended nonmalicious packets or when they are under attack, the proposed mechanism yields energy savings up to $10^5\%$ and its efficiency does not depend on the length of the received packet but mainly on the number of nonintended messages received. As shown in Fig. 10, even if only one nonintended packet is identified in (Δt), our method permits great improvements in terms of energy savings.

F. Lossless Data Aggregation With Physical Authentication

We finalize the analysis by jointly considering data aggregation and the PHY layer security mechanisms, albeit over a lossless channel so as not to clutter analysis. The derived energy savings are relative to the case where a node receives a message which is the result of two aggregated packets. That is, the nodes in the presence of the aggregation protocol receive a legitime aggregated packet $(\delta=1)$ every Δt. Instead, for network without aggregation, the number of packets received in Δt are two $(\delta=2)$. This is to ensure that we compare networks that carry the same amount of information in the time period.

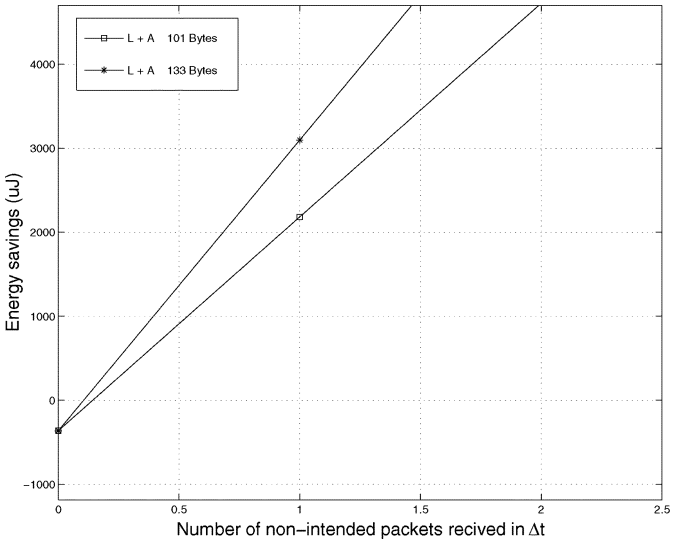


Fig. 10. Energy savings when a variable number of nonintended messages are received from the receiver node. In this case, we want to show that the cost of the proposed physical authentication mechanism is the same as to receive about 0.15 nonintended messages every Δt or 1 nonintended message every $7\,\Delta t$.

TABLE VIII
COMPARISON OF ENERGY SAVINGS FOR NETWORKS WITH AND WITHOUT THE SECURE AGGREGATION PROTOCOL AND THE AUTHENTICATION PREAMBLE MECHANISM

$\mathcal{N}+\rho$	$P\_wo-ag\&A(Bytes)$	$P\_w-ag\&A(Bytes)$	$\Delta E(\%)$
0	61 * 2 = 122	101	6.8%
2	61 * 2 = 122	101	22806%
4	61 * 2 = 122	101	45606%
0	77 * 2 = 154	133	5.3%
2	77 *2 = 154	133	29205%
4	77 *2 = 154	133	58405%

Table VIII presents the energy savings comparing both approaches with and without proposed methods of aggregation, minimizing energy due to less overhead, and PHY layer security, minimizing energy due to less overhearing and protection against exhaustion attacks. This way, even if the aggregation protocol increases the packet length of the messages exchanged in the network, the authentication preamble permits securing the node's limited resources. These results are very encouraging and will be facilitated in the forming smart metering standard by the Wavenis Open Standards Alliance [7].

V. POSITIONING WITH RESPECT TO STATE-OF-THE-ART

This section positions our proposed security suite, which includes PHY, hop-per-hop, and end-to-end security as well as lossless data aggregation, w.r.t. state of the art contributions. We first position data aggregation, and thereafter the proposed PHY layer authentication approach.

A. Positioning of Secure Data Aggregation

In many M2M applications, the data collected by meters are aggregated by some intermediate nodes with the objective of increasing the network lifetime by reducing unnecessary resource consumption. Aggregation is mainly performed in two ways: lossy and lossless aggregation. We will thus first give an overview of a few canonical approaches and then offer a more detailed security taxonomy to position our proposed protocol.

