Integrated Network Security Protocol Layer for Open-Access Power Distribution Systems

Todd Mander, Farhad Nabhani
University of Teesside, U.K.

Lin Wang, Richard Cheung
Ryerson University, Canada

***Abstract*—Power distribution system cyber-security concerns are increasing rapidly with growing demands for open accesses to the distribution systems for electricity generation and trading imposed by new government deregulations. This paper proposes a new integrated network security protocol layer, located below the data-link layer of DNP3 – a popular utility protocol, to enhance the data transmission cyber-security for power distribution systems. The security layer utilizes distribution system characteristics to provide comprehensive security while maintaining virtually no impact on the existing DNP3 specification. The proposed security layer provides end-to-end security and link security through encryption, authentication, and padding operations. 'Recipe' formats, with independent cipher and authentication, are designed for the security layer operations to increase flexibility, coverage and quality of service capabilities of the security layer and to provide rapid responses for changes in cyber-security threats in the power distribution systems. This paper describes its significant applications in distribution system stability controls.**

***Index Terms*--Computer networks, Computer network management, Computer network security, Power system communication, Power system security, Protocols, Security.**

I. Introduction

CYBER-security for the power distribution system is becoming a serious concern for power system utilities with ongoing power system automation and government-imposed open access [1]-[3]. The continuing power system automation increases the use of intelligent electronic devices (IEDs) with communication capabilities for efficient distribution system protection, control and monitoring operations with connections to external networks. In order to process collected data, IEDs require external data from their peer IEDs within the same network or through an external network. However, increased data access with peer IEDs within the same network or through external networks could aggravate the opportunities for cyber-hackers to manipulate data that may cause IEDs to malfunction or even fail.

With open access requirements, access to distribution system utility computer networks from external networks, for electricity generation and trading transactions, increases the number of users who are allowed to access the utility network through the Internet where not long ago, only trained utility staff had access to the utility network. This has considerably aggravated the risks for proper power system operations due to potential cyber-attacks. Under new government open-access deregulation policies, the number of local independent electricity generation sources increases rapidly. The connection of small generation capacity sources and dispersed generation to the power distribution system, when subjected to disturbances, may aggravate considerable stability problems [4]. The stability problems may first disturb the local utility service supplies, second impact the distribution system, and then affect the transmission systems [4]. For this reason, numerous IEDs are installed to monitor the distribution system operation and transmit operation data to the controller of generators to enhance the system stability. This also creates a critical need for a power distribution system cyber-security implementation.

Commercial networks using the Internet can implement substantial and flexible communication security, such as Transport Layer Security (TLS), Internet Protocol Security (IPsec), and other network security such as ATM security and firewalls [5]-[8]. However, these commercial security implementations, with unnecessary functionality for power system operations or without considering power system characteristics, were not designed effectively for the power system computer networks to enhance its security. For example, the TLS implements its own fragmentation services [5] that would not be necessary for Distributed Network Protocol (DNP3), a typical power system computer network protocol [2]. The X.509 security certificates contain certificate handling protocols and chains of authority [9] that would be unnecessary for a utility using its control center as the certificate authority (CA). In addition, the commercial security does not provide encryption confidentiality for the entire frame, i.e. with the IPsec in tunnel mode some of the source and destination network information is still in the clear [7], which can be intercepted by a cyber-attacker.

To improve power system computer network security and reliability, this paper proposes a new security protocol layer to provide cyber-security for data transmissions in power distribution system computer networks. The security layer presented for DNP3 is located between the physical layer and the data-link layer for utility communications. The security layer includes end-to-end security and link security with encryption, authentication, and padding operations. The end-to-end security provides cyber-security for data transmissions between the data transmission source and data transmission destination IEDs, preventing intermediate IEDs and transmission links in the data transmission path from accessing the user data. The link security provides cyber-

T. Mander and F. Nabhani are with University of Teesside, U.K.
L. Wang (lwang@ee.ryerson.ca) and R. Cheung are with Ryerson University.

1-4244-1298-6/07/$25.00 ©2007 IEEE.

security between two directly connected IEDs in the data transmission path, providing security for all of the transmitted data between two nodes, i.e. not only is the user data encrypted but all of the data-link layer header data as well, with the link security, so that none of the transmitted data is in the clear that can be accessed by a cyber-attacker. In addition the security layer not only provides flexible operations, allowing new security measures to be added into the security layer, but also importantly provides quality of service (QoS). Therefore, the implemented security for a data transmission is based upon the demands of the local environment, i.e. minimal security within a small facility LAN.

An important potential application of the proposed cyber-security is to provide effective protection data transmission for the controller of the generator in distribution system to improve the stability of distribution system.

