Journal of
*Sensor and
Actuator Networks*

MDPI

Article

Group Authentication Scheme for Neighbourhood Area Networks (NANs) in Smart Grids

Bashar Alohali *, Kashif Kifayat, Qi Shi and William Hurst

School of Computing and Mathematical Sciences, Liverpool John Moores University, L3 5UA Liverpool, UK; K.Kifayat@ljmu.ac.uk (K.K.); Q.Shi@ljmu.ac.uk (Q.S.); W.Hurst@ljmu.ac.uk (W.H.)
* Correspondence: B.A.Alohali@2012.ljmu.ac.uk; Tel.: +44-15-1231-2777

Academic Editor: Jamil Y. Khan
Received: 1 January 2016; Accepted: 22 April 2016; Published: 4 May 2016

Abstract: A Neighbourhood Area Network is a functional component of the Smart Grid that interconnects the end user domain with the Energy Services Provider (ESP) domain. It forms the "edge" of the provider network, interconnecting homes instrumented with Smart Meters (SM) with the ESP. The SM is a dual interface, wireless communication device through which information is transacted across the user (a home) and ESP domains. The security risk to the ESP increases since the components within the home, interconnected to the ESP via the SM, are not managed by the ESP. Secure operation of the SM is a necessary requirement. The SM should be resilient to attacks, which might be targeted either directly or via the network in the home. This paper presents and discusses a security scheme for groups of SMs in a Neighbourhood Area Network that enable entire groups to authenticate themselves, rather than one at a time. The results show that a significant improvement in terms of resilience against node capture attacks, replay attacks, confidentiality, authentication for groups of SMs in a NAN that enable entire groups to authenticate themselves, rather than one at a time.

Keywords: Smart Grid; authentication; Smart Meters; key management

1. Introduction

The Smart Grid (SG) can be defined as an electric system that uses information, two-way, cyber-secure communication technologies, and computational intelligence in an integrated fashion [1]. The system is used across the SG functional units, such as electricity generation, transmission, substations, distribution, and consumption to achieve a system that is clean, safe, secure, reliable, resilient, efficient, and sustainable. This definition covers the energy system from the generation to the end points of consumption of the electricity. Security is a critical issue because millions of electronic devices are inter-connected via communication networks throughout critical power facilities, which has an immediate impact on reliability of such a widespread infrastructure [2]. The Electric Power Research Institute (EPRI) identifies cyber security as one of the greatest challenges facing smart grid deployment [3]. The security of the grid will strongly depend on authentication, authorization, and privacy technologies. Privacy technologies are well matured. Federal Information Processing Standard (FIPS) approved Advanced Encryption Standard (AES) [4] and Triple Data Encryption Standard (3DES) [5] implementations are readily available.

However, the available schemes and tools for a generic Internet infrastructure cannot be directly used on a SG infrastructure. Apart from the fact that the devices used in the various domains of the SG are very different in terms of function, capabilities as well as form factor, the security objectives of the SG are different from those of a generic Internet infrastructure [6–8]. The broad security objectives for the SG are mentioned as Availability, Integrity, and Confidentiality in the report of the Smart Grid Interoperability Panel (SGIP), National Institute of Standards & Technology (NIST), USA [7].

It mentions the need for additional security relating to cyberspace and the physical security of the devices. The scope of our discussion is limited to the former. In particular, our focus is on key management that enables the security schemes.

The SG is a heterogeneous network with multiple devices and technologies interconnecting them. As a data network, Figure 1 illustrates, it comprises three parts—the Home Area Networks (HANs), the Neighbourhood Area Networks (NAN), and the Wide Area Network [7]. The HAN and NAN are functional groups of the smart grid infrastructure that are interconnected in a functional hierarchy. The HAN performs the basic data collection, and interfaces with the smart grid via the smart meters. The SMs, in turn, interconnect and as part of the Advanced Metering Infrastructure (AMI), termed as the NAN, interface to a substation which houses the control gear for electricity supply. Several substations interconnect via a WAN to the core network at the provider's premises.

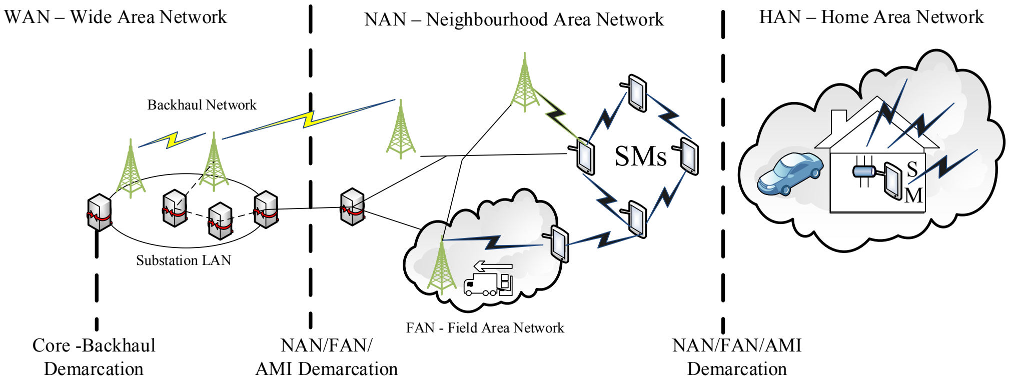


Figure 1. Various segments of the smart grid (HAN, NAN, WAN) and the interconnectivity between them.

The devices in the HANs and NANs communicate with the core in the backhaul, accessible via the WAN. Interconnected wireless sensors/sensor enabled appliances constitute the HAN. The WAN and the HAN are interconnected via the NAN. The interconnection of wireless SMs providing a path from the HAN to resources in the WAN constitutes the AMI. The NAN segment of the smart grid is our area of interest in this paper.

SMs require communicating with a data sink and a control centre for purposes of monitoring and management. The interconnectivity between the SMs includes an interface to the upstream network, typically another SM, playing the role of such an interface and termed as a gateway SM. The topology depends upon the wireless coverage, reachability, potential redundant paths, and similar design parameters. A single hop to the gateway SM from all devices in a locality is not practical and multiple hops to the gateway SM become necessary. It requires the intermediate nodes in the path to the gateway to forward data from the downstream nodes. Security mechanisms deployed must ensure that each node is authenticated centrally, as well as by the group. Each group member must be verifiably assured that the data they are forwarding is, indeed, from one of the members of the group that is currently active and transacting. The SMs in the group need to be updated about the group's membership status, and active nodes, periodically. The security information that is relayed to the members of the group must reach only the validated members of the group. This is the setting for the discussion and addresses how a secure scheme is provided for a group of SMs that have a multi-hop path within the group, to reach the gateway SM.

The rest of the paper is organized as follows. In Section 2 we present a literature review for key management and authentication solutions for NANs. Section 3 describes the network model for a smart grid and NAN. Section 4 proposes key management for NAN. Section 5 discusses the implementation and analyses the security features of the proposed scheme. Section 6 concludes the paper with a summary of results and future work.

2. Group Authentication

The significance of encryption of cryptography in smart grids remains a highly-discussed and debatable topic. There is a need for hiding information, which is present in the form of both data and messages, in order to improve the business productivity of smart grids. Researchers have used different techniques in order to secure data in the smart grids in order to maintain the confidentiality, integrity, and authenticity of data, which have been discussed in the subsequent sections. In this section, the existing group authentication schemes are examined to identify how they are applicable in the context of the SG NAN.

2.1. The Need for Group Authentication

In a large-scale environment, such as the smart grid, network scalability and availability are two crucial design parameters for a secure scheme. To manage a large scale NAN, organising the NAN into groups of SMs is necessary to

1. Localise the topology: the SMs are distributed geographically based on the location of the consumers. It is essential that these devices are within the radio range of each other to be able to communicate with each other. Therefore, it is necessary to form groups of SMs. Groups are typically formed with some nodes in each group having overlapping radio range with other group/s. Such overlap provides potential redundant paths, when necessary.
2. Balance workload of intermediate relay hosts: SMs communicate to an upstream data sink in the smart grid via an intermediate host, typically a SM performing the role of a group gateway. It is necessary to limit the processing and storage load on the intermediate host that does the forwarding of data to and from the SMs. Typically, the SMs are organised into groups and assigned gateways to communicate with.
3. Distribute the SMs into functional groups: from an electricity provider's perspective, it helps to organise different categories of users into different groups (domestic, commercial, industrial, essential service provider, *etc.*) for purposes of estimating demand, geographically, validating the usage, and controlling theft. Often, domestic and non-domestic users are located geographically close and the need for creating groups of SMs for operational semantics is necessary.

With the obvious need for grouping SMs in a smart grid, group management is a necessary function within the smart grid. Identification of a group member, and members' joining/leaving the group, are typical group management functions that require authentication. The authentication may be performed autonomously by the group head or by an upstream entity in the smart grid.

Often, it is not cost-effective to operate the SMs in a single-hop topology (to the upstream gateway) and, therefore, a multi-hop topology is necessary. The group members need to be validated as part of the group. Such validated members can communicate between themselves, primarily for purposes of forwarding data to/from the group head (providing multiple redundant paths to reach the group head). In the following section, we review literature relating to group authentication.

