HomePlug AV Security Mechanisms

Richard Newman[1], Larry Yonge[2], Sherman Gavette[3], Ross Anderson[4]
University of Florida
[1]Computer and Information Science and Engineering Department
PO Box 116120 Gainesville, FL 32611-6120 USA
nemo@cise.ufl.edu
[2]Intellon Corporation, USA
[3]Sharp Labs, USA
[4]Cambridge University, UK

***Abstract*— This paper describes the security mechanisms provided in the HomePlug AV specification. It highlights the AV approach for solutions to problems in detection of other nodes with which to form a network, efficient transmission of the initialization vector (IV), reducing risks of key and IV reuse, and implementing "push-button" security for casual users. A novel key agreement protocol based on channel adapted powerline communications is described and analyzed. It also describes mechanisms to allow extensibility for higher layer key distribution protocols.**

Keywords - user authentication, powerline communication, security.

I. INTRODUCTION

IN contrast to earlier in-home powerline communications systems, such as X10 [1] or HomePlug 1.0 [2], the high-speed HomePlug AV standard is designed to support multimedia applications [3,4]. To provide the user experiences desired for consumer electronics, as opposed to computer communications or home automation, simplicity for the user is a must. A consumer buying equipment furnished with this technology should be able simply to plug it into the mains, whereupon it will discover other relevant equipment. The devices will form a logical network without the need for additional physical wiring.

Since the powerline is a broadcast medium and signals can cross property boundaries, security is a significant issue. How can the owner of in-home powerline communication (PLC) equipment be sure that it connects to his home network rather than his neighbor's? There may be other boundaries at an even finer granularity. For example, students occupying a shared house might want to have one network each. So the HomePlug AV standard must support multiple virtual networks. However, security management in traditional systems is beyond the average person's patience. The majority of home wireless LANs remain unprotected [5].

Furthermore, the devices can be expected to range widely in computational resources as well as user interface capabilities. While many devices will have CPUs capable of public-key cryptography, not all will. Moreover, although many home networks will have a device with a reasonable user interface (e.g., a TV or PC) that can be used as a controller, not all will. Finally, even if users are unconcerned about security, for performance reasons it is undesirable for hundreds of devices in a large apartment block to join the same logical network promiscuously.

Aside from these challenges of environment, usability, and equipment, there are unique opportunities afforded by the HomePlug AV physical layer (PHY). In particular, tight channel adaptation using bit loaded orthogonal frequency division multiplexing (OFDM) modulation [6] for each direction of communication on each virtual link makes successful reception and demodulation by an unintended destination difficult, especially if the destination is physically more remote than the other devices in the same residence. Hence, HomePlug AV achieves a certain amount of confidentiality, even before it performs encryption.

II. HOMEPLUG AV OVERVIEW

The low voltage powerline medium is inherently a broadcast medium, with frequency-selective attenuation dependent on the outlet pair at which the transmitter and the receiver attach. Attenuation is high for all frequencies, and there is much noise of various types, so carrier detection is difficult, much less collision detection. Hence, earlier systems used CSMA/CA for access to the medium, as in IEEE 802.11. Virtual Carrier Sense (VCS), based on information supplied in the robustly broadcast frame control field, is used to inform medium access decisions. Since the frame control must be very reliable, it is heavily coded and is inefficient.

To make the most of the channel available, each pair of communicating stations adapts the OFDM modulation used according to the current channel characteristics. In HomePlug AV, this means choosing one of eight possible modulation

rates (from none to 1024-QAM) for each of 917 carriers. This modulation information, along with the forward error correction coding rate (1/2 or 16/21) and the guard interval duration (three choices) constitutes the tone map. This receiver-determined tone map is used by the sender to transmit the data payload of a Physical Layer Protocol Data Unit. Without the tone map, demodulation is not possible. Even with the tone map demodulation by a station other than the intended recipient is problematic, since the modulation rate for each carrier is adapted to be very close to the maximum rate possible depending on the signal to noise ratio. While not impossible, interception of the data payload of a PHY protocol data unit is a significant challenge for an attacker.