In the former [43], [44], the aggregation nodes combine input data and output less data but with some statistical similarities, e.g., just sending the average of input data from several meters. The latter [45] is referred to concatenating individual data items into larger packets, thus amortizing per-packet protocol overhead. This type of scheme is needed when security policies require to unequivocally identifying the source of sensed data. Obviously, this approach becomes more effective when data packets from meters are much shorter than the optimal packet length thus leaving much room for concatenation.

With the use of aggregation, new security challenges appear, especially those related to nodes exhausting the network or alter data of aggregated packets. Several proposals have tackled these risks [45]; however, to the best of our knowledge, they are all related to lossy aggregation. This section attempts to compare our secure aggregation scheme with other existing ones. Since our protocol is lossless instead lossy, an analysis of cost would be unfair: lossy ones focus on reducing transmitted bytes while lossless aim to provide a high level of security but leaving measured data unaltered. Before starting the comparative analysis, we would like to underline that our lossless data aggregation protocol is the only protocol that not only challenges network exhaustion but also node exhaustion. In the next section, we will show the difference between those threats.

SDA [43] appears in 2003 as the first secure data aggregation solution. It mainly focuses on solving the problem of data aggregation when a node is compromised. Nevertheless, this solution does not provide confidentiality, and therefore it is sensitive to eavesdropping attacks.

ESA [46] adds confidentiality to SDA by using one-hop pair-wise keys (to encrypt data between a node and its parent) and two-hop pair-wise keys (to encrypt data between a node and its grandparent).

SecureDAV [47] adopts the SDA and ESA bases but propose an alternative way to ensure integrity. Here the average data aggregated value is sent to all members of a cluster and each node compares it with the own sensed value. If the difference is less than a certain threshold, then the node signs the aggregated data. One drawback of this protocol is the lack of data freshness service.

Comparing our protocol with the three latter schemes, apart of being lossless, has the advantage of being robust against stealthy attacks (the attacker without revealing its presence injects fake traffic into the network) and exhaustion attacks (sending of useless messages to consume the meters' resources). In fact our proposal provides integrity and authentication mechanisms in every hop (hop-by-hop) for alleviating the impact of a network exhaustion attack.

Another lossy secure aggregation protocol is SIA [48] that focuses on mitigating stealthy attacks. This scheme also guarantees data integrity, authentication, data freshness, and confidentiality; however, it is vulnerable to network exhaustion attacks (the packets validity is checked only at the final gateway so every node involved in relaying wastes energy by sending invalid packets).

New ideas are presented from SDAP [49]: "divide-and-conquer" and "commit-and-attest." These principles are introduced to reduce the damage when an aggregator is attacked and also to help the base station to identify if the aggregated data are correct. Nevertheless, this protocol is too costly in terms of energy consumption and it is also vulnerable to stealthy and exhaustion attacks.

Ozdemir in [44] and in [50] proposed an alternative solution based on the use of a web of trust. This proposal allows increasing the reliability of their data aggregation protocol, providing a solution against network exhaustion. However, this solution does not provide confidentiality, and therefore it is sensitive to eavesdropping attack.

Castelluccia in 2009 [8] proposed a new homomorphic encryption scheme that allows intermediate sensors to aggregate encrypted data of their children without decryption. The goal of this protocol is to ensure that an external attacker, that does not know the group key, cannot tamper with any aggregate without being detected. It offers efficient and provably secure techniques for end-to-end privacy and authenticity, with reasonably good security assurances. However, this solution lacks data freshness mechanisms and it is vulnerable to exhaustion attacks since only the base station controls the integrity of every data aggregated.

In conclusion, our scheme is more robust than the previous ones in terms of security services and defense provided against classical attacks in M2M networks. Moreover, as far as we know, we can affirm that our proposed solution is the first lossless aggregation scheme that permits energy savings, based on an intelligent concatenation mechanism depending on various wireless communication factors, with a high level of security (hop-by-hop authentication, end-to-end encryption) and in addition with the addition of physical layer authentication. It is thus the first data aggregation scheme that provides defense against virtually all kinds of exhaustion attacks.

B. Positioning of Physical Layer Authentication

Packets being received can either be intended or not intended for the specific receiver. The nonintended packets can be of nonmalicious but as well as of malicious nature. Nonintended packets are typically received fully, just to be rejected at higher layers due to nonmatching MAC address, IP address, or security primitives.

