Secure Remote Access to Devices in a Smart Grid

Eric McCary[1]
[1]Department of Computer Science, The University of Alabama
Tuscaloosa, Alabama, 35401, US

Abstract

Seamless and efficient access to remote devices is imperative in the network operations of a smart grid. Traditional management mechanisms will have to be modified in order to sustain networks such as the ones utilized in the smart grid and the types of devices lying on them. Current multi-domain collaborative environments not only need to have cross-domain authentication measures, it will also be necessary to manage decentralized secure domain interoperation which will make the schemes scalable and more equipped to handle the growing smart grid devices. These networks must also have lightweight and effective entity authentication mechanisms for remote access to the networks. This paper will survey remote access techniques and authentication techniques in the smart grid.

Keywords: *Smart Grid, Remote Access, Domain, Cryptography, Efficiency.*

I. INTRODUCTION

REMOTE access has received much attention especially in the smart grid landscape due to the wireless and distributed nature of current industrial control systems (ICS) and their functional networks. When considering the geographical, operational, and logistical constraints in an environment such as the smart grid, attributes such as interoperability, openness, scalability, simplicity and security must all be considered and addressed [1]. A valid and secure remote access policy will assist in completing these requirements, but the implications of communications crossing the physical confines of their immediate network while accomplishing these benefits, inevitably brings about additional security requirements. Even at this point in the smart grid evolution many devices, especially in the customer domain, are not only ill-equipped with measures to be universally accessible through secure means, but also lack sufficient and efficient security measures and policy enforcement. Some of this can be attributed to customer lack of knowledge, while in other instances; vendors are not required to build their devices with the best security features standard. The remote access problem is exacerbated in the smart grid's distributed architecture where devices on which its operation depends on are unmanned and not necessarily continually monitored and serviced.

The smart grid also means multi-domain collaboration, enhanced authentication measures, and well-defined authorization policy. All of this must be pieced together in an efficient manner so as to maintain the requirements for the resource constrained and legacy devices operating in the network. Networks servicing a smart grid cover large geographical areas and are composed of devices which have specialized purposes and needs. This normally means that functionality is spatially compartmentalized and devices with certain functionality are remote resources to devices in need of it. Since this feature is very important to a smart grid, remote access policy and securing these methods takes center stage.

Most means of securing computing components in distributed architectures requires cooperation of several security principles and methods. [2] points out that integration of security components in a smart grid is lacking in current literature and that while individually well-documented, a more holistic approach must be addressed. With that in mind, this paper considers multiple angles dealing with remote access including authentication, authorization, cross-domain controls, and federation.

II. BACKGROUND

A smart grid can be described as the currently ongoing cyber and physical infrastructure upgrades to the power grid that is in place. This allows the grid to diagnose and heal itself, dynamically integrate renewable energy from various sources which helps relieves dependency on centralized generation, providing the customer more control over electricity demand and cost [3]. The National Institute of Technology and Standards (NIST) defines six key areas which make up the grid below [4]:

- Bulk Generation Domain
- Transmission Domain
- Distribution Domain
- Operations Domain
- Service Provider Domain

- Customer Domain

With the cyber make-up being considered a network of networks, and many of the networks belonging to the grid being connected by the internet, it is novel that they have the capability to contact remote networks securely. This will require preparations to be made with each device requiring communication to remote devices whether the reasoning be for management, monitoring, or information passing to devices on remote networks.

A. Security Requirements in the Smart Grid

The vulnerabilities in an ICS such as those in a smart grid and the networks that it services are extensive due to the availability of the networks and devices connected to those networks as well as the criticality and sensitivity of the data transported on it. The reliability in these environments is dependent on the reliability of the control and communication systems located therein, and the more sophisticated the methods of communication used in the grid are the more complex the security solution will have to be to provide the same level of security. In the next sections, the primitives of security will be discussed as well as the authentication of the entities in need of access.

Many security solutions have been proposed in traditional and industrial information technology (IT) networks, and many have been sufficient in mitigating particular threats. However, these security mechanisms do sufficient for smart grid control and automation networks. Smart grid network security objectives differ in the sense that the integrity and availability of the data is most important as opposed to the data confidentiality being the first concern.

It is also important to understand that the architecture which needs to be secured differs from traditional IT networks as the network structure and types of devices are normally different. Software on the systems in use have been proprietary modified Unix-based or Windows systems with different requirements and application program interfaces (APIs). Networking protocols in use may be IP, but in many portions of the grid, the communication protocols differ. Table 1 gives a detailed list of networking protocols in the smart grid.

Communication Protocol	Description
Zigbee 2.0	For use in HAN for device communication
IEC 61107/62056	Smart meter communication protocol
ANSI C12.*	Smart meter and HAN device communication protocols
HomePlug	Suite of specifications for communication over home electrical wiring
M-Bus	Protocol for remote metering
Modbus	Standard for communication in industrial devices
OPC Protocols	Open standard specification for publish/subscribe procedure
DNP3	Substation device automation
IEC 60870	Outlines control messages
IEC 61850	Outlines communications between transmission and distribution domains in automation and security

Table 1: Smart Grid Networking Protocols

The differing communications infrastructures means that current security mechanisms will either need to adapted or cannot be used in these areas. Therefore it is difficult to develop common network-based security solutions for grid applications [5]. Taking this into consideration, it is easy to understand that security requirements differ in these two infrastructures. These requirements and differences are discussed in [6,7].

