Wang, L. et al. (2007) 'Security operation modes for enhancement of utility computer network cyber-security', IEEE power engineering society general meeting, Tampa, Florida, June 24-28. IEEE, Art. no. 4275951.

Security Operation Modes for Enhancement of Utility Computer Network Cyber-Security

Lin Wang, Todd Mander, Helen Cheung, Farhad Nabhani, Richard Cheung

Abstract—**Concerns for utility computer networks' security and reliability are growing rapidly due to increasing utility devices with connections to external networks. This aggravates vulnerability of utility networks to cyber-attacks through external connections. Though encryption can provide security for user data transmissions, encryption itself could not provide protections against traffic-analysis attacks. Techniques against traffic-analysis attacks through statistically controlling the transmission rate of padded and encrypted frames are unsuited for power system applications. This paper proposes three security operation modes for the newly developed security layer, located below DNP3 data-link layer, to strengthen encryption and authentication operations against the effectiveness of traffic-analysis and cryptanalysis attacks. The security modes use padding to disguise the amount of user data transmitted and disguise the user data-link layer frame amongst a group of manufactured frames similar to statistically controlling data transmission rate. The proposed security operations have been successfully applied to enhance power system security controls.**

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

I. Introduction

CYBER-security becomes a growing concern for power system utilities with increasing power system computer network interconnections, power system automation, and open access requirements under government deregulation policies [1]-[3]. Typical utility network protocols such as DNP3 [4] were originally designed for networks that were only accessible by limited number of trained utility staff. As a consequence, DNP3 and other utility network protocols did not implement security such as encryption and authentication, now causing them to be vulnerable to cyber-attacks in the more open networking environment that has been aggravated with open access utility power systems.

A. Cyber-Security for Utilites

With implementation of encryption and authentication security, with only authentication currently proposed for the DNP3 specification [5], utility communication is still vulnerable to attack due to the predictability of data transmission timing and sizes. Traffic-analysis attacks based on encrypted data transmission headers, frame sizes, and timing can be used to accurately determine the data transmission type, i.e. unsolicited protection data transmissions are unlikely to occur at a normal solicited data transmission time and control data will use less frames than monitoring data. Based upon the traffic analysis attacks, cyber-attackers may be able to determine weaknesses to exploit within the power system, such as locating equipment to damage that will have a larger effect on power system operations than what would normally occur or implementing a denial-of-service attack on a networked device so that it cannot respond appropriately to protection events, i.e. unable to transmit a control command to a device to close circuit breakers. In addition, cryptanalysis attacks can be combined with traffic analysis attacks to break the encryption on the data transmissions, allowing a cyber-attacker to manipulate data and devices directly, i.e. influencing the behavior of operations by altering or creating data and controlling the operations of a device by activating relays. Therefore failure to provide adequate security for power system data transmissions may have severe consequences for power system operations.

B. Proposed Security Operation Modes

A new cyber-security pseudo-layer is proposed to enhance encryption security by providing increased effectiveness against traffic analysis and cryptanalysis attacks than simply using encryption security only. The proposed security layer is located below the DNP3 data-link layer. The security layer comprises three security operation modes that are derived from methods used to statistically control the transmission rate of frames. The three security operation modes are: padding, frame transmission group (FTG), and split-frame transmission group (SFTG). The security operation modes provide enhanced encryption confidentiality capabilities and limited traffic analysis prevention capabilities.

The security operation modes enhance typical methods used to counteract the traffic analysis attack potential, which can use padding to disguise the size of the user data and statistically control the transmission rate of frames [6]-[7]. These methods ensure that all data transmissions are all the same size and that data transmissions occur at a specific interval, where data transmissions will be created if no user data is available for transmission. With these methods, combined with encryption security for the entire frame including the entire frame header, traffic appears to be entirely uniform to an attacker. A cyber-attacker is unable to

T. Mander and F. Nabhani are with University of Teesside, U.K.
L. Wang, H. Cheung and R. Cheung are with Ryerson University, Canada.

determine the nature of the data being transmitted, such as differentiating between control and protection oriented data transmissions.

For power system utilities padding can be effectively implemented, such as with the padding mode in this paper, but statistically controlling the transmission rate of frames is not as practicable resulting in the FTG and SFTG security modes proposed in this paper. There are two main reasons for difficulties in applying the statistical transmission rate.

