EAI Endorsed Transactions
on Security and Safety

Research Article EAI.EU

A secure and lightweight multicast communication system for Smart Grids

Tiago Antônio Rizzetti[1,*], Bolívar Menezes da Silva[2], Alexandre Silva Rodrigues[1], Rafael Gressler Milbradt[1], Luciane Neves Canha[1]

[1]Electrical Engineering Graduate Program, Federal University of Santa Maria, Brazil
[2]Informatics Graduate Program, Federal University of Santa Maria, Brazil

Abstract

In the Smart Grids context, all communications must be handled in a secure way, including multicast traffic. The Application Layer Multicast (ALM) algorithms provide better flexibility and can employ security mechanisms, however, causes overhead to all nodes to build the multicast tree. In this work is proposed another approach to provide a secure multicast focusing on filtering packets on nodes without need an overlay protocol. It uses the multihop property of Wireless Mesh Networks (WMN) usually employed to bring connectivity to smart meters. Also, there is the support to message authentication code (MAC) using symmetric cryptography and presents an algorithm to provide a secure key distribution system. The results show that this approach is lightweight, secure, and assures multicast message delivery, even on failures caused by attacks on the key distribution system. The key management protocol used to provide authentication and integrity are evaluated using an automated test tool.

Received on 08 September 2018, accepted on 27 November 2018, published on 03 December 2018

Keywords: Security, Key Distribution, WMN, Multicast, Multihop, AMI, Smart Grids, Secure Multicast, Message Authentication

doi:10.4108/eai.13-7-2018.156004

1. Introduction

Several efforts were made in past years to promote automation through the use of communications network and information technology applied to utility services and industrial controls, such as power systems [1]. The Smart Grids concept is an example of it, using a two-way communication network capable of promoting remote monitoring, and control to the power grid, this way enabling a new set of applications. To utilities an primary advantage is to improve monitoring controls, allowing fast healing of anomalies [2]. Besides, better use of resources enables a cost reducing, and minimize outages providing a better quality of its services, thus reducing possible fines applied by regulatory agencies. From customer perspectives promote better control of its use, enabling large-scale insertion of distributed generation, this way the user could produce energy besides of consumes it. In general, this integration promotes a better quality of services and system reliability. One of the most explored applications of Smart Grids is the Advanced Metering Infrastructure (AMI) on the power system. It allows a better distribution of load balancing of power grid [3], especially on power distribution systems, once could promote incentives to customers to reassess his habits to use energy when it is cheaper [3].

To make AMI a reality is necessary a massive deployment of Smart Meters (SM). Promote network connectivity to a high number of these devices is a challenge. At power plants and power transmission systems there is a static topology, with a limited number of devices connected to it, and usually confined to a specific area. In these scenarios an infrastructure communication network, using fiber optics is usually used. However, on the distribution power system this kind of physical media is applied only to substations, and some feeders, thus encompassing a small part of it. To enable full AMI functionality, all energy customers must have a smart meter. Thus, dozens of

*Corresponding author. Email: tiago.rizzetti@ufsm.br

thousands must be deployed to all consumers spread over a large geographic area, and all must have data network connectivity. In this case, the use of wired communications could have a cost prohibitive. Several studies were performed to use power line communications (PLC), using the distribution system cables itself. However, with several transformers on the data path, there are just low throughput solutions available and have little use [4], as Ultra narrowband power line communication (UNB-PLC) [5]. Other solutions allow large throughput, but demands modifications on power system installing filters with bypass cables on transformers [5].

An alternative to providing communications network to these devices is using a wireless mesh network (WMN) [4]. The WMN is cheaper, faster and easy to deploy. Besides, could be used to a wide geographical area allowing, for example, to use it on SMs [4]. On a WMN all devices can collaborate on the infrastructure. The mesh routers usually have more capability and especially have no power constraints [6]. The client nodes also collaborate to relay packets from other nodes, one of the mains differences between routers and clients is about power availability [6], as also interconnection connectivity. The relay functionality present on each node implies that devices throughput will handle its network packets as well as the packets of other devices as a router does.

For multicast transmissions, the same packet must be delivered to each device of the multicast group. On AMI this must be done to any information from controls systems (i.e., SCADA) to sets of smart meters, such as dynamic pricing and outages notifications. Some techniques must be used to avoid packet replication. Several approaches are made to handle multicast at the network layer, modifying routing protocols [7] [8] [9]. Other approaches handle multicast at application layer [10]. Both of these approaches are suitable for general usage. However, sometimes there are drawbacks related to security and modifications in routing protocols to network layer multicast. Also, there is a high overhead caused by overlay network on traditional Application Layer Multicast (ALM) algorithms.

This work proposes a different approach to handle multicast on specific scenarios, such as smart meters (SM) used by Advanced Metering Infrastructure (AMI). It is proposed a hybrid solution for secure multicast, using a sniffer on link layer to take advantage of the WMN multihop property. There is no need of overlay network to provide multicast, such as traditional ALM algorithms, thus reducing the overhead of message exchange and latency to delivery the message to all nodes. Also, provides a secure and fail proof multicast system, one that does not need nodes agreement and does not any modification at routing protocol used by WMN.

The Secure Communications Platform (SCP) is the primary scope where this work takes place. The SCP uses a new approach to provide local authentication and access control through security properties propagated to every authorized node in the network. Thus, supporting both unicast and multicast traffic. This work discusses the approach to multicast traffic on the SCP framework. The contribution of this paper is a fail-proof and straightforward multicast delivery system, lightweight to the nodes of the WMN network, handling secure keys appropriately.

The structure in this paper is as follow: the section 2 is discussed related works and shows what issues they presents; the section 3 briefly discuss main aspects of SCP platform showing the big picture where this work takes place; section 4 is showed the proposed solution to provide a lightweight, secure multicast system; on section 5 are presented the tests, and results performed over the proposed solution with its discussion; on section 6 is presented a conclusion and future works.

2. Related Works

IP Multicast use the network layer to provide multicast message delivery. Using this method network routers infrastructure will take care of multicast, avoiding replicate packets using particular addresses. There are some technical issues, such as routers must be capable of handling it. Therefore modification at network routing protocols must be done. Sometimes this represents a difficult task [10], primarily to provide security and flexibility to its deployment.