Tone-mapped communications requires that sender and receiver agree on the tone maps, which in turn requires some initial communication. Two well-known broadcast tone maps are defined for this purpose, ROBO and mini-ROBO. These robust (hence the names) modulation schemes work well for almost all channels, and are used for broadcast as well as for pairs that have not yet adapted to their channel. Both ROBO modes are very reliable.

For greater efficiency, reliability, and deterministic latency needed by multimedia applications, HomePlug AV uses a beacon-based Medium Access Control (MAC) approach. This also allows for coordination among adjacent, interfering networks. Each logical network has a central coordinator (CCo) that issues the beacon for that network, and the beacon specifies the time allocations for specific contention-free streams as well as a period for CSMA/CA access. To handle hidden nodes in a logical network, a proxy coordinator may repeat the beacon.

III. Security Goals and Logical Networks

As is the case with most systems in which physical eavesdropping cannot be prevented, HomePlug AV uses cryptographic isolation to create virtual private LANs, called AV Logical Networks (AVLNs). The security goals of HomePlug AV are for a logical network to be equivalent to a wired LAN as much as practical. Specifically:

- Stations (STAs) within an AVLN should be able to communicate confidentially (message contents should not be exposed to stations outside the AVLN).
- STAs within an AVLN should have confidence in the integrity of the messages they receive (i.e., they were neither damaged nor deliberately changed, nor are they replays or forgeries).
- Network stations (STAs) should not be allowed to join a user's AVLN unless the user is confident that the station is equipment he wants to add.
- It should be hard for a different AVLN to "capture" a STA, but it should be easy for a user to reclaim a device he owns that was "captured" by another network.
- A user should be able to reset a device and give or sell it to another user.

A set of stations capable of communication with each other that share a common Network Membership Key (NMK) with a CCo defines the nodes belonging to an AV Logical Network. From the NMK, a Network Identifier (NID) is derived by cryptographic hashing. The NID is advertised in the beacons, and allows a new station to discover AVLNs for which it possesses the NMK. The first two security goals are practically achieved by use of cryptography at the PHY level and data check sequences in the data plane handling. The latter three goals are handled through management of the NMKs. In all cases, encryption is performed using AES-128 in Cipher Block Chaining (CBC) mode [7,8].

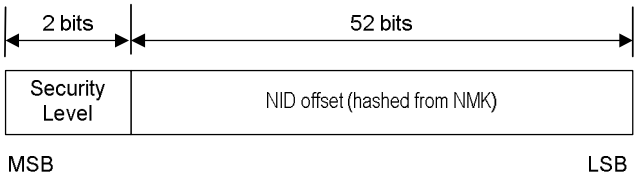

Figure 1 Network Identifier

To reflect the different degrees of assurance obtained from the NMK distribution mechanisms, the NMK and its AVLN are associated with a security level (SL). Two security levels are defined in HomePlug AV: Secure (HS) and Simple Connect (SC). In all, it is assumed that STAs within the same AVLN are trustworthy (i.e., they do not perform hostile actions or divulge keys deliberately).

To form an AVLN, the NMK is distributed to all the stations in the AVLN. Using the NMK as a master key, the coordinator distributes a periodically changing Network Encryption Key (NEK) to each station in the AVLN. The NEK is used to encrypt the data payloads of most PHY Protocol Data Units sent in the AVLN. Transmissions between networks, and those used initially to distribute encryption keys are not encrypted with the NEK.

Stations must associate with the CCo to obtain a Terminal Equipment Identifier (TEI), used for addressing local to the AVLN. In order to obtain the NEK, an associated station must authenticate (obtain the NMK and use it in the initial NEK distribution protocol). The information exchanged between HomePlug AV stations and how it is handled depends on the association and authentication status of the STAs relative to each other. STAs that are associated and authenticated with the same AVLN can exchange both management messages and data securely. Communication between STAs that are not associated and authenticated with the same AVLN is restricted to a subset of the Management Messages; exchange of any application level data is prohibited.