The first reason is due to the specific transmission rate for solicited data transmissions, i.e. control and monitoring data, which are highly consistent and predictable in their timing. Therefore, cyber-attacks would be able to use traffic analysis accurately to discard most of the frames created by the statistical transmission rate to fill in the data transmission gaps when no user data was being transmitted. As a consequence, DNP3 devices would have to process and transmit more data without discernable increased security.

The second reason is due to protection oriented data transmissions. The protection oriented data transmission timing is unpredictable and cannot be delayed since they are time-critical to ensure reliable power system operations. Since the protection data transmissions are time-critical, DNP3 devices using the statistical transmission rate for frames would have to increase the transmission rate to produce a uniform traffic pattern that will not delay protection data transmissions. However, this would cause a DNP3 device to expend greater resources inefficiently to create frames between the typical data transmission rate, for solicited control and monitoring data, which are unlikely to contain any protection data. For example, if the allowed transmission delay for protection data was 4 milliseconds and the normal interval between transmission times was 2 seconds, the DNP3 outstation device would typically have to produce 500 unnecessary frames between user data transmissions within the 2 second interval. Time-critical protection data transmission therefore limits the applicability of statistically controlling the transmission rate used in power system computer networks.

The FTG security mode and the SFTG security mode are designed in this paper to counteract these drawbacks for implementation of statistically controlling the transmission rate of frames for power system computer networks. The FTG security mode incorporates the padding mode and places the user data-link frame within a group of manufactured frames, forcing a cyber-attacker to spend resources on determining which frame contains the user data. The SFTG security mode incorporates the FTG mode, but splits the user data-link frame into a group of manufactured data-link layer frames, forcing the attacker to spend resources on reassembling the user data-link layer frame before they can attack it.

The performances of the three security modes are analyzed and the results show that the padding mode is suited for lower security demands; the FTG security mode provides much higher security than the padding mode, but with increased processing overhead; the SFTG security mode provided much higher security than the FTG mode, but with higher processing demand. The FTG and SFTG modes are recommended for links requiring high security or for links that temporarily require higher security during cyber-attacks.

C. Application for Enhancement of Power System Controls

The power distribution system operations can be significantly enhanced with the use of modern real-time computer communication and networking technology and state-of-the-art digital signal processing technology. The security operations proposed in this paper have been successfully applied for enhancement of laboratory prototype power distribution system stability control. An illustration is given in this paper.

II. Security Operation Modes

A. Padding Mode

The padding security operation mode is used to pad all DNP3 data-link layer frames to the same size, which is the maximum 292-octet data-link frame size. Encryption and authentication is applied to the data-link layer frame by the security layer after the padding has been added into the frame. The security-layer padding mode is used when a normal level of security is required for the power system computer network since it does not introduce any significant overhead for the security operations or bandwidth. This mode would therefore be typically used in substation LANs, for low risk links such as connecting devices into the substation, or for minimal risk links such as links that have never been attacked.

The padding of each individual data-link frame provides security for that particular data-link frame but not for the application message fragment. This limits the usefulness of the padding operations since a cyber-attacker could count the number of data-link frames used to convey the application message fragment to determine if control, monitoring, or protection data is being transmitted. However, the padding does help obfuscate the differences between data-link layer only messages that are 10 octets [8], application layer messages using function codes for which the application header and possibly only the object header is required [9], or for other application messages that are less than the maximum allowed 249 octets for transport layer fragmentation [10].

For application layer messages divided into several data-link layer frames, the padding hides the size of the last data-link layer frame in the sequence. Disguising the size of the last fragment may provide security against cyber-attacks if specific types of data always have the same number of octets in the last data-link layer frame used for the application layer fragment.

The padding is placed randomly within the data-link layer frame in order to obscure the data boundaries in the frame, i.e. the cyber-attacker is unable to assume that the twelfth octet in the frame would be the application header. The padding mode operation is shown in Fig.1 before encryption and authentication.

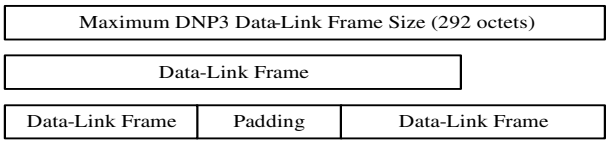

Fig.1. DNP3 data-link frame padded to maximum 292 octets.