II. Security Layer Architecture

A. Security Layer Placement

The security protocol layer proposed in this paper is located between the physical layer and the data-link layer for the DNP3 protocol stack, shown in Fig. 1. The location of the security layer provides several advantages to DNP3 for cyber-security, including:

1. The proposed security layer is capable of providing confidentiality for the entire data-link layer frame, both the header data and the user data, which is not typically possible with commercial networks.
2. The proposed security layer consolidates security operations into a single protocol layer minimizing protocol overhead and redundant operations. For example, in order for the Internet to achieve the same security coverage as the security layer, the TLS would be used for the end-to-end security between the source and destination computer nodes. The TLS would then be used over the IPsec in tunnel mode to provide security between the source and destination networks. Security at the network level, such as ATM security, would be used to provide security for data transmissions through the networks on the link basis.
3. The proposed security layer virtually has no impact on the DNP3 specification since it does not require alterations to the existing specified protocol stack.

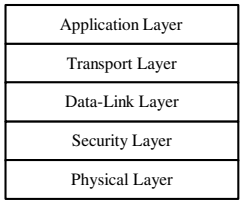

Fig. 1. DNP3 protocol layer stack with the proposed security layer

Due to the position of the proposed security layer, the entire protocol stack specified by DNP3 is above the security layer. Therefore, the security layer can rely on the upper layers to perform all of the error control and fragmentation operations that a typical security protocol has to handle. This security layer is designed for DNP3, allowing the security layer to use the DNP3 protocol stack for data transmissions by the security layer. This simplifies the proposed security layer since it does not implement its own transmission protocols that are required for typical security implementations.

B. Security Layer Scope

The security layer proposed in this paper provides end-to-end security and link security. The end-to-end security offers security between the source and the destination IEDs for the user data, which would consist of application layer data, transport layer data, and the cyclic-redundancy-check (CRC) values added into the data blocks by the data-link layer. The end-to-end security prevents intermediate IEDs or routers between the source and the destination from accessing the user data that may have been compromised.

The link security provides security between two directly connected IEDs in the data transmission path. The link security is applied to all of the data transmitted by an IED, both the frame header and user data, so that there is no data in the clear over the data transmission medium. The link security is therefore used to prevent a cyber-attacker from reading the frame's header for traffic analysis attacks. In addition, the link security is necessary for preventing attacks that are not handled by the end-to-end security, i.e. an attacker manufacturing DNP3 data-link frames using the data-link function codes [10] in an attempt to cause a destination IED to operate incorrectly to the reception of a frame, i.e. a NACK, or to cause a denial-of-service attack, i.e. sending empty data blocks with a confirmed user data function code.

If a simple master-outstation configuration is used, where there are no intermediate computer nodes between the source and the destination IEDs, the link security is equivalent to the end-to-end-security. This allows the end-to-end security to be replaced entirely by the link security. However, if concentrators are used or if routing capabilities are used as proposed in [11], both end-to-end security and the link security are required.

The security layer does not place restrictions on the types of security measures used for a data transmission, for both the end-to-end security and the link security operations. The security measures used on a data transmission can be any combination of encryption ciphers and authentication operations. This is similar to TLS and IPsec which are algorithm independent, allowing new ciphers and message digests to be added into their specifications as necessary without altering the underlying security specification [5]-[6]. The security measures defined for a data transmission use a security profile that is similar to the TLS record [5] or the IPsec Security Association (SA) [6]. The security profile is a 'recipe' for the security measures to be applied to a data transmission. Unlike with TLS which specifies that HMAC message authentication is to be used for all data transmissions [5], [12], the security profile allows both the specific type of security used for the data transmission and the number of security operations to be used for a data transmission to be variable including the authentication. The security profile is referenced with the security profile number (SPN), defined in Section III of this paper, which resembles an IPsec security parameter index (SPI) [6].

The proposed security layer also provides the capability to limit traffic analysis attacks by using padding in a similar fashion as IPsec [6]-[7]. The padding is used to cause all data-link layer frames to have the same number of octets, which would be 292 octets for DNP3. With padding, a cyber-attacker is unable to determine from the size of the frame if the frame contains 0 or more data blocks. The cyber-attacker is therefore unable to guess the contents of the user data based upon the size of the frame, i.e. link management frames would only be 10 octets [10] while certain application messages would only be an additional 2 octets [13]. The padding option is only available for the link security since padding for the end-to-end security may unnecessarily consume available network bandwidth.