1) Confidentiality

The networks in the smart grid transport and create sensitive data. This data can be easily used to either immediately gain identity information about the customer in a specific location, or to glean information about their actions at the specific times that they are performing them. This can harbor dire consequence for a customer that for instance, takes regularly scheduled vacations and leaves their homes unoccupied and available for a malicious individual such as a thief to act uninhibited. Solutions to this can be found in appropriate encryption on the data where needed. One mistake that utilities and network administrators have made about network data encryption in the past is that it is safe for closed networks to operate on a trust basis and therefore not implementing encryption on data. But with the network of networks infrastructure of the smart grid assures, most networks interface with another,

and at some point there will be an internet interface which can have certain vulnerabilities.

Due to the resource constrained nature of many of the devices on smart grid networks, conventional encryption methods would have efficiency hindering on the operation of the devices that are receiving and sending encrypted messages. The encryption protocols used must be secure while simultaneously allowing the devices to achieve their principal purposes.

2) Integrity

All information on smart grid networks, like any other network operating and transmitting sensitive, must not allow for the modification of data. Smart grid networks many times not only host data revealing details about customers, but also data about their bills and power usage. Command messages sent to devices over these networks are critical to the grids emergency operation, and in the instance that that a malicious individual forges, for instance, an automatic shutoff message to smart meters on a large scale would be devastating to the operation of the grid and classified as a terrorist act. Security objectives in this area include message replay, injection, and delay in the smart grid networks.

3) Availability

Availability is the necessity of a system to grant privileges and functions for users that are authorized to utilize the requested resources. Any form of DOS is counteractive to this smart grid requirement. All devices, networks and systems should provide continuous and guaranteed services and bidirectional real-time communication in any smart grid environment [8] [9].

III. REMOTE AUTHENTICATION REVIEW

Throughout history equipment manufacturers have put much of their work of implementing remote access into switches, routers, and modems. The evolution of networks and the types of devices being used on them, each needs platforms for secure communication over these unsecured environments. As the challenge of securing remote communication is not trivial and is integral to a smart grid's operation, there have been several works in the area. [10] proposes a light-weight entity authentication mechanism which allows for remote access into the Home Area Network (HAN) in a smart grid. Under this architecture the Energy Services Interface acts as a gatekeeper and provides dynamic authentication through Elliptic Curve Cryptography (ECC). This protocol is state-based with three states:

- Initialization (public-secret key establishment)
- Pre-computation (HAN devices compute coupons)
- Verification

The verification is a nine step process where the HAN device will compute its key and the shared secret. So, the mobile device confirms correct destination while the HAN device authenticates the messages originating from the mobile device. Furthermore the HAN gateway also verifies both communicating entities without knowing any secrets involved in the protocol.

[11] Utilizes as an identification physically unique properties of each mobile device. In other words, the dynamically generated key of the mobile device relies on its physical properties. [11] also creates network protocol functions for enforcing access control which are self-explanatory and listed below:

- Request(admin, challenges)
- Enroll(admin, pwd, $C_1 \ldots C_m$, params, nonce)
- Access(user, file, action)

Before network transmission, this protocol makes use of SHA-1 hashing and AES encryption.

[12] analyzes current SSL VPN technology and proposes a wireless remote access protocol based on SSL VPN and designed according to the specifications of typical energy power utilities. The platform is divided into four layers:

- Terminal Layer
- Channel Layer
- Access Layer
- Interview Layer

Mobile devices are located in the terminal layer outside of the utility power stations and networks and communicate through the Channel layer. The certification and authentication systems sit on the Access layer while systems such as Supervisory Command and Control (SCADA) sit in the Interview layer. [13] continues in explanation of possible protocols to be used on the platform to secure the information and devices located there as it is flexible to do so.

[14] Reviews past solutions to remote access in Industrial Control Systems (ICS). These methods included:

- Point-to-Point Protocol (PPP)
- Short Message System (SMS)

- Ethernet
- General Packet Radio Service (GPRS)
- GSM

[14] proposes a new Transport Layer Security (TLS) extension/protocol (MTLS) which provides application multiplexing and demultiplexing through a single TLS session. MTLS adds functionality to the TLS handshake and Record protocols. For the handshake, the client and server will negotiate the protocol or the new extension and record types are added to the client. The Record type will only be used after the handshake is completed.

[15] proposes a Layer 2 VPN solution in a holistic architecture. The architecture is made up of three components including:

- Remote Access Server
- Access and Web Service Control
- Monitoring API

An OpenVPN server is used to gain valid access to the remote access server with authentication based either on certificates or shared key policy. The registration policy requires the remote user to provide valid credentials upon which this used is provided with a key and the VPN is established.

[16] proposes a dynamic ID-based remote user authentication scheme. This removed the static nature of repetitive authentication requests which may eventually reveal data about the requester. It's based on one-way hash functions but was later found not to preserve anonymity during its authentication functions [17].