A wide range of node capabilities is anticipated. Some will be computers with a full user interface and powerful

processing capacity. Others will be consumer electronic devices with a single button that may be depressed to signal user intent. In between, we will have televisions, PVRs, and the like with various user interfaces and computing powers. All security processing defined within the specification must be handled without higher layer intervention (i.e., on the chip). The protocols have to support devices over this entire range, and their users.

The typical user experiences supported by HomePlug AV reflect the way in which the user interacts with the AV devices as they are being configured. They will depend upon how the device manufacturer implements the user interface for the device and what configuration is performed before the user installs the device.

Four basic user experiences are anticipated:

- User plugs devices in a set into the outlets and they connect by themselves
- User enters a network password to get a device to join an AVLN (devices with rich user interfaces)
- User enters a device password to add another device to its AVLN (at least one device with rich user interface)
- User pushes a button on each of two devices to get them to connect to each other

The first of these relies on pre-positioning an NMK for the devices to use, while the latter three require some effort on the part of the user. The last two user experiences are supported by underlying protocols that distribute the Network Membership Key over the medium.

IV. Discovery and AVLN Formation

A STA may join an AVLN when it sees the beacon of a CCo whose NID matches the one derived from an NMK it possesses. A STA may be added to an AVLN by passing it the NMK using one of two directly supported NMK distribution methods, or by using a higher layer protocol. Two unassociated STAs can form a new AVLN when they have the same NMK and Security Level, or by passing the NMK from one to the other. A STA that sees one or more AVLNs but cannot join any advertises itself as unassociated in the hope that another unassociated STA has the same NMK and SL, and so will unite with it to form an AVLN. The NID and SL are included in these advertisements, so that other STAs may recognize fellow AVLN members. If it sees no AVLNs, it becomes a CCo itself, advertising the NID in its beacons.

When an AVLN is formed, one STA becomes the CCo and starts issuing beacons with the NID. Other STAs with matching NIDs attempt to join that AVLN by associating, then authenticating by requesting the NEK. When an AVLN is formed as a result of passing the NMK over the powerline medium, the nature of the process is closely related to the key distribution mechanism.

V. Key Distribution

Four types of keys are used in HomePlug AV: Network Membership Keys (NMKs), which enable a STA to authenticate to an AVLN; Network Encryption Keys (NEKs), which enable a STA to perform the cryptographic processing needed to exchange data with other STAs within the same AVLN; Device Access Keys (DAKs), which are unique to a device and allow other devices to pass it the NMK securely; and Temporary Encryption Keys (TEKs), which are generated and used in the key distribution protocols. The NMK is associated with a security level, which limit the ways in which it can be distributed.

The NMK may be provided to a STA in one of three ways: it may be provided by the host directly; it may be passed to a STA using that STA's DAK; it may be passed using the less secure Unicast Key Exchange (UKE) protocol, which supports push-button AVLN formation. The host may provide the key directly by the user entering the Network Password (NPW) onto the host and hashing it to generate the NMK, or it may be obtained by the host through a higher layer protocol, or it may be obtain through some other out of band mechanism (e.g., nearfield communications, flash memory token, etc.). Keys are generated from passwords using the PBKDF1 function (from the PKCS #5 v2.0 standard [9]) using truncated SHA-256 as the underlying hash algorithm [10].

