International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 4, August 2019, pp. 2281∼2295
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i4.pp2281-2295

Modified timed efficient stream loss-tolerant authentication to secure power line communication

Boyce Sigweni, Mmoloki Mangwala, Joseph Chuma
Faculty of Engineering and Technology, Botswana International University of Science and Technology
Department of Electrical Computer and Telecommunications Engineering, Botswana

Article Info

Article history:
Received Sep 24, 2018
Revised Mar 8, 2019
Accepted Mar 12, 2019

Keywords:
Load management
Power line communication
Smart meters security
TESLA

ABSTRACT

This paper investigates the feasibility of Timed Efficient Stream Loss-tolerant Authentication to serve security needs of Power Line Communication (PLC) system. PLC network has been identified as the ideal choice to function as the last mile network, deliver load management messages to smart meters. However, there is a need to address the security concerns for load management messages delivered over power line communications. The ubiquitous nature of the power line communication infrastructure exposes load management systems (LMS) deployed over it to a security risk. Ordinarily, PLC network does not employ security measures on which the smart meters and data concentrators can depend on. Therefore, the need to provide a secure mechanism for communication of load management system messages over a PLC network. In LMS, source authentication is of highest priority because we need to respond only to messages from an authenticated source. This is achieved by investigating suitable robust authentication protocols. In this paper we present modifications to Timed Efficient Stream Loss-tolerant Authentication for secure authentication to secure messages for load management over PLC. We show that PLC may be used to securely and effectively deliver Load Management messages to smart meters, with minimal overhead.

Corresponding Author:
Boyce Sigweni,
Botswana International University of Science and Technology,
Private Bag 16, Botswana.
Email: sigwenib@biust.ac.bw

1. INTRODUCTION

The introduction of smart meters enables electricity suppliers to manage electricity demand efficiently, by implementing load management systems (LMS), thus coping with electricity demand. These LMS systems forecast the demand [1, 2, 3] therefore advising on mitigating steps. This demand would be in terms of quantity and quality –which is still increasing by the escalation of new and more electronic devices in homes as population grows. Prior to Smart grids, power suppliers could not sufficiently exploit the advances in communication and information technology to improve the electricity grid's efficiency, reliability, security, and quality of service (QoS). Smart grid addresses all these desired features by modernizing the electricity grid by incorporating of communication technologies [4, 5]. The term "smart grid" has been expanded from just smart meters, to more focused on advanced metering infrastructure (AMI) [6].

Successful implementation of electrical load management system via smart meters requires a secure communication channel which must also be robust to deliver load management commands such as load redistribution, dimming of lights and switching off of hot water geysers. While, the effects of transferring data at high bit rate through the mains network generates acceptable radiated emission regulated by international standards. The increment in speed for New Generation PLC may cause higher levels of emissions that could be mitigated

through the use Time Reversal (TR) technique [7]. In the load management system source authentication is of highest priority because we need to respond only to messages from an authenticated source. Privacy is not a priority for load management messages because they are broadcast to everyone on the network to manage the load. Therefore, there is no need to make load management messages private through encryption, but there is a need to respond only to commands from authentic sources because of possible attacks, such as *denial of service* (DOS) [8] elaborated in title-24 [9]. For example —an attacker could falsify data thereby transmitting wrong commands to smart meters –such as "electricity demand low" therefore users may switch on non-essential gadgets. This could cause overloading that may lead to grid instability or even power outages, thus defeating the sole intended purpose of load management. The scheme we present can be used by any application employed on PLC network to authenticate messages but it is heavily biased towards PLC based load management systems. These are systems that employ data concentrators and smart meters as the two primary components. Figure 1 shows a typical power line communication network for advanced metering infrastructure (AMI).

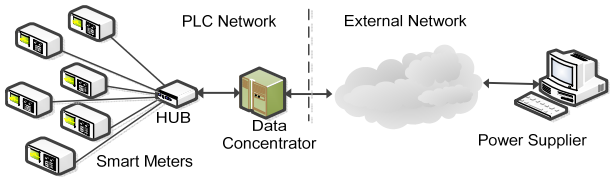

Figure 1. Typical PLC Network [10]

The rest of this paper is organised as follows; In section 2. we discuss PLC channel characteristics, followed by its security threats, risk management methods and mitigation techniques. (Both crypto and non-crypto). Timed Efficient Stream Loss-tolerant Authentication (TESLA) scheme is presented in section 3., followed by research methodology in section 4. Modification to TESLA scheme are outlined in section 4.2. Finally, performance analysis and results are presented in section 5.

2. BACKGROUND

2.1. PLC channel characteristics

In PLC systems, a transmit signal propagating from one location to another suffers from reflections at impedance discontinuities along its path. Branching and impedance appearing at the termination points are the main source of impedance discontinuity in power line networks (PLNs) giving rise to reflections. These mechanisms are illustrated in Figure 2.

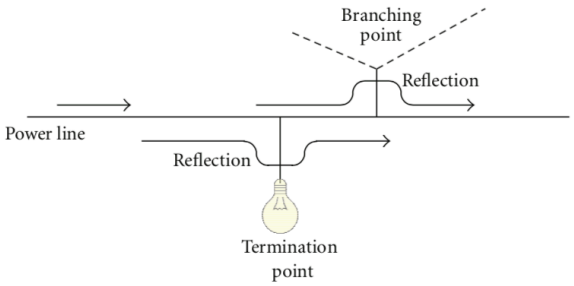

Figure 2. Propagation mechanism for PLC channels [4]

Due to the propagation mechanisms effective in both environments, when a signal is emitted by a transmitter, the signal received at the receiver consists of attenuated, delayed, and phase-shifted replicas of the transmit signal leading to time dispersion. In communications community, significance of time dispersion is quantified by a parameter called root-mean-squared (RMS) delay spread. RMS delay spread for both communication mediums is to be discussed in a more detailed way in the subsequent sections. Besides time dispersion characteristic, both wireless and PLC channels are time selective. Mobility (or relative motion between transmitter and receiver from a broader perspective) is the main reason behind time selectivity of wireless channels, whereas the reason for time selectivity in PLC channels is related to the varying impedance conditions in the

PLN especially at the termination points. Time selectivity is another aspect that the study will focus on. For digital communication systems, the most common figure of merit is the bit error rate (BER) which is directly related to signal-to-noise ratio (SNR). Being a function of SNR, BER can be computed by only having information regarding amplitude statistics of the received signal and the noise characteristics in the communication channel. In this respect, amplitude statistics and the noise characteristics of wireless and PLC channels are among issues that the study has focused on.