The energy spent on these to-be-rejected packets is not negligible. Nonintended nonmalicious packets arrive at a fairly regular frequency which depends on the neighborhood cardinality and the neighboring nodes' transmission rates. Nonintended malicious packets arrive rarely but consistently in the case of a denial of service (DoS) attack.

Nonintended nonmalicious packets typically originate from transmitting nodes in the one-hop neighborhood of the receiving node. These can be data packets as well as control packets. Typically, energy is spent in receiving the entire packet, performing the security checks on the entire packet, checking on intended destination; only then the packet is discarded. No specific security solutions are known to provide energy savings against these packets.

Nonintended malicious packets yield DoS attacks with the aim to jeopardize device and/or link availability. Typical attacks in low-power embedded networks are exhaustion attacks with the aim to drain a device's battery. To counter this, access security mechanisms are typically deployed. Energy is thus spent in receiving the entire packet and performing the security checks on the entire packet; only then the packet is discarded.

A specific example of node exhaustion exploits the two-way request-to-send/clear-to-send (RTS/CTS) handshake that many MAC protocols use to mitigate the hidden-node problem. An attacker can exhaust a node's resources by repeatedly sending RTS messages to elicit CTS responses from a targeted neighbor node; strong link-layer authentication can mitigate these attacks however a targeted node receiving the bogus RTS messages still consumes energy and network bandwidth.

Commercial and industrial standards [51] for embedded networks, such as Zigbee, WirelessHART, and ISA 100.11a, are based on the PHY and MAC layers of the IEEE 802.15.4 standard, and they provide a simple solution against exhaustion attacks: authentication/integrity mechanism at link-layer. This mechanism permits to identify an invalid message only after the reception of the whole packet by verifying the Message Authentication Code presented in the last bytes of the packet. With these authentication mechanisms at MAC layer, the intention of such attacks is not solved because the exhaustion of the victim's limited energy resources is still possible due to the high reception costs.

In [52], an alternative technique is presented, which is based on defining specific network topology-based patterns to model normal network traffic flow, and to facilitate differentiation between legitimate traffic packets and anomalous attack traffic packets. In this paper, the performance of the proposed attack detection scheme is evaluated in terms of the size of the sensor resource set required for participating in the detection process for achieving a desired level of attack detection accuracy. The results signify the need for distributed pattern recognition for detecting distributed node exhaustion attacks in a timely and accurate manner. This solution seems to be interesting but numerous drawbacks are identifying comparing it with our physical authentication: our solution does not depend on patterns or in detecting the attack by a huge participation of all the nodes and also it is simple and very fast just because it should not receive the whole packet.

In [53], a possible solution to exhaustion is to apply rate limits to the MAC admission control such that the network ignores excessive requests, thus preventing the energy drain caused by repeated transmissions [54]. A second technique presented in the same paper consists of using time-division multiplexing where each node is allotted a time slot in which it can transmit [54]. This eliminates the need of arbitration for each frame and can solve the indefinite postponement problem in a back-off algorithm. All these solutions do not decrease the reception costs; in others words, they mitigate the problem but do not solve it integrally.

In conclusion, we propose a new and innovative mechanism to protect networks and the nodes that compose them, from node and network exhaustion threats, which does not involve a large additional cost in terms of energy. The goal of our solution is to

ensure that the energy necessary to provide the defense against exhaustion attacks is very low compared with the solutions discussed above, with energy savings quantified in Section IV.

VI. Characteristics of the Security Suite

In this section we characterize our complete security suite by means of a taxonomy useful for industrial use [7], and position it with the most prominent state-of-the-art protocols of Section V.

A. Attacks Against Data Aggregation Schemes

Embedded systems are particularly susceptible to different kind of attacks. A protocol that performs data aggregation can be very useful to save energy but at the same time could create possible weaknesses in the network. Because of its nature and its characteristics, designing a network to be totally secure is very difficult and every particular threat requires attention in the protocol and system design depends on a suitable threat and risk analysis. The latter will be different for each application under consideration. We now briefly summarize the malicious attacks and which scheme is design to protect the network to them:

- **Network Exhaustion Attacks (NeExh):** The attacker can fake a message asking the sensors nodes to continuously retransmit messages to exhaust its energy (DoS attack).
- **Node Exhaustion Attacks (NoExh):** Every fake message recited from a valid node involves an energy consumption, thus an attacker can exhaust the reciter energy by only sending invalid messages (DoS attack).
- **Node Compromise (Comp):** Nodes are vulnerable to physical access, such as tampering, which allows the attacker to gain access to the node and to the data information stored on it.
- **Sybil (Syb):** A Sybil attack is defined as a "malicious device illegitimately taking on multiple identities."
- **Selective Forwarding (SForw):** In a selective forwarding attack, malicious nodes behave like a black hole and may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further.
- **Replay (Rep):** As the medium is wireless, the attacker can intercept the message flows easily and replays those to start a new session.
- **Stealthy (Ste):** In this attack the content of a relayed packet is changed such that it is not or little correlated to its original content. The attacker, without revealing its presence, injects fake traffic into the network.