In Fig. 1, padding octets are generated for the DNP3 data-link layer frame so that it is the maximum allowed 292 octets. The padding is then randomly placed into data-link layer frame at any point.

B. Frame Transmission Group Mode

The frame transmission group (FTG) security mode is used to disguise an encrypted data-link layer frame amongst a group of encrypted manufactured frames. The FTG security mode includes the padding mode operation so that all of the frames in the transmission group are the same size.

In the FTG mode, the data-link layer frame containing the user data is placed randomly within the group of manufactured frames, resembling statistical control of the data transmission timing. Therefore, there are a limited number of frames being transmitted at the expected transmission time, but with the real frame randomly placed within those frames. A cyber-attacker is therefore unable to precisely determine which data-link layer frame contains the user data and therefore must spend resources on examining each of the frames within the transmission group to determine the location of the user data. The FTG security mode is shown in Fig. 2.

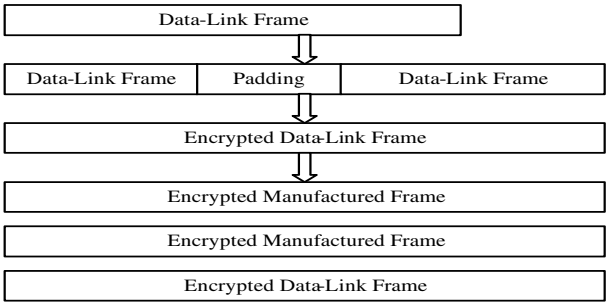

Fig. 2. FTG security mode operations are shown randomly placing the user data within the frame transmission group.

In Fig. 2, the user data-link layer frame is padded and then encrypted and possibly authenticated. The encrypted user data-link layer frame is then randomly placed amongst the encrypted manufactured frames in the transmission group.

The FTG security mode has the same limitation as the padding mode in which a cyber-attacker could count the number of data-link frames used to convey the application message fragment to determine if control, monitoring, or protection data is being transmitted.

The FTG mode provides more security than the padding mode, and is therefore used for links that are more vulnerable to attack such as those connecting to smart meters or for links between important DNP3 devices such as between substations. However, since the FTG security mode manufactures multiple frames to disguise the user data, this mode requires more processing and bandwidth capability which limits its applicability to low bandwidth devices.

C. Split Frame Transmission Group Mode

The split frame transmission group (SFTG) security operation mode is used to disguise a data-link layer frame amongst a group of manufactured frames. The SFTG security mode is derived from the FTG security mode. However with the SFTG security mode, the encrypted and authenticated user data-link frame is divided into several manufactured frames that are then encrypted rather than disguising the actual frame amongst a group of manufactured frames.

In the SFTG mode, the data-link layer frame containing the user data is encrypted without padding. The encrypted data-link layer frame is then divided into a number of segments, with the number of segments being equal to the size of the transmission group. Each segment is random in size and each segment is placed randomly within an assigned manufactured frame. In essence, the operations for the segments are similar to the padding mode operations. All of the manufactured frames are then padded to the same size as was performed in the other two security modes before being encrypted. The SFTG security mode is shown in Fig. 3.

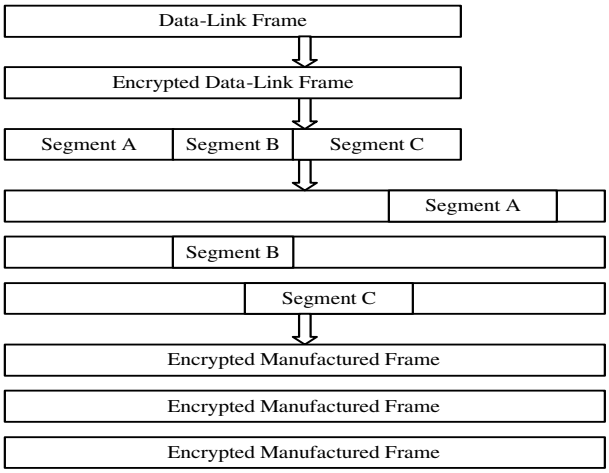

Fig. 3. SFTG security mode operations are shown randomly placing the user data within the frames of the transmission group.