Several ALM algorithms are proposed on literature as an alternative to providing more flexibility than IP Multicast. The work presented by [11] does an extensive discussion about ALM algorithms and the techniques employed in them. In general, ALM algorithms need an overlay network, built over a real network, to provide a multicast delivery system without any changes in real routing protocols. Some ALM approaches are based on the source tree, building a delivery path based on the packet source. Others use shared trees, a more complex solution, however delivering more flexibility and scalability to large groups [11]. Regardless of the approach, it causes overhead to the devices participating in the multicast and possible failures on the overlay network will turn the multicast system inoperative.

The best delivery path to multicast messages is a complex problem. In the study presented by [12] is discussed an ALM algorithm to find the minimum delay tree path to delivery multicast messages. Find a minimum delay path using general models is an NP-complete problem. Thus it employs heuristics to try best solution[12].

Wireless networks are subject to interference, and work presented by [13] discuss the problem of interference-aware multicasting in wireless multihop networks. The authors classify nodes in multicast trees and analyze interference models. Thus, they proposed a routing and scheduling algorithm to be used to multicast using multihop property [13]. To build multicast trees nodes must exchange information, and there no are discuss security to multicast.

In the study presented by [14] is discussed a multicast solution to WMN based on channel-radio association using the multicast protocols SRSC, SRMC, and MRMC. These protocols operate at network layer but using radio association at the link layer. The authors focus on finding the best path to delivery of multicast packets. However, security is not discussed.

In the paper presented by [15] the authors present an architecture of mesh certification authority (MeCA), which is based on a self-organized certificate system without the need for a central certification authority. To implement it some nodes of network participate in a distributed certification authority mechanism. Thus, its focus on building a distributed Certificate Authority (CA) and keys management considering protection without external adversaries [16]. However, it causes some overhead and must make changes at routing protocol.

On the work presented by [16] is proposed a secure multicast algorithm to WMN called SEMRAW. It focuses on providing a reliable tree path using a Public Key Infrastructure (PKI) to assure node authenticity but without handle the key distribution. They use asymmetric signatures to provide authenticity and integrity to multicast routing mechanism, thus causing overhead on each WMN router once each of them must verify signatures of one-hop and two-hop neighborhood. Also, [16] provides the formal proof of its model. Several signature verification operations could be an onerous task, especially on constrained hardware.

Usually, ALM algorithms are evaluated through metrics comparing them with IP multicast (network layer) algorithms and the overhead caused by the overlay network to provide multicast [11]. At work presented by [17] are summarized some properties to evaluate them: link stress (LS), overlay cost (OC), resource usage (RU), relative delay penalty (RDP), stretch for a member (SFM), losses after failures(LAF) and time to first packet (TFP).

The privacy for user data in smart grids is a critical matter, several works discuss this subject, such as [18] [19]. However, in the scope of this work, the multicast system handles data on the unidirectional way, from utility to smart meters. Users do not produce these data, thus usually can't threat its privacy.

As discussed many of these works use complex algorithms to promote multicast and also several of them do not apply security. The section 4 shows our proposal to provide a multicast system, using a simple fail-proof mechanism, also focused on security and fast message delivery. However, first, the SCP framework must be presented.

3. SCP Architecture

This work is developed into the major context of creating an integrated platform to provide the necessary security infrastructure to smart grids, mainly aimed at the power distribution system, to provide the necessary flexibility to incorporate new applications. The proposed platform is called Secure Communications Platform (SCP), which has three layers: application, security, and network. Each one of which is responsible for handling specific aspects of security and communication. There are two major components of the architecture used to guide how all platform will operate: the Application Data Profile (ADP), and the Application Data Context (ADC). These structures maintain high-level specifications of the requirements for application security through the ADP and the communications grouping context through ADC. The fig. 1 shows these layers which use the ADP and ADC specifications to configure its services.

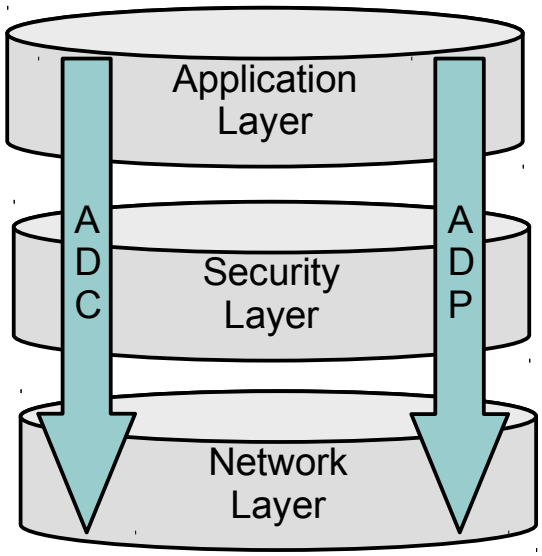

Figure 1. SCP plataform.

The application layer handles communication between applications in the smart grid and the security layer of the SCP framework. It also handles aspects of data aggregation, which is out of the scope of this paper.

The security layer has the mechanisms to provide all security features needed by the applications transparently. Aims to establish automatic mechanisms for

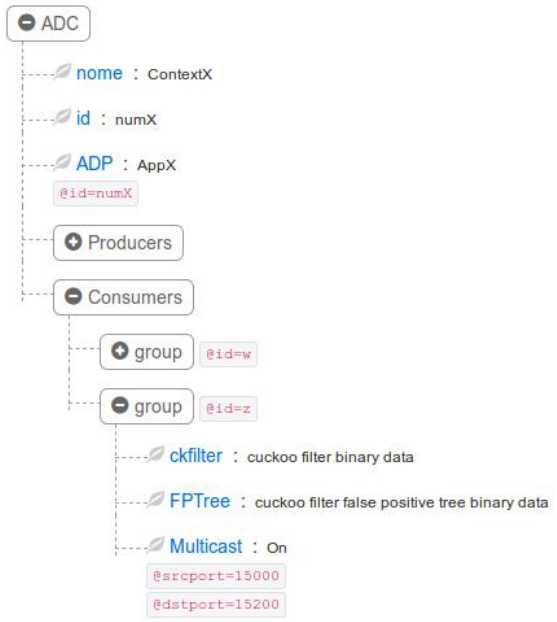

Figure 2. ADC Specification and multicast group.

the provision of application needs, including the possibility of assuring integrity, confidentiality, anonymity, authenticity, availability, and non-repudiation. The core of the SCP framework resides on cuckoo filters [20] to provide all necessary information to locally, on each device, handle all authorization and authentication process, both for unicast and multicast traffic. On the scope of this paper, the group authentication uses symmetric keys that are used, among other things to provide multicast authorization and authentication.