[18] evaluates a previous remote access scheme and proposes its own scheme which is smart-card based and improves upon the latter. This scheme is composed of five phases:

- Registration
- Login
- Authentication
- Password-Change
- Revocation

For mutual authentication a handshake is performed and timestamps are compared. Anonymity is retained by making the timestamp a variable in the ID function.

There has also been much research done in the area of remote authentication which has more or less been focused in specific areas such as authentication without cryptography [19,20], ECC-based implementations [21,22], and even biometric methods [23,24].

When discussing security in remote access protocols, it is imperative to understand the Open Systems Interconnection (OSI) model and its layers and which layer the security mechanisms work on. Most services that we know as the internet operate on layer 3, 4, and 5, application and presentation layers respectively, while TCP/IP services occupy layers 3, 4, and 5 [25]. Utilizing these security mechanisms, and other IP-based protocols is not a trivial task without the use of encapsulation and other mechanisms. Protocols like Zigbee and DNP3 do not provide a platform for protocols such as SSL/TLS so DNP3 is placed over IP to accomplish this and even though Secure DNP3 is primarily an authentication protocol, there is a requirement that DNP3 over TCP/IP implement TLS encryption per the IEC 62351-3 specification [26]. Also, this leads to more smart grid protocols being creating in a manner which they coexist in the OSI model so that they can take advantage of services which are already established. As is already understood, most protocols in use on the smart grid were created with a "security through obscurity" mindset, or with no consideration to security at all.

So the creation of the more recent protocols within the bounds of the OSI model, allows them operate over IP and therefore allowing common security mechanisms [27].

Security in the remote access area relies to authentication and integrity of the communication between devices. Due to the availability of message passing to the public domain, passive eavesdropping must be expected and the initial vulnerabilities that it presents must be mitigated at the highest level. Even more troubling is the lack of standardization in the area, which brings to our attention the widespread use of PKI authentication mechanisms employed in these smart grid networks and the devices on the network that are not necessarily pre-provisioned with the appropriate key materials for PKI exchange and operation [28].

Major operational differences that need to be addressed in the remote access area begin with the focus on reliability, security and message delivery time requirements. A smart grid's networking concern lies more with message delay than with data throughput. This means that authentication mechanisms, for example, with high network overhead are frowned upon.

The reliability of the smart grid can be defined in many different areas including the probability of failed communications, message latency, and the integrity of the messages [29]. These must all be taken into consideration and ported to the necessity for high performance data communication capability and protocols with backward functionality for legacy devices.

The difficulty in remote access in a smart grid in part, is in the need for interoperable and automated authentication procedures. With these procedures, it is important that

bottlenecks in the framework be avoided as denial of service (DOS) is a very real possibility. This means that certificate-based protocols with a single certificate authority (CA) may not be the best choice. Also, the intelligent electronic devices (IED) such as advanced meter infrastructure (AMI), in home smart appliances, and various sensor nodes all are resource-constrained in the terms of pc-class hardware. This means that processing and networking capability is limited.

Functions that remote access allows such as software updating and remote management rely on some of the computation to be carried out on the device in which the operations are being performed on. These devices also must carry out their dedicated functions to support the smart grid without fail or interruption. So the remotely initiated procedures must be efficient enough to accomplish their goals in a light-handed manner that allows for the devices to complete its primary function.

IEC- 62443-2-1 [30] details the general considerations for remote authentication are detailed. Among these are:

- Users of a system should be defied before use
- Secure accounts user ID and passwords
- Correct application configuration
- Execution of configuration locally

Research in [31], details how organizations are to remotely access IEDs while complying with North American Electric Reliability Corporations (NERC) critical infrastructure protection (CIP) standards. This paper also reports that in an effort to comply with the CIPs, some utilities have limited of removed remote access to data and devices inside their networks instead of updating to the standard requirements. A good reason for this is that any legacy devices that remote access is provided must use a service such as a secure virtual private network to connect to a terminal server to remove vulnerabilities in the legacy software and hardware. Also, non-essential software should be hosted from hardware that is physically separate from the legacy device [32]. Existing solutions for remote access over IP networks such as virtual private networks (VPN) are still relevant. Though they only support a best effort service, that does not make certain of quality of service (QOS) necessary in the grid along with latency, jitter, throughput and packet loss requirements [33]. It is known that the security vulnerabilities in WiFi do not endanger the VPN technology which would be placed on top of it when it is configured properly [34].

Outside of VPN there still exists several remote access options for currently established for IP networks. These include tunneling, providing direct access to applications, access portals, and remote desktop access [35].

A. Architectures

When discussing architectures in remote access in the smart grid, it is important to continually consider interoperability and ease of implementation. This is brought to our attention due to the increasing number of protocols which call for modification of software and/or additional hardware to implement a framework for secure remote access [11,14,26,34]. In most instances, this functionality is a responsibility a gateway device (e.g. smart meter) or devices on the edge of the network.

The evolution of technology has caused the general structure of networks to change, which is no different for internal grid networks. Past utility networks were limited in terms of networking, and even retained older networking mediums. Current advances have encouraged merging of devices and infrastructure with new networking hardware and have allowed insecure habits and access methods to survive. Reason for this may be that also updating a specific system is not a high priority when compared to making profits or that it hinders productivity.