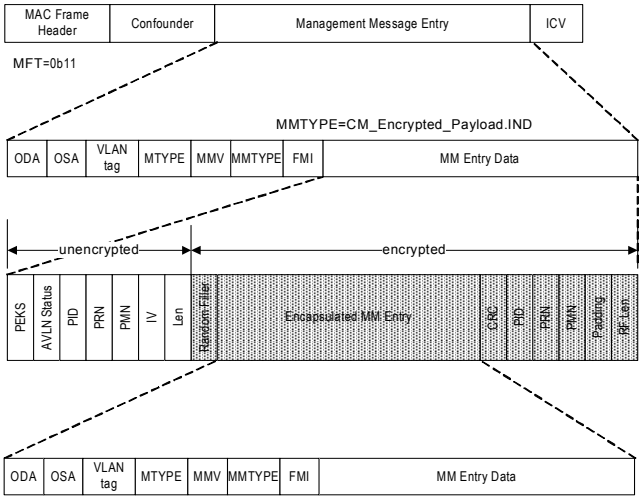

Figure 2 Encrypted Payload MME

Keys are distributed over the powerline medium using Encrypted Payload MAC Management Entries (MMEs). These are usually not encrypted at the PHY level, as the principals usually do not have an NEK in common. The Encrypted Payload MME includes an explicit, random 128-bit IV along with a field to indicate which key type and key is used to encrypt its payload. Three additional fields, the Protocol Identifier (PID), Protocol Run Number (PRN), and Protocol Message Number (PMN), are included in both plaintext and encrypted to permit proper determination of multiple protocol runs and the progress of the protocol.

Nonces are used to prevent replay attacks, and TEKs are used for actual key distribution.

When the NMK is passed to another STA using its DAK, the sender obtains the DAK from hashing a random Device Password. The sender then broadcasts an Encrypted Payload MME containing a TEK encrypted with the DAK. All STAs attempt to decrypt this MME, but only the STA whose DAK has been used to encrypt it will succeed. All others silently discard the MME, but a STA that succeeds will respond with an Encrypted Payload MME containing a nonce and encrypted with the TEK it just obtained. The sender then unicasts an Encrypted Payload MME containing that nonce and the NMK to the responder, encrypted with the DAK. The STA confirms correct receipt by using the NMK to encrypt its response.

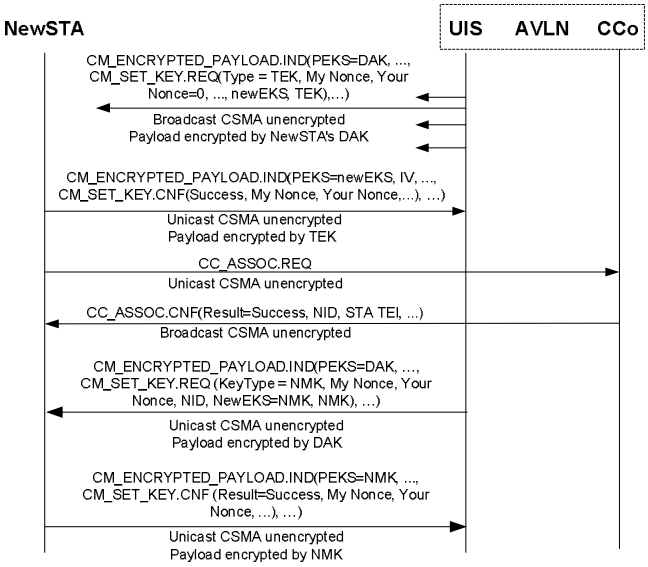

Figure 3 DAK-based NMK Distribution Protocol

The remaining method for distributing the NMK over the powerline medium is UKE. In this method, the user must signal intent for an AVLN to add a new device, and for a device to join an AVLN that is willing to accept it. If two devices are instructed to join an AVLN, then they will form a new AVLN. This supports a "button push" AVLN formation user experience, as it only requires a very simple user interface. The device that has been instructed to join an AVLN advertises its promiscuous state, and waits for another device to send it a response. From this confirmation, the device knows with which AVLN it should associate, or the two devices know that one must become a CCo and create a new AVLN. When the two STAs have associated with the same AVLN, they may then perform channel estimation and establish channel adapted tone maps (bit loading parameter sets). Then, using unicast transmission, the STAs continue the protocol by exchanging long random strings with each other. These "hash keys" are concatenated and hashed to produce a TEK that the two devices then use to distribute the NMK.