Power line communication characteristics such as, frequency-distance-dependent attenuation in low voltage (LV), based on extensive measurements is defined as:

$$A(f,d) = \exp((-a_0 - a_1 f^k)d) \tag{1}$$

where:
f correspond to frequency of the signal,
d is the distance covered by the signal
while a_0, a_1 and k are all cable-dependent parameters extracted by empirical measurements [4, 11]

2.1.1. Multipath characteristics

A complete characterization of the PLC channel can be given by its channel frequency response (CFR) as follows:[4, 11]

$$H(f) = \sum_{i=0}^{N} \left[\prod_{k=1}^{K} \gamma_{ik} \prod_{m=1}^{M} \tau_{im} \right] A(f,d_i) \exp(-j2\pi f \tau_i) \tag{2}$$

given that the total number of replicas received at the receiver is considered to be limited to N [4, 11] .
where:
K and M represent the number of reflection and transmission coefficients
γ correspond to the reflection coefficient along the propagation path,
τ is the transmission coefficient along the propagation path
while $A(f,di)$ corresponds to the frequency and distance-dependent attenuation derived from the physical characteristics of the cable, and $\exp(j2\pi f\tau_i)$ refers to the phase of the *i*th component due to the time delay.

Finally, it is worth mentioning that multiplication of γ's and τ's in (2) is referred as the reflection factor $(|r_i|e^{j\theta_i})$ of a particular propagation path. Note thatτ_i, the time delay, is related to the speed of propagation within the communication medium, power line cables in our consideration as follows:

$$\tau_i = \frac{d_i\sqrt{\epsilon_r}}{c_0} \tag{3}$$

where:
ϵ_r is the dielectric constant of the insulation material
c_0 is the speed of light in vacuum.

The time-and frequency-varying behaviour of a power-line network is the result of variable impedance loads connected to its terminal points. Any signal transmitted through such a network is subject to time-varying multipath fading [12]. In addition to this basic frequency domain-based PLC multipath model, there are other characterization approaches, such as —A matrix-based approach for the calculation of multipath components based upon the presented model in PLC networks is given in [12, 13].

PLC channel models that are based on treating the transmission line as a two-port network are given in [14, 15, 16]. Besides these deterministic models, some statistical PLC channel characterization efforts regarding attenuation, multipath-related parameters, and so forth, that consider the PLN as a black box without dealing with its attributes such as cable characteristics, network topology, and so forth are presented in [17]. Each of these channel modeling approaches has some advantages and disadvantages. For instance, all attributes of the PLN such as the network topology, cable distance-frequency-dependent attenuation characteristics, and termination impedance conditions must all be known prior to computation if a frequency or transmission line theory-based approach is to be adopted. Statistical models can be employed if any information regarding the network attributes cannot be acquired a priori. However, an extensive measurement campaign may be required in order to draw statistically meaningful conclusions from the data sets obtained from various networks with different topologies.

2.2. Security threats

A threat to a Power Line communication system is any malicious occurrence that would have an undesirable effect on the assets and resources associated with the power line communication. Network threats take advantage of the distributed aspects of information transmission [18, 19] and [20]. Amoroso [21] categorized threats to a communication system as follows:

(a) Denial of Service (DoS) threat: The DoS threat arises when access to the power line communication channel is intentionally blocked as a result of malicious actions taken by an attacker. For example, someone could flood the data concentrators with junk commands —therefore preventing load management messages to be delivered to smart meters.
(b) Integrity threat: The integrity threat involves unauthorized change to information stored for example on a smart meter (meter reading for billing purposes) or in transit between the data concentrator and smart meter.
(c) Disclosure Threat: This involves the dissemination of private information. Protection of power line communication system against unintended disclosure.

2.3. Risk management methods

Security risk for PLC based load management programs can be assessed using a risk management approach [9]. This is whereby assets that need protection are identified and their sensitivity to attack analysed. There is a need to identify a possible source, strength and intent of threats, as well as enumerating vulnerabilities and finally determining appropriate mitigation methods. Hence, the need for anomaly detection and monitoring [22].

2.3.1. Potential attacks

Several attack scenarios were considered to determine vulnerabilities, assets and threats. The following are some of the attacks on a load management system [18]:

(a) An attacker could block load reduction commands, therefore preventing the required reduction percentage. Therefore, resulting in forced load shedding or blackouts.
(b) An attacker could broadcast incorrect synchronisation time, which can cause events to occur at wrong times, either earlier or later than scheduled.
(c) An attacker could modify the software set-point for air-conditioning unit in the smart meter so that it appears to be drawing less or no power. This action results in command for load reduction being ignored by the smart meter, therefore the unit is not switched off nor have its power reduced.
(d) An attacker could switch ON all the appliances (heaters, air cons) controlled through the smart meter for load management, causing an unexpected and excessive load, leading to possible blackouts or even grid instability.
(e) In order to annoy the public, an attacker could switch off the air conditioning units or set temperature thermostat to uncomfortable levels.
(f) By flooding the network with multiple requests for time synchronisation, the attacker can cause Denial-of-Service.

In the next subsection we look at non-cryptographic and cryptographic mitigation techniques, so that we can explore ways as to how these potential attacks could be mitigated in PLC load management system.

2.4. Mitigation techniques

The focus tends to be cryptography as the primary defence against attacks when the security of information systems is in question. Due to the unique characteristics, constraints and design of the PLC based load management system, it presents an opportunity to consider several non-cryptographic methods.

2.4.1. Non-cryptographic mitigation techniques

The ideologies involved in non-cryptographic mitigation techniques methods are outlined in [9] and these include:

(a) Depending on prevention (physical barrier around smart meters) as well as detection (temper alert) mechanisms as deterrents. Intrusion detection system that could be employed on the network; consists of receivers placed on strategic locations where they would compare transmitted data with data they are receiving to identify bogus transmitters

(b) Reducing the capability of an attacker by making the system available only at certain times or responds to external commands after some random time. Therefore, if an attacker does something, it will only take effect after some time. Essentially, by that time the breach would have been detected (as discussed in the previous point) and acted upon. The capability of an intruder to do damage could be further reduced by setting the safe set-point for devices if one is changing settings remotely via commands. For example one cannot set the temperature to unsafe levels (too low or too high) remotely.

(c) Preventing messages that will result in load increase to be sent remotely, that is, the system must not be able to send commands to smart meters to switch appliances on. If appliances have been remotely switched off, the customer could manually switch them on, or have appliances fitted with a device that is set to check the smart meters' mode. If the demand is low, they could automatically switch on. Note that this would be a one way communication as the smart meter would not communicate or control these devices, the smart meter can only switch off the appliance but cannot turn it on or instruct the device to turn the appliance on.