Below Table IX summarizes the various protocols and how they fit into above taxonomy. It also positions our proposed protocol. For each data aggregation examined, we make a cross in those attacks that are potential threats for the protocol in question.

TABLE IX
Attacks Against Data Aggregation Schemes

SCHEME	NeExh	NoExh	Comp	Syb	SForw	Rep	Ste
SDA	X	X	X		X		X
ESA	X	X	X		X		X
SIA	X	X	X		X		
SDAP	X	X	X		X		X
SecureDAV		X	X		X	X	X
SELDA		X	X			X	X
RDAT		X	X				X
AIDA	X	X	X	X	X	X	X
Castelluccia	X	X	X		X	X	
Agg protocol + Auth_pre			X		X		

TABLE X
Security Services Provided

SCHEME	Conf	Int	Fres	Auth	Avail	Lossy Scheme	Lossless Scheme
SDA	X	X		X		X	
ESA	X	X	X	X		X	
SIA	X	X	X	X		X	
SDAP	X	X	X	X		X	
SecureDAV		X		X		X	
SELDA	X	X		X	X	X	
RDAT		X		X	X	X	
AIDA							X
Castelluccia	X	X		X		X	
Agg protocol + Auth_pre	X	X	X	X	X		X

B. Security Services Provided

Each network, to be able to combat typical attacks described above, should be designed considering different security requirements. A network can be considered safe, even for opponents with a strong potential to attack, when all or the majority of the following security services are provided:

- **Confidentiality (Conf):** It essentially means keeping information secret from unauthorized parties.
- **Integrity (Int):** It means that the data produced and consumed by the sensor network must not be maliciously altered.
- **Freshness (Fres):** It prevents the adversaries from confusing the network by replaying the captured messages exchanged between sensor nodes.
- **Authentication (Auth):** An adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision has to be originating from the correct source.
- **Availability (Avail):** Users of a sensor network must be capable of accessing its service when they need them. This security service is important when there is a compromised node, in order to ensure the normal function of the network, isolating this bad node.

Below Table X summarizes known protocols and how they fit into above taxonomy. It also positions our proposed protocol, showing that it meets all essential security requirements. For each data aggregation examined, we make a cross in those security service offered from the protocol in question.

C. Cryptographic Primitives for Aggregation Schemes

Security services are fundamental requirements against dangerous threats but in order to have a fair analysis we have to study also the cryptographic primitives on which they are based. In embedded systems, there are protocols which are based on algorithms that use symmetric keys to ensure confidentiality of data while others use public keys. The cryptography primitives analyzed are:

TABLE XI
CRYPTOGRAPHY PRIMITIVES TO SECURE DATA AGGREGATION SCHEMES

SCHEME	MAC	DgSn	SK	PK	ReCom	PrHom	BrAuth
SDA	X		X				X
ESA	X		X				
SIA	X		X		X		X
SDAP	X		X		X		X
SecureDAV		X		X	X		
SELDA	X		X				
RDAT	X		X				
AIDA							
Castelluccia	X		X		X	X	
Agg protocol + Auth_pre	X		X		X		

- **Message Authentication Code (MAC):** The MAC value protects both: a message's data integrity as well as its authenticity.
- **Digital Signature (DgSn):** It is a mathematical scheme for demonstrating the authenticity of a packet.
- **Symmetric Key (SK):** Cryptographic keys for both decryption and encryption.
- **Public Key (PK):** A secret private key and a published public key to authenticate a user and encrypt the data.
- **Reading Commitment (ReCom):** It is possible identify the source of the data sent to the base station.
- **Privacy Homomorphic (PrHom):** Homomorphic technique used to protect the privacy of the data.
- **Broadcast Authentication (BrAuth):** It enables the receivers to verify that the messages received from the claimed source were valid and were not modified en-route.