C. Security Levels

The security layer operations used on a data transmission, defined by the security profile and referenced using a SPN, depend on the security level required for the data transmission. For the link security, the security level used for the data transmission depends on the local security requirements between the two directly connected IEDs, i.e. minimal security for LANs. For the end-to-end security, the security level for the data transmission between the source and the destination IEDs is dependent on the highest required link security level in the transmission path. For example, if only one of the links in the transmission path requires high security, the end-to-end security must use a high security level security profile. In general, the higher the security level the more security operations are required for the security profile. The security layer defines four security levels: No Security, Low Security, Normal Security, and High Security.

The No Security level does not define any security operations for the data. For the link security, this may represent LAN links within a facility. For the end-to-end security, this may represent peer communication within the same LAN.

Only simple encryption operations are defined for the Low Security level, such as DES. The security for this level represents data or links that have marginal value to cyber-attackers by the time the security is broken, i.e. data transmissions from a substation IED into the substation's LAN or for link status data-link layer messages.

The Normal Security level is used for typical power distribution system data transmissions and only uses symmetric ciphers. The use of the symmetric ciphers, opposed to the asymmetric ciphers, minimizes any processing delays by the security layer. Message digests and HMAC are not allowed for the Normal Security level in order to ensure that the data transmission sizes are minimal. For example, the TLS truncated HMAC uses 10 octets [14] which would represent a data transmission size increase of 3.4% to 100%, where the former would represent a full size data-link frame of 292 octets and the latter the minimum sized data-link frame of 10 octets. Instead, the authentication requirements are relaxed since the data-link layer implements several CRC checks for a frame [10] making it difficult for a cyber-attacker to create a frame that would decrypt properly with all of the CRC values being correct, the data-link function codes being correct, the transport layer state and sequence number being correct, and the application layer header including the sequence numbers being correct.

The High Security level is used for high-risk areas with potential transient or sustained attacks on the power distribution system computer networks. For this security level symmetric or asymmetric ciphers may be used and message authentication may be necessary, either a message digest or more likely the HMAC. In addition, padding may be used for the link security.

Since the security levels represent the nominal and the transient securities necessary for a particular link or between particular source and destination IEDs, multiple SPNs are required to be maintained for QoS. For example, if a transient cyber-attack occurs on the computer network, it is desirable to implement higher security operations immediately without having to negotiate the security operations. It is also desirable to return to the nominal security level immediately once the transient attack condition ends, in order to increase the efficiency of the network with decreased processing for the security operations.

III. Security Profiles

A. Security Profile Records

The security profiles proposed in this paper are similar to TLS records [5] or SAs [6] in that they indicate the security operations to be used on the data transmission. However, the security profile referenced by the SPN resembles a recipe more than a record, as the profile contains zero or more security operations to be performed on the data, such as the use of multiple symmetric ciphers on the same data transmission. The security profile records are common to all of the IED applications communicating to the same destination IED in order to decrease the number of security profiles and security profile maintenance.

The security profile recipe format for the security layer operations may cause psychological intimidation for a cyber-attacker since the cyber-attacker may have to break several encryptions on the data transmission before they can obtain the user data. In addition, allowing multiple symmetric ciphers on a data transmission can prolong the usefulness of a cipher for which a weakness has been detected, i.e. one cipher will cover the weakness of another cipher such as using two smaller key ciphers that could be broken relatively quickly on their own but are more difficult to break when used together.

The security profile records contain the following information: SPN, sequence number, expiration, validity, security operation, cipher key, cipher mode, cipher key size, and additional parameters.

SPN provides the reference to the particular security profile used for the data transmission. A received data transmission contains the SPN in the data transmission security header.

Sequence number provides the order in which the security operations are to be applied to the data transmission, with the reception operations performed in the reverse order. For

example with a high security level SPN, a symmetric encryption may be performed followed by the HMAC.

Expiration indicates the time at which the SPN is no longer valid. The SPN is not deleted immediately after expiration since some data transmissions in transit to the destination may be using the expired SPN. In this situation, to cut down on possible data retransmissions, the SPN is deleted after a specific time lapse following the expiration, i.e. based on the DNP3 application layer function codes used to determine the typical transmission time between a master and an outstation [13]. Once the SPN entry has been deleted, a cyber-attacker is unable to use a replay attack since the same SPN value would either not exist or would represent another security profile record which would cause the replay data transmission to be interpreted as a corrupted data transmission, and discarded.

Validity indicates if the SPN is currently valid or not for the end-to-end and link security. The SPN entry may be invalid if it has expired but has not been deleted yet. In addition, the SPN entry may be invalid if it is waiting for activation, which is discussed in Section VI of this paper. The state machine for the validity of the security profile is shown in Fig. 2.