2.4.2. Cryptographic mitigation techniques

There are many cryptographic mitigation techniques available to secure PLC for smart meters. These include Distributed Network Protocol (DNP3) [23], [24], X.509 [25], RSA [26], and TESLA [27]. All these techniques have different capabilities and limitations. For example; digitally signing each packet using X.509 provides proficient data source authentication. Unfortunately, it incurs a high overhead in terms of time needed to sign and verify and also in terms of required bandwidth. Signature verification through X.509 is computationally costly. Therefore, smart meters with their modest computation capabilities would be overwhelmed trying to verify the signatures. For example, if an attacker floods the network with fake packets containing theoretically a robust signature. These are some of the reasons X.509 may not ne suitable for the system.

Security provided by X.509 is also not completely infallible. Some researchers have exploited some of its weaknesses, e.g. [26] demonstrated that two certificates containing identical signatures can be constructed using a collision attack on the MD5 hash function.

Distributed Network Protocol (DNP) secure authentication may not be suitable for securing communication over PLC for smart meters due to its key management and specialisation even though it may be used on smart grid [28]. Ortega et al proposed for the DNP3 over TCP/IP for smart grid application. This is not feasible for PLC due the following: DNP Session Key is periodically changed and used to calculate the HMACs. The Update key occupies the second level and is used for encryption of the Session key before it is sent to the remote device. For load management on PLC, DNP would place a large processing overhead[29]. Another drawback of DNP Secure Authentication if it is used on PLC network to authenticate load management messages between smart meters and data concentrators, is that when Update keys are compromised or corrupted, or if the custodian of the key leaves the organisation, the power supplier has no choice but to dispatch personnel to the remote devices to change the Update key. Thousands or even millions of smart meters are connected on the grid, therefore pending remote download of Update Keys, practical systems are restricted to perhaps hundreds of devices. DNP Secure Authentication utilises 16-bit values for addresses and user numbers, thus presenting a scalability challenge. Challenge-Handshake Authentication Protocol (CHAP) in a smart grid system that includes smart meters is not feasible [30].

In the next section we therefore present TESLA as the most effective scheme that may be employed to efficiently secure PLC for load management. TESLA in its modified form can authenticate packets immediately and due to its low computational and per-packet communication overhead.

3. TIMED EFFICIENT STREAM LOSS-TOLERANT AUTHENTICATION (TESLA)

TESLA is widely used to authenticate broadcast messages [31, 32], such as DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things [33]. We first present an overview of TESLA by outlining properties that make TESLA suitable for securing PLC for load management systems. We then discuss threat model and security guarantee and the modification to TESLA needed to secure load management through PLC. These modifications include, using indirect time synchronisation for loose time synchronisation to combat the DoS threat and instantaneous authentication to prevent delay. We selected TESLA for securing PLC for load management based on its following properties:

Low per-packet communication overhead: The calculation of MAC utilises the n_m parameter [27], which is the length of the truncated output of the function. The n_m values depend on the MAC function

selected, hence, per-packet communication overhead can be as low as 80 bits.

Low computation overhead: The primary reason for the use of smart meters is to save electricity. Smart meters have limited or low processing power which saves electricity. Hence, TESLA is ideal because of its authentication protocol, which is not power hungry. It involves one hash computation done on the message and one MAC function computation done on the key and message per packet. Therefore, TESLA requires minimal computational effort, therefore can be managed by smart meters and data concentrators.

No receiver-side buffering: Every packet will be authenticated as soon as it arrives at the receiver; therefore, there is no need for packet buffering at the receiver. Packet loss tolerance: All packets received within their time interval will be authenticated even if the preceding packet was lost.

Superior assurance of authenticity: Providing the cryptographic and timing assumptions are enforced as the receiver has a high pledge of authenticity, therefore, the system provides a formidable authenticity.

Scalability: There are no acknowledgements after the initial set-up connection has been established, therefore, during normal communication data flows only from the sender to the receiver. This entails that the sender's authentication overhead is not dependent on the number of receivers; making the scheme very scalable. For instance it will allow one data concentrator to communicate with many smart meters as per the current set-up for load management were one data concentrator can have over 1000 smart meters connected to it [34].

3.1. Threat model and security assurance

Smart meters are installed in customer homes, therefore, the owners have unlimited access to smart meter in the privacy of their homes. In addition, customers also have unrestricted access to the PLC channel through power points in their houses where they plug their appliances. We present a modified TESLA that is secure against a formidable adversary who by virtue of being able to access the channel and device has the following capabilities:

(a) The challenger has a right to use to a fast network with insignificant delay.

(b) The challenger can listen in, capture, retransmit, drop, hold-up, and modify packets thereby having full control over the PLC channel.

(c) The challenger's computational resources may be very formidable, but not unbounded. In particular, this means that the adversary can perform efficient computations, such as computing a reasonable number of pseudo-random function applications and MACs with negligible delay. Nonetheless, the adversary cannot invert a pseudo-random function (or distinguish it from a random function) with non-negligible probability.

3.1.1. Security assurance

The security assurance with this modified TESLA scheme is that the receiver should not accept any message M_j as authentic except for when M_j was sent by the alleged sender. This security assurance includes protection against message duplication through message numbering and time-stamping and we also address denial-of-service (DoS) attacks.

4. RESEARCH METHODOLOGY

4.1. Repeated measures design

We used repeated design measures for this study because of —Reduction in the variance of results. This allows statistical inference to be made with fewer runs and many experiments can be completed more quickly, as fewer cases need to be trained to complete an entire experiment. This enables us to monitor how message size change over time for both requests and response messages.

Straw-man reference design for demand response information exchange [35] is used to present a guide to how security is provided through implementation of the proposed authentication protocol, in the enabling services layer of the load management infrastructure. The message is sent down the stack to the security layer which performs a hash computation on the message and key and then sends the hashed message over the PLC network [36]. When the security layer at the receiver receives the hashed message from the PLC and authenticates it using disclosed key or MAC (i.e. HMAC-MD5). If authentication is successful the message is sent up to the application layer otherwise it is discarded.

The next subsection show who modification are made on TESLA for PLC security.

4.2. TESLA modification for PLC

The original TESLA is modified in several ways to make it efficient and practically suitable for PLC network for Load Management via use of Data concentrators and smart meters. Smart meters are connected to the data concentrator from different distances because some houses are close to the distribution transformer while others are quite a distance away. Therefore, the first modification is the use of the authentication chains with different disclosure delays to cater for the different distances of the smart meters from the data concentrator. Secondly, we present the technique to support Instantaneous Authentication, implying that the receiver would be able to authenticate a packet immediately upon arrival without delay. A data concentrator can be connected to many smart meters. For example, Echelon NES data concentrator [34] can connect over 1000 smart meters, and over 4000 other devices. Therefore, there is the a need for modifications to address the scalability issue and vulnerability, both due to time synchronisation protocol.

In the next sub-sections, the issue of smart meters being at different distances away from the data concentrator resulting in different network delays is addressed by employing a space optimisation method whereby the data concentrator uses several TESLA instances for one stream. To successfully address this issue we have to look into time synchronisation and attend to the key management techniques as well as address the vulnerability that could rise from use of these methods and techniques and how to eradicate or minimise them.