Network layer abstracts all communications issues used by the security layer. Security information structures are propagated by a DHT network used on the network layer, thus providing an overlay network with high fault tolerance to assure availability.

The ADC describes the membership of group communication. With it, communications can be filtered, allowing data flow just to authorized devices on specific applications. On ADC specification, groups of devices are detailed, as also the rule of that devices has in this communication context. Each group device can act as a producer, a consumer or both. Also, in each group could be specified if it has multicast flow allowing to the framework handle it transparently to applications.

With it, any application can use multicast flow, just by its configuration on ADC structure, without any changes on the application itself. The fig. 2 shows an example of an ADC. Must be noted the multicast specification to consumers on example group.

These multicast settings present on ADC were used by the Gateway Multihop Application Multicast (GMAM), a set of internal components of the SCP framework built to handle multicast traffic. The next section will discuss the GMAM.

4. Gateway Multihop Application Multicast

The Gateway Multihop Application Multicast (GMAM) is an intra-site solution based on the application layer, but using packet filtering at the link layer. It is different from traditional ALM algorithms as also independently of routing protocol used. This solution takes advantages of multihop forwarding existing os WMN, where each node analyzes transit packets that met specific filters and process those that correspond to its interest. The GMAM is based on performing unicast covering the higher number of distinguished devices possible, and avoiding using a partial path previously used, this way avoiding duplicate packets on each WMN node. The GMAM requirements are a) gateway must be aware of network topology to decide the best unicast address to reach the highest number of nodes in the path; b) each node must be able to filter wanted packets, and c) all of it must be done without interfering on routing mechanisms.

This solution was mainly designed to smart grids, especially to be used on AMI. In this scenario is a reasonable approach to building a wireless mesh network where nodes are static, this way, a low rate of path change would be expected. Another assumption is about the power supply, SM devices are connected to the power grid, and there is no prerequisite to it

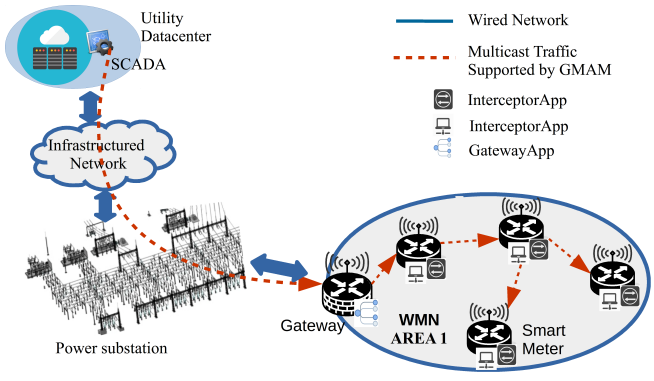

Figure 3. Components of GMAM platform and where it takes place.

The GMAM solution, in the scope of SCP, has three main software components: the interceptorApp, nodeApp, and gatewayApp. The interceptorApp take place on all WMN nodes. It is responsible for setting

the filters, sniffer and handling traffic at each WMN node. The nodeApp also runs on all WMN node, and it receives unicast transmissions which have as destination the node. The gatewaApp runs just on the gateway, and it is responsible for creating the multicast path tree information. It will determine to which nodes the unicast packets must be sent to reach the higher number of nodes, using the multihop property of WMN.

With this scheme, SCADA systems can, for example, sent information to a set of smart meters just sending a single message to this group. The GMAM solution, on the final gateway, will receive this packet and forward it, using a unicast message to the nodes with more hops in its way. Thus, any WMN node in the data path could intercept the packet and use it, if ADC and ADP of this application determine it. Of course, all of this must be done on securely way, using methods to certify the authenticity and integrity of data. GMAM supports these features and will be detailed in the next sections. The fig. 3 shown an example scenario, illustrating where each software component of GMAM architecture must take place. Also indicates the scope limitation of GMAM solution, which supports only unidirectional multicast traffic. Thus, without the need for an overlay network or changes on the network layer to support it, once its functionality is based on the multihop property with interception scheme to propagate the message. The message itself and the GMAM/SCP architecture provide all information needed.

The gateway is a common point between the external network and any WMN node. Usually, multicast data is sent from SCADA applications or other manager software placed on Operation Center to the devices of WMN. The gateway has more processing power than a typical WMN node. Thus GMAM concentrates processing power on the gateway to define best paths to reach the highest number of nodes possible. On this architecture, all nodes will be registered in gateway after initial authentication using certificates summarized in ADC to join in the WMN network. Thus this information is already available at the gateway, using SCP architecture.

The gateway could use already available network tools to build the multicast tree path. In IP networks, Internet Control Message Protocol (ICMP) could be employed to discover the path necessary to deliver a message for all devices on the WMN. This task is straightforward but takes some time to build a network connectivity path to every device. The *traceroute* tool could be used to generate this information. After gathering this information, the gateway must process it, finding the list of paths of terminal nodes with more distinguished nodes in its path. First, the gateway will sort this list by the ascendant way, putting terminal nodes with more hops first. From second to the last element is measured the number of distinguished nodes presents on that path, and storing this information, thus pointing nodes already visited. The last step is to sort the list by the number of distinguished hops. It means that in this list all devices will be mapped. However, nodes with more distinguished nodes in the path will be first. The algorithm 1 shows the operations to perform it.

Algorithm 1 Sorting destination nodes on the gateway by greatest path impact, reaching the higher number of distinguished nodes possible.

```
    ▷ Input: Nodes
    ▷ Output: Nodes
 1: procedure PathTrace.Sort(&nodes)
 2:     sort(nodes, sort_by_absolute_hops)
 3:     for i < nodes.size(), i++ do
 4:         for j < nodes.at(i).hops.size(), j++ do
 5:             it ← visited.find(nodes.at(i).hops.at(j))
 6:             if it == visited.end() then
 7:                 nodes.at(i).differents++;
 8:                 visited[nodes.at(i)].hops.at(j)] ← 1
 9:             end if
10:         end for
11:     end for
12:     sort(nodes, sort_by_differents_hops)
13: end procedure
```

The proposed approach is not intended for general use. The primary goal is to optimize traffic from the gateway to node direction. On AMI applications several of them could follow this data flow to spread information to all nodes, such as dynamic price, outages schedules, and so on. After sending packets that will potentially reach all nodes, performs a delay, allowing the return of confirmations. If not, a packet will be sent to all other nodes to assure packet delivery. In this multicast system, all nodes confirm message was received to the gateway since the reliability of data propagation on smart grids is a major concern. The algorithm 2 shows these operations.