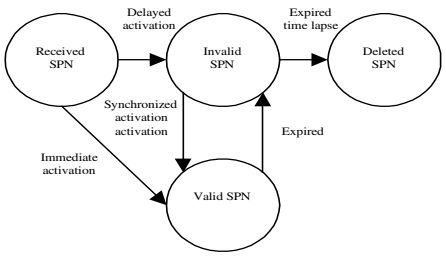

Fig. 2. Security profile record state machine.

Security operation indicates the security operation to be performed on the data transmission, such as DES, AES, Idea, Blowfish, MD5, SHA-1, HMAC, RSA, padding, etc.

Cipher key provides the cipher key to be used for the encryption operations for the data transmission. For symmetric ciphers, this key is used for both the encryption and the decryption operations. For the asymmetric ciphers, this entry contains the source's private key with the destination's public key contained in the additional parameters entry. For HMAC, this entry contains the master secret used for the authentication with the message digests.

Cipher mode indicates the cipher mode used for the symmetric keys, i.e. electronic codebook (ECB), cipher chain blocking (CBC), and cipher feedback (CFB).

Cipher key size indicates the size of the cipher key used for the data transmission since some ciphers allow different key sizes, i.e. RSA-1024, RSA-512, AES-256, and AES-192.

Additional parameters contains any other additional parameters required for the security profile record, such as the destination's public key for asymmetric ciphers and Initialization Vectors (IV) for symmetric ciphers.

B. Multiple Security Profiles

The security levels require multiple SPNs to be created for both the end-to-end security operations and the link security operations to allow quick transitions between security levels.

Multiple SPNs per security level are necessary for three other factors:

1. Increased security for subsequent security profile exchanges.
2. Increased lifespan of security profiles.
3. Increased security for data transmissions.

For factor 1, with more security profiles being used, a cyber-attacker is less capable of mounting a denial-of-service attack on the data transmissions containing a security profile replacement. If a security profile is lost in transit to an IED, there would be a sufficient number of other security profiles that can be used so that the data transmissions would not be delayed or forced to be transmitted in the clear before the replacement security profile is received.

For factor 2, the usefulness of a security profile is a function of both time and the number of data transmissions using that profile. The longer the time that a cyber-attacker has, the more time they have in which to generate possible attacks on the security profile, i.e. generating cipher keys in a brute force attack. However, the time factor is not critical given that it would take a relatively long time for the cyber-attacker to obtain the corresponding cipher key and that the security profile would be replaced before then, especially if the security profile uses multiple ciphers. With traffic analysis and cryptanalysis attacks, the more data transmissions using the same security profile, the more data the cyber-attacker has to create an attack.

Typically each security profile should be used as few times as possible before being replaced. However, due to the first factor and the fact that the DNP3 IED may use a slow link speed, limited usage of a security profile is not recommended. The limited usage of a security profile may increase the security risks involved in replacing a security profile and may as well consume network resources at the expense of time-critical data transmissions, such as transmissions of power distribution system protection data. If multiple SPNs are used, the number of transmissions for which the SPN can be used is increased by the factor of the number of SPNs available. This provides a longer time before security profiles need to be replaced, allowing them to be exchanged at a greater discretion in regards to the available network resources, i.e. during nominal operations and not during protection events.

For factor 3, since there is a different security profile for each data transmission in both the end-to-end and the link security, individual message fragments will use different security operations. Therefore, it becomes more difficult for a cyber-attacker to correlate message fragments together to determine the application message using traffic analysis or cryptanalysis. This is in comparison to IPsec, where the entire message is encrypted before being fragmented [6], allowing the cyber-attacker to piece together the fragments to determine the structure of the user data.

The actual number of security profiles used for the end-to-end security and the link security operations is dependent on the network's capability to maintain the security profiles. The limit for the total number of security profiles for all of the security levels for the end-to-end security or the link security is 256, reflecting the one octet size of the SPN within the

security header discussed in the next section. For the required security level, one of the valid security profiles is chosen at random for the security operations.

C. Security Header

A security header is required to be appended onto a DNP3 data-link layer frame in order to convey the necessary security information between IEDs for the end-to-end security and for the link security, such as the SPNs used for the security operations. The security header, as shown in Fig. 3, is placed after the start field, since the start field may be used in the physical layer as a frame delimiter. The security header, except for the link security SPN, is encrypted using the link security ciphers. Then the only data that is in the clear between directly connected IEDs is the start field and the link security SPN.

L-SPN	Option	E-SPN	Pad	L-Len	E-Len	CRC	L-Var	E-Var

Fig. 3. A full security header generated by the security layer.