4.2.1. Optimal Disclosure Delay and Time Interval Parameters

The following parameters must be determined by the sender for optimal performance as per the requirements of PLC based load management. These parameters are (T_{int}), the interval duration which usually ranges from 100 milliseconds to 1 second expressed in milliseconds and the key disclosure delay (d_d) which is the waiting time before the key is disclosed. A good choice of T_{int} and d_d is essential for the efficiency of the scheme. For example, if the product of T_{int} and d_d is too large, it causes an excessive delay in the process of authentication, and when it is too low, it will deny most receivers the opportunity to verify packets. The parameters T_{int} and d_d must not be altered throughout the duration of a session to prevent introduction of vulnerabilities.

4.2.2. Optimal Time Interval

To determine the optimal time interval duration, the sender would divide the time into standardised intervals of duration T_{int}. The numbering for the time interval starts at 0 and incremented successively. An unsigned 32-bit integer is used to store the interval index. Therefore, the wrapping to 0 can only take place after 2^{32} intervals thus making the system to be very scalable. For example, if: $T_{int} = 0.5$ seconds, then the wrapping will only happen after $0.5 \times 2^{32} = 2147483648s$, which translates to approximately just over 68 years before wrapping to 0 can take place [27].

4.2.3. Optimal Disclosure Delay

To determine the optimal disclosure delay involves a trade-off. This is because smart meters that are close to the data concentrator have low network delay, hence, demand short key disclosure delays because it results in short authentication delays. Unfortunately, using a short key disclosure delay means that smart meters that are far from the data concentrator (with long network delay) will not be accommodated because most of their packets will arrive outside the set period hence violating the set security condition. Therefore, they will be discarded without authentication. Employing a long key disclosure delay will result in unnecessary delay in authentication for smart meters close to the data concentrator. It is important to note that the security aspect of the system is not affected whether long or short key disclosure delay is used. This is mainly a performance factor, and performance is very important for effective Load Management. How the system will perform depends heavily on the choice of the key disclosure delay. We illustrate how to determine a key disclosure delay (d_d) for a system using indirect time synchronisation. We do that by proving that if the round trip time (R_{tt}) is a sufficient upper bound time between the smart meter and data concentrator, then the optimal choice for d_d is as follows;

$$d_d = \left\lceil \frac{D_{SR} + \varepsilon}{T_{int}} \right\rceil + 1 \tag{4}$$

where:

T_{int} is the duration of the interval,

D_{SR} is a sufficient upper bound on network delay for packets traversing from sender

to receiver
and ε Time synchronisation error sum for both sender to receiver

To derive the disclosure delay we first have to make sure it does not make packets to violate the security conditions. We take into account a packet P_j created in the time interval I_i and the key will be disclosed d_d time intervals later, when the packet P_j at the receiver its local time is given as equal to l_{TR}, thus the security condition is that:

$$d_d > \left\lfloor \frac{l_{TR} + \Delta - T_n}{T_{int}} \right\rfloor - I_i \tag{5}$$

where:
T_{int} is the duration of the interval,
T_n is the beginning of the *n*th time interval
and Δ Time synchronisation error sum (full round-trip time).

We use the assumption the packet P_j was sent when the senders' local time was l_{TS}, hence:
$l_{TS} < T_{int} = (I_i \times T_{int}) + T_n + T_{int}$, therefore the round trip time $R_{tt} = D_{SR} + D_{RS}$, with D_{RS} denoting the network delay from the receiver to the sender. Using the derivation from Perrig *et. al.* [37] referring to Figure 3, Resulting in eqn $D_{SR} \cong l_{SR} + \delta - l_{TS}$. Finally we have a tight bound for d_d satisfying equation 4 and this d_d affords most packets the opportunity to meet the set security condition and the receiver would not have to wait longer than necessary before authenticating the packets.

The optimal d_d does not solve the issue that smart meters are at different distances away from the data concentrator. It is just the best time for meters at one particular distance. To address this issue, one approach would be to use multiple TESLA instances and treat them independently each with its own key, hence d_d. Unfortunately this approach results in unmanageable communication overhead because of this multiple keys for each instance. In the next section we present an optimisation that reduces the space overhead of multiple instances by using the same key chain with a different key schedule for all instances [27].

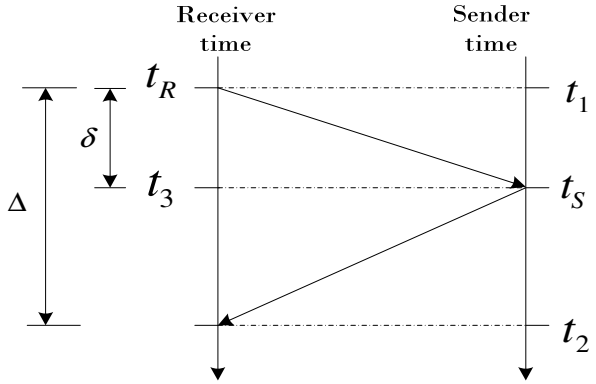

Figure 3. Receiver and Sender delays [37]

4.2.4. Multiple concurrent TESLA instances

The core idea for this technique is to make use of the same key but a different schedule for all instances as an alternative to utilising one self-determining key chain for each instance. It works as follows; all instances for a stream share the same key chain and the same time interval period. That is each time interval I_i, is associated with the corresponding key K_i, in the provided key chain. Therefore, we can expect K_i to be revealed in the time interval I_i. Figure 4 depicts an example of how multiple instances could be arranged to be used for concurrent TESLA instances. In this case there are two TESLA instances, having a key disclosure time of one interval and the other five intervals [27].
In Figure 4 the bottom row of keys shows the key revealing plan. It shows which key is revealed at which time interval. The top and middle rows of key show the key schedule of the two instances, the latter being the first instance while the former being the second instance. Following this method, the sender needs only to disclose

one key chain inspite of how many instances are used concurrently. This technique allows space saving. For example, if each key is 16 bytes long, then for a stream with n concurrent instances, this method will conserve 16(n - 1) bytes per packet and for small packets such as the ones used for PLC Load Management. This is a significant saving. Using concurrent instances also helps in achieving scalability. One issue to consider is the vulnerability of the TESLA due to the mechanism employed for the key chain reconstruction at the receiver. First, the receiver must check if the key chain arrived within the stipulated time interval. If that time has expired then the packet is discarded else the receiver will try to verify the key revealed in the packet by putting into operation the pseudo-random function until the very last committed key chain value. This operation can be exploited by an attacker who would timestamp their packet with a time far in the future. Therefore, when the receiver checks if the time has expired it will find that the time is still valid and therefore attempts to verify the key, preventing it from verifying the legitimate packets. That results in denial of service for deserving packets. A novel approach to deal with this is to have lower and upper time limits for packets so that if a packet is sent with future timestamp it is dropped [27].