All multicast messages transmitted has a message ID which one is used to controlling confirmations send by nodes to the gateway. This message ID also is used by WMN node to controls possible message duplications. This schema is very light to the nodes minimizing transmissions and has high fault tolerance. In the worst case scenario, with several topology changes, the message will be received anyway by unicast after a while.

Communications on Smart Grid must provide data authenticity [21] [1]. Thus multicast communications must support mechanisms to provide it. This could be achieved using signatures with Public Key Infrastructure (PKI), using asymmetric keys, or through

Algorithm 2 The multicast algorithm on the gateway.

```
    ▷ Input: Nodes, message and message ID
 1: procedure SendMulticast(nodes, message, &messagid)
 2:     sort(nodes, sort_by_absolute_hops)
 3:     greaterPingTime ← ping(nodes.begin().address);
 4:     for i < nodes.size(), i++ do
 5:         if nodes.at(i).differents == 0 then
 6:             sleep(greaterPingTime);
 7:         end if
 8:         if nodes.at(i).confirmed == false then
 9:             sendPacket(message, messageid);
10:         end if
11:     end for
12:     messageid++;
13: end procedure
```

Hash Message Code Algorithm (HMAC) with symmetric keys. Both are suitable to be used for authentication but has a significant performance difference. Recommended key size to provide a reasonable level of security for different types of mathematics approaches of cryptography algorithms is presented by [22]. For asymmetric keys using RSA recommended key size is 3072 bits, and for ECC 256 bits. For symmetric keys AES, the minimum recommended key size is 128 bits and cryptographic hash codes 256 bits (SHA-256), at least. Usually, the HMAC is a better approach to reduce overhead caused by authentication.

All components of architecture can identify and appropriately thread multicast packets by the ADP ID and ADC ID, together with the scope present on packet structure.

4.1. Multicast subscribe and unsubscribe process

As discussed on the SCP section, the GMAM is part of SCP framework, where all authorization and access control are based on ADP and ADC security structures. Each device on the network must have to pass through a bootstrap process where generating its identity. In this step, also is set, on the device, what kind of applications it handles, specifying them through the ADP. The system operator manages all security structures.

When a device initiate, after proceeding through a bootstrap process, all ADCs sted by a network operator will be informed to it. A DHT network is responsible for providing a highly fault tolerant delivery system of these security structures. Thus, each device knows, locally, what kind of applications must handle, as also which contexts of communications is allowed to it. The communication contexts are specified in groups of devices, usually determined by a geographic area. The fig. 4 shows an overview of these structures spread over all devices of the smart grid.

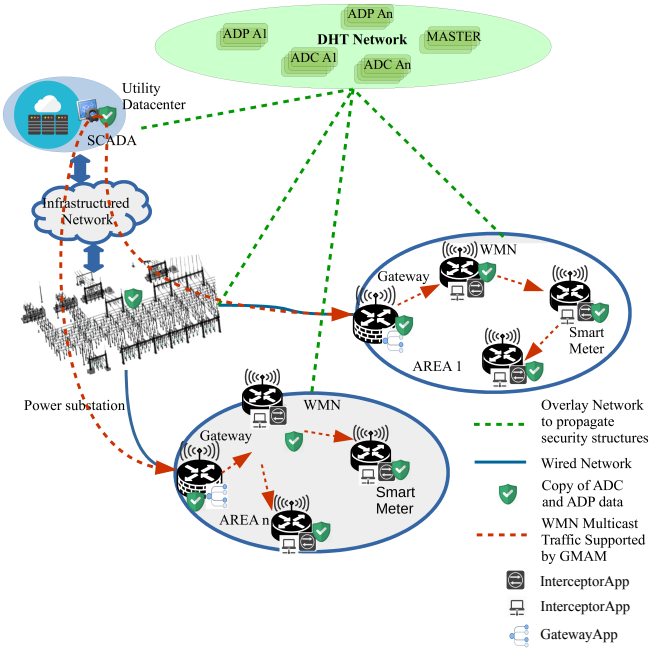

Figure 4. Group subscription information propagated by ADCs.

In ADC each group of devices allowed to communicate with one each other will be described, including what rule it acts on the ADC. Therefore, locally on each device, the grouping information is available. Also, on ADC is specified if there are multicast traffic to it. This way, each device can subscribe to the group by contacting its gateway, once the node knows that must handle multicast traffic.

The GMAM functionalities are available on each device. However, filters and all other components will be active if the ADC for that specific application is set to work with multicast traffic. In the figure 2 was shown an ADC with this information. In case of a node which is a member of an ADC with multicast traffic, GMAM it will become active, using the filters necessary to intercept and analyze this specific multicast traffic. The multicast ports present on the ADC will be used to provide the filter information. Thus, subscribe and unsubscribe process, on a multicast group is managed by the ADC and ADP. Both of these structures are under the control of the network operator.

Worth to say that just one multicast group for the tuple of ADC and device group can be set. If other multicasts group are necessary, another ADPs and ADCs could be created to support them.

4.2. Key Distribution

In work presented in [23] is presented a key agreement scheme for the smart grid, using provably secure

authenticated key agreement. However, in the scope of this work, must be used a key agreement integrated with the SCP scope, using asymmetric keys.

The gateway is responsible for managing and delivery the shared keys to each WMN node acting as a Key Distribution Center (KDC). It reduces the processing needed at SMs. An alternative could be using key agreement processes [24]. However, it involves several messages exchange to converge all nodes to a shared key, especially on larger groups. On scenario presented in this work, the KDC approach is a better choice to distribute a symmetric key through him to all other WMN nodes, thus using a key transport solution based on Public Key Infrastructure (PKI).