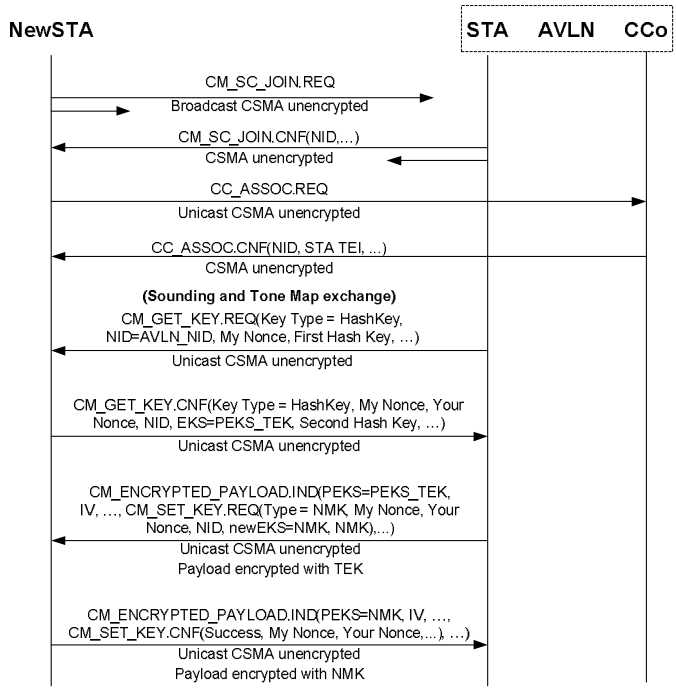

Figure 4 UKE Distribution Protocol

The protocol traffic in the initial key exchange (including both the keys and the tone maps) is all sent in the clear, and so in theory a capable opponent who observes the exchange can derive the TEK. This is harder than it seems. The key exchange uses high bitrate communications, and it is hard for stations other than the participants to decode this, even given knowledge of the participants' tone maps, because the analogue characteristics of power networks are generally such that the signal-to-noise ratio will in general be too poor at different locations (that is why tone maps have to be negotiated). Using the hash of both strings requires the attacker to be able to demodulate traffic in both directions. Furthermore, chips compliant to the HomePlug AV specification will not support such attacks, so an attacker would have to produce a partial implementation of the HomePlug protocols. This would furthermore be unlicensed and thus unlawful.

In anticipation of vendors and users wishing to use higher layer protocols to distribute the NMK, HomePlug AV provides a mechanism by which the MAC simply passes an Encrypted Payload MME from the host on one device to the host on another device without processing it cryptographically. Using a special PID set aside for this purpose, the hosts may exchange management messages. The hosts must form the actual an Encrypted Payload MME and pass it as an MSDU to the MAC, which then recognizes it and sends it over the medium. Restrictions apply that make this inappropriate for general data transfer, and the field normally used to hold the 128-bit IV for the encrypted payload is instead used to hold a Universal Unique ID (UUID), so that the host can route these messages correctly [11,12].

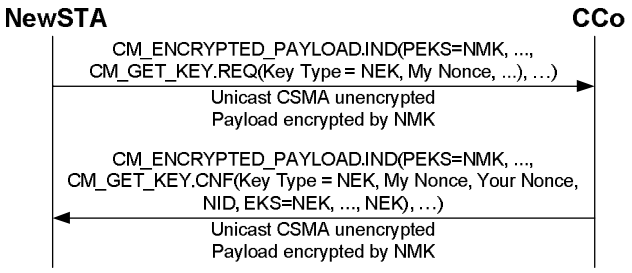

Figure 5 Authentication Protocol

Once a STA has associated and has a valid NMK, it authenticates by requesting the NEK from the CCo in an Encrypted Payload MME that contains a freshly generated nonce, encrypted by the NMK. If the CCo verifies the STA's NMK, it gives the STA the current NEK in an Encrypted Payload MME containing the nonce and encrypted with the NMK. If the CCo cannot decrypt the request encrypted by that NMK, it responds with a failure message and the new STA flags the NMK as invalid on this AVLN. It may then either attempt to obtain a valid NMK for this AVLN or try to join a different AVLN. Once a STA has authenticated successfully, the CCo provides the STA with new NEKs as long as the STA remains associated. Thus, a STA is not required to re-authenticate subsequent to TEI renewal. To provide a new NEK to a STA already in the AVLN, the CCo asks it for a nonce and the STA provides it in its response. The CCo then sends the new NEK and Encryption Key Select (EKS) in an Encrypted Payload MME containing the nonce, encrypted with the NMK. The STA confirms receipt and waits for the new NEK to become effective before using it. This is announced in the beacons using a countdown mechanism, which is only commenced when the CCo has given the new NEK to all AVLN STAs.