For instance, adding flexible and intelligent hardware such as a router which interfaces the internet can be an upgrade in efficiency. This is a step in the right direction on the interoperability side of the equation, but creates vulnerabilities when viewed from a cyber security posture.

B. Cryptography

Outdated and insecure protocols are often used in smart grids (e.g. FTP Telnet). In some situations in remote access session, passwords may be sent in the clear with some of these protocols. SCADA and ICS communication protocols for control devices, such as Modbus/TCP, Ethernet/IP and DNP3, in some situations do not need authentication to remotely execute commands on a device [38].

Typical characteristic many times associated with networks and devices in a smart grid have proven adoption of cryptographic protocols a challenging endeavor. This is due to the resource constrained nature of many of the devices that are integral to the grids operation. These include sensors and AMI just to name a few. Taking this into consideration, ECC has the edge in securing devices in the smart grid due to its smaller key sizes and equivalent security to other protocols with larger key sizes. Even with this knowledge, it is important to consider whether encryption is essential or only a best practice. Since remote access can occur from networks inside and outside a specific host domain (or network), it should be determined that network communications are best encrypted when messages are sent at least to any public network. It is also

important to understand that an attacker can easily take advantage of a trust-based network, especially in the still unexplored infrastructure of the smart grid where there are still unsuspected vulnerabilities created in new areas.

[11] discusses physically uncloneable functions (PUF) and how the fact that no two devices are physically identical can lead to authentic cryptographic constructs. This type of cryptographic key generation boasts that some of its benefits lie in the fact that keys do not reside in memory, but if the malicious individual has access to memory they also have access to the physically uncloneable structure resident in the device. Also, this method is still only as secure as the keyed type of encryption in addition to their idea of physically restricted access control.

VPN solutions normally are secured with one of the following or a combination of the following methods [31]:

- Internet Protocol Security (IPsec)
- Transport Layer Security (TLS)
- Secure Shell (SSH)
- Datagram Transport Layer Security (DTLS)

VPNs face several security issues that are available because of configuration or that are inherent due outdated security, these are listed below [38]:

- Vendor or host fingerprinting
- Insecure and default credentials
- Lack of consideration in authentication (IKE Aggressive Mode with Pre-Shared Key (PSK) authentication)

Microsoft also has a point to point protocol Microsoft Point-to-Point Encryption (MPPE) and a tunneling solution (Secure Socket Tunneling Protocol (SSTP) [39].

The area of authentication schemes that that do not utilize cryptography is exceptional with the number of today's encryption-based encryption services. Authentication in [19] is based on the user that is attempting to login matching all the colors corresponding to the characters of her password correctly and in order once selected from a digital keyboard which randomly assigns a color to each key. The work also mentions that techniques related to its own are normally difficult to learn and implement. It does not seem that the solution to these problems is solved in this implementation.

[10,21,22,30] use ECC-based methods for security in their remote authentication schemes.

C. *Secure Shell (SSH)*

SSH provides users with an open protocol for application in network communications. This protocol specifies the details of a connection between an SSH client and an SSH server and is less complex and expensive than hardware-based VPN solutions [40] . SSH is usually presented in a client/server format where the client is presented with a command shell and querying and file requests over TPC/IP links. RSA authentication key communication is utilized in this protocol and encryption algorithms such as blowfish, 3DES, and IDEA provide confidentiality [41].

In terms of authentication, SSH utilizes public key and password authentication while servers use hosts keys to authenticate themselves.

D. *SSL/TLS*

In some instances, SSL/TLS mechanisms that provide a wrapper for data over the network introduce much unwanted communication and computational overhead. These conditions would negatively affect latency and bandwidth in networks such as these where resources in some devices are severely constrained. Even under these circumstances, a combination of VPN and SSL /TLS can create a reliable transport vehicle on an open software technology framework in the smart grid.

The TLS protocol itself is based on the SSL protocol specification which was published by Netscape [42] and the differences between the two protocols are not overwhelming. Both of the protocols, SSL and TLS, are negotiation and authentication mechanisms, eventually resulting in a symmetric key encrypted data passing session between a server and client utilizing the protocol. They also depend on digital certificates and CAs in their authentication schemes and public key assignment. SSL/TLS have many application in remote authentication in the smart grid, and has even been used in standardized protocols such as IEC 61580 [43].

TLS authenticates nodes using X.509 certificates and public keys to negotiate the session keys for the data exchange. Version 1.2 utilizes more recent NIST approved protocols such as AES and SHA-256 [44]. Also, TLS is approved by IEC 62351-3 for smart grid operation due to its ability to

- Support AES-128
- Support multiple CAs
- Renegotiate symmetric keys
- Validate certificates bi-directionally

As SSL and TLS are both schemes that utilize PKI, and without utilizing a PK scheme with minimal overhead such

as ECC, neither is ideal for the smart grid infrastructure. These types of cryptographic methods incur substantial overhead in comparison to data packet processing, and also contribute more than desirable computational overhead. For traditional computing personal computer (PC)-class devices, the computation requirements are not strained, but when dealing with legacy devices or resource constrained devices such as sensors or smart meters, a less heavy-handed approach is sought-after [45].