Below Table XI summarizes again the various protocols and how they fit into above taxonomy. It also positions our proposed protocol, showing that we have used standard primitives to facilitate secure data aggregation in the network. For each data aggregation examined, we make a cross in those cryptography primitives implemented in the protocol in question.

VII. CONCLUDING REMARKS

machine-to-machine (M2M) devices in smart grids aim to infer the meter information and deliver this information reliably and securely to the gateway, so that it can reach the utility companies. The inferred data however is often composed of a few bits which, if used in the context of standardized solutions with minimum and maximum packet lengths, yields high overheads and hence poor energy efficiency. Aggregation is hence a natural solution where, due to the need to identify each node and its associated inferred metering data, requires lossless aggregation mechanisms.

Aggregation, however, poses extra challenges on per-hop and end-to-end security since aggregating nodes essentially need to access the information content. Design issues are further complicated by the fact that the wireless medium is lossy in nature and thus reliability is potentially jeopardized where longer aggregated packets suffer from a disadvantage w.r.t. shorter nonaggregated packets. In addition, long nonintended nonmalicious or malicious packets can be received from a valid node causing exhaustion of the node's battery.

The aim of this paper was thus to propose a viable and readily deployable security and aggregation protocol suite which exhibits above features, as well as quantifying the performance gains assuming some realistic wireless channel and typically deployed hardware. Based on IEEE 802.15.4 standards settings, we have shown that the developed protocol is indeed secure providing per-hop authentication as well as end-to-end confidentiality and also, enriched with the authentication preamble, becomes really reliable and energy efficient. Notably, the developed protocol has been analyzed considering different wireless channel (fading and shadowing) conditions, PHY layer configurations (modulation, coding), MAC layer configurations (packet length, number of (re-)transmissions) and networking characteristics (multihop route from source towards gateway). We have quantified the energy gains of the proposed secure aggregation protocol with and without the physical authentication mechanism, notwithstanding the fact that security requires an extra overhead. This allows the utility company to correctly configure the M2M network so that coverage, security, and efficiency is guaranteed. The use of the proposed security suite is facilitated by the emerging low-power smart metering standard of the Wavenis Open Standards Alliance [7] and is expected to impact other emerging standards in smart metering.

REFERENCES

[1] National Broadband Plan 2009 [Online]. Available: www.broadband.gov/download-plan, [Online]. Available:

[2] L. Maleysson and C. Dugas, "Configuring and managing a large-scale monitoring network solving real world challenges for ultra low powered and long-range wireless mesh networks," in *Proc. 2005 Joint Conf. Smart Objects Ambient Intell. (sOc-EUSAI'05)*, New York, pp. 225–230.

[3] Machine to machine communications [Online]. Available: http://www.etsi.org/Website/Technologies/M2M.aspx Last accessed Oct. 2010

[4] 3GPP [Online]. Available: http://www.3gpp.org; MTC Last accessed Oct. 2010

[5] *Broadband Wireless Metropolitan Area Networks (MANs)* , IEEE 802.16 [Online]. Available: http://standards.ieee.org/getieee802/802.16.html, last accessed Oct. 2010

[6] K. Doppler, M. Rinne, and C. Wijting, "Device-to-device communication as an underlay to lte-advanced networks," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 42–49, 2009.

[7] Wavenis Open Standard Alliance [Online]. Available: http://www.wavenis-osa.org Last accessed Oct. 2010

[8] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 5, no. 3, pp. 1–36, 2009.

[9] S. Peter, K. Piotrowski, and P. Langendoerfer, "On concealed data aggregation for wireless sensor networks," 2005.

[10] E. Mykletun, J. Girao, and D. Westhoff, "Public key based cryptoschemes for data concealment in wireless sensor networks," in *Porc. IEEE Int. Conf. Commun. (ICC2006)*.

[11] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in *Proc. 13th ACM Conf. Comput. Commun. Security (CCS'06)*, New York, 2006, pp. 278–287.

[12] A. Mahimkar, "Securedav: A secure data aggregation and verification protocol for sensor networks," in *Proc. IEEE Global Telecommun. Conf.*, 2004, pp. 2175–2179.