2.2. Related Work

Broustis *et al.*, term the first scenario as a reverse single sign-on and succinctly describe a framework for group authentication which is applicable for mobile telecom networks and extendible to the M2M context, which is relevant to our discussion [9]. They introduce a gateway entity to coordinate/represent the group and this entity performs the required upstream authentication. The group authentication is based on a group challenge sent by the gateway to all devices. The devices individually respond to the gateway with their credentials. In the absence of the gateway, the upstream authentication server does the authentication and the overall saving in communication overhead remains one-sided (from the authentication server to the device group) [9].

The proposal in [9] is similar to our proposal in terms of having a gateway as an intermediary. In the scenario we consider, each node in the network authenticates with a central entity, the network operations centre (NOC). This includes all intermediate nodes (group leaders) that provide a path to the end nodes to reach the NOC. Operationally, each group leader has no autonomy to authenticate a group member, but it has sufficient information to validate that a group member attempting to relay packets through it has indeed been authenticated, centrally. There are a hierarchy of groups where necessary, functionally to reach the NOC, resulting in a multi-hop path from the end device to the NOC. Broustis, *et al.* [9] does not discuss an authentication requirement with multi-hop paths.

Harn proposed a Group Authentication Scheme (GAS), where the role of a group manager is responsible for registering all members of the group and issuing a distinct token to each member [10]. Subsequently, the members of the group authenticate and interact with each other without the need for the group manager's involvement. They propose a non-interactive basic t-secure m-user n-group authentication scheme ((t; m; n) GAS), where t is the threshold of the proposed scheme; m is the number of users participating; and n is the total number of group members. This scheme, based on Shamir's secret-sharing [11], works for synchronous communications only. Therefore, they also propose an asynchronous (t; m; n) GAS, which can determine whether all users that participate in a group actually belong to that group [10]. The proposal in [10] is primarily for a many-to-many communication within a group (intra-group). It enables autonomous authentication within the group as well as detection of invalid members. The requirement for a SG scenario that we consider does not necessarily require a many-to-many characteristic. In addition, the limiting factor for the authentication scheme is the threshold t. There is no estimate of the scalability of t or the generic suitability of the scheme to resource-constrained devices. In the specific scenario we consider, the proposal in [10] is over-dimensioned.

Mahalle *et al.*, present a Group Authentication scheme for IoT based on Threshold Cryptography-based Group Authentication (TCGA) [12]. They extend [10] to use Pallier Threshold Cryptography [13], using its properties; namely, homomorphic addition, indistinguishability, and self-binding. Primarily, they address the problem of different groups (applications) requiring communicating with each other. The authentication scheme has a pre-authentication phase where a group head does the key distribution and followed by a group authentication phases where a secret session key is distributed. The group members rely on the group head to initiate all group communication. They demonstrate that their scheme performs better than [10]. However, the implementation is on WiFi-based laptops and reflects a scaled performance of their scheme on IoT platforms. Our scenario does not require communication within the group. Group members do not need to communicate between themselves. The authentication is done centrally and the intermediate nodes verify that a downstream node is already authenticated. We also intend to use only symmetric encryption on the sensor node to minimize any processing delays at the intermediate nodes.

Yang *et al.*, propose a generic framework for group authentication [14]. Their scenario considers password-based authentication in one go, for a user group. The focus is on reducing the time taken for authentication, like in [13], rather than authentication of a member, anonymously. The scheme is fairly close to our application scenario since the hierarchy of authentication (NOC—Gateway—Device) is quite similar (Server—group authenticator—end user). However, there is no evidence that it is applicable for low resource devices that we consider or the fact that the scheme will work (similar to the proposal in [9]) for multi-hop scenarios where an intermediate device needs to perform authenticated forwarding, as in our case.

Wang *et al.*, present a group authentication and a group key distribution scheme for *ad hoc* networks [15]. They argue that conventional group authentication protocols cannot serve the requirements of *ad hoc* networks since there is no designated group leader and the fact that the number of nodes in the network are not known in advance and can change dynamically. Therefore, schemes such as those in [10,13] cannot be deployed. The scheme proposed uses an identity-based bilinear pairing. There are five distinct phases, which include join and leave phases for the individual nodes. This is quite similar to the key management architecture schemes for SCADA networks discussed in [16]. Again, there is no specific mention of a multi-hop scenario requiring authenticated forwarding.

Multi-hop scenarios are necessary for functional grouping as well as to build the radio path up to the NOC. Unlike in the case of WLANs used in [12], the radio range and the transmit power of the sensor nodes that we consider, are limited.

Nicanfar *et al.*, address the authentication between a smart meter and the utility server termed as a Security Associate (SA). The SA is a dedicated server delegated to perform authentication by the central server at the NOC and is used for authentication by a group of SMs. They propose two separate schemes for authentication and key management, termed SGAS and SGKM, respectively. They propose a four-phase authentication approach, which has not been implemented and measured for performance [17]. They consider a mesh topology for SMs constituting the NAN, and use WiMax for interconnecting the smart meters. Their work is fairly close to the scenario we consider, from a topological perspective. Their functional requirement is similar to our requirement in that the authentication has to be done with a central entity. However, they delegate the central authentication autonomy to the SA. There are clear differences in the scenario we consider. Firstly, in our scenario such an intermediate node is merely a SM with the role of a gateway and with no autonomy. The risk of such delegation, we believe, is that the SA nodes are susceptible targets for attacks and can cause considerable impact in terms of the central server delegating the autonomy to a backup SA and the reachability of the SA from the end nodes. Secondly, they do not consider what we term as "authenticated forwarding". The traffic from the downstream nodes is not validated at the intermediate nodes. Thirdly, they use an asymmetric encryption method for privacy and a broadcast mechanism for key distribution. We believe, while key distribution via broadcast does reduce the communication overhead, multicast is a more secure option. Our scenario uses a single central entity for authentication and individually distributes the keys to each of the nodes.

Subir *et al.*, proposed an Extensible Authentication Protocols (EAP) based [18] unified key management mechanism (UKMF) that can generate ciphering keys for multiple protocols of multiple communication layers from a single peer entity authentication procedure [19]. The unified key management mechanism is suitable for smart grid use cases, especially for smart metering, where smart meters are assumed to be low-cost wireless devices for which repeated peer entity authentication attempts for each protocol can contribute to increased system overhead. The proposed mechanism is flexible in that peer entity authentication can be treated as either network access authentication or application-level authentication. However, the mechanism has established that information discovery for bootstrap application ciphering is an important and as yet missing piece to realize the unified key management framework vision. This part needs further analysis by researchers.

In summary, the key features that we intend to utilize for authentication and key management are a relatively simple authentication scheme for a group of devices, an activity monitor that characterizes the traffic from the devices, as well as a means of authenticated forwarding. In Section 2.2, we clarify what we mean by group authentication in our context and define each of the features we require for our scheme, compare the availability of these features with the schemes discussed so far, and establish the security requirements of our scheme. The requirements are drawn for the SG model detailed in Section 3. These requirements are in addition to the basic security requirements, namely, confidentiality, integrity, non-repudiation, and forward/backward secrecy.

2.3. Security Requirements

For a group of SMs to authenticate, there are two potential scenarios to consider

1. All the devices being able to authenticate in one go (single message) rather than one-to-one with the authentication server and each device with a unique verified identity, (Centralised Authentication) and
2. All devices being able to authenticate between themselves in the absence of an upstream authentication server (Distributed Autonomous Authentication)

The case we consider is in-between. Each node authenticates with the NOC, a central authority. There is no local autonomy to the group leader (or the gateway, as termed in this paper) to perform authentication, unless a group member has been previously authenticated by the NOC. Once a group member has been authenticated by a NOC, the group leader exercises control over the group. In the context of the SG, there is no apparent need to economise on communication overheads and the resulting delays, for two reasons. Firstly, smart meters have sustained power availability and rarely have to use an on-board power source, which is limited. Secondly, the performance requirements for the SM on the AMI are of the order of a few seconds and can, therefore, accommodate multiple message exchanges for authentication.

The topology determines three critical factors for any network—performance, availability, and cost—each one of them comprising several factors by themselves. In our context of threats and attacks, availability (redundancy, robustness, scalability) is critical. Performance, in terms of end-to-end delays (network latency, complexity of data routing, and processing) is sufficiently lenient. Costs are not considered as part of our discussion. The topology of the smart meter network can be different, including star, tree, mesh, or a cluster tree network. The topology formation depends upon the wireless range of the devices and, therefore, dependent on the location of the SMs. The most practical topology operationally feasible, we believe, is a partial mesh or a cluster tree topology. Therefore, the authentication scheme we propose should attempt to be topology-neutral and address a multi-hop scenario.

With a multi-hop scenario, it is essential to ensure that any data being forwarded indeed belongs to the group and no one else. This evolves the need for validated forwarding of packets, both upstream and downstream. Each packet of data received is checked for its integrity as well as source. Therefore, validated forwarding at intermediate nodes where every forwarder on the routing path should be able to verify the authenticity and integrity of the messages is a necessary feature in the authentication scheme.