The secrecy of the symmetric key is a critical issue. An adversary could use it to performs a flooding attack on the proposed multicast system, causing unavailability of communication service. To avoid it was created a secure protocol based on PKI to assure key distribution without vulnerabilities with known attacks. Each node solicits a shared key to the gateway, and he sends back the shared key used in this round using asymmetric cryptography to assure confidentiality, secrecy, and integrity. The proposed algorithm was inspired by Needham Schroeder Public Key algorithm, however using only two players with an already active and valid certificate. The node (smart meters) acts as an initiator and the gateway as a responder. First of all, a Diffie-Hellman agreement is done. With the key derived by the DH algorithm, the authentication using PKI structure and filters of ADC is applied. The fig. 5 shows

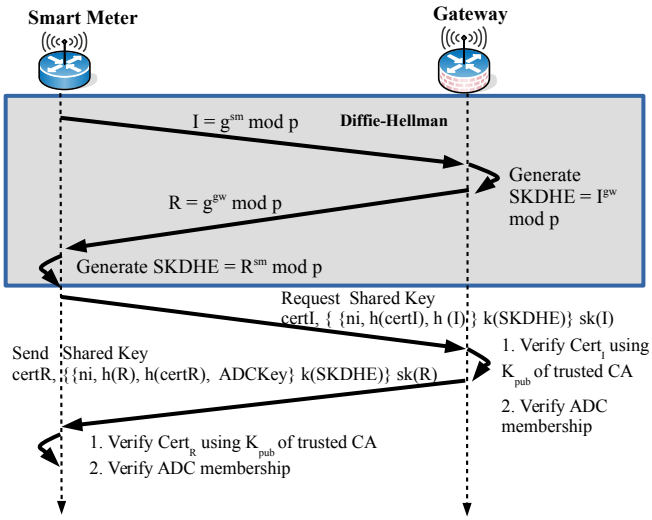

Figure 5. Dataflow of proposed key distribution algorithm. Smart meter act as Initiator and Gateway acts as a Responder.

All messages sent are signed by the private key of the sender node. Thus the Initiator (SM) and the responder (gateway) are correctly authenticated one to each other. Besides that, initiator generates a nonce value ni, used to avoid replication attacks. The hash of the certificate sent together with the message assures the integrity of the presented certificate. All necessary data are encrypted using the symmetric key provided by the DH agreement, using the ephemeral key, previously done. The symmetric key is lighter and faster than asymmetric cryptography to provide data encryption. Besides, each node also verifies the validity of the counterpart certificate and also, if the counterpart is a member of an authorized ADC. The algorithm 3 shows the primary code used to this protocol written using the syntax of the scyther software [25].

To a group of n devices will be necessary $4n$ message exchanges. The gateway will have a more massive computational load requiring $4n$ cryptography operations (signature verification, decryption, encryption), and two hash operations to each. Each gateway must compute the keys needed by its area. Thus the SMs, the weakest link on this chain will need to compute three cryptography operations to each key plus two hash operations. According to [26] the symmetric key could be changed one time a year, so the computational overhead is minimum at the SM, and only two messages must be exchanged to provide the proposed solution.

4.3. Comparative between GMAM, IP Multicast, and ALM

The proposed method is a hybrid solution using a multicast approach through the resources of the link layer, and application layer, thus a comparative between it, IP multicast, and traditional ALM algorithms must be done. To evaluate this method was used the parameters presented by [17] and discussed by [11] to compare ALM algorithms to IP multicast.

1. The link stress indicates how many duplicates copies of the packet are on the link. If link L(N1, N2) is a common way to y nodes, where at least one distinguished node is in the path, then the link stress of L is y. The link stress for some specific node is $ls \leftarrow \sum_{i=0}^{i=j} y_i$, where j is number of links in the path . At best scenario, all nodes are connected in the serial form, achieving the same link stress that IP multicast. At worst case, a long common path will be shared by several nodes, but with several ramifications at the end. Anyway, even on topology changes, all nodes will receive the packet after a timeout. The performance of this algorithm will depend on network topology.

2. The *overlay cost* is the cost of extra hops compared to IP multicast to propagate packets. For GMAM it is the same of IP multicast, once network layer built path transmits the packet directly, without extra hops.

Algorithm 3 Key transport algorithm rules: Gateway (g) and Node (n). BNF Syntax used by Scyther software [25]

```
usertype String;
const request: String;
hashfunction H;

procedure ruleNode(n, g)
    var ckfI;
    fresh ni: Nonce;
    var certRrecv: Certificate;
    var ADCKey: Nonce;
    //sends to gateway a key request encrypted with ephemeral DH shared key and signed by node private key.
    send_1(I, R, certI, ni, h(certI), h (I) k(SKDHE) sk(I));
    recv_2(R, I, certRrecv, ni, h(R), h(certRrecv), ADCKey k(SKDHE) sk(R));
    //Verify if cert received is signed by trusted CA
    match(certR, certRrecv);
    // Test if this otherside certificate is present at ADC filter
    match(ckfI, h(certRrecv));
end procedure

procedure ruleGateway(n, g)
    var ckfR;
    var ni: Nonce;
    var certIrecv: Certificate;
    fresh ADCKey: Nonce;
    // receives the node information encrypted with ephemeral DH shared key signed by the private key of the node.
    recv_1(I, R, certIrecv, ni, h(certIrecv), h (I) k(SKDHE) sk(I));
    // Verify if cert received is signed by trusted CA
    match(certI, certIrecv);
    // Test if this otherside certificate is present at ADC filter
    match(ckfR, h(certIrecv));
    // agree/auth for the ADCKey
    claim(R, Running, I, ADCKey);
    /send its cert on plain text, and an encrypted hash of own cert and ADCKey fresh generated encrypted with DHE session key
    send_2(R, I, certR, ni, h(R), h(certR), ADCKey k(SKDHE) sk(R));
end procedure
```

3. The *resource usage* is the sum of delay multiplied by link stress. On GMAM It will be determined by network topology, on best scenario, with nodes arranged on the serial form will be the same of IP multicast, on worst scenario will be the same of providing multicast by unicast.

4. *Relative delay Penalty* indicates the time overhead caused to transmit a multicast packet on the overlay network. To GMAM will be the same of IP multicast, once it uses the path provided by the network layer without the use of overlay network.

5. The *Stretch for a member* will indicate overhead caused by hops to provide ALM multicast compared to IP multicast. The GMAM use the path provided by the network layer. Thus the cost is the same as IP multicast.

6. *Losses after failures* indicates what happens if unexpected errors occur on protocol or if nodes fail. In the worst scenario, GMAM will perform a multicast using unicast to each node. Therefore there are no losses, in the worst scenario, when occurs a major failure of tree path-building algorithm, will occur an extra delay in messages delivery.

7. The *Time to First Packet* represents the time necessary to a node join to multicast and receive the first multicast message. Once the node registers with the gateway, it will get the symmetric key to message authentication and will be able to receive the messages. At the first moment, it could not take full advantage of GMAM multihop functionalities, receiving unicast packets. However, as soon as the path construction algorithm finish rebuilding the path tree, it will take full advantages of the GMAM multihop.