E. Multiprotocol Label Switching (MPLS)/Diffserv

MPLS is a protocol introduced by the Internet Engineering Task Force (IETF) to provide QoS in network communications. [46] details connection-oriented paradigm into IP traffic flow. This protocol utilizes a short path labeling scheme to route messages to distant nodes instead of the commonly used layer 3 dotted decimal notation of IPv4 addresses or the IPv6 numerical labels

MPLS maintains a control mechanism composed of a label binding system and IP tables on virtual routing and forwarding technology [47]. Forwarding of the specially labeled packets is managed by forwarding mechanisms in MPLS nodes via look-up tables and label swapping. The lookup tables are maintained and modified based on open shortest path first (OSPF) updates in the network. Encapsulated packets with MPLS labels are assigned special values to the encapsulation protocol header.

[48] describes MPLS as the protocol of choice for utilities' transmission and subtransmission communications networks. Value in MPLS seems to be speeding up transmission of data by integrating layer 2 data such as bandwidth and latency into layer 3 within specific autonomous devices. This also provides infrastructure for more QoS constraints.

Differentiated Services (Diffserv) also provides QoS constraints within a network. The protocol does this by aggregating traffic via packet markings similar to MPLS. The Diffserv protocol also only routes packets accordingly in a Diffserv domain, which is also similar to MPLS. This protocol is normally implemented on modern IP networks.

F. IPSec

IPSec provides security to network traffic with two protocols, Encapsulating Security Payload (ESP), and Authentication Headed (AH). AH adds confidentiality to the services provided by the protocol functionality [49]. IPSec also offers two modes. Transport mode provides end to end security while tunnel mode is used in the instance that the crypto endpoint and the final communication destination are not the same. For devices located behind network address translation (NAT) or behind a specific gateway, the latter mode would be utilized.

IPSec's security mechanism is flexible to the extent that specific types of traffic can be encrypted with one specific cipher and traffic with a different classification can be encrypted with another cipher or algorithm. Policies which are created for specific devices or traffic types are kept in a dedicated database and utilized when required. Key management is handled by Internet Key Exchange (IKE) Protocol [50] and ISAKMP [51]

IV. DESIGN EFFICIENCY

In smart grid, there will always be real-time application of processes and information flow. This must be taken into consideration in all aspects of grid design. This means optimum placement of devices in the grid space to allow for appropriate functions, as well as lightweight protocols operating on data in the networks that will not present a bottleneck due to the limited resources in said devices. All of this must be done while meeting all minimum requirements for the smart grid.

In the remote authentication area, it is of course important to have sufficient authentication, but also for these techniques to be efficient as to not prevent timely execution of the operations in the grid where the authentication measures are being applied. These authentication techniques introduce computational and communication overhead into networks caused by operations in heavy-handed cryptography and inefficient messaging protocols.

[53] brings to our attention several details important to efficiency in authentication protocols in the smart grid including availability and evolvability.

A. Communication and Computational Efficiency

Efficiency in communications can be discerned by the number of messages necessary to complete a specific task or by the authentication protocol as a whole. The dilemma here is that specific protocols are designed for specific purposes, for example, for operation in lossy environments, which are expected to drop messages. These types of designs may or may not affect message overhead but is important to consider. Several schemes for authentication protocols exist, including one-pass, two-pass, schemes which presumably will have much different overhead consequences. A single pass initially will present a more efficient method than a two-pass scheme, but choices of infrastructure must be

addressed such as the authority in charge of authentication, and manner in which trust is achieved in the network.

A single authentication authority presents a bottleneck or a single point of failure in any distributed infrastructure, and should be avoided in remote authentication procedures. Schemes presenting a more involved authentication procedure may also pose problems, so these methods with mechanisms that can reduce the transmission requirements and retain high entropy in their cryptographic algorithms are advantageous.

The main consideration of computational overhead in remote access is the cryptographic algorithm. Resources are utilized in most cryptographic mechanisms, namely certificate based authentication consideration and PKI for example. Today's common remote access protocols utilized in remote access such as SSL and TLS have relatively high computational overhead and also utilize PKI. [54] reports that SSL increases the cost of transactions over a link by a factor of 5-7. Key sizes and storage requirements are also important to consider as in most cases keys must be calculated on the host machine and stored on some type of disk or EEPROM.

V. CURRENT GRID PROTOCOLS

The smart grid is host to many protocols which are specific and integral to its operation. Normally these protocols are used in a specific portion of the smart grid in order to optimize certain networks functionalities.

A. Zigbee

Zigbee is composed of a full protocol stack standard for the HAN communication networks and is retrofitted functionality to support AMI functions while providing support for 802.15.4 in the NAN as well as HomePlug. [55]. Zigbee employs IPSec and TLS for upper layer security and utilizes AES-based symmetric encryption with a 32-bit MAC for AMI communications and a flexible public key interface which can employ one of several flavors of cryptography including ECC and RSA [56].