The data from the end devices transits multiple nodes before reaching the central server. It could require multiple encryption/decryption tasks per packet at the intermediate nodes. This impacts the processing, memory requirement (packet length), and energy requirements per SM. Using symmetric cryptography contains these three factors when compared to asymmetric cryptography, for a given key length, in addition to a higher crypto-strength. The security scheme should use symmetric cryptography and provide a secure means for key management.

Time synchronization of all devices on the network is another feature that several security schemes deploy. Using a time stamp in all packet data provides a sufficient time tracking for data freshness validation. It requires the time stamps to be monitored continually. Given that the data flow is between the devices and the NOC, the NOC provides a centralized repository for tracking the time stamps. We avoid adding the communication overhead of time synchronization across the network to the routing overhead we may incur due to the choice of topology.

The features required by the security scheme for a scenario that we consider are indicated in the last column in Table 1. The scheme is expected to provide for an authentication mechanism for the nodes on the network with the primary goals of the authentication are to tag a node as part of the network and active, to distribute shared keys once the node's identity is established as valid, and to distribute a shared secret within the group that is used for validated forwarding in intermediate nodes.

By scalability, we mean the ability to add a large number of end devices and sufficient number of gateways for the number of groups formed. Scalability impacts performance (in terms of end-to-end delays), storage requirements (number of shared keys) on the intermediate devices including gateways, processing (delays due to forwarding traffic), and the delays in redistributing keys when a new node joins or an existing one leaves. Scalability is a desirable feature of the scheme.

In the next section, we discuss the smart grid network model and consider the requirements for its secure operation. We also highlight the potential security threats we consider as a case study for testing the proposed solution.

Table 1. A comparison of the availability of features in security schemes.

Features	**Security Schemes**						
	Broustis *et al.* [9]	**Harn [10]**	**Wang *et al.* [15]**	**Yang *et al.* [14]**	**Nicanfar *et al.* [17]**	**Subir *et al.* [19]**	**Our Goal**
Topology S/M/CT	M	N/A	N/A	S	M	N/A	S, M, CT
Multi-hop paths	Yes	Yes	Yes	No	Yes	N/A	Required
Validated Forwarding at intermediate nodes	Yes	Yes	Yes	No	Yes	No	Required
Symmetric Crypto	Yes	No	No	No	No	EAS	Required
Resilient to NC attack	No	No	No	Yes	No	Yes	Required
Resilient to replay attack	No	Yes	Yes	Yes	Yes	Yes	Required
Resilient to Sybil attack	Yes	Yes	Yes	Yes	Yes	Yes	Required
Centralized Authentication	No	No	No	No	Yes	Yes	Required
Specifically designed for NAN	No	No	No	No	Yes	Yes	Required
Nodes are not time synchronized	No	Yes	Yes	No	Yes	No	Required
Scalability	N/A	N/A	N/A	N/A	N/A	N/A	Required

3. The Smart Grid Network Model

In this section, we present the smart grid network model considered for the discussion and detail the requirements for its secure operation. We also explain the potential security threats we consider for a case study to test the proposed solution. The smart grid network model considered for our discussion, is shown in Figure 2.

It comprises of three network segments:

1. Home Area Network (HAN): one smart meter (SM) and N smart devices (SDs). This group of devices is interconnected in a star topology with a SM as the star point.
2. Neighbourhood Area Network (NAN): mesh network (not necessary full mesh) of M SMs. SMs are divided into G groups. Group g (g = 1,..., G) has Mg SMs. Hence the following equation is considered:

$$M = \sum_{g=1}^{G} Mg \tag{1}$$

One SM of each group is selected as Group Controller (GC). The GC is hereafter termed as the gateway node, GW.

3. Wide Area Network (WAN): Network (e.g., Internet) that connects GCs to the Network Operations Centre (NOC).

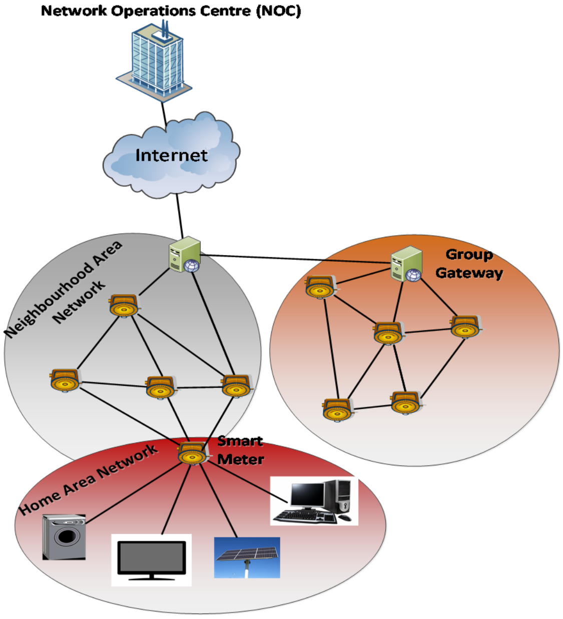


Figure 2. Smart Grid Network Model.

The data generating elements are part of the HAN. This data traverses the entire network to reach the NOC. The smart meters, which are a part of the NAN, generate data, as well as receive data from the NOC. Therefore, traffic to the NAN elements is two-way. Data may or may not be forwarded into the HAN by the smart meters, depending upon the deployment requirement.

3.1. Threat Model and Assumptions

There are two basic types of threats that need to be countered—attacks that originate due to malicious users eavesdropping to monitor the wireless communications between the nodes in the network, and attacks that originate due to the capture of a node, physically, or causing it to fail.

Eavesdropping: unauthorized users may try to eavesdrop on exchanged data and control messages within the HAN and NAN. The eavesdroppers can use the information exchanged and the exchange patterns to launch man-in-the-middle (MITM) attacks or replay attacks to impersonate a node. Therefore, all nodes should be authenticated and all messages should be encrypted. The keys used for privacy should not be easily guessable.

Node Capture: physical node captures or forced failure of nodes, such as in a DoS attacks, amount to a node capture attack. In such an event, if the keys on the node are captured, the attacker should not be able to gain access to the network. The solution should minimize the impact of such attack on the remaining nodes and ensure the rest of the network functions normally.

Authentication Scheme for NAN: in a Neighbourhood Area Network, authentication is required to secure routing in the network. Smart meters have to be registered with the group controller to obtain permission to communicate in the network. For our authentication process, we make the following assumptions:

1. Smart meters are grouped together based on a policy and are aware of the group members. The events and functionalities of the policy are not in the scope of this paper. This work does not address the policy on which smart meter groups are constituted.
2. Every smart meter in a group has a unique identity, which is a serial number and each group has a unique group identity, which are used in the authentication process. All network devices involved in the group authentication process know these details.
3. The link layer between the smart meters and gateway are protected at the link layer, which makes communication encrypted at the link layer.
4. Every smart meter in a group maintains a wireless connection with its gateway and the network topology between the home smart meter and the gateway node is a tree. The topology between the gateway and the utility could be a mesh. They form a cluster-tree topology between the SM and the gateway.
5. The smart meters have pre-distributed shared symmetric keys, which are used for initiating the authentication process and keys during authentication.
6. Symmetric cryptography yields a better cryptographic strength for a given key length compared to asymmetric cryptography. The resulting data length is close to the size of the input.
7. Smart meters cooperate with one another to forward packets on multi-hop paths to the NOC. A routing protocol to handle the mesh topology is active and provides the shortest route from a given end device to the GW, within the group.
8. GW nodes have sufficient power (more than the end devices) to be able to perform the forwarding from the group to the NOC and vice versa.
9. In the event of the failure of a gateway node, all nodes in the group will be unable to access the NOC, until the GW is reinstated/active. There is no fall-back node that will take on the role of a gateway. The failure rates of the GW are low.
10. The groups and the group gateways are pre-identified and formed. These formations are not *ad hoc* and, therefore, there is no need for a node to play the role of a gateway.
11. The nodes on the network are not time synchronized.
12. The value of the clock ticks of a node cannot be retrieved to set the same clock value on another node. Such an operation is possible only with a reset of the node, which essentially implies that the clock tick value is lost since the clock is reset. It can be argued that such is the exact function of a time protocol such as Network Time Protocol (NTP), but sufficient care is taken to ensure that this value is not accessed by any network function.
13. The NOC provides a central authentication service. It comprises a sufficiently large server with a fail-over configuration and able to maintain the state of all of the devices on the network. Given the nature of the service requirement of the smart meters in the smart grid,

all authentication attempts, except the one at start-up upon installation, must be approved before the NOC sends an authentication response to the node requesting authentication.

14. The NOC maintains a history of the metadata (originator-ID, timestamp, group-ID) over a sufficiently long period to derive statistics, such as message arrival epochs, message arrival times, inter-message times, message size, and activity profiles so that it knows when it can expect the next packet from a specific ID. Such a history is essential to detect malicious attack traffic since our scheme does not require the devices on the network to be time synchronized.