5. Tests and Results

To test the proposed solution was implemented a small scale scenario on Core Network Emulator [27] with 50 WMN nodes. The scenario was composed by a gateway where algorithm 1 was executed. All smart meters are deployed as WMN node, using Quagga extension to enable mesh routing through OSPF MDR algorithm. All tests were performed to a Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz, 8 GB of RAM on Linux Mint 18.02. Fig 6 shows the test scenario.

Was used the C++ Language to build the three software components: gateway manager, interceptor and node application. To intercept packets at intermediate nodes was used the *libtins* [28] Library, a fast and easy to use sniffer API. Mesh nodes run the interceptor, and node application to evaluate packets in transit, and receive its unicast traffic, respectively.

All smart meter devices run the interceptor component, which is responsible for filtering transit data. If a data matches the search criteria, the node will handle

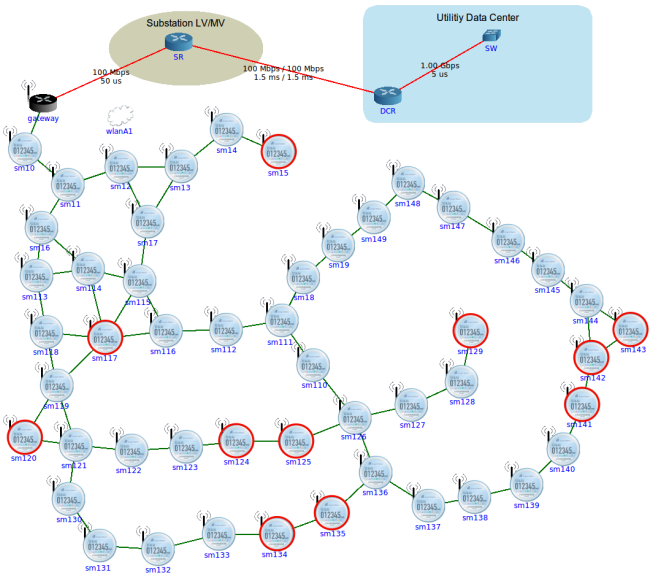

Figure 6. WMN scenario to deploy Smart Meters emulated on Core Emulator.

it, and send an ACK back to the source. The filters, as explained before are based on the ADC structure. Applying algorithm 1 for scenario presented at Fig. 6 produces the list of nodes ordered as shown at table 1.

Table 1. Path priority decision applying algorithm 1

Target Node	Distinguished Hops	Total Hops
sm143	17	17
sm134	10	12
sm141	8	16
sm129	3	13
sm124	3	10
sm15	3	6
sm117	2	5
sm142	1	17
sm135	1	12
sm125	1	11
sm120	1	7

With the eleven nodes presented at table 1 all nodes of WMN will be reached. All other devices omitted from this table have none distinguished hops and will use as a failsafe mechanism if a previous response for an intermediate node does not arrive at the gateway. This issue could occur if a topology change is made while multicast tree path refresh does not.

Providing security to multicast causes a processing overhead on devices. Thus, to take a comparative cost of algorithms to provide authenticity was performed some operations, and results shown at table 2. On this scenario to perform each RSA 3072 bit verification takes 0.10 *ms*.

Asymmetric signature verification is an expensive operation, within larger packets it could represent less significant processing, but in any scenario, it is slower than MAC operations, for instance. For this reason, MAC algorithms can be used in most of the cases. The table 2 shows the performance of different cryptography techniques used to promote authentication.

Table 2. The performance of local data authentication (without network transmission).

Algorithm	Throughput message 1Kb	Throughput message 2Kb	Throughput message 4Kb
HMAC SHA-256 128-bit key	154624 packets/s	77312 packet/s	38656 packet/s
SHA-256	187392 packets/s	93696 packet/s	46848 packets/s
RSA 3072 Verification	9493,39 packets/s	9035,64 packets/s	8241,03 packets/s

The interception processing time to a filter match packet presented an average of 3.48 ms, measured at first node (sm10), a common path to any other WMN node in this scenario. The time to process and reply a message at an intermediate node takes 0.62 ms on average. These values were achieved by the mean value of a thousand executions.

The *iperf tool* measured the overload caused by a packet filter for the unicast traffic. In a clean environment it achieves the throughput of 52.3 Mbps, and running the interceptor software performing packets analyzes was achieved the throughput of 52.0 Mbps. These data show that this solution causes an overhead of 0,57% on devices, to filter packets. In this scenario, wireless communication bandwidth was set to 54 Mbps with 2 ms of delay, and no jitter or packet loss.

5.1. Security Analysis of Key Distribution

First of all, its necessary to analyze the distribution protocol for the shared key through an informal approach, and after that analyze it through use of an automatic tool to validate the main security claims needed.

Informal analysis. Some of the leading security issues are highlighted and discussed as follow:

- Replication Attacks: In replication attacks, an opponent captures a legitimate packet and reinserts it on the network. Key distribution protocol uses one time identifiers, or *nonces*, representing a round of the protocol. Replication attacks are not practical since nonce used eliminates this possibility of intercepted messages

being accepted in a sequence other than that provided by the protocol.

- Man-in-the-middle (MITM) attacks: For an attack of this type, an adversary must be able to act as a bridge between two communication entities, intercepting and retransmitting modified or monitored data. The proposed protocol performs the authentication and authorization process on a secure channel, using the Diffie-Hellman protocol with ephemeral keys. Once the secure channel is established, basic authentication is performed through the use of digital signatures, using PKI. This process prevents MITM-type attacks once the DHE session keys need sender signature, and a possible adversary would not be able to change it to their DHE instance, nor would it be possible to sign it with the private key of the original sender. Therefore, it can be stated that the protocol is not susceptible to MITM-type attacks, due to the use of mutual authentication between the parties using the long-term asymmetric keys.

- Impersonation attack: It is not possible for one device to pass through another since the initial process uses signature through asymmetric keys. There is no risk that an imposter will be accepted unless he has access to the private key of the element he wants to pass through.