In Fig. 3, the L-SPN is the link security SPN, Option is the security options field, E-SPN is the end-to-end security SPN, Pad is the padding options field, L-Len is the link length field for the L-Var field, E-Len is the end-to-end length field for the E-Var field, CRC is the 16-bit CRC field, L-Var is the link variable field, and E-Var is the end-to-end variable field.

The security header has a variable structure depending on the security operations performed on the data transmission. At the minimum the security header contains the link security SPN, the security options field shown in Fig. 4, and the CRC. The minimum-security-header structure represents a special case where there are no intermediate IEDs or routers between the source and destination IED and therefore the end-to-end security is not required.

E-SPN Used	Padding Used	L-Variable Field Used	E-Variable Field Used

Fig. 4. Security options field of the security header.

For a typical case, the security options field indicates which security operations are used. The E-SPN Used field indicates if end-to-end security is used for the data transmission. The Padding Used field indicates if the link security has used padding on the data transmission. The L-Variable Used field indicates if the link length field and the link variable field exist. The E-Variable Used field indicates if the end-to-end length field and the end-to-end variable field exist.

In most instances the end-to-end security SPN field will be present in the security header, with the link security SPN, the security options field, and the CRC. This deals with the typical cases where both the end-to-end and the link security are used for the data transmission at the Normal Security level. This security header will only add an extra of 5 octets to the DNP3 frame, which corresponds to a frame size increase of between 1.71% and 50% depending on the data-link frame size.

For some high security level cases, padding may be required for the data transmission to limit the effectiveness of traffic analysis attacks. The padding is randomly located in the frame in order to obscure data boundaries, making it more difficult for a cyber-attacker to apply cryptanalysis against the frame. The padding options field is required to indicate where the padding is located after the security header and how much padding was used for the frame.

For high security cases, the message digest and HMACs may be used by the security profile that requires the resultant values from these operations to be placed into the security header. The length fields indicate the sizes of the variable field while the variable fields contain the message digest or HMAC values. The message digest and HMAC use should be limited as much as possible since if the end-to-end security and the link security both use a truncated HMAC [12], the security header size would be increased by 22 octets. The CRC in the security header is not used for the variable fields since they are in effect an error checking mechanism similar to a CRC. The message authentication for the link security is authenticate-then-encrypt, while for the end-to-end security it is encrypt-then-authenticate.

IV. Quality Of Service

The security levels, proposed in this paper, define one type of quality of service (QoS) for the security layer, ensuring that data transmissions only use the current minimum amount of required security for the data transmission path. However, a limited amount of selective QoS security operations can be used for data transmissions based on the data-link layer function code and the application layer function code [10][13].

Certain function codes used by DNP3 can be used to disrupt the power distribution system computer network operations, such as through the use of the data-link layer function code reset-link states or through the application layer function codes dealing with application settings [10][13]. These function codes require authentication to ensure that they are not manufactured data transmissions, where the authentication can be obtained by using a High Security level security profile.

The security layer will apply the high security operations to the data transmission if the function code is listed for the QoS operations. The data-link layer function codes are determined from the data-link header. The application layer function code is determined by locating a transport layer header with the FIR value set, which indicates a start of a new message fragment [15] and therefore an application layer header containing the function code. The security layer will continue to apply the high security level operations to the frames until it locates a frame where the transport layer header FIN bit is set, indicating an end of the application layer message fragment.

Further application of QoS, based on the object type field [13], could be difficult since this would require parsing capabilities on the part of the security layer to locate the object type fields within the transport layer fragments.

V. Interoperability

The security layer's capability to be interoperable with DNP3 devices not implementing a security layer is critical to provide a smooth security layer adoption phase. Simultaneous

adoption of the security layer for the DNP3 devices would not be practical for a live operating power system.

DNP3 devices not using the security layer could not directly indicate if they use a security layer to the destination IED. As a consequence, an indirect approach is used to determine if security is used on the data transmission based on the data-link header CRC field using the method proposed in [16].

If the security layer has been used for the data transmission, the calculated CRC value will not match the received value located in the typical location for the header CRC field. This is true for a transmission error, causing corrupted data to be processed by the security layer. However, the SPN, security layer CRC, and all of the DNP3 layers' CRCs, sequence numbers, and states would have to match in order for the frame to be accepted by the DNP3 IED that is unlikely.

Before transmitting the encrypted data transmission, the security layer must ensure that the encrypted security layer does not contain a value that would cause the destination to interpret a value from the security layer header as a valid CRC value that would incorrectly indicate no security operations. If this occurrence is detected in the security layer, another security profile is randomly chosen for the data transmission in order to remedy this situation. Once the security layer is used for a connection, for either the end-to-end or the link security, the security layer will expect all data transmissions to use the security header, even if the No Security level is used. Otherwise, any data transmission that does not use the security header and security layer operations will be discarded.