3.2. Notations

Having stated the assumptions made, we proceed with detailing the security scheme for the scenario in Figure 1. The following subsection begins with a listing of the notations (Table 2) used to detail the security scheme. This is followed by the details of the authentication process.

Table 2. Notations for the authentication scheme for the NAN.

Symbol	Description
G	Unique group number
$SM_{n,g}$	Smart meter ID
GW_g	A gateway for a group of smart meters to the NOC
MK_{NOC}	Master Key for NOC
MK_{GW}	Master key for the group Gateway
$K_{sm,noc}$	Symmetric key generated by $K_{sm,Noc}$ = F($MK_{NOC} \mid\mid SM_{ng}$), and shared with NOC, and SM_{ng}.
$K_{GW,SM}$	Symmetric key generated by GW_g, and shared with GW_g, and SM_{ng}.
$Proxy\ SM_{n,g}$	Existing smart meter for authenticating a new smart meter
$K_{SM,SM}$	Symmetric key shared between $Proxy\ SM_{ng}$, and SM_{ng}
K_{GW_g}	Symmetric key shared with NOC and GW
AV_i	Authentication value inside the group where $AV_i = F(R\|\|MK_{GW})$
R	Random number generated by GW_g to produce AV_i

The scheme addresses two cases—smart meters in multi-hop (mesh), and smart meters in star topology.

3.3. Authentication of Group Gateway GW

We now describe the method that is used by NOC to authenticate GW_g. Since not every GW has a direct link to NOC, some GW will be authenticated via other GW_g.

Figure 3 shows a NAN topology indicating the hierarchical authentication structure/path that is used for GW_g authentication. For completeness, in the figure we also show SMs. The authentication of SMs is discussed in later sections. The group controller of a group g is denoted by GW_g. The smart meter n of group g is denoted by SM_{ng}.

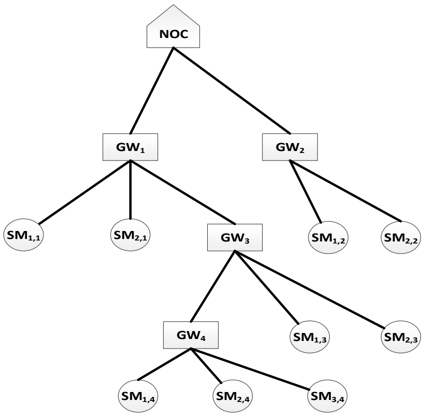


Figure 3. Authentication for Group Gateway.

NOC creates a random master key K_{NOC}. This key will be used to generate keys for each child GW_g (GW_1 and GW_2, *etc.*):

$$K_{GW_g} = \mathcal{F}\left(K_{NOC}||GW_g\right) \tag{2}$$

where $\mathcal{F}\left(\ \right)$ is a secure one-way hash function and | | is the concatenation operator. The key K_{GW_g} is stored at the corresponding GW_g. The NOC does not need to store it, since it can be generated from K_{NOC}. In a similar way, each child node GW_g produces shared keys for its own child nodes. For example, if GW_1 has several child nodes as group gateways, GW_1 uses its master key K_{GW_1} to generate a key for each of its child nodes, $GW_{g\prime}$:

$$K_{GW_{g\prime}} = \mathcal{F}\left(K_{GW_1}||GW_{g\prime}\right) \tag{3}$$

The keys generated are stored at the corresponding child nodes. Similarly, each of these nodes will generate keys for its child nodes and so on, until all the leaf nodes with no children have been reached.

3.4. Case 1—Star-Star Topology

In this scenario, we consider a star for NAN topology in the group, with GW_g at the centre. The GW nodes directly communicate with the NOC. This scenario is simple since each SM has a direct link (one-hop) to its GW. This means that no network discovery needs to be made, since GW can detect its network. The process of SM authentication is also simple, because each SM can be directly authenticated by the GW_g.

First, the pre-deployment phase is discussed. This phase assigns the master key MK_{NOC} to the NOC and is depicted in Figure 4.

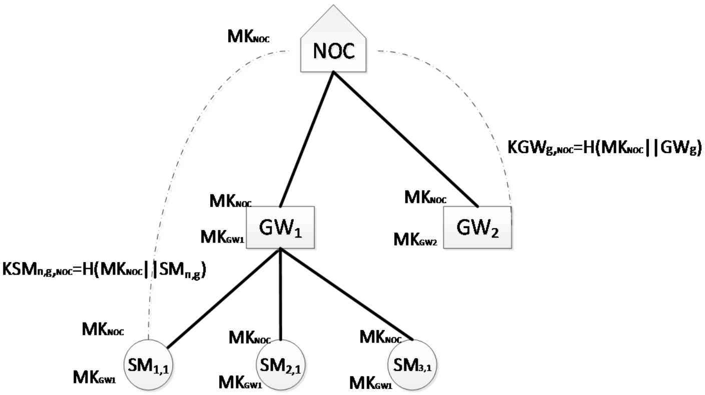


Figure 4. Pre-deployment for NAN in a star topology.

Secondly, the smart meter authentication is highlighted. Specifically, a SM_{ng} that wants to join a group needs to be authenticated by GW_g. As shown in Figure 5, initially, the new SM_{ng} will send a request message to GW_g. This message includes B, which is the encrypted message (serial number of new SM_{ng}) using symmetric key $K_{sm,noc}$. Identity number of new smart meter, SM_{ng}, and a timestamp, TS (this is used to mitigate the replay attacks).

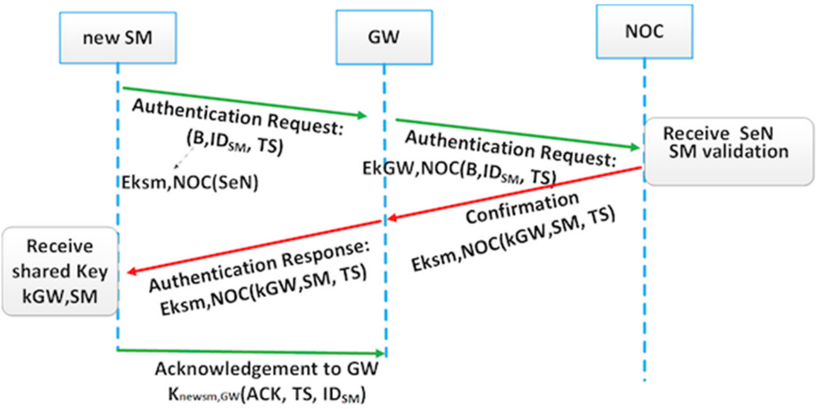


Figure 5. Authentication for NAN in a star topology.

The gateway GW_g will re-encrypt the message using K_{GW_g} and forward the message to the NOC. The NOC received B and decrypted it using $K_{sm,noc}$ and in order to validate the serial number of the new SM_{ng}. The NOC responds to GW_g with a confirmation after validating the serial number of the new SM_{ng}. The NOC will encrypt ($K_{Gw,,sm}$, TS) using $K_{sm,noc}$ and send it to the new SM_{ng} via GW_g. After SM_{ng} receives the message it decrypts it using $K_{sm,noc}$ and obtains the shared key with GW_g. $K_{GW,sm}$ SM_{ng} then replies with an acknowledgement message encrypted with the key.

3.5. Case Two—Multi-Hop (Mesh)

The SMs are interconnected in a partial mesh or a full-mesh topology. Each group in the NAN consists of a GW and its nodes. The GW nodes are, in turn, interconnected to the NOC in a star configuration, *i.e.*, all the GW nodes are one-hop away from the star point, the NOC. Nodes within a group will require multiple hops to reach either the GW or the NOC. A full-mesh topology is where every SMs has a circuit connecting it to every other SMs in a group. Figure 6 illustrates this topology. In this case, there are six SMs that form a partial mesh topology between them with a multi-hop path to the NOC. A pre-installation phase comprises storing the shared key between the SM and the NOC, $K_{sm,noc}$, the ID of the device $SM_{n,g}$, a group ID G, and a serial number SN on the devices.

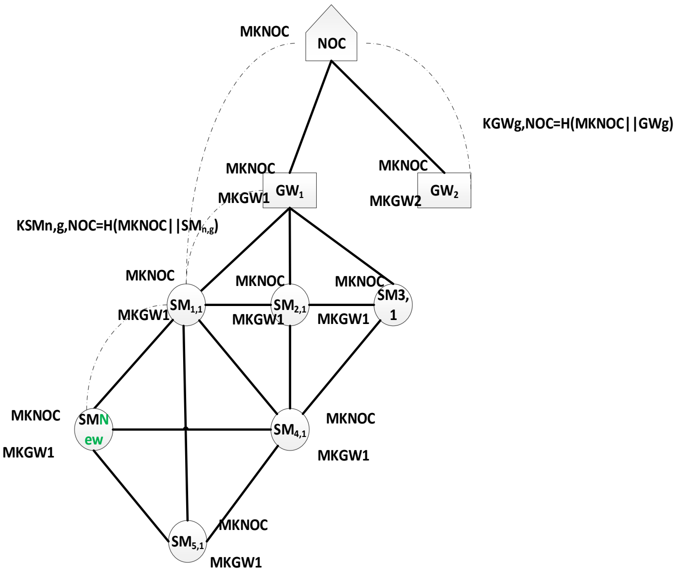


Figure 6. Authentication for a multi-hop NAN topology.