Simulations in [57] show that Zigbee's throughput advertisements were not experienced in their implementation. In actuality the delays in the measurements derived can be partially attributed to the software layering of the Zigbee protocol and the computational responsibilities the devices has in the protocols AES encryption. Also, the packet loss incurred by data not being appropriately passed up to the application layer due to lack of latency between messages is to blame for increased delay. Some other works that supported the claims are found here [58,59]

The standard encryption offerings (AES-128) of Zigbee present a situation where the computational overhead causes undesirable events and is insufficient for the resource constrained devices normally operating on it. These difficulties are more likely to come about in a more densely populated area and links operating at higher data rates. Zigbee implementations, much like any other environment, vary greatly and each must be tightly integrated with their software and hardware platforms.

B. ANSI C12.22

The C12.22 standard extends C12.18 and details the transport of C22.19 tables of networks and communications between meters and clients. This protocol creates an interface for interoperability between communication modules and smart meters and establishes routing and the two-way communication for the HAN that is so celebrated in smart grid. [60].

C12.22 utilizes AES in EAX mode for encryption and authentication of the data on the network. [61] suggests IPSec to enhance C12.22 and C12.19 security provisions. The protocol also includes provisions for AES-128/EAX message privacy and authentication and message windows, as well as role-based access controls [62].

C. DNP3

Distributed Networking Protocol (DNP3) defines how devices talk to each other in a DNP environment which normally are found in the command and control industry area. In smart grid networks, DNP defines communications between SCADA masters, IEDs, and other RTUs. As DNPs is non-proprietary and capable of supporting high integrity and latency requirements, it is ideal to operate in the smart grid.

Many of the commercial implementations for securing DNP3 are not designed for critical infrastructure, which are normally proprietary. DNP does perform cyclic redundant checks (CRC), data synchronization, and is designed to use several data formats though not initially designed to include security mechanisms and services [63] newest version, DNP3, or DNPSec utilizes a challenge-response authentication procedure and key materials specifications for source verification. DNPSec differs from DNP3 in that DNP3 modifies application layer data while the DNPSec modifies link layer data.

[63] presents findings that conclude DNP3 over TCP/IP achieves an end-to-end delay 8ms to 20ms in their network implementation. These types of behaviors make its

performance sufficient in low-speed applications with delay requirements that can span into the real-time range, although not sufficient for messages dealing with fault management and protection applications whose delay should range from 3ms to 16ms [64].

D. Powerline

Homeplug is a powerline communication designed specifically for the HAN and use in the customer premises. Many of the protocols used in this areas maintain specifications in communications to data concentrators and/or to the utility themselves. Homeplug operates by connecting smart appliances in the home to the smart meter for that residence. Homeplug AV uses cryptographic isolation to create virtual private LANs, called AV Logical Networks (AVLNs).

PRIME and G3-PLC are also powerline communication specifications that garner some attention.

REFERENCES

[1] Ernest and Young. “Attacking the Smart Grid”. [Online] Available: http://www.ey.com/Publication/vwLUAssets/Attacking_the_smart_grid/$FILE/Attacking-the-smart-grid_AU1058.pdf

[2] Ruj, S.; Nayak, A., "A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids," Smart Grid, IEEE Transactions on , vol.4, no.1, pp.196,205, March 2013

[3] Farhangi, H.; “The path of the smart grid,” IEEE Power and Energy Mag., vol. 8, pp. 18-28, 2010.

[4] Vaidya, B.; Makrakis, D.; Mouftah, H., "Secure remote access to Smart Energy Home area Networks," Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES , vol., no., pp.1,7, 16-20 Jan. 2012

[5] E. Santacana, G. Rackliffe, L. Tang, X.M. Feng, “Getting smart,” IEEE Power and Energy Mag., vol. 8, pp. 41-48, 2010.

[6] G. N. Ericsson, “Cyber Security and power system communication - Essential parts of a smart grid infrastructure”, *IEEE Trans, Power Delivery*, 25(3), pp:1501-1507, July 2010

[7] C. J. Hauser *et.al*, “Security, Trust, and QoS in next generation control and communication for large power systems”, *Int. Journal on Critical Infrastructures*, 4(1), pp: 3-16, 2008.]

[8] C. Popper, M. Strasser, and S. Capkun, “Jamming-resistant broadcast communication without shared keys,” in Proc. 18th USENIX Security Symposium (Security 09), Aug. 2009.

[9] Y. Liu, P. Ning, H. Dai, and A. Liu, “Randomized differential DSSS: Jamming-resistant wireless broadcast communication,” in Proc. 29th IEEE Conference on Computer Communications (INFOCOM 10), Mar. 2010.