The SFTG security mode transmits a limited number of frames at the expected transmission time for a cyber-attacker, but with the user data-link layer frame randomly placed into those frames. The cyber-attacker must therefore manipulate all of the frames in the transmission group and reassemble the user data-link layer frame before being capable of obtaining the user data.

The SFTG security mode has the same limitation as the FTG security mode in which a cyber-attacker could count the number of data-link frames used to convey the application message fragment to determine if control, monitoring, or protection is being transmitted.

The SFTG mode provides more security than the FTG mode since a cyber-attacker has to manipulate more data, and is therefore used for links that are undergoing attack or links that are critical to power system operations and can therefore be expected to be attacked. However, since the SFTG security mode manufactures multiple frames to disguise the user data and uses more encryption operations, this mode requires more processing and bandwidth capability which limits its applicability to low bandwidth devices.

D. Security Header

The security modes require that a security header be appended onto the data-link layer frame so that the receiving DNP3 device could determine which security operations are to be performed on the data-link layer frame. The security layer header is shown in Fig. 4.

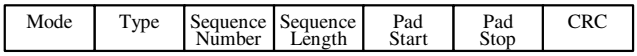

Fig. 4. Security header appended onto the DNP3 data-link layer frame before encryption and authentication.

In Fig. 4, there are six fields in the security header, which are: mode, type, sequence number, sequence length, pad start, pad stop, and CRC.

Mode: indicates the security mode used for the data transmission. With this indication within the frame, source and destination devices can independently and immediately transition to another mode without informing the other device prior to the transition. This increases the security layer responsiveness to changes in the security requirements.

Type: indicates if the frame contains user data or if the frame is manufactured.

Sequence Number: provides the frame sequence for the SFTG mode so that the frame containing the user data can be properly reassembled from the manufactured frames. This field has no relevance to the other modes.

Sequence Length: indicates the number of frames in the SFTG transmission group. This field provides the flexibility for a security layer to alter the number of frames used in SFTG transmission group without previously negotiating this value. This increases the security layer responsiveness to changes in security requirements.

Pad Start: For the padding and FTG security modes this field provides the starting octet location of the padding within the frame. For the SFTG mode, this field indicates where the encrypted user data-link layer frame segment begins within the manufactured frame.

Pad Stop: For the padding and FTG security mode this field provides the ending octet location of the padding within the frame. For the SFTG mode, this field indicates where the encrypted user data-link layer frame segment ends within the manufactured frame.

CRC: provides a cyclic redundancy check for the security header.

E. Interoperability and Security Mode Transitions

A difficulty in adopting any changes to a standard such as DNP3 is interoperability between devices that have not adopted the security, as well as devices using different security modes. The interoperability between devices using security and those not using security is required since immediate adoption of the security would be difficult and expensive to perform. Interoperability between devices using different security modes is necessary to allow devices using lower security capabilities to communicate with devices using higher security capabilities. The security layer interoperability issues are handled through the security layer operations and the security header appended onto the DNP3 data-link layer frame before encryption.

For the interoperability between DNP3 devices using the security and devices that do not, the frame size indicates if security has been used on the data-link layer frame. All the security modes pad the data-link layer frame to the maximum allowed 292 octets. The security header is then added onto the frame. Therefore, if the frame is larger than 292 octets, security has been used otherwise the security layer modes were not used for the data-link layer frame.

Previously discussed for the security header were the mode and sequence length fields. These two fields allow the security layer to transition between security modes independently in regards to any other DNP3 device. For the padding and FTG security modes each received frame is independent of the frames previously received or which will be received. These modes are only concerned if the frame is manufactured or not. Manufactured frames are discarded immediately by these modes while the user data-link layer frame is sent to the DNP3 protocol stack for processing. For the SFTG security mode, the current size of the frame transmission group is the only concern for reassembling the user data-link layer frame. The size or types of previously received or that will be transmission groups do not affect the SFTG operations.

The security layer is designed to operate on a link basis rather than for all of the links connected to the device. Therefore security is independent for each link, allowing the security layer to implement a different security mode for each link. Changes to the security mode are initiated by a master. An outstation implements the changes upon reading the mode and frame transmission group size from the security header received from the master.