[13] B. Przydatek, D. Song, and A. Perrig, "Sia: secure information aggregation in sensor networks," in *Proc. 1st Int. Conf. Embedded Netw. Sensor Syst. (SenSys'03)*, New York, pp. 255–265.

[14] Y. Yang, X. Wang, S. Zhu, and G. Cao, "Sdap: A secure hop-by-hop data aggregation protocol for sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 4, pp. 1–43, 2008.

[15] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," *Comput. Netw.* vol. 53, no. 12, pp. 2022–2037, 2009 [Online]. Available: http://www.sciencedirect.com/science/article/B6VRG-4VXB88W-1/2/19d5ff6af92871bd6aff85ac5de4ae8d

[16] E. Mlaih and S. A. Aly, "Secure hop-by-hop aggregation of end-to-end concealed data in wireless sensor networks," CoRR vol. abs/0803.3448, 2008.
[17] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," in *Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst. (SenSys'04)*, New York, pp. 162–175 [Online]. Available: http://dx.doi.org/10.1145/1031495.1031515
[18] "Recommendation for block cipher modes of operation: Galois/Counter mode (GCM) and GMAC," NIST Special Publ. 800-38D, Nov. 2007.
[19] B. Van Rompay, "Analysis and design of cryptographic hash functions, MAC algorithms and block ciphers," Ph.D. dissertation, Katholieke Universiteit Leuven, Leuven, Belgium, 2004.
[20] B. Preneel, "Analysis and design of cryptographic hash functions," Ph.D. Dissertation, Katholieke Universiteit Leuven, Leuven, Belgium, 1993.
[21] T. Grembowski, R. Lien, K. Gaj, N. Nguyen, P. Bellows, J. Flidr, T. Lehman, and B. Schott, "Comparative analysis of the hardware implementations of hash functions sha-1 and sha-512," in *Information Security*, ser. Lecture Notes in Computer Science, A. Chan and V. Gligor, Eds. Berlin/Heidelberg, Germany: Springer, 2002, vol. 2433, pp. 75–89 [Online]. Available: http://dx.doi.org/10.1007/3-540-45811-5-6
[22] 2008, "Minimum SNR values for signal coverage," [Online]. Available: http://www.wireless-nets.com/resources/tutorials/define-SNR-values.html
[23] Atmel128l Data Sheet 2011 [Online]. Available: http://www.atmel.com/dyn/resources/prod-documents/doc2467.pdf
[24] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks," *Wirel. Netw.*, vol. 8, no. 5, pp. 521–534, 2002.
[25] D. Wallner, E. Harder, and R. Agee, "Key management for multicast: Issues and architectures," RFC 2627, 1999.
[26] Harney and Harder, "Logical key hierarchy protocol (LKH)," Internet Draft 1999, harney-sparta-lkhp-sec-00.
[27] A. Sherman and D. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Trans. Softw. Eng.*, vol. 29, no. 5, pp. 444–458, May 2003.
[28] J. G. Proakis, *Digital Communications*, 3rd ed. New York: McGraw-Hill, 1995.
[29] H. Shin and J. H. Lee, "On the error probability of binary and Mary signals in Nakagami-m fading channels," *IEEE Trans. Commun.*, vol. 52, no. 4, pp. 536–539, Apr. 2004.
[30] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. San Diego, CA: Academic, 2000.
[31] P. Mary, "Performance of wireless systems over fading and shadowing channels," Ph.D. dissertation, INSA-Lyon, Lyon, France, 2008.
[32] S. Manji and N. B. Mandayam, "Block error probability using list Viterbi decoding with hard decisions," [Online]. Available: http://citeseer.ist.psu.edu/317496.html
[33] A. Bachir, M. Dohler, T. Watteyne, and K. Leung, "MAC essentials for wireless sensor networks," *IEEE Commun. Surveys Tutorials*, to be published.
[34] R. Zhang, "Analysis of energy-delay performance in multi-hop wireless sensor networks," Ph.D. dissertation, Centre Innovation en Telecommunications et Integration de Services (CITI), Lyon, France, 2009.