[10] Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Rongxing Lu; Xuemin Shen, "A Lightweight Message Authentication Scheme for Smart Grid Communications," *Smart Grid, IEEE Transactions on* , vol.2, no.4, pp.675,685, Dec. 2011

[11] Kirkpatrick, M. S., & Kerr, S. (2011, February 2011). Enforcing Physically Restricted Access Control for Remote Data. Paper presented at the 1st ACM Conference on Data and Application Security and Privacy (CODASPY), San Antonio, Texas

[12] Wu Kehe; He Jianping; Ding Tao, "Secure wireless remote access platform in power utilities based on SSL VPN," Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th IEEE Joint International , vol.1, no., pp.93,97, 20-22 Aug. 2011

[13] Drumea, A.; Svasta, P.; Popescu, C., "Remote access solutions for industrial control systems," Electronics Technology: Meeting the Challenges of Electronics Technology Progress, 2004. 27th International Spring Seminar on , vol.1, no., pp.30,35 vol.1, 13-16 May 2004

[14] Badra, M.; Hajjeh, I., "Enabling VPN and Secure Remote Access using TLS Protocol," Wireless and Mobile Computing, Networking and Communications, 2006. (WiMob'2006). IEEE International Conference on , vol., no., pp.308,314, 19-21 June 2006

[15] Onno, S.; Neumann, C.; Heen, O., "Conciliating remote home network access and MAC-address control," Consumer Electronics (ICCE), 2012 IEEE International Conference on , vol., no., pp.98,99, 13-16 Jan. 2012

[16] Das, M. Saxena, A. Gulati, V. “A dynamic ID-based remote user authentication scheme”, IEEE Transactions on Consumer Electronics 50 (2) (2004) 629–631.

[17] H.Y. Chien, C.H. Chen, A remote authentication scheme preserving user anonymity, in: International Conference on AINA’05, vol. 2, 2005, p. 2005. [24] C.I. Fan, Y.C. Chan, Z.K. Zhang, Robust remote authentication scheme with smart cards, Computers & Security 24 (2005) 619–628.

[18] Khan MK, Kim SK, Alghathbar K. Cryptanalysis and security enhancement of a ’more efficient and secure dynamic ID-based remote user authentication scheme’. Computer Communication 2011;34(3):305–9.

[19] Y. C. Yeh, W. C. Ku, W. P. Chen, and Y. L. Chen, “An easy-to-use login-recording attacks resistant password scheme,” Proceedings of the 2011 Conference on Innovative Applications of Information Security Technology, 2011.

[20] Yu-Chang Yeh; Wei-Chi Ku; Wei-Ping Chen; Yi-Lun Chen, "An enhanced simple secure remote password authentication scheme without using cryptography," Communications in China (ICCC), 2012 1st IEEE International Conference on , vol., no., pp.231,235, 15-17 Aug. 2012

[21] Tien-Ho Chen; Yen-Chiu Chen; Wei-Kuan Shih, "An Advanced ECC ID-Based Remote Mutual Authentication Scheme for Mobile Devices," Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2010 7th International Conference on , vol., no., pp.116,120, 26-29 Oct. 2010

[22] Tien-Ho Chen; Hsiu-lien Yeh; Wei-Kuan Shih, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing," Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on , vol., no., pp.155,159, 28-30 June 2011

[23] Al-Assam, H.; Jassim, S., "Robust Biometric Based Key Agreement and Remote Mutual Authentication," Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on , vol., no., pp.59,65, 25-27 June 2012

[24] Chin-Feng Lee; Shin-Ruei Huang; Hung-Yu Chien; Narn-Yih Lee, "Two-party and three-party remote user authentication schemes using biometric data only for emergency," *Aware Computing (ISAC), 2010 2nd International Symposium on* , vol., no., pp.51,55, 1-4 Nov. 2010

[25] Linder, Greg. *FAILURE ANALYSIS AND SMART GRID CONTROL PROTOCOLS FOR ANAEROBIC DIGESTERS A thesis*. Diss. Clarkson University, 2009

[26] International Electrotechnical Commission, Communication Network and System Security—Profiles including TCP/IP, Technical Specification IEC TS 62351-3, Geneva, Switzerland, 2007.

[27] Clark, Gordon. Reynders, Deon. *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*, New York: Newnes, 2004, pp. 13-45.

[28]

[29] Nordell, D.E., "Terms of Protection: The Many Faces of Smart Grid Security," *Power and Energy Magazine, IEEE* , vol.10, no.1, pp.18,23, Jan.-Feb. 2012