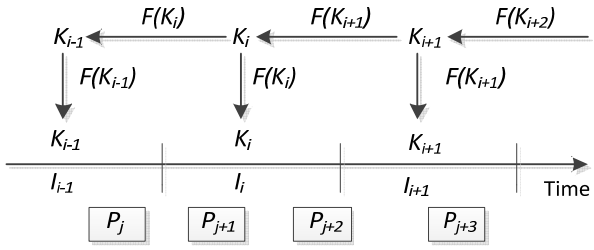

Figure 4. Receiver and Sender key delays [37]

4.3. PLC TESLA instantaneous authentication

Basic TESLA requires the receiver to buffer packets before they can be authenticated. This is because the sender sends the key required for authentication at a later stage. This delayed authentication is not suitable for Load Management because monitoring and control command actions need to be carried out in real-time. For example, if the grid is experiencing some instability, the information must be relayed immediately to the control centre without delay. Also, if the load exceeds supply and needs to switch off non-critical but high power consuming devices such as heaters, that action must happen immediately without delay or there will be the risk of power outages while waiting for the command to switch off devices to be authenticated.

This delayed authentication also causes storage problems, requiring data concentrators and smart meters to have large memories to store these packets while they are waiting to be authenticated. The other disadvantage of this delayed authentication is that it makes the system to be vulnerable to Denial-of-Service attack. It is because of the reasons above that modifications to the original TESLA are required so that packets can be authenticated instantaneously upon arrival with no delay. Therefore, this eliminates the need for buffering at the receiver side, thus reducing the risk of DoS attack where the attacker floods the receiver with spurious packets. As it would be seen later in this section, this modification comes at a cost of at least one extra hash per packet and the need for buffering at the sender side. This is acceptable since it does not induce the risk of DoS (by flooding), or introduce significant delay.

In this method, sender buffering replaces receiver buffering. The sender buffers packets during one disclosure delay so that it can put the hash value of the data of the next packet in an earlier packet. Therefore, the instant the earlier packet is authenticated the next packet will be authenticated as soon as it arrives at the receiver through its hash value that was contained in the earlier packet thus achieving instant authentication with no more delays. To simplify the illustration of how this is achieved, we assume that the sender will send out a constant number n of packets per time interval.

Figure 5 shows how a packet for the message segment M_j in the interval T_j is constructed. The hash value of the next message M_{j+vd} is appended to the current message, that is $H(M_{j+vd})$ is appended to M_j. The sender then calculates the MAC value over the key K_i together with $H(M_{j+vd})$ to get $MAC(K_i, D_j)$ where $D_j = H(M_{j+vd})||M_j$ (note that $||$ means that messages are concatenated).

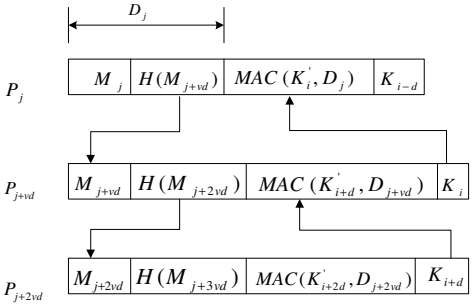

Figure 5. Instantaneous Packet Authentication[36]

With reference to Figure 5, the technique for instantaneous authentication for the packet P_{j+vd} is as follows; P_j incorporates a hash of the data M_{j+vd} and this data is in P_{j+vd} and if P_j has been authenticated it implies that $H(M_{j+vd})$ is also authentic. Therefore, the message M_{j+vd} is authenticated immediately, hence using the same technique. The next packet P_{j+2vd} would also be authenticated immediately, so will the next packet. If a packet is lost or discarded then the next packet would not be authenticated immediately but would be authenticated later through its MAC value. For example, if P_j was lost or discarded, then P_{j+vd}would not be authenticated immediately but will be authenticated as soon as the next packet P_{j+2vd} arrives. . It will be authenticated through its MAC value because upon arrival packets disclose the key of the previous packet, therefore P_{j+2vd} would disclose the key K_{i+d} which was used for P_{j+vd} MAC value, therefore P_{j+vd} would then be authenticated. Delayed authentication can be easily be overcome by incorporating hashes of multiple future messages. This can easily be done in PLC Load Management because all the messages and their sequence of transmission is known. This is a technique similar to Efficient Multi-chained Stream Signature (EMSS) [38], and the introduced message overhead is negligible. Using multiple hashes eliminates the need to send packets at a constant rate which is difficult in a hostile environment like PLC.

4.3.1. Indirect time synchronisation for load management via PLC

Complicated time synchronisation protocols are available but they require considerable management overhead, these are protocols such as the Network Time Protocol (NTP) [39], which have a high complexity and attain properties electrical load management via PLC do not involve. Loose time synchronisation is an essential component in TESLA but also a security Achilles' heel, due to the mechanism for time synchronisation which makes the system vulnerable to DoS through network flooding with requests for synchronisation. It is for this reason that we present a modified TESLA time synchronisation protocol that is simple and yet secure, that will meet the modest requirements of Load Management via smart metering through a PLC channel.

The sender (data concentrator) and each receiver (smart meter) must synchronise independently securely through an external time reference, when Indirect Time Synchronisation (ITS) is used. To achieve this synchronisation several options are available:

(a) Senders and receivers could synchronise via NTPv3, NTPv4 (Network Time Protocol version3 /4) [39] or SNTPv4 (Simple Network Time Protocol version 4) hierarchy of servers [40]. Unfortunately, this cannot be adopted for synchronisation of smart meters and data concentrators because for load management via PLC the gateway for smart meters is the data concentrator; therefore, smart meters cannot have an independent path direct to the servers.

(b) The second option which would guarantee direct access for both sender and receiver to external time reference would be for the sender and receiver to synchronise via a GPS system or any similar device that can provide a high precision time reference. Unfortunately, spoofing attacks on the GPS system have been reported [41] therefore the level of security required for PLC load management cannot be guaranteed when synchronisation is achieved through GPS.

(c) The other option, we adopt for PLC based load management system is whereby a dedicated hardware is embedded in each receiver and the sender that provides a clock that has a time-drift that is negligible in-terms of the time accuracy requirement for TESLA. To deal with this insignificant clock drift anyway, the device makes it possible for the sender and receiver to have their embedded clock to be synchronised with the official time reference periodically. This can be done during equipment servicing interval or after a period of known maximum allowed clock drift and thereafter left to be autonomous. That is, the device would continuously consult its internal clock which has minimal clock drift.

One aspect is that scalability is a requirement for a PLC based load management system and it is for this reason that we chose specialised hardware based synchronisation because it would easily meet that requirement since synchronisation will not depend on the number of devices connected together and no delay or bandwidth will be used for synchronisation [27].