[35] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[36] "Error function," [Online]. Available: http://en.wikipedia.org/wiki/Error_function Last accessed Oct. 2010.
[37] S. Atapattu, C. Tellambura, and H. Jiang, "Representation of composite fading and shadowing distributions by using mixtures of gamma distributions," Apr. 2010, pp. 1–5.
[38] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*. New York: Dover, 1965.
[39] "Roll status pages," [Online]. Available: http://tools.ietf.org/wg/roll Last accessed Oct. 2010.
[40] T. Watteyne, D. Barthel, M. Dohler, and I. Auge-Blum, "Sense&sensitivity: A large-scale experimental study of reactive gradient routing," *Meas. Sci. Technol. (Special Issue on Wireless Sensor Networks—Designing for Real-World Deployment and Deployment Experiences)*, to be published.
[41] 2010, The IEEE 802.15.4 Standard Association Website [Online]. Available: http://web.archive.org/web/20080224051703/standards.ieee.org/getieee802/download/802.15.4-2006.pdf
[42] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proc. 3rd IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2005, pp. 324–328.
[43] J. Albath and S. Madria, "Secure hierarchical data aggregation in wireless sensor networks," in *Proc. IEEE Wirel. Commun. Netw. Conf. (WCNC)*, Apr. 2009, pp. 1–6.
[44] S. Ozdemir, "Secure and reliable data aggregation for wireless sensor networks," in *Proc. 4th Int. Conf. Ubiquitous Comput. Syst. (UCS'07)*, Berlin, Germany, 2007, pp. 102–109.
[45] T. He, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Aida: Adaptive application independent data aggregation in wireless sensor networks," *ACM Trans. Embedded Comput. Syst. (Special Issue on Dynamically Adaptable Embedded Systems)*, 2004.
[46] P. Jadia and A. Mathuria, "Efficient secure aggregation in sensor networks," in *High Performance Computing-HiPC 2004*, ser. Lecture Notes in Computer Science, L. Bougé and V. Prasanna, Eds. Berlin/Heidelberg, Germany: Springer, 2005, vol. 3296, pp. 111–119 [Online]. Available: http://dx.doi.org/10.1007/978-3-540-30474-6-10
[47] A. Mahimkar, "Securedav: A secure data aggregation and verification protocol for sensor networks," in *Proc. IEEE Global Telecommun. Conf.*, 2004, pp. 2175–2179.
[48] B. Przydatek, D. Song, and A. Perrig, *Sia: Secure Information Aggregation in Sensor Networks*. New York: ACM Press, 2003, pp. 255–265.
[49] Y. Yang, X. Wang, S. Zhu, and G. Cao, "Sdap: A secure hop-by-hop data aggregation protocol for sensor networks," in *Proc. ACM MOBIHOC'06*, 2006, pp. 356–367.
[50] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks," *Comput. Commun.*, vol. 31, no. 17, pp. 3941–3953, 2008.
[51] J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks," in *Foundations of Security Analysis and Design V*, ser. Lecture Notes in Computer Science, A. Aldini, G. Barthe, and R. Gorrieri, Eds. Berlin/Heidelberg, Germany: Springer, vol. 5705, pp. 289–338.
[52] Z. Baig, "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks," *Comput. Commun. (Special Issue on Information and Future Communication Security)* vol. 34, no. 3, pp. 468–484, 2011 [Online]. Available: http://www.sciencedirect.com/science/article/B6TYP- 4YV82N2-3/2/e8f1172fd6b4b962e1c04cd6069e3afe
[53] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Commun. Surveys Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.
[54] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