[30] Vaidya B., Makrakis D., Mouftah H. "Secure communication mechanism for ubiquitous Smart grid infrastructure". J Supercomput. doi:10.1007/s11227-011-0674-5. 2011
[31] ISA / IEC 62443 Final Draft International Standard Available: http://isa99.isa.org/ and https://ecommittees.bsi-global.com/bsi/controller/AMT_7_10_0074.pdf?livelinkDataID=38273702&download=true
[32] Subnet Solutions "Manage Utility IEDs Remotely while Complying with NERC CIP" [Online] Available: http://www.subnet.com/downloads/Managing_Utility_IED_Access-SUBNET.pdf
[33] The ABB Group. "Security in the Smart Grid". [Online] Available: http://www02.abb.com/db/db0003/db002698.nsf/0/832c29e54746dd0fc12576400024ef16/$file/paper_security+in+the+smart+grid+(sept+09)_docnum.pdf
[34] Hossain, E. Zhu H. Poor, V. eds. Smart Grid Communications and Networking. Cambridge University Press, 2012. Cambridge Books Online. Web. 11 June 2013. http://dx.doi.org/10.1017/CBO9781139013468.
[35] Tomur, E. Deregozu, R. Genc, T., "A wireless secure remote access architecture implementing role based access control: WiSeR," in Proceedings of the World Academy of Science, Engineering and Technology, December 2006.
[36] Gharavi, H.; Bin Hu, "Dynamic key refreshment for smart grid mesh network security," *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES* , vol., no., pp.1,6, 24-27 Feb. 2013
[37] Ning Cai; Jidong Wang; Xinghuo Yu, "SCADA system security: Complexity, history and new developments," *Industrial Informatics, 2008. INDIN2008. 6th IEEE International Conference on*, vol., no., pp.569,574, 13-16 July 2008
[38] Singh, A.K.; Samaddar, S.G.; Misra, A.K., "Enhancing VPN security through security policy management," *Recent Advances in Information Technology (RAIT), 2012 1st International Conference on* , vol., no., pp.137,142, 15-17 March 2012
[39] Microsoft "What is a VPN" [Online] Available: http://technet.microsoft.com/en-us/library/cc739294(v=ws.10).aspx
[40] Bruce Schneier 1996," Applied Cryptography- An excellent, practically oriented presentation of cryptographic algorithms, protocols, and methods", John Wiley & Sons, II Edition.
[41] Iyappan, P.; Arvind, K. S.; Geetha, N.; Vanitha, S., "Pluggable Encryption Algorithm In Secure Shell(SSH) Protocol," *Emerging Trends in Engineering and Technology (ICETET), 2009 2nd International Conference on* , vol., no., pp.808,813, 16-18 Dec. 2009
[42] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2, " IETF RFC 5246, 2008, http://www.ietf.org/rfc/rfc5246.txt.
[43] S. Feuerhahn, M. Zillgith, C. Wittwer, and C. Wietfeld, "Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications," in Second IEEE International Conference on Smart Grid Communications, 2011.
[44] Benoit, B. "AN Introduction to Cryptography as Applied to the Smart Grid". Cooper Power Systems
[45] J. Naruchitparames, M. H. Gunes, and C. Y. Evrenosoglu, "Secure Communications in the Smart Grid," *2011 IEEE Consumer Commun. and Networking Conf.*, Jan. 2011, pp. 1171–75.
[46] V. C. Gungor and F. C. Lambert "A survey on communication networks for electric system automation", *Comput. Netw.*, vol. 50, no. 7, pp.877 -897 2006
[47] Multi-Protocol Label Switching (MPLS) [Online] Available: http://www-ee.uta.edu/online/wang/MPLS.pdf
[48] Lam, F., "Why an IP/MPLS Network Makes Sense for Smart Grids" [Online] Available: http://www2.alcatel-lucent.com/techzine/why-an-ipmpls-network-makes-sense-for-smart-grids/
[49] Weerathunga, P., Samarabandu, J., Sidhu, T., "Applications of IPSec in Smart Grid cyber security defense"
[50] RFC 2409 IETF, "The Internet Key Exchange (IKE)", November 1998.
[51] RFC2478, "Internet Security Association and Key Management Protocol (ISAKMP)", November 1998.
[52] Hallam-Baker, P. Security Assertions Markup Language. *May*, *14*, 1-24. 2001
[53] http://www.oasis-open.org/specs/index.php#ws-trust
[54] OpenID Authentication 2.0 – Final Technical Specification. http://openid.net/specs/openid-authentication-2_0.html.
[55] S. Das, Y. Ohba, M. Kanda, D. Famolari and S.K. Das, "A Key Management Framework for AMI Networks in Smart Grid," IEEE Communications Magazine, Vol. 50, Issue 5, pages 30-37, Aug. 2012.
[56] H. Khurana "Design Principles for Power Grid Cyberinfrastructure Authentication Protocols", *Proc. 43rd Ann. Hawaii Int\'l Conf. System Sciences (HICSS 10)*, 2010
[57] K. Kant, R. Iyer, & P. Mohapatra, (2000) "Architectural impact of secure socket layer on internet servers", proceedings ICCD' 00 Proceedings on the 2000 IEEE International Conference on Computer Design: VLSI in Computers & Processors, pp 7-14
[58] ZigBee Alliance and HomePlug Powerline Alliance. ZigBee Smart Energy Pro le 2.0 Technical Requirements Document (DRAFT), March 2010
[59] Moise A. Beroset, E. Phinney, E. and Burns. M. "EAX Cipher Mode". American National Standards Institute (ANSI) C12 SC17 Committee, May 2011
[60] Moise, A., Brodkin, J., "ANSI C12.22, IEEE 1703, and MC12.22 Transport Over IP". March 2011.
[61] ANSI, "Protocol Specification For Interfacing to Data Communication Networks", ANSI C12.22-2008, approved January 9, 2009
[62] Alcaraz, C.; Zeadally, S., "Critical Control System Protection in the 21st Century: Threats and Solutions," *Computer* , vol.PP, no.99, pp.1,1, 0
[63] Knapp, E. "Industrial network security, securing critical infrastructure networks for Smart Grid SCADA, and other industrial control systems", Elsevier, Syngress, pp. 1-360, 2011.
[64] Xiang Lu; Zhuo Lu; Wenye Wang; JianFeng Ma, "On Network Performance Evaluation toward the Smart Grid: A Case Study of DNP3 over TCP/IP," Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, vol., no., pp.1,6, 5-9 Dec. 2011