4.3.2. Calculation of Delay Bound

This delay bound calculation is based on the assumption that the synchronisation has already been established using the mechanism discussed in the previous section; therefore, the sender and the receivers have a single time reference. The sender computes D_{ST} (delay sender time), that is the upper bound of the delay of the senders' clock with respect to the agreed time reference. During the bootstrapping the D_{ST} value is sent to the receivers; therefore, the D_{ST} must not be altered throughout the duration of a session. Correspondingly, the receiver calculates D_{RT} (delay receiver time), that is the upper bound of the delay of the receivers' clock with respect to the agreed time reference, with respect to the clock of the sender, the overall upper bound of the delay of the receiver is $D_{OT} = D_{ST} + D_{RT}$.

4.3.3. Resistance to Denial of Service attack

Due to the modifications we adopted for TESLA, our scheme is robust against DoS attacks as will be seen in the next section where we investigate DoS attack against sender, receiver and the key chain. We show how our modifications make the scheme to be resistant to these attacks [38].

4.3.4. DoS attack on the Sender

Our modified TESLA scheme uses indirect time synchronisation; therefore, a DoS attack on the sender is not possible because the sender does not receive anything and does not perform any per-receiver operations.

4.3.5. DoS attack on the Receiver

Our scheme is robust against DoS because the receiver does not have to buffer packets before authentication because they can be authenticated immediately upon arrival. If it is not possible for them to be buffered, a bogus packet will be discarded immediately, where one with a compromised (correct) key will be buffered until the correct packet comes and is authenticated and then all other packets discarded for that time interval. This is only possible if the buffer size is large enough another option would be to randomly replace packets with new ones as they arrive. Fortunately, this flooding attack can last only one interval time duration and the mechanism for detecting intrusion (sub section 2.4.) would pick the bogus traffic and it would be dealt with before it could cause any noticeable disruption to performance and service.

4.3.6. DoS attack on the Key Chain

The default method of key chain construction makes the system to be vulnerable. A novel approach to deal with this is to have lower and upper time limits for packets so that if a packet was sent from the future is dropped (timestamp); just applying the limits makes the system robust against DoS attack [38].
The security provided by the TESLA is sufficient for securing load management messages in recognition of the security proof as provided by [38]. We presented modifications that included, optimal disclosure delay and time interval parameters, multiple concurrent TESLA instances, PLC TESLA instantaneous authentication, indirect time synchronisation for load management via PLC, calculation of delay bound. These modifications provide resistance to a denial of service attack on the sender, the receiver, and on the key chain construction. It also provides immediate authentication for critical emergency load management.

5. PERFORMANCE ANALYSIS AND RESULTS

5.1. TESLA performance results

In this section we compare the relative performance of various security hashing options available for source authentication by TESLA. To perform this tests, we use Microsoft Application Centre Test (ACT). ACT allows us to build realist scenarios where the same method can be called many times with input parameters randomised. The other useful aspect of ACT is its ability to record results which would then be used to measure performance. Our focus is on hashing algorithms; MD5, HMACSHA1, HMACMD5 and HMACSHA512. Hash algorithms plot a piece of data of random size to a small exclusive value of fixed length. We will compare the MD5, HMAC-SHA1, HMAC-MD5and HMACSHA512 algorithms. The performance of the sender is

analysed independently from the receiver because their tasks are different. We first present the results from performance analysis of the sender then the receiver.

5.1.1. Sender performance

The key chain is pre-computed, therefore, for each packet to be sent, the sender only has to compute one HMAC for each packet per authentication chain. For the sender we look at the performance of MD5, HMACSHA1 and HMACMD5 functions provided by [42].

We analyse the performance of our scheme by getting the number of packets per second that the sender can generate using each of the hash functions against different message block sizes and the performance results are displayed in Figure 6.

We also analyse the performance of the system when a different number of authentication key chains are used against the different packet sizes. The results are shown in Figure 7. The results show that as the block size increase the number of operations per second decrease. Figure 6 show that even with the largest block size 1024 (tested) the sender can carry out about $0.25x10^5$ operations for all the HASH functions. This is more than sufficient for a smart meter since all it has functions in our regard is send messages with minimal computation required. Figure 7 shows that for the largest size the sender can send $1.25x10^4$ packets per second of which is sufficient to send a single command.

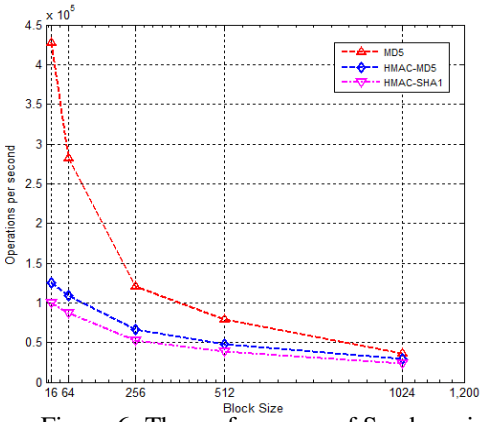

Figure 6. The performance of Sender using different hash functions against block size [36]

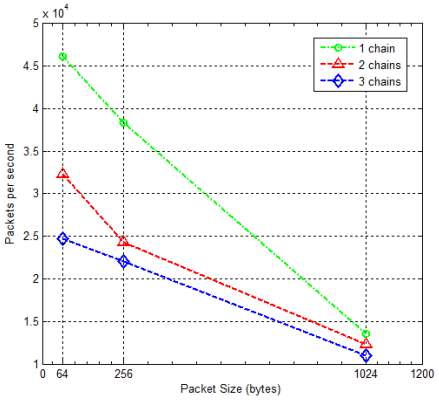

Figure 7. Performance of our scheme for a varying number of authentication chains [36]

5.1.2. Receiver performance

We analyse the performance of the receiver by counting the number of packets it can authenticate per second. This is slightly a longer process in terms of time when compared with the sender because besides to computing the hash it also has to extract the key and then compare the hashes. We also check how long it takes to process a request to determine if the packet is authentic or not (Response Time). For our analysis we used different packet sizes and the function we employed are MD5, HMACSHA1, HMACMD5 and HMACSHA512. It was important to include HMACSHA512 because it has a longer hash. The longer the hash the higher the security but we wanted to know at what cost this improved security would be achieved terms of performance.