VI. Data Plane Handling

When data in the form of MAC Service Data Units (MSDUs) arrive at the service interface of the MAC, they are packaged as MAC Frames. In addition to the encapsulated MSDU, MAC Frames have a small header that includes the MAC Frame length and a type field, and a CRC-32 Integrity Check Value (ICV). Streams that require latency guarantees also have a 32-bit arrival time stamp (ATS). MAC Frames are concatenated into a MAC Frame stream, which is in turn chopped up into fixed length segments. Each segment is packaged as the payload of a PHY Block (PB).

PBs are the basic unit of data transmission in HomePlug AV. A PB consists of a PB Header, a PB Body (PBB) and a PB Check Sequence (PBCS). The PBB holds the data segment, and the PBCS detects transmission errors. The PB Header specifies the amount of meaningful data in the PBB, in case padding was required, as well as a PB sequence number and the location of the first MAC Frame boundary within the PBB (if any). This and a few control flags are used for proper reassembly of the MAC Frame stream by the receiver. One or more PBs are sent as the payload of a long MAC PDU (MPDU), which has a Start of Frame (SOF) delimiter that provides the information necessary to route, and decrypt the payload. In fact, after the PBB is encrypted, each PB is formed into a Forward Error Correction (FEC) block by the PHY according to the bit loading adaptation to the channel. The receiver uses the FEC code to correct the received PBs, checks them using the PBCS, and acknowledges them using a Selective Acknowledgement MPDU (SACK). PBs are retransmitted as necessary, and are independently encrypted on each transmission.

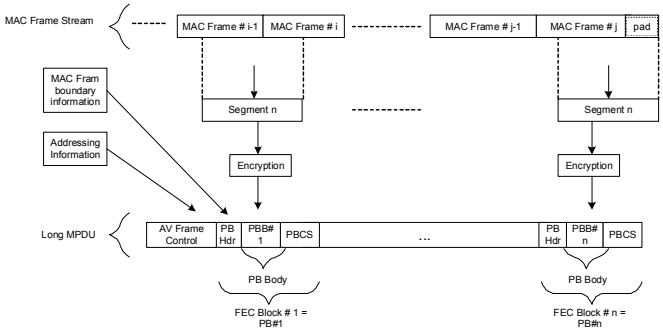

Figure 6 MAC Frame Segmentation and Encryption

The CCo generates and distributes a new, random AES-128 Network Encryption Key at least once every hour. The NEK is used in CBC mode to encrypt the PHY Blocks (PBBs). The PB Header and the PBCS are not encrypted, as these contain information necessary to the proper reception of the PBs. Within the SOF, the Encryption Key Select (EKS) field indicates which key is used. Space is at a premium in the broadcast delimiters and the PB Headers, so the 128-bit Initialization Vector (IV) is generated from fields of the PB Header and the SOF. In CBC mode, the primary use of the IV is to prevent the same plaintext from generating the same ciphertext when encrypted with the same encryption key, so the predictability of the IV is not considered an issue.

While it is possible for an IV to repeat in less than the hour maximum between NEK changes, the primary threat in CBC mode is recognized ciphertext. The contents are likely to be different in high-speed multimedia streams, and for MMEs, a random confounder is included in the MAC Frame header to thwart this attack. Proper decryption is only checked using the ICV at the MAC Frame level, and MAC Frames whose ICV check fails are silently discarded, so no oracle attacks are possible.