3.5.1. Network Discovery and Registration

When a SM_{ng} is initially switched on, it must learn about its neighbours in the network, which are within its range, in order to forward packets through them. To discover its neighbours, it broadcasts a Hello message and, at the same time, is listening for Hello packets that are broadcast by its neighbours (other SM_{ng}, GW_g, or NOC). The network discovery process is repeated every T time units to accommodate updates in the NAN topology. After receiving a Hello message, each SM_{ng} inserts information about its neighbour in the Neighbours table. These tables can be optionally sent to the NOC, so that it has a total view of the NAN.

3.5.2. Authentication of the Smart Meters, SM_{ng}

When SM_{new} requests to join a group, it needs to be authenticated by GW_g. There are some SMs that have no direct link to GW_g. Therefore, the authentication method shown in Figure 5 is not suitable, and we propose a two-step authentication scheme. The new SM, SM_{new}, will be authenticated through another, already authenticated, SM_{ng}, which is referred to as proxy SM_{ng}.

Initially, the new SM_{new} sends an authentication request to the proxy SM_{ng} (Figure 7). This message includes the following information:

1. Mi, the serial number of SM_{new} and SNNSM, encrypted using $K_{new,NOC}$,
2. Identity number of new SM_{ng}, IDSM_{ng},
3. Timestamp TS.

The proxy SM_{ng} encrypts Mi along with its identity and TS using the shared key between proxy SM_{ng} and GW_g. After GW_g receives and decrypts the message, GW_g re-encrypts Mi using the key K_{GW_g}. NOC will decrypt Mi using $K_{g,noc}$, check the serial number of new SM_{new}, SNNSM, and validate SM_{new}.

The NOC sends an authentication response, addressed to the new SM. The message, Xi consists of the encrypted master key of GW_g, MK_{GW} using $K_{sm,\text{noc}}$. When the new SM_{new} receives MK_{GW}, it sends an encrypted acknowledgement to GW_g, using MK_{GW}. GW_g generates a random number R and multicasts the encrypted random number R, as a message, using the shared key $K_{GW,SM}$, thereby refreshing the keys of the group when the new SM, SM_{new}, is authenticated. When all SMs receive the encrypted message they decrypt the message using $K_{GW,SM}$ to obtain the random number R. Then, each SM applies a one-way hash function on the random number R to generate the authentication value AVi. This authentication value is used by the gateway to authenticate nodes within the group. For example, for a group of SM with numbers between 10 to 20, the GW will multicast the key to all SM within a time duration of 5 s (timeout value) when using a wireless mesh network such as ZigBee or Wi-Fi.

Figure 6 illustrates the following steps in a ladder diagram.

1. SM sends an authentication request.
2. NOC validates data and sends an authentication response.
3. Authentication response contains MK_{GW}.
4. GW sends R to the new SM.
5. New SM sends an ACK to GW.
6. GW multicasts R to the group.

Following the authentication, the SM sends data to the NOC. The steps involved in communication are listed below. Notice the authenticated forwarding in steps 4 and 5. The intermediate nodes use a MAC to check the integrity and source of the packet that arrived. Additionally, note that the source node will ascertain that its data is delivered only when it receives an acknowledgement from the NOC. The details of the communication phase are out of the scope of this discussion.

1. SM decides the neighbour to forward to, for a packet destined to the NOC.

2. SM generates its encryption key K_{forw}, $\mathcal{F}'$ $(R\,|\,|\,SM_{n,g})$ where $\mathcal{F}'$ is the one-way-hash function.
3. SM generates a MAC for the message using K_{forw}.
4. The neighbour receives the message with MAC and validates it. Knowing what node id it came from, it generates the forwarding key of the source.
5. If successful, it generates a MAC and forwards it to a neighbour (to the GW, if it is the neighbour). If the MAC fails, the packet is simply dropped.

Our scheme is scalable for the requirements of a SG. In our scheme, each gateway and its group transact individually with the NOC and have no interdependency on other gateways or groups, except for forwarding data to the NOC. When the devices are scaled, an appropriate number of gateways are included to match the number of groups formed. Each gateway and its group need access to keys for their own group, the gateway and the NOC. Each node will, therefore, have a pre-installed NOC key, a master GW key sent by the NOC, and a random secret R sent by the group gateway. All other keys necessary are derived from this information. Therefore, our scheme is scalable to any number of end devices. However, we realise the need to limit the number of nodes per group to keep the number of paths low, the routing delays low and, consequently, the end-to-end delays low.

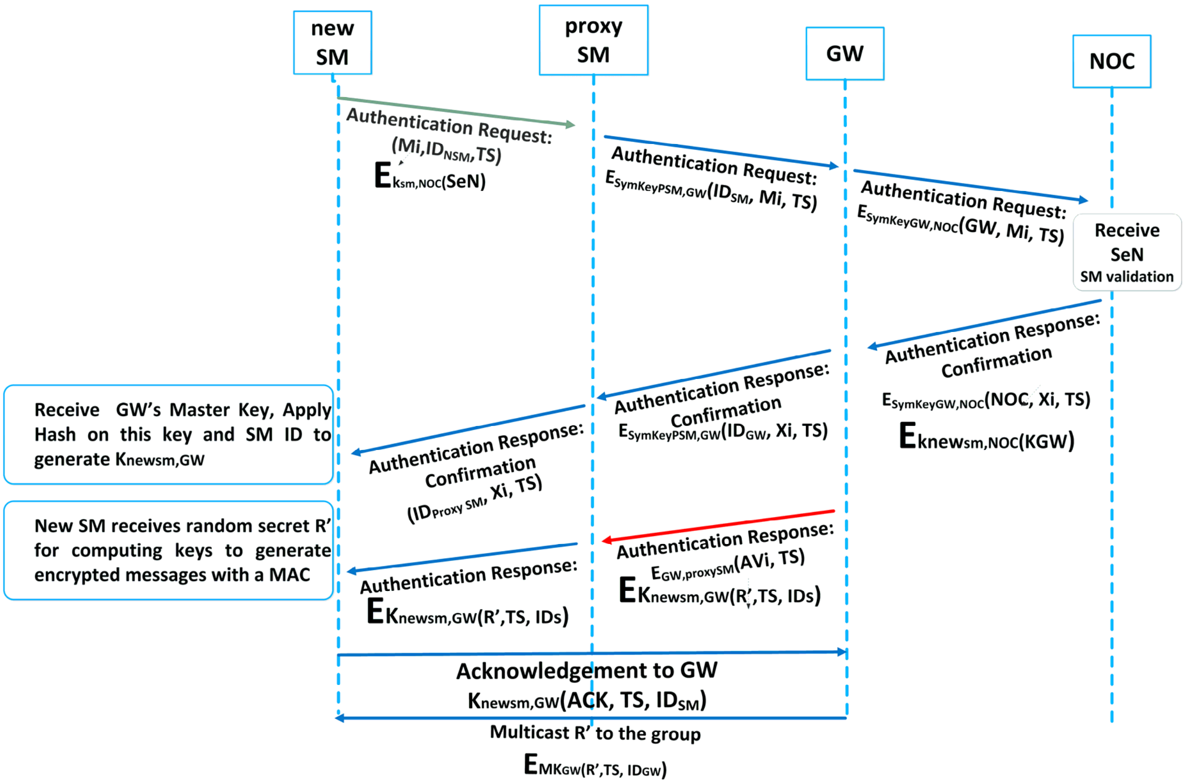

new SM
proxy SM
GW
NOC
Authentication Request: (Mi,ID$_{NSM}$,TS) E$_{ksm,NOC}$(SeN)
Authentication Request: E$_{SymKeyPSM,GW}$(ID$_{SM}$, Mi, TS)
Authentication Request: E$_{SymKeyGW,NOC}$(GW, Mi, TS)
Receive SeN SM validation
Authentication Response: Confirmation
E$_{SymKeyGW,NOC}$(NOC, Xi, TS)
E$_{knewsm,NOC}$(KGW)
Authentication Response: Confirmation E$_{SymKeyPSM,GW}$(ID$_{GW}$, Xi, TS)
Authentication Response: Confirmation (ID$_{Proxy\ SM}$, Xi, TS)
Receive GW's Master Key, Apply Hash on this key and SM ID to generate K$_{newsm,GW}$
New SM receives random secret R' for computing keys to generate encrypted messages with a MAC
Authentication Response: E$_{GW,proxySM}$(AVi, TS)
E$_{Knewsm,GW}$(R',TS, IDs)
Authentication Response: E$_{Knewsm,GW}$(R',TS, IDs)
Acknowledgement to GW
K$_{newsm,GW}$(ACK, TS, ID$_{SM}$)
Multicast R' to the group
E$_{MKGW}$(R',TS, ID$_{GW}$)

Figure 7. Authentication of a SM—Case 2.