We analyse the performance of our scheme by getting the number of packets per second that the receiver can authenticate using each of the hash functions as the load is increased and the performance results are displayed in Figures 8 and 9. This important because we wanted to see the effect of increasing the number of smart meters on the ability of the data concentrator to authenticate their messages within a given period of time. The first test performed used data size 8 Kb while the second test used 256 Kb; we used different data sizes to see how the data size impacts on the performance of the system. When data size is 8 Kb, all algorithms have similar performance as shown in Figures 8 and 9 respectively. Individually it is as follows; SHA512 performance's less in terms of request per second and response time. SHA1 produces a hash of size 160 bits and its computation process is based on MD5. MD5's hash has 128 bits, while SHA512 has 512 bits. The performance difference in the algorithms increases as data size is increased from 8 Kb to 256 Kb as shown in Figure 10. With the load at 5% MD5 is about 45% better than HMACSHA1 and HMACMD5. The performance of HMACSHA512 becomes degraded as the data size increases, becoming about 50% of

HMACSHA1 and HMACMD5, it also takes longer to respond as depict in Figure 11. The longer the hash size, the harder it is to attack it using brute force. This means that even if the performance of HMACSHA512 is low, it would be harder to attack than the other algorithms.

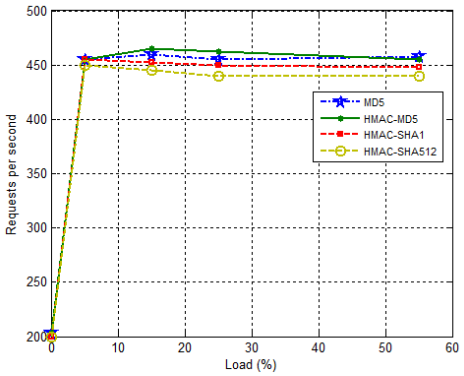

Figure 8. Performance of Hash algorithms (8 KB) Requests per Second [36]

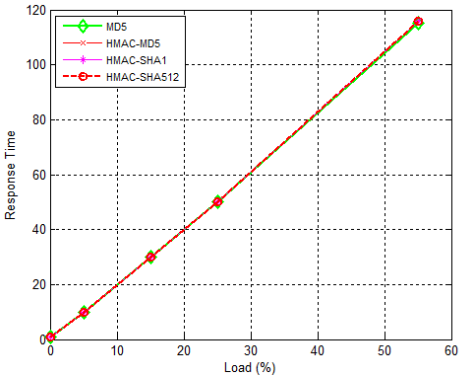

Figure 9. Performance of Hash algorithms (8 KB) response [36]

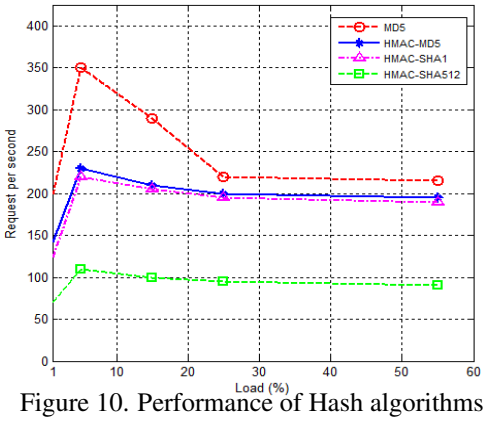

Figure 10. Performance of Hash algorithms (256 KB) Requests per Second [36]

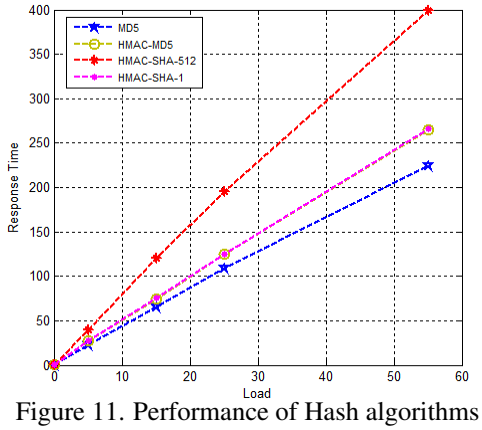

Figure 11. Performance of Hash algorithms (256 KB) response time[36]

6. CONCLUSION

The security provided by the TESLA is adequate for securing load management messages. However, our simulation also verifies that by using various message sizes and hash functions that the system can cope with the number of smart meters per data concentrator. A typical load message size is about 20 bytes but the message size that we concentrate on, in our simulation is 32 bytes (256 kb). This is because we have taken into consideration the fact that in addition to the normal message size, we have now introduced addressing and security components. Using a message size of 256 Kb from our simulations and the selected hash function, the sender can perform a maximum of 120772 and a minimum of 52700 operations per second. Therefore, this should be sufficient because for our modest data concentrator we only need about 1000 operations per second limited by the number of smart meters that can be connected to the data concentrator [34]. The performance at the receiver shows that the data concentrator can authenticate all the messages from the smart meters in the required time, peaking to 350 and evening out to just above 200. Therefore, within five seconds at least 1750 messages would have been authenticated. Messages from smart meters are not as urgent as messages from the data concentrator. Therefore, a few seconds delay on their part would not affect the performance of the system or the bit rate [43].

ACKNOWLEDGEMENT

The authors gratefully acknowledge the contributions of Prof. Bakhe Nleya.

REFERENCES

[1] Y. Tanoto, W. Ongsakul, and C. O. Marpaung, "Levenberg-marquardt recurrent networks for long-term electricity peak load forecasting," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 9, no. 2, pp. 257–266, 2013.

[2] N. Ranjbar, S. A. Zaki, N. M. Yusoff, F. Yakub, and A. Hagishima, "Short-term measurements of household electricity demand during hot weather in kuala lumpur," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 3, 2017.

[3] P. Bunnoon, "Electricity peak load demand using de-noising wavelet transform integrated with neural network methods," *International Journal of Electrical and Computer Engineering*, vol. 6, no. 1, p. 12, 2016.

[4] S. Güzelgöz, H. Arslan, A. Islam, and A. Domijan, "A review of wireless and plc propagation channel characteristics for smart grid environments," *Journal of Electrical and Computer Engineering*, vol. 2011, p. 15, 2011.

[5] J. S. Vardakas, N. Zorba, and C. V. Verikoukis, "A survey on demand response programs in smart grids: Pricing methods and optimization algorithms," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 152–178, 2015.

[6] H. Tai and E. Hogain, "Behind the buzz [in my view]," *IEEE Power and Energy Magazine*, vol. 7, no. 2, pp. 96–92, 2009.

[7] A. Mescco, P. Pagani, M. Ney, and A. Zeddam, "Radiation mitigation for power line communications using time reversal," *Journal of electrical and computer engineering*, vol. 2013, p. 2, 2013.

[8] Y. Zhao, H. Liu, and Y. Feng, "An algorithm of traffic perception of ddos attacks against soa based on time united conditional entropy," *Journal of Electrical and Computer Engineering*, vol. 2016, 2016.