VII. Conclusions

This paper has described the security goals and mechanisms of HomePlug AV. The main security problem is that users may recruit the wrong devices to their networks, and conventional trust mechanisms such as public-key certificates [13] simply don't deal with this, as we note in a broader, more philosophical discussion of these issues elsewhere [14]. To

ensure that the right device is recruited, one must check its label, or perform some other physical action with it, in which case there are usually cheaper ways to do things than to use public key certificates. Furthermore, the resources needed to perform public key cryptography are beyond what some devices will have. Thus, simple but effective mechanisms are provided.

Encryption in the data plane is typically performed by hardware in real time, and neither impacts throughput nor delay at the MAC level. Outside of the data plane encryption, the key distribution protocols are used infrequently, and so have minimal impact on either system performance or station requirements. Derivation of the NMK or DAK from a password is done by a higher layer entity, and only the actual key is passed to the MAC, so repeated hashing of the password does not impact the station requirements at all.

The design provides two simple modes of operation: Simple Connect Mode to prevent accidental recruitment and Secure Mode for those willing to exert the effort to obtain higher assurance. In addition, HomePlug AV provides a mechanism for licensees and third-party vendors to form logical networks using their own approaches.

REFERENCES

[1] Brown, P.A., 'Power line communications - past, present, and future, Proceedings of International Symposium on Power-line Communications and its Applications, Sept 1999, pp. 1--8.

[2] Lee, M. K., R. Newman, H. A. Latchman, S. Katar, and L. Yonge, "*HomePlug 1.0 Powerline Communication LANs –Protocol Description and Comparative Performance Results*", International Journal on Communication Systems on Powerline Communications, pages 447-473, May, 2003.

[3] Afkhamie, K. H., S. Katar, L. Yonge, and R. Newman, "An Overview of the upcoming HomePlug AV Standard," proceedings of International Symposium on Powerline Communications (ISPLC 2005), Vancouver, BC, 2005, pp. 400-404.

[4] Katar, S., R. Newman, H. Latchman, and L. Yonge, `Efficient Framing and ARQ for High-Speed PLC Systems', proceedings of International Symposium on Powerline Communications (ISPLC 2005), Vancouver, BC, 2005, pp. 27-31.

[5] W. David Gardner, 'Wireless Survey: Many Nets Open To Security Breaches', Information Week, Mar 10, 2005 , see http://www.informationweek.com/story/showArticle.jhtml?articleID=159400875.

[6] Prasad, R., van New, R., OFDM Wireless Multimedia Communications, Artech House, Norwood, MA, 2000.

[7] Federal Information Processing Standards Publication 197: Specification for the Advanced Encryption Standard (AES) - November 26, 2001

[8] National Institute of Standards and Technology Special Publication 800-38A, 2001 Edition: Recommendation for Block Cipher Modes of Operation, Methods and Techniques - December 2000

[9] RSA Labs, PKCS #5 v2.0 standard, Password-based Cryptography Standard.

[10] FIPS 180-2, NIST, "Secure Hash Standard," August 26, 2002, (including the change notice dated February 25, 2004, concerning truncation)

[11] ITU-T Rec. X.667 | ISO/IEC 9834-8 "Information Technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: Generation and Registration of Universally Unique Identifiers (UUIDs) and their Use as ASN.1 Object Identifier Components," http://www.itu.int/ITU-T/studygroups/com17/oid/X.667-E.pdf, Sept. 2004

[12] [10] Leach, P. and R. Salz, IEFT RFC 4122, "A Universally Unique IDentifier (UUID) URN Namespace," http://www.ietf.org/rfc/rfc4122.txt, July 2005

[13] X.509, The Directory - Authentication Framework., CCITT, ITU-T, 1988, the IETF version is available as 'Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile at http://www.ietf.org/rfc/rfc3280.txt

[14] Richard E. Newman, Sherman Gavette, Larry Yonge, and Ross Anderson, ``Protecting Domestic Powerline Communications,'' Symposium on Usable Privacy and Security (SOUPS 2006), Pittsburgh, PA, July 12-14, 2006, pp. 122-132.