VI. Security Profile Management

A. Security Layer Initialization

One of the difficulties for typical network security, such as IPsec and TLS is obtaining the trusted public key of the intended recipient that can then be used to create a security session between the source and the destination. This difficulty results in complex protocols to provide the automated key exchanges, such as Internet key exchange (IKE) [17] and the Internet X.509 public key infrastructure certificate management protocol [9]. However, the complexity of the automated key exchanges and the security certificates can be avoided for the security layer if a control center is used as the CA and the IED security layers are manually configured.

With the power system network control center as the CA, the security certificates are reduced to the identity of the source or destination IED with the source's or destination's public key that is to be used for the connection. The amount of asymmetric cipher information maintained by an IED security layer is therefore small, i.e. 258 octets per connection for RSA-1024 using the data-link destination address as the identity and assuming the source uses a separate private key per connection.

With manual configuration, the security certificates can be directly downloaded at the physical site within the distribution system into the IED's memory as well as the security profiles, as shown in Fig. 2 for the immediate activation. This entirely avoids the risk of the initial downloading of security information via the network for the security layer. The initialization of the security profiles, and the security certificates used to maintain subsequent asymmetric cipher security profiles, is performed for all current connections to the IED that use the security layer.

B. Initialization of New Peer Connection

When a new peer connection is created for the security layer, i.e. due to the adoption of the security layer by the peer node or temporary use of a laptop computer for site maintenance, the power system network control center acts as both the CA and a relay point for the security profile initialization between the peers, as shown in Fig. 5. Once the peer security profiles have been initialized, the master is responsible for the subsequent end-to-end security profile maintenance with the outstation.

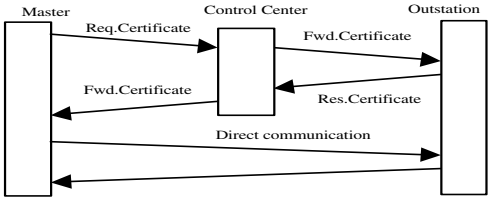

Fig. 5. Peer security initialization after the security layer has been initialized.

With the control center performing the CA and relay functions, the complexity of the security initialization is simplified in comparison to IPsec and TLS. Since all IEDs can be expected to have typical communication with the control center acting as the CA, the IEDs will be able to use a High Security level security profile using asymmetric ciphers to convey the security initialization request to the control center. The request will include a security certificate containing the master's address and its public key that is to be used by the peer IED for the connection. The control center will forward the security certificate to the outstation using a High Security level security profile that uses asymmetric cryptography. The outstation will respond to the security certificate with its own security certificate that is to be used for the peer connection by sending the certificate to the control center using asymmetric cryptography. The control center will forward this certificate to the master at which the master will be capable of directly communicating with the outstation.

The security certificate exchange using the control center provides several advantages to the security layer and the power distribution system. Since the control center is used for typical communication, the asymmetric cryptography provides authentication and non-repudiation for the security initialization between the peers. The control center can guarantee the identities of the IEDs to each other. Also there is no data that is transmitted in the clear between any of the IEDs involved in the peer connection, providing additional security to the distribution system data communications. In addition, since the control center is used only to relay the security certificates, the control center does not have to maintain the certificates or revocation lists. The peer IEDs are capable of maintaining the connection without the control center's involvement due to the specific public keys used for

the connection rather than a single public key for all connections.

C. Subsequent Security Profile Management

The security profiles have an expiration given by the security profile record that requires periodic replacement of the security profiles as they expire and are deleted as shown in Fig.2. The master is responsible for the security profile replacement operations for itself and for the outstation that it is communicating with. Once a security profile has expired, the master will generate a replacement security profile which has the security operations corresponding to the current security level for the end-to-end security or the link security, i.e. symmetric ciphers, asymmetric ciphers, authentication, and padding. The security layer transmits the security profiles using a High Security level security profile, where asymmetric ciphers are recommended for greater authentication and non-repudiation capabilities.

Since the security profiles are exchanged using a High Security level security profile, a mechanism must be introduced to detect when a data transmission contains a part of the security profile. The security layer is a DNP3 application in order to minimize its impact on the current DNP3 specification. In this situation, the security layer uses the DNP3 protocol stack, shown in Fig. 1, to transmit the security profiles as data sets. As a consequence, the QoS dealing with function codes cannot be used to determine if a security profile is being transmitted. Instead, the QoS must be extended to the object group number to determine if a security profile is being transmitted. This requires application layer object group numbers specific to the security layer rather than relying on the object group numbers used for the data sets [18]. The difficulties of using DNP3 data sets for the security profiles include: the data set identifier element values that are not static or the same for all IEDs [18], and data set identifier element values that would require more parsing capability on the part of the security layer to detect a security profile. The object group number required for the security profiles have an added requirement that there is only a single data set per message fragment in order to avoid the need to create parsing capabilities to search through the user data for other security profile data sets.