3.5.3. Updating of MK_{GW}

When $SM_{n,g}$ leaves its group and from the network, destroying old MK_{GW} and allocating a new master gateway key to all nodes $SM_{n,g}$ in that group is very crucial. This is because the leaving node $SM_{n,g}$ may be replaced by a vulnerable node to relay false messages and communicate with other nodes; therefore, MK_{GW} revoking/re-keying is required. The NOC is responsible to inform the other $SM_{n,g}$ $\in GW_g$ nodes in that group and send a new MK_{GW} which is encrypted using $K_{sm,noc}$.

The following are the process steps of the updating MK_{GW}:

1. A smart meter node $SM_{n,g}$ must send a network leaving request L_{REQ} to the assigned dedicated node GW_g of that group. $K_{GW,SM}$ (L_{REQ}, TS, ID $SM_{n,g}$).

2. The GW_g will inform the other $SM_{n,g}$ nodes in its group (multicast) and NOC (unicast) about the leave using the messages $K_{GW,SM}$ ($L_{SM_{n,g}}$, TS, ID GW) and $K_{GW,NOC}$ ($L_{SM_{n,g}}$, TS, ID GW).
3. Removing the node $L_{SM_{n,g}}$ with L_{REQ}.
4. NOC regenerates a new master gateway key MK'_{GW} and sends it to the specific gateway.

This, in turn, multicasts to all the remaining $SM_{n,g}$ in the group, encrypted using $K_{sm,noc}$.

The updating of MK_{GW} process described above introduces a cost of re-keying. This cost has two factors:

1. Additional processing overhead. Assume that the generation of a MK_{GW} key requires × CPU cycles. The processing overhead, Oproc noc = 1 × (because NOC has to generate one key MK_{GW} for GW.
2. Communication overhead that includes two multicast and two unicast messages. The unicast messages are between the gateway and the NOC and the multicast messages are within the group.

4. Security Analysis

The authentication scheme is analysed against the two classes of threats mentioned in Section 4. A Sybil attack is an impersonation attack that is the result of eavesdropping and the node capture attack is the physical nodes capture which is very likely in the context of the SG network.

The authentication scheme described in the previous sub-section is two-way secure, meaning that after the authentication process, both parties' new SM and GW can verify the authenticity of each other. The authenticity of GC is varied since the Authentication Request from the SM is encrypted using GW's key. Additionally, in the Authentication Response, GW sends the SN of the new SM. Only GW and SM know the mapping of SN to the ID number of SM. The authenticity of the new SM is verified in a similar way. First of all, the Authentication Response is encrypted using SM's key and, therefore, only SM is able to decrypt it using its shared key. Additionally, the new SM provides to proxy SM both its ID number and SN, which provide additional security.

Denial of service (DoS) makes a node, as well as the service on it, inaccessible by others. An attacker sends a large number of packets, malicious or otherwise, addressed to the node and effectively at a rate which can block out all other communication. This causes the node receiving the packets to exhaust its storage and computing power, processing the packets that arrive from the attacker. Such a risk is imminent in a multi-hop network where the communication between two end points is routed via intermediate smart meters. The proposed authentication scheme authenticates every participant on the network before accepting any traffic from it. While this reduces the probability of spurious data on the network, the spurious traffic remains a problem. If such traffic targets a gateway node, then an attack can potentially incapacitate all nodes that communicate using that gateway. Additional means of detecting such intrusions and methods of isolating the attack traffic are necessary to handle such vulnerabilities.

Our scheme does not handle jamming attacks. Jamming attacks are DoS attacks that targets the wireless communication frequency in the smart grid. When nodes are in close range, large amounts of noise may be generated in these appliances. It is difficult to avoid jamming in our scheme because the victim and its client may not catch the attack. In this kind of attack, the attacker prevents legal users from having access to information and services by targeting the victim's device and the network connection. This attack stops the user from making outgoing connections on the smart grid. The communication can be jammed so as to make the signal noise very low, and this could lead to the failure of specific portions of the smart grid [20].

4.1. Node Capture Attack

A node capture attack is both a challenging and interesting attack with the goal of taking control over a smart meter's communication after physically gaining access. This attack could easily be carried out because smart meters are placed on customer premises and not within the utility provider's physical premises. Abdullah *et al*. [21] presented studies on the attacks and vulnerabilities of smart meters in a NAN and list node attack as the least attended, yet significantly dangerous, to the smart grid network. Most of the schemes discussed in [22–26] show a vulnerability to node capture attacks. A successful attack could reveal shared keys, thereby permitting an attacker to participate in encryption and decryption processes or, in a worst case scenario, inject false data into the smart grid network to comprise other nodes.

Our proposed group authentication scheme is secured against node capture attacks. Even if the keys are captured by an attacker and used to send data, the data packet would get validated for forwarding, but the packet would be tagged as an invalid packet since the time stamp of the packet sent by the attacker would not match the timestamp value expected by the NOC. The NOC records the timestamps of all the packets it receives, node ID-wise, so it knows what to expect in the next incoming packet from a particular node. However, if by some means, the malicious node is able to retrieve the timestamp information from the captured node and set its local clock to that of the captured node, then the scheme will be effectively broken. This condition breaks the assumption number 12 in Section 3.1.

4.2. Replay Attack

Both schemes present in [26,27] show a vulnerability to replay attack. Our scheme is secure against replay attacks because it uses shared keys for communication, as well as time stamps. Both the communicating parties, based on a shared random secret, generate the shared key. By knowing the shared random secret one cannot derive the shared secret key. Therefore, it will be computationally difficult for an attacker to generate data, which is validated with an appropriate time stamp. Similarly, replaying previously transmitted data will render the data invalid since the time stamps are encrypted along with the data and, when verified at the receiving end, will not match with the expected value of the time stamp recorded on the receiving device [28].

In the event that an attacker, by some means, is able to decrypt the captured packet and retrieve the contents of the packet, the node identity, the authentication value, and its time stamp will be available to the attacker. Using them, valid data packets can be generated and spurious data can be sent to the NOC. However, this requires the attacker node to estimate the clock ticks of the active node and replay the packets for them to be accepted by the NOC. If the attacker is able to retrieve the value of the clock ticks of the node it has captured packets from, and regenerates the packets with valid time stamps, then the scheme can be broken. This again breaks assumption 12 in Section 3.1. However, such an attack is not termed as a replay attack, since the packets are re-crafted using the time stamp from the clock tick value synchronized with the node and other values from the captured packets.

4.3. Sybil Attack

In a Sybil attack, a malicious node assumes multiple fake identities and attempts to inject traffic into the network. Our scheme prevents vulnerability to such attacks by falling back on the need to validate the authentication value and time stamp value in a packet. The authentication value is derived from the random number shared by the gateway. This value is encrypted with the key shared with the gateway and verified at the gateway. So, in order to fake multiple identities, the attacker node must have access to all the shared keys of the nodes it intends to fake [28]. If the attacker is able to get these keys and the random value from the gateway, the ID of the node can be faked. However, in order to successfully transmit data the attacker will require having valid time stamps that the NOC can validate. Like in the earlier cases, the scheme will be broken if the attacker successfully synchronizes the clock tick values of the nodes that are being faked. In such a scenario, assumption 12 in Section 3.1 is broken.

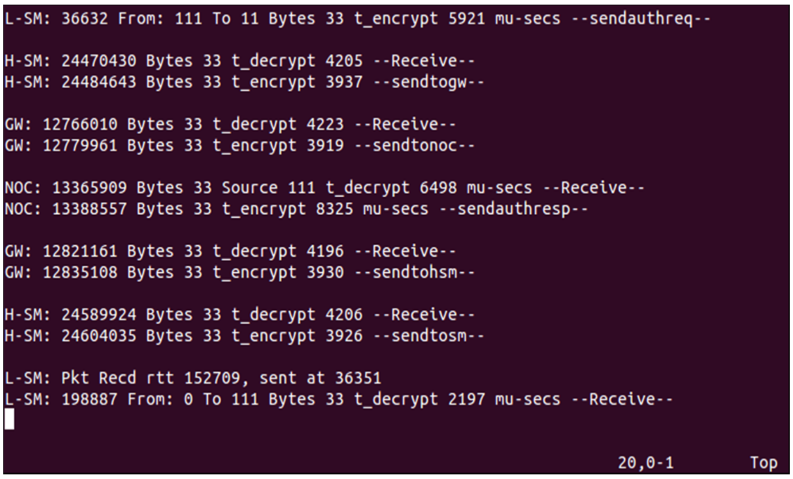
The attacker can simply re-initiate an authentication process, to overcome the time stamp problem. Re-authentication is a directed activity controlled by the NOC and therefore, any attempt to re-authenticate will immediately be detected by the NOC, thereby mitigating the attack. If this authentication attempt is successful, then the scheme breaks. This can occur if assumption 13 in Section 3.1 is broken.