[9] E. W. Gunther, "Reference design for programmable communicating thermostats compliant with title 24-2008." California Public Utilities, March 26 2007. [Online]. Available: osgug.ucaiug.org/sgsystems

[10] B. Sigweni and M. Mangwala, "An effective addressing scheme for smart meter targeting," *International Journal of Electrical Energy*, vol. 2, no. 3, pp. 249–253, September 2014.

[11] M. Zimmermann and K. Dostert, "A multipath model for the powerline channel," *IEEE Transactions on communications*, vol. 50, no. 4, pp. 553–559, 2002.

[12] D. Anastasiadou and T. Antonakopoulos, "Multipath characterization of indoor power-line networks," *IEEE Transactions on Power Delivery*, vol. 20, no. 1, pp. 90–99, 2005.

[13] X. Ding and J. Meng, "Channel estimation and simulation of an indoor power-line network via a recursive time-domain solution," *IEEE Transactions on Power Delivery*, vol. 24, no. 1, pp. 144–152, 2009.

[14] T. Sartenaer and P. Delogne, "Deterministic modeling of the (shielded) outdoor power line channel based on the multiconductor transmission line equations," *IEEE Journal on Selected areas in Communications*, vol. 24, no. 7, pp. 1277–1291, 2006.

[15] S. Galli and T. Banwell, "A novel approach to the modeling of the indoor power line channel-part ii: Transfer function and its properties," *IEEE Transactions on Power Delivery*, vol. 20, no. 3, pp. 1869–1878, 2005.

[16] H. Meng, S. Chen, Y. Guan, C. Law, P. So, E. Gunawan, and T. Lie, "Modeling of transfer characteristics for the broadband power line communication channel," *IEEE Transactions on power delivery*, vol. 19, no. 3, pp. 1057–1064, 2004.

[17] M. Tlich, A. Zeddam, F. Moulin, and F. Gauthier, "Indoor power-line communications channel characterization up to 100 mhz—part ii: Time-frequency analysis," *IEEE transactions on power delivery*, vol. 23, no. 3, pp. 1402–1409, 2008.

[18] R. Gustavsson, "Security issues and power line communication," in *the Proceedings of the 5th International Symposium on Power-Line Communications and its Application (ISPLC)*, 2001.

[19] V. Paruchuri, A. Durresi, and M. Ramesh, "Securing powerline communications," in *Power Line Communications and Its Applications, 2008. ISPLC 2008. IEEE International Symposium on*. IEEE, 2008, pp. 64–69.

[20] K. Bhat, V. Sundarraj, S. Sinha, and A. Kaul, "Ieee cyber security for the smart grid," 2013.

[21] E. G. Amoroso, *Fundamentals of computer security technology*. Prentice-Hall, Inc., 1994.

[22] M. Vadursi, A. Ceccarelli, E. P. Duarte, and A. Mahanti, "System and network security: anomaly detection and monitoring," *Journal of Electrical and Computer Engineering*, vol. 2016, 2016.

[23] E. Gunther, "DNP Secure Authentication - Essential to Smart Grid Progress - SmartGridNews," Nov.

2008. [Online]. Available: http://www.smartgridnews.com/story/dnp-secure-authentication-essential-smart-grid-progress/2008-11-18

[24] M. Kgwadi and T. Kunz, "Securing rds broadcast messages for smart grid applications," *International Journal of Autonomous and Adaptive Communications Systems*, vol. 4, no. 4, pp. 412–426, 2011.

[25] A. Lenstra and B. De Weger, "On the possibility of constructing meaningful hash collisions for public keys," in *Information Security and Privacy*. Springer, 2005, pp. 267–279.

[26] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 26, no. 1, pp. 96–99, 1983.

[27] V. Roca, A. Francillon, and S. Faurite, "Use of timed efficient stream loss-tolerant authentication (tesla) in the asynchronous layered coding (alc) and nack-oriented reliable multicast (norm) protocols," Tech. Rep., 2010.

[28] A. Ortega, A. A. Shinoda, C. M. Schweitzer, F. Granelli, A. V. Ortega, and F. Bonvecchio, "Proposal dnp3 protocol simulation on ns-2 in ieee 802.11 g wireless network ad hoc over tcp/ip in smart grid applications," in *Innovative Smart Grid Technologies Latin America (ISGT LATAM), 2015 IEEE PES*. IEEE, 2015, pp. 635–640.

[29] NTA8130, "Netherlands technical agreement nta 8130 (e) minimum set of functions for metering of electricity, gas and thermal energy for domestic customers," KEMA Consulting, Tech. Rep. NTA8130, April 2008.

[30] T. Mander, H. Cheung, A. Hamlyn, and R. Cheung, "Communication security architecture for smart distribution system operations," in *Electrical Power Conference, 2007. EPC 2007. IEEE Canada*. IEEE, 2007, pp. 411–416.

[31] G. Caparra, S. Sturaro, N. Laurenti, and C. Wullems, "Evaluating the security of one-way key chains in tesla-based gnss navigation message authentication schemes," in *2016 International Conference on Localization and GNSS (ICL-GNSS)*, June 2016, pp. 1–6.

[32] X. Lin and R. Lu, *TESLA-based Broadcast Authentication*. Wiley-IEEE Press, 2015, pp. 216–. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7160611

[33] N. Ruan and Y. Hori, "Dos attack-tolerant tesla-based broadcast authentication protocol in internet of things," in *Mobile and Wireless Networking (iCOST), 2012 International Conference on Selected Topics in*. IEEE, 2012, pp. 60–65.

[34] Echelon, "Dcn 1000 series data concentrator," Echelon, Tech. Rep. P/N 003-0507-01D, April 2013. [Online]. Available: http://www.echelon.com/metering/datasheets/dataConcentrator.pdf

[35] E. Gunther, "A strawman reference design for demand response information exchange," EnerNex Corporation for California Energy Commission, Tech. Rep., October 2004. [Online]. Available: http://uc-ciee.org/enabling-technologies/5/12/103/nested

[36] B. Sigweni, "Power line communication network security for advanced metering infrastructure," Master's thesis, University of NorthWest, 2011.

[37] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, 2005.

[38] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*. IEEE, 2000, pp. 56–73.

[39] D. Mills, "Network time protocol (version 3) specification, implementation and analysis," March 1992.

[40] D. L. Mills, "Simple network time protocol (sntp) version 4 for ipv4, ipv6 and osi," 2006.

[41] P. Ganapati, "Researchers demonstrate how to spoof gps devices," 2008. [Online]. Available: http://www.wired.com/2008/09/researchers-dup/

[42] MSDN, "System Security Cryptography Namespace," 2015. [Online]. Available: https://msdn.microsoft.com/en-us/library/system.security.cryptography

[43] A. Maiga, J.-Y. Baudais, and J.-F. Hélard, "Bit rate optimization with mmse detector for multicast lp-ofdm systems," *Journal of Electrical and Computer Engineering*, vol. 2012, p. 4, 2012.