- Perfect Forward Secrecy (PFS): If an adversary can find out the current key, and he can not get any information about the keys already used or the future keys, it is said that the protocol has *Perfect Forward Secrecy*. In the proposed protocol all message exchanges use signature through the long-term asymmetric key to guaranteeing authenticity. However, shared symmetric keys are encrypted with ephemeral Diffie-Hellman keys (DHE). This ensures that even if an opponent can obtain the long-term private key of an entity, it will not have information on keys already used, or future keys, and will not be able to decrypt data from other sessions. Even in the use of shared group keys, in the case of ADC keys, this is shared through P2P DHE keys between a node and the gateway. Thus, for the proposed protocol, one can guarantee the PFS property.

- Eavesdropping: No confidential information can be obtained. In the proposed protocol, the only information transmitted in plain text is the entity's certificate, which represents public information. Also, tamper attacks are not effective since a hash of this certificate is encrypted with the symmetric key agreed by the DH algorithm used in the communication.

- DDoS Attacks: As soon as a certificate is received it is checked against the ADC filters locally. If there is no match, the request is quickly deleted. In this way, fewer system resources are employed, thus maximizing availability. Message exchange terminates as soon as an authorization violation is detected, both by the Initiator (I) and the Responder (R).

Automated analysis. To validate the key distribution algorithm was used the Scyther software [25]. This software is an automated tool which uses semantic analysis to evaluate all possible iterations between players and detect possible failures on protocol. It uses a Backus–Naur form (BNF) semantic to describe communication interaction, keys and data exchange between players. If some failure occurs, this tool provides a graphic scenario showing the interaction vulnerability. The scyther tool can verify the following security claims: Secrecy (Secret), Session key revelation (SKR), Aliveness, Weak Agreement (Weakagree), Non-Injective Agreement(NiAgree), Non-Injective Synchronization (NiSync), Variable Integrity (Running, Commit) and Reachability (Reachable). Figure 7 shows the Scyther analysis results for the proposed protocol to distribute ADC key used to multicast authentication.

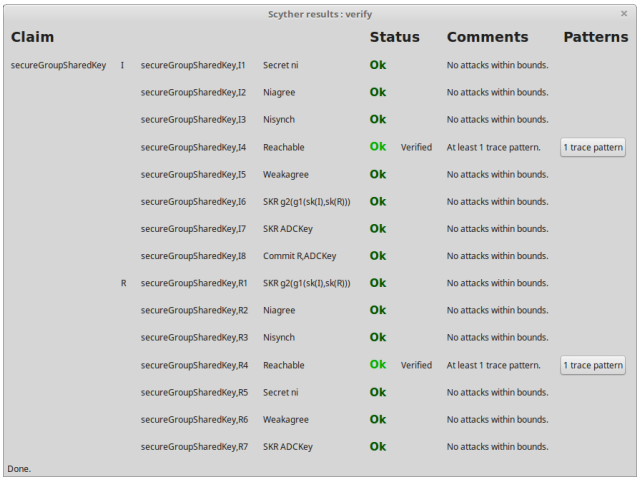

Figure 7. Scyther Report for the proposed key distribution algorithm.

There no are known security vulnerabilities detected by scyther on this protocol. The hash function used over the public key (pk) is much faster than any cryptography operation. In the proposed schema, an XXHash library [29] could be used for promoting hash operations primarily at memory speed [29].

5.2. Discussion

The results show that the presented proposal is an alternative to provide secure multicast without the

need to any change at the network layer, and without the need of a more complex solution as generic inter-domain ALM algorithms. When compared to other generic solutions, such as [16], the GMAM reduces processing need by avoiding asymmetric key verifications. Indeed, the GMAM reduces information exchange and processing at nodes since in the GMAM do not need to build an overlay network. This is an advantage on this specific scenario when compared to the works proposed by [16] [14] [13] [12]. Another point to highlight is about possible failures on the protocol. Even if the GMAM build tree fails, all nodes will receive the message by unicast.

The GMAM is built inside of SCP platform, and by its scope delimitation, can allow nodes and gateway to handle multicast traffic without overhead caused by overlay network. The shared keys used by the authentication process is not changed often, so the overhead caused by it is minimum. Once a day is enough to the more critical systems except where there are membership exclusions, in this case, the process to change the key must take place. When the change triggers, the node has to exchange only five messages with the gateway to take the shared key, this already including the DH channel to the proposed protocol operates. Thus, processing time at the node is almost insignificant. To the gateway, it must exchange 4n messages, which is acceptable, once it has more powerful processing capabilities.

The multicast tree construction is source-based on the gateway. The message exchange is treated just by the gateway to discovery the path to each node. When new nodes ingress on WMN or when unicast messages to undistinguished paths are used, the rebuilding process must be triggered. The ADC is the metadata structure defines which applications must be handled. All nodes receive the ADC structure by a DHT network used to propagate security information allowing to GMAM set the appropriated filters. So, the GMAM uses the infrastructure provided by the basis of SCP.

The proposed solution reduces duplicate packets, maximizing packet delivery, especially in scenarios there are more hops. The initial cost of computing paths to each node will be justified if WMN presents a low change rate. For environments with high mobility, other solutions, such the ones presented in the related works could be taken to build a traditional ALM algorithm. Also, in any scenario the proposed solution has support to authentication and integrity check for each multicast packet, therefore meeting the requirements of an AMI application. Replications attacks and wrong signatures could be easily detected, and a blacklist could be built to exclude these nodes from multicast communication.

6. Conclusion

This work presents a secure multicast solution designed to AMI environment without the need to exchange controls packets managed by WMN nodes. The approach takes advantage of multihop characteristics used by WMN. Thus, as discussed several performances indicator of ALM algorithms applied to this solution shows it is more like the IP multicast. However, opposite to IP multicast the security is a concern addressed by this solution based on PKI, and using message authentication code to assure the authenticity of messages to prevent Denied of Service (DoS), and Distributed Denied of Service (DDoS) attacks.

In AMI environment multicast data usually have a single flow from SCADA systems to smart meters, providing a reliable, and secure multicast mechanism without changes at the network layer, and employing a simple mechanism to control it causing a minimum overhead for implement this solution. A direct application of GMAM could be to spread dynamic pricing to all devices connected to a specific area through a gateway. Other general information, such as power quality, scheduled outages, and so on, could be delivered by GMAM as well.

Future works could be done to detect, and excluding malicious nodes from the key sharing system, using behavior analyses of the nodes participating in multicast.

7. Acknowledgment

The authors would like to thank the technical and financial support of CEEE-D Power Utility by project, ANEEL P&D Code PD-5707-4301/2015, (Capes-PROEX.), Federal University of Santa Maria (UFSM) and the National Center of Scientific and Technological Development (CNPq 311516/2014-9).