5. Implementation

The authentication scheme was implemented on TelosB sensor nodes using TinyOS version 2.1 [29]. TelosB is an open source platform that includes a mote with sensors and the development platform. TinyOS is a small, open-source, energy-efficient software operating system, which supports large scale, self-configuring sensor networks. Both TelosB and TinyOS were developed by UC Berkeley (Berkeley, CA, USA) [29].

Six sensor nodes were used, one each in a role as the NOC and as a GW, and four others in a mesh communicating to the NOC, via the GW. The motes were pre-loaded with the addresses of the NOC and the GW nodes, as well as the master key of the NOC. The NOC and the GW nodes were switched on, respectively, and the GW authenticated with the NOC. Subsequently, the nodes were switched on, one-by-one. Note that the implementation on the motes did not use the link layer encryption facility. The nodes were physically located such that each node was in the radio range of only two other nodes. This ensured that there were at least two two-hop paths from the nodes to the GW.

Two specific measurements were made. The time taken for encryption/decryption (AES [5,28], with block size 16, key size 128 bits) was measured. Figure 8 provides a snapshot of the packet transit across the nodes labelled L-SM (leaf node), H-SM (intermediate node), GW (group gateway), and NOC (the NOC). Each line starts with a time stamp in microseconds, indicates the source and destination node addresses (L-SM and NOC only), followed by the application data size (33 Bytes), the time to encrypt/decrypt the packet contents on the node (in microseconds), and the name of the routine providing the information.



```
L-SM: 36632 From: 111 To 11 Bytes 33 t_encrypt 5921 mu-secs --sendauthreq--

H-SM: 24470430 Bytes 33 t_decrypt 4205 --Receive--
H-SM: 24484643 Bytes 33 t_encrypt 3937 --sendtogw--

GW: 12766010 Bytes 33 t_decrypt 4223 --Receive--
GW: 12779961 Bytes 33 t_encrypt 3919 --sendtonoc--

NOC: 13365909 Bytes 33 Source 111 t_decrypt 6498 mu-secs --Receive--
NOC: 13388557 Bytes 33 t_encrypt 8325 mu-secs --sendauthresp--

GW: 12821161 Bytes 33 t_decrypt 4196 --Receive--
GW: 12835108 Bytes 33 t_encrypt 3930 --sendtohsm--

H-SM: 24589924 Bytes 33 t_decrypt 4206 --Receive--
H-SM: 24604035 Bytes 33 t_encrypt 3926 --sendtosm--

L-SM: Pkt Recd rtt 152709, sent at 36351
L-SM: 198887 From: 0 To 111 Bytes 33 t_decrypt 2197 mu-secs --Receive--


                                                                   20,0-1        Top
```

Figure 8. The output of the motes from the L-SM to NOC and back.

The total delay for the authentication process of a mote, using a two-hop path, was measured. The average encryption and decryption times on end nodes are 6 ms and 6.2 ms; on intermediate nodes (authenticated forwarding), including the GW node, 3.9 ms and 4.2 ms; and on the NOC, 8.2 ms and 6.5 ms. The average RTT from an end node to the NOC was 196 ms. The average RTT between a pair of nodes on the network was 25 ms. The entire authentication process Figure 8 took 331 ms.

The time taken for encryption and decryption of a 16-byte block of the application packet is shown in Figures 9 and 10 respectively. This measurement was done using the microsecond timer implemented in TinyOS. The timer was fired before and after the encrypt/decrypt operations, within the application. Therefore, the measurement includes the TinyOS overheads (interrupt servicing, packet reception, *etc.*). The dataset contains a hundred measurements on each mote and Figures 8 and 9 indicate the mean of the dataset and the standard deviation.

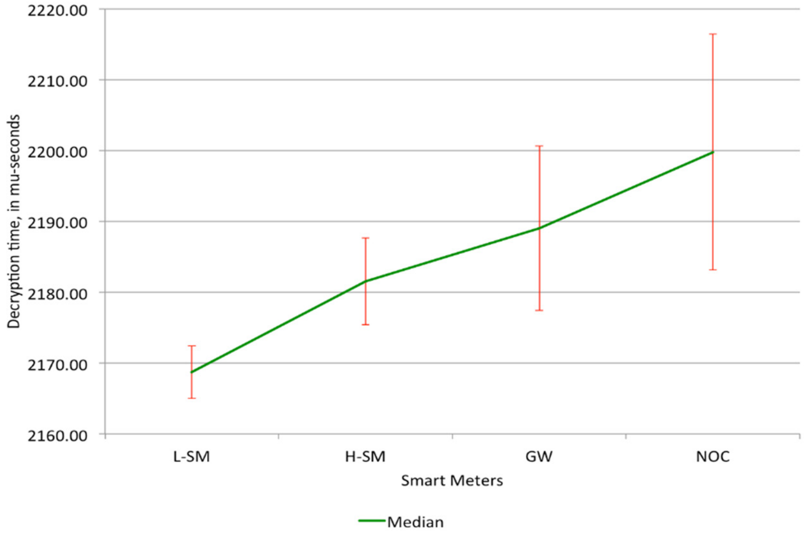


Figure 9. Time taken for AES encryption of a 16 byte block on motes in a mesh topology.

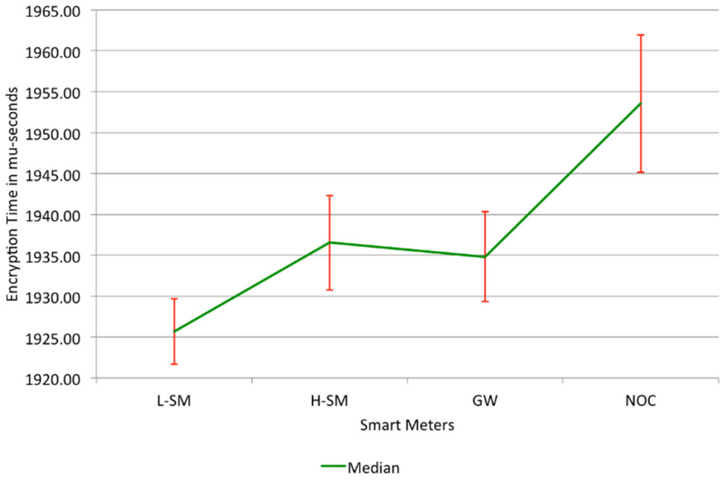


Figure 10. Time taken for AES decryption of a 16 byte block on motes in a mesh topology.

The path from the L-SM to the NOC is a three-hop path. Each mote in the path will need to process packets from its downstream, in addition to its own packets, which leads to an increase in the overall encryption time. This is evident from the increasing encryption and decryption times as well as the increasing value of the standard deviation of the dataset, which is plotted as an error bar.

The round trip time (RTT) for an authentication packet (network transit time + processing time on each sensor node) from the L-SM to the NOC and back, was measured for the star and mesh topologies. Figures 11 and 12 indicate the RTTs without and with the security turned on (labelled as RTT-SECURE). The RTT for the mesh (Figure 12) topology is an order of magnitude higher than that for the star topology (see Figure 11). The limitation of the implementation is the inability to examine the performance of the authentication scheme when the number of nodes is scaled up. This requires physical configuration and deployment of a large number of motes. Specifically, the load on the gateway node and its impact on the authentication delay require evaluation.

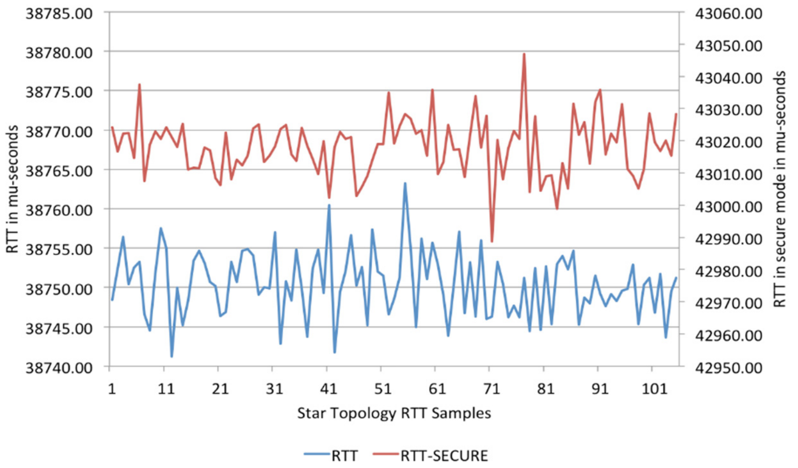


Figure 11. RTT from L-SM to NOC in a star topology (one hop).