Andrea Bartoli received the Telecommunication Engineering degree from University Polytechnic of Milan, Italy, in 2009, with a graduation thesis concerning "A security system based on Open Source" made at Universitat Politecnica de Catalunya (UPC), Barcelona, Spain, (where he also made the Erasmus project in 2008), and the M.Sc. degree from UPC. He is working toward the Ph.D. degree in telecommunication engineering at Centre Technologic de Telecomunicacion de Catalunya (CTTC), Barcelona.

He is working on security in embedded networks for an industrial project called Machine-to-Machine & Embedded Systems Security Protocol Suite (MAESTRO) in association with ORANGE/France Telecom. He is also a member, since 2010, of a security group to implement a secure standard for green and low-power networks for commercial use; this standard is called Wavenis Open Standard Alliance (WOSA).

Juan Hernández-Serrano was born in Salamanca, Spain, in 1979. He received the M.S. degree in electrical engineering emphasis in telecommunication and the Ph.D. degree from the Technical University of Catalonia (UPC), Barcelona, Spain, in 2002 and 2008, respectively.

In 2002 he joined the Information Security Group (ISG) within the Telematics Services Research Group (SERTEL) at the Department of Telematics Engineering, UPC. He currently works as Assistant Professor at the Castelldefels School of Technology (EPSC), UPC. His research interests include security for large deployment of sensor networks and cognitive networks. In the last six years he has participated in six national and international R&D projects, both public (CICYT or European Commission) and private funded. He is coauthor of 1 book chapter, 5 ISI-JCR papers, and more than 20 conference papers related to network security.

Prof. Hernández-Serrano is on the program committee of several international conferences including the 12th International Conference on Information and Communications Security (ICICS'10), IFIP Networking 2011, and the 9th International Conference on Applied Cryptography and Network Security (ACNS'11).

Miguel Soriano received the M.S. degree in telecommunications engineering and the Ph.D. degree from the Polytechnic University of Catalonia (UPC), Barcelona, Spain, in 1992 and 1996, respectively.

In 1991, he joined the Cryptography and Network Security Group, in the Department of Applied Mathematics and Telematics. Currently, he is a Professor at the Telecommunications Engineering School of Barcelona (ETSETB), and leads the Information Security Group, both affiliated to the Department of Telematics Engineering of UPC. He is also an Associate Researcher at the Centre Technologic de Telecomunicacion de Catalunya (CTTC). His research interests encompass network security, electronic commerce, and information hiding for copyright protection.

Dr. Soriano has been a member of the program committee of many security conferences, and he is editor of the *International Journal of Information Security* (Springer-Verlag).

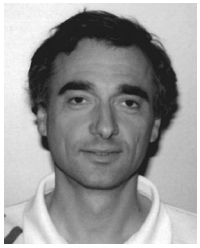
Mischa Dohler (SM'07) received the M.Sc. degree in telecommunications from King's College London, U.K., in 1999, the Diploma degree in electrical engineering from Dresden University of Technology, Germany, in 2000, and the Ph.D. degree in telecommunications from King's College London, U.K., in 2003.

From September 2003 to June 2005, he was a Lecturer at King's College London, U.K. At that time, he was also a London Technology Network Business Fellow receiving appropriate Anglo-Saxon business training, as well as Student Representative of the IEEE UKRI Section and member of the Student Activity Committee of IEEE Region 8 (Europe, Africa, Middle East, and Russia). From June 2005 to February 2008, he was Senior Research Expert in the R&D division of France Telecom, France. He is currently leading the Intelligent Energy (IQe) group at CTTC, Barcelona, Spain, with focus on smart grids and green radios. He has published 138 technical journal and conference papers at a citation h-index of 24 and citation g-index of 49, holds 13 patents, authored, coedited, and contributed to 19 books, has given 25 international short courses, and participated in standardization activities. He is working on wireless sensors, machine-to-machine, femto, cooperative, cognitive, and docitive networks.

Dr. Dohler has won various competitions in mathematics and physics, and participated in the third round of the International Physics Olympics for Germany. In the framework of the Mobile VCE, he has pioneered research on distributed cooperative space-time encoded communication systems, dating back to December 1999. He has been TPC member and cochair of various conferences, such as technical chair of IEEE PIMRC 2008 held in Cannes, France. He is EiC of ETT and is/has been holding various editorial positions for numerous IEEE and non-IEEE journals. He is fluent in six languages.

Apostolos Kountouris was born in 1969 in Patras, Greece. He received the Diploma degree in electrical engineering from the University of Patras in 1992, the M.Sc. degree in computer engineering from the University of Southern California (USC), Los Angeles, in 1994 and the Ph.D. degree in computer science from the INRIA institute, Rennes, France, in 1998.

From 1999 to 2004 he worked as a Research Engineer for Mitsubishi Electric R&D investigating software radio (SDR) architectures and reconfigurable radio design. Currently he is with France Telecom R&D, Grenoble, where, after having worked on software radio cognitive reconfiguration, he is currently investigating attack resilient wireless sensor network routing and associated MAC/PHY security issues.



Dominique Barthel graduated from Ecole Polytechnique and Ecole Supérieure de Electricité, France.

After a first career devoted to architecture and design of microprocessors, DSPs, media processors, and scientific computers, his interest evolved to networked smart devices and sensor networks, with an emphasis on low power architectures and implementations. He currently leads the France Telecom, Grenoble, research project on Technologies for mobile terminals and embedded devices. He holds six patents and is a devoted radio amateur.