References

[1] Chih-Che Sun, Adam Hahn, and Chen-Ching Liu. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, 99:45 – 56, 2018.

[2] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A Survey on Smart Grid Communication Infrastructures : Motivations , Requirements and Challenges. *IEEE Communications Surveys & Tutorials*, 15(1):1–16, 2013.

[3] Tao Jiang, Yang Cao, Liang Yu, and Zhiqiang Wang. Load Shaping Strategy Based on Energy Storage and Dynamic Pricing in Smart Grid. *IEEE Transactions on Smart Grid*, 5(6):2868–2876, 2014.

[4] V. Cagri Gungor, Dilan Sahin, Taskin Kocak, Salih Ergut, Concettina Buccella, Carlo Cecati, and Gerhard P. Hancke. A Survey on smart grid potential applications and communication requirements. *IEEE Transactions on Industrial Informatics*, 9(1):28–42, 2013.

[5] Lars Torsten Berger, Andreas Schwager, and J. Joaquín Escudero-Garzás. Power Line Communications for Smart Grid Applications. *Journal of Electrical and Computer Engineering*, 2013:1–16, 2013.

[6] Duygu Karaoğlan Altop, Muhammed Ali Bingöl, Albert Levi, and Erkay Savaş. DKEM: Secure and efficient Distributed Key Establishment Protocol for Wireless Mesh Networks. *Ad Hoc Networks*, 54:53–68, jan 2017.

[7] De-gan Zhang, Ke Zheng, Ting Zhang, and Xiang Wang. A novel multicast routing method with minimum transmission for WSN of cloud computing service. *Soft Computing*, 19(7):1817–1827, jul 2015.

[8] J. Yuan, Z. Li, W. Yu, and B. Li. A Cross-Layer Optimization Framework for Multihop Multicast in Wireless Mesh Networks. *IEEE Journal on Selected Areas in Communications*, 24(11):2092–2103, nov 2006.

[9] Xin Zhao, Jun Guo, Chun Tung Chou, Archan Misra, and Sanjay K. Jha. High-Throughput Reliable Multicast in Multi-Hop Wireless Mesh Networks. *IEEE Transactions on Mobile Computing*, 14(4):728–741, apr 2015.

[10] G Sankara Rao, E Jagadeeswararao, and N Sai Prathyusha. Application Layer Multicasting Overlay Protocol - NARADA Protocol. *Global Journal of Computer Science and Technology: E Network, Web & Security*, 14(6), 2014.

[11] Ashutosh Singh. *Algorithms for Reliability in Large Scale Structured and Unstructured Peer-to-Peer Overlay Multicast Networks for Live Streaming*. PhD thesis, Indian Institute of Technolgy Kanpur, 2016.

[12] Hwa-Chun Lin, Tsung-Ming Lin, and Cheng-Feng Wu. Constructing application-layer multicast trees for minimum-delay message distribution. *Information Sciences*, 279:433–445, sep 2014.

[13] Daniel Lertpratchya and Douglas M. Blough. Interference-aware multicast trees and meshes for wireless multihop networks. *Ad Hoc Networks*, 47:99–113, sep 2016.

[14] Mohsen Jahanshahi and Alireza Talebi Barmi. Multicast routing protocols in wireless mesh networks: a survey. *Computing*, 96(11):1029–1057, 2014.

[15] Jongtack Kim and Saewoong Bahk. Design of certification authority using secret redistribution and multicast routing in wireless mesh networks. *Computer Networks*, 53(1):98–109, jan 2009.

[16] Rakesh Matam and Somanath Tripathy. Secure Multicast Routing Algorithm for Wireless Mesh Networks. *Journal of Computer Networks and Communications*, 2016:1–11, 2016.

[17] Sonia Fahmy and Minseok Kwon. Characterizing Overlay Multicast Networks and Their Costs. *IEEE/ACM Transactions on Networking*, 15(2):373–386, apr 2007.

[18] Daisuke Mashima, Aidana Serikova, Yao Cheng, and Binbin Chen. Towards quantitative evaluation of privacy protection schemes for electricity usage data sharing. *ICT Express*, 4(1):35 – 41, 2018. SI: CI & Smart Grid Cyber Security.

[19] Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, and Lei Shu. A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustainable Cities and Society*, 38:806 – 835, 2018.

[20] Bin Fan, Dave G. Andersen, Michael Kaminsky, and Michael D. Mitzenmacher. Cuckoo Filter. In *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies - CoNEXT '14*, volume 38, pages 75–88, New York, New York, USA, 2014. ACM Press.

[21] Khalid Mahmood, Shehzad Ashraf Chaudhry, Husnain Naqvi, Taeshik Shon, and Hafiz Farooq Ahmad. A lightweight message authentication scheme for smart grid communications in power sector. *Computers & Electrical Engineering*, 52(Supplement C):114 – 124, 2016.

[22] Elaine B. Barker and Allen L. Roginsky. Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. Technical Report November, National Institute of Standards and Technology, Gaithersburg, MD, nov 2015.

[23] V. Odelu, A. K. Das, M. Wazid, and M. Conti. Provably secure authenticated key agreement scheme for smart grid. *IEEE Transactions on Smart Grid*, 9(3):1900–1910, May 2018.

[24] Lein Harn and Changlu Lin. Efficient group Diffie–Hellman key agreement protocols. *Computers & Electrical Engineering*, 40(6):1972–1980, aug 2014.

[25] C.J.F. Cremers. The Scyther Tool: Verification, falsification, and analysis of security protocols. In *Computer Aided Verification, 20th International Conference, CAV 2008, Princeton, USA, Proc.*, volume 5123/2008 of *Lecture Notes in Computer Science*, pages 414–418. Springer, 2008.

[26] U.S. National Institute of Standards and Technology. Guidelines for Smart Grid Cybersecurity NISTIR 7628 Revision 1. Technical Report September, U.S. National Institute of Standards and Technology, 2014.

[27] U.S. Naval Research. Common Open Research Emulator (CORE). http://www.nrl.navy.mil/itd/ncs/products/core, last accessed on 09/11/17.

[28] Matias Fontanini. libtins - packet crafting and sniffing library, 2017. http://libtins.github.io/, last accessed on 27/11/17.

[29] Y.C. xxHash - Extremely fast non-cryptographic hash algorithm, 2017. http://cyan4973.github.io/xxHash/, last accessed on 09/12/17.