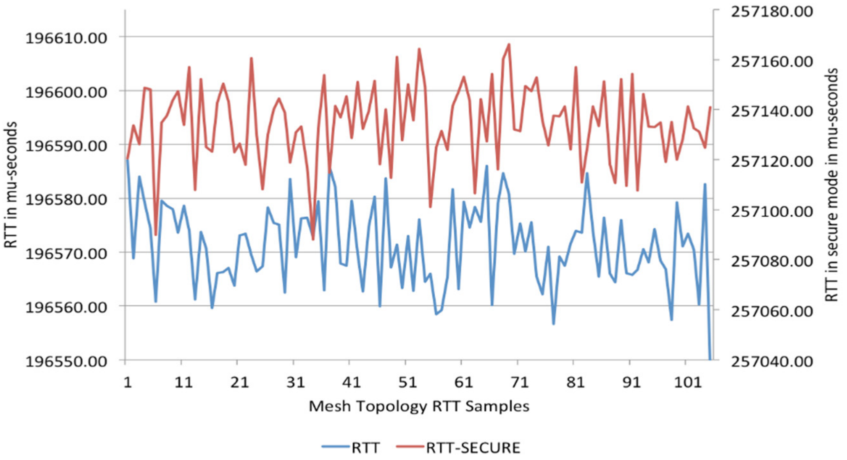


Figure 12. RTT from L-SM to NOC in Mesh topology (three hops).

Such an evaluation is currently being attempted as a simulation in OPNET [30]. A network of nodes interconnected using ZigBee is simulated. These nodes, in a cluster-tree topology, are scaled up to large numbers towards two specific objectives. First, to measure end-to-end network delays (from the leaf nodes to the NOC, multi-hop path), and second, to emulate the application (authentication and sensor data) packet flows and measure the authentication delays, when nodes join/leave the network. Subsequently, the intent is to study the effect of physical node capture and node failures in terms of the extent of impact on node reachability and, hence, the portion of the network that is effectively non-functional.

6. Conclusions

In this paper, we proposed a security scheme for groups of SMs in a Neighbourhood Area Network that enable entire groups to authenticate themselves, rather than on at a time. In particular, the scenario of a multi-hop network is considered where the nodes require multiple hops to communicate with the NOC, which is the entity that issues the keys. Two topology scenarios, star-star and mesh, are considered and separate authentication processes are defined for their operation. We propose a hierarchical control scheme for authentication; all nodes initially authenticate with the NOC and, subsequently, the group gateway autonomously issues an authentication token to the authenticated members in its group. We mention how the proposed approach is two-way secure as both involved parties, the group controller and the smart meters, are able to successfully verify each other.

The authentication scheme was implemented in real-world environment using TelosB motes. We found out that the average encryption and decryption times on end nodes are 6 ms and 6.2 ms, on intermediate nodes (authenticated forwarding), including the GW node, 3.9 ms and 4.2 ms, and on the NOC, 8.2 ms and 6.5 ms. The whole authentication protocol took 331 ms.

In our future work we are going to evaluate the performance of the authentication scheme in a large network using a simulation tool [30]. We intend to examine the performance of the scheme in a large network, simulating failures of gateway nodes and measuring the impact of single and multiple gateway node failures in terms of the number of nodes that are rendered unreachable. The topology of the networks will be star, partial mesh, and full mesh between the gateway nodes. In addition, the impact of node failures resulting from attacks on the overall network will be evaluated. In addition several of security scenario case studies will be analysed [21].

Author Contributions: This paper has been written by the first author (Bashar Alohali) and is based on the research conducted by him under the guidance of the second, the third authors and the fourth authors.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid; the new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980. [CrossRef]
2. Wang, W.; Lu, Z. Cyber security in the smart grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
3. Dollen, D.V. Report to Nist on the Smart Grid Interoperability Standards Roadmap. Available online: http://www.nist.gov/smartgrid/upload/InterimSmartGridRoadmapNISTRestructure.pdf (accessed on 9 December 2015).
4. Technology, N.I.O.S.A. *Announcing the Advanced Encryption Standard (Aes)*; Federal Information Processing Standards Publications (FIPS PUBS), National Technical Information Service (NTIS): Springfield, VA, USA, 2001.
5. Technology, N.I.O.S.A. *Data Encryption Standard*; Federal Information Processing Standards Publications (FIPS PUBS), National Institute of Standards and Technology: Gaithersburg, MD, USA, 1999.
6. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010. [CrossRef]
7. Meng, W.; Ma, R.; Chen, H.-H. Smart grid neighborhood area networks: A survey. *IEEE Netw.* **2014**, *28*, 24–32. [CrossRef]
8. Zhong, F.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Ziming, Z.; Lambotharan, S.; Woon, C. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 21–38.
9. Broustis, I.; Sundaram, G.S.; Viswanathan, H. Group authentication: A new paradigm for emerging applications. *Bell Labs Tech. J.* **2012**, *17*, 157–173. [CrossRef]
10. Harn, L. Group authentication. *IEEE Trans. Comput.* **2013**, *62*, 1893–1898. [CrossRef]
11. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
12. Mahalle, P.N.; Prasad, N.R.; Prasad, R. Threshold cryptography-based group authentication (TCGA) scheme for the internet of things (IoT). In Proceedings of the 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), Aalborg, Denmark, 11–14 May 2014; pp. 1–5.
13. Ghanbarimaman, R.; Pour, A.N. A new definition of group authentication increasing performance of server calculation. In Proceedings of the 2012 International Conference on Information Science and Applications (ICISA), Suwon, Korea, 23–25 May 2012; pp. 1–6.
14. Yang, H.; Jiao, L.; Oleshchuk, V.A. A general framework for group authentication and key exchange protocols. In *Foundations and Practice of Security*; Springer: Gewerbestrasse, Switzerland, 2014; pp. 31–45.
15. Wang, F.; Chang, C.-C.; Chou, Y.-C. Group authentication and group key distribution for ad hoc networks. *Int. J. Netw. Secur.* **2015**, *17*, 199–207.

16. Choi, D.; Jeong, H.; Won, D.; Kim, S. Hybrid Key Management Architecture for Robust SCADA Systems. *J. Inf. Sci. Eng.* **2011**, *2011*, 197–211.
17. Nicanfar, H.; Jokar, P.; Leung, V.C.M. Smart grid authentication and key management for unicast and multicast communications. In Proceedings of the Innovative Smart Grid Technologies Asia (ISGT), Perth, Australia, 13–16 November 2011; pp. 1–8.
18. Aboba, B.; Simon, D.; Eronen, P. Extensible authentication protocol (EAP) key management framework. Network Working Group, Request For Comments 5247, August 2008. Available online: https://tools.ietf.org/html/rfc5247 (accessed on 9 December 2015).
19. Das, S.; Ohba, Y.; Kanda, M.; Famolari, D.; Das, S.K. A key management framework for ami networks in smart grid. *IEEE Commun. Mag.* **2012**, *50*, 30–37. [CrossRef]
20. Alohali, B.; Merabti, M.; Kifayat, K. A cloud of things (COT) based security for home area network (HAN) in the smart grid. In Proceedings of the Eighth International Conference on Next Generation Mobile Apps, Services and Technologies (NGMAST), Oxford, UK, 10–12 September 2014; pp. 326–330.
21. Abdullah, M.D.H.; Hanapi, Z.M.; Zukarnain, Z.A.; Mohamed, M.A. Attacks, vulnerabilities and security requirements in smart metering networks. *TIIS* **2015**, *9*, 1493–1515.
22. Efthymiou, C.; Kalogridis, G. Smart grid privacy via anonymization of smart metering data. In Proceedings of the First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, USA, 13 August 2010; pp. 238–243.
23. Lu, R.; Liang, X.; Li, X.; Lin, X.; Shen, X.S. Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Trans. Parall. Distrib. Syst.* **2012**, *23*, 1621–1631.
24. Li, F.; Luo, B.; Liu, P. Secure information aggregation for smart grids using homomorphic encryption. In Proceedings of the First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, USA, 13 August 2010; pp. 327–332.
25. Kim, S.; Kwon, E.Y.; Kim, M.; Cheon, J.H.; Ju, S.-H.; Lim, Y.-H.; Choi, M.-S. A secure smart-metering protocol over power-line communication. *IEEE Trans. Power Deliv.* **2011**, *26*, 2370–2379. [CrossRef]
26. Ayday, E.; Rajagopal, S. Secure, intuitive and low-cost device authentication for smart grid networks. In Proceedings of the Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2011; pp. 1161–1165.
27. Choi, J.; Shin, I.; Seo, J.; Lee, C. An efficient message authentication for non-repudiation of the smart metering service. In Proceedings of the First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI), Jeju Island, Korea, 23–25 May 2011; pp. 331–333.
28. Merabti, M.; Alohali, B.; Kifayat, K. A new key management scheme based on smart grid requirements. In Proceedings of the 9th International Conference on Computer Engineering and Applications (CEA'15), Dubai, UAE, 22–24 February 2015; pp. 436–443.
29. Levis, P.; Madden, S.; Polastre, J.; Szewczyk, R.; Whitehouse, K.; Woo, A.; Gay, D.; Hill, J.; Welsh, M.; Brewer, E. Tinyos: An operating system for sensor networks. In *Ambient Intelligence*; Springer: Heidelberg, Germany, 2005; pp. 115–148.
30. Riverbed. 2014. Riverbed Modeler Version 17.5, pl6, Riverbed Software. Available online: http://www.riverbed.com/ (accessed on 9 December 2015).