The activation of the security profiles is synchronized so that the security profiles become active at the same time at both the master and the outstation, which is shown in Fig. 2. The synchronized activation of the security profiles is possible with the power system since accurate time stamps are critical for many applications and therefore the IEDs are expected to have accurate means of maintaining time, i.e. global positioning system (GPS). With the synchronized activation of the security profiles, a potential problem of one IED attempting to use a security profile before the other IED has activated the security profile is avoided. The synchronized activation represents the expected amount of time, based on the application layer function codes used for determining delays between IEDs [13], before the outstation receives and processes the new security profile.

The transmission of the security profiles requires a minor alteration to the application layer specification for data retransmission errors. Since the security profiles are synchronized, retransmission of a security profile may be received at the outstation after it should have been activated. Therefore, the DNP3 application layer has to indicate to the security layer when a security profile has to be retransmitted so that its synchronized activation time can be updated.

VII. Application for Distribution System Stability

The proposed security protocol layer for DNP3 has tremendous application potentials for live power system operations, such as a unique application to provide comprehensive security of data transmission for distribution system stability control.

Stability concerns increase rapidly with today's growing demands for open access to power systems for electricity generation and trading, facilitated by new government deregulations. As proposed by the authors previously [4], a novel generator control based on step-ahead predictive control methodology and state-of-the-art real-time digital signal processing (DSP) technology has been proposed to significantly improve the stability and operational coordination of distribution systems particularly those with dispersed generations, open access operations, or weakly connections to bulk power systems. However, due to limited computational capabilities of general-purpose microprocessors, the predictive control method was originally proposed only for the Single Machine Infinite Bus (SMIB) system. In general, it is fairly difficult to control the disturbances and its consequently potential stability problems in the power distribution system due to its constantly varying loads. The control method designed for the SMIB system often experiences difficulties for application in power distribution systems.

With the utilization of the integrated network security proposed in this paper, the novel generator stability control that was previously proposed by the authors [4] can be applied to enhance the stability of power distribution systems. For this stability control application, a real-time equivalent circuit of the power distribution system has to be created for use in the predictive control. For example, in order to use the predictive control method to control the generator GEN-1 shown in Fig.6 that is simplified from the benchmark distribution system given in IEEE Std. 399-1997 for distribution system studies [19], an equivalent-circuit for the power distribution system at the point of connection for the generator GEN-1, as shown in Fig.7, has to be obtained through the calculation of the equivalent impedance and equivalent voltage.

In general, it would be difficult to obtain an accurate equivalent circuit for a power distribution system because its loads often switch on or off. With data collecting devices or IEDs installed at the buses to monitor the disturbances caused by load changes or faults in the power distribution system, the operation data on each bus in the distribution system can be transmitted to the controller of the generator to update the equivalent circuit impedance and voltage. The cyber-security

protocol proposed in this paper can be used to ensure the integrity of data transmissions for creation of an equivalent circuit for use in the stability control of distribution systems.

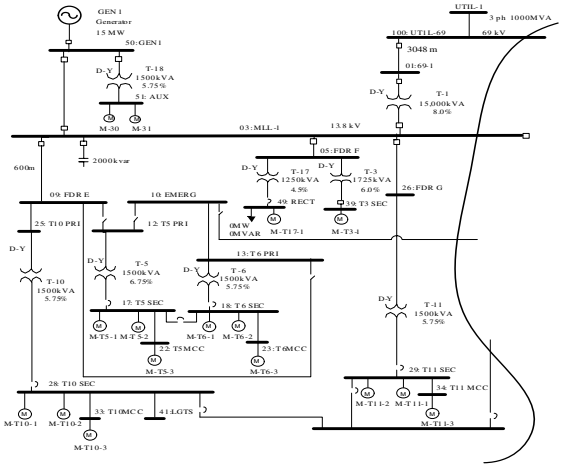

Fig.6 Simplified one-line diagram for IEEE power system

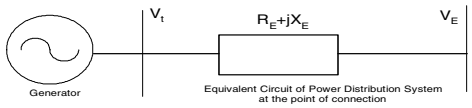

Fig.7 Equivalent circuit for the power distribution system shown in Fig. 6

VIII. Conclusion

Ongoing automation and the open access implementation of the power distribution system are increasing cyber-security vulnerability of utility computer networks. The security protocol layer for DNP3 has been proposed in this paper to provide comprehensive security for distribution system computer networks. The proposed security protocol layer, located below the DNP3 data-link layer, considers the power distribution system characteristics and minimizes the impact on the DNP3 specifications by limiting its overhead and interaction with the currently specified DNP3 protocols.

The security protocol layer provides flexibility, coverage, and quality of service capabilities for security operations on data transmissions through the use of the security profile recipe format proposed in this paper. Since security profile recipe formats provide independent cipher and authentication operations, the security layer can adopt new ciphers and authentications without specification changes to security layer.

The security layer provides security operations for control, monitoring, and protection data transmissions between the source and destination IEDs on an end-to-end security basis and a link security basis. It also provides various levels of security, with each security level containing multiple security profiles of one or more ciphers and zero or more authentications. With multiple security levels containing multiple security profiles, an IED could switch to a higher security state immediately during transient or sustained attacks, and then immediately transition back to the nominal state after the attack to improve security layer performance. Therefore, the proposed security protocol layer for DNP3 can provide strong security for the power distribution system data transmissions.

IX. References

[1] Justin Blum, "Hackers target U.S. Power Grid," Washington Post, March 11, 2005.

[2] "The World Market for Substation Automation and Integration Programs in Electric Utilities: 2005-2007 Executive Summary North American Market," Newton-Evans Research Company, September 2005.

[3] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendation," U.S.-Canada Power System Outage Task Force, April 2004.

[4] L. Wang, Q. Jin, F. Chen, R. Cheung, "Predictive Generator Control for Improvement of Power Distribution System Stability," in *Proc. 2006 IEEE Large Engineering Systems Conference on Power Engineering Conference,* TC-Distribution System Studies I, pp.67-71, July 2006.

[5] *RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1*, Internet Engineering Task Force (IETF), April 2006.

[6] *RFC 4301: Security Architecture for the Internet*, Internet Engineering Task Force (IETF), December 2005.

[7] *RFC 4303: IP Encapsulating Security Payload (ESP)*, Internet Engineering Task Force (IETF), December 2005.

[8] *ATM Security Specification Version 1.1,* The ATM Forum, March 2001.

[9] *RFC 4210: Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*, Internet Engineering Task Force (IETF), September 2005.

[10] *DNP3 Specification Volume 4: Data Link Layer*, DNP User's Group, December 2002.

[11] T. Mander, F. Chen, R. Cheung, and F. Nabhani, "Mechanism of Unlimited WAN Expansion for Networks in Power Distribution Systems," in *Proc. 2006 IEEE Large Engineering Systems Conference on Power Engineering (LESCOPE 2006) Conf.*, pp. 72-76.

[12] *RFC 2104: HMAC: Keyed-Hashing for Message Authentication*, Internet Engineering Task Force (IETF), February 1997.

[13] *DNP3 Specification Volume 2: Application Layer*, DNP User's Group, October 2005.

[14] *RFC 4366: Transport Layer Security (TLS) Extensions*, Internet Engineering Task Force (IETF), April 2006.

[15] *DNP3 Specification Volume 3: Transport Function*, DNP User's Group, November 2002.

[16] T. Mander, L. Wang, R. Cheung, and F. Nabhani, "Adapting the Pretty Good Privacy Security Style to Power System Distributed Network Protocol," in *Proc. 2006 IEEE Large Engineering Systems Conference on Power Engineering (LESCOPE 2006) Conf.*, pp. 79-83.

[17] *RFC 4306: Internet Key Exchange (IKEv2) Protocol*, Internet Engineering Task Force (IETF), December 2005.

[18] DNP3 Technical Bulletin TB2004-004e: Data Sets, DNP User's Group, March 2006.

[19] IEEE Std. 399-1997, "IEEE Recommended Practice for Industrial and Commercial Power Systems Analysis," 1997.

X. Biographies

Todd Mander received his B.Eng. degree from Ryerson University. He is currently working on his doctorate degree in power system computer networks at the University of Teesside through Ryerson University.

Farhad Nabhani has B.Sc., M.Sc., and Ph.D. degrees. He is a Reader and M.Sc. Course Leader at the University of Teesside.

Lin Wang received her B.Eng., M.Eng., and Ph.D. degrees from Huazhong University of Science and Technology, and was an Associate Professor. She is currently conducting research at Ryerson University.

Richard Cheung received his B.A.Sc., M.A.Sc., and Ph.D. degrees from the University of Toronto. He was a Research Engineer in Ontario Hydro. Currently he is a Professor at Ryerson University, and he is an active Power Engineering consultant and is the President of RC Power Conversions Inc.