The flexibility in transitioning between security modes provides the means for a device to operate in a nominal mode and then transition to a higher security mode when necessary. Therefore, DNP devices with low processing or bandwidth capability can still elicit the FTG and SFTG security modes on a temporary basis when necessary, increasing security while decreasing the device polling by a master to obtain the necessary bandwidth to handle the security mode operations (either the number of polls or the type of data being polled).

III. Security Layer Analysis

The security layer is designed to provide additional strength to encryption and authentication operations in limiting the effectiveness and applicability of traffic analysis and cryptanalysis attacks. The security layer increases the amount of data that a cyber-attacker must manipulate as well as the amount of time for them to obtain the user data. The security layer is not designed to protect against attacks such as replay attacks. However, the DNP3 protocol stack provides protection from replay attacks due to the use of two sets of sequence numbers, the fragmentation sequence numbers used by the transport layer and the message fragment sequences of

the application layer [9]-[10]. The transport layer sequence number space is larger than the application layer sequence number space [9]-[10]. Therefore, a replayed frame is unlikely to have sequence numbers that match both the expected transport layer and application layer sequence numbers, causing these frames to be discarded.

A. Padding

The padding security mode adds very little processing overhead to the security operations and therefore provides nearly the same performance as simply encrypting and authenticating the data. The padding operations provide essential security to limit the capability of traffic analysis attacks based on the frame size. However, as mentioned this security can only be provided for each individual data-link layer frame that is transmitted since the security does not alter the DNP3 specification. Therefore, a cyber-attacker can still count the number of frames in the data transmission to determine the nature of the data transmission, whether it is control, monitoring, or protection data. This weakness could be remedied if the application layer padded all message fragments to the same size, however, this would require a DNP3 specification change which would violate the constraints created for the security layer.

Since the padding operations are nearly equivalent in performance and security as to simply using encryption on data transmissions, it is used as the basis for comparison with the other security modes. The time in which to break the encryption for a security layer frame using the padding operation is given in (1) as a general equation for any cipher and cipher mode for a brute force attack. Cryptanalysis is assumed to shorten this time by a scalar factor dependent on the cipher, key length and technology currently available for cryptanalysis attacks. However, the relative amount of time to break the encryption is the same for all of the modes, eliminating the need to discuss complicated factors that affect the strength of the cipher such as those pertaining to cryptanalysis.

$$T = ET \tag{1}$$

where T is the total time to break the frame encryption, and ET is the time to break the security layer frame encryption for the padding mode dependent on factors such as cipher, cipher mode, key size, and currently available cryptanalysis attack techniques.

B. Frame Transmission Group

The FTG security mode increases the overall processing for the security layer where the security layer generates *(N-1)* frames, where N is the size of the data transmission group. However, the processing requirements for the destination device are much lower since the security layer can discard the manufactured frames based on the security header.

For the FTG security mode, the security layer also requires a bandwidth increase by a factor of N to provide the same performance as a device that did not use the security layer due to the additional manufactured frames. The bandwidth may not be an issue for LANs or for networks using fiber-optics as the transmission medium since the DNP3 frames are much smaller than the available bandwidth.

The strength of the FTG security mode in comparison to the padding mode can be classified into three scenarios: best-case, worst-case, and average-case. The best-case scenario is given in (2) and represents the cyber-attacker having to attack all the frames in the transmission group before locating the frame containing the user data as determined from the type field in the security header. For the best-case scenario the security for the data transmission is equivalent to the number of frame used in the transmission group.

$$T = N \times ET \tag{2}$$

where T is the total time to break the frame encryption, N is the number of frames in the transmission group, and ET is the time to break the security layer frame encryption dependent on factors such as cipher, cipher mode, key size, and currently available cryptanalysis attack techniques.

The worst-case scenario is given in (3) and represents the cyber-attacker locating the user data on the first attempt, where a cyber-attacker can determine a successful attack from the type field in the security header. The worst-case scenario of (3) is the same as the padding security mode given by (1).

$$T = ET \tag{3}$$

where T is the total time to break the frame encryption, and ET is the time to break the security layer frame encryption dependent on factors such as cipher, cipher mode, key size, and currently available cryptanalysis attack techniques.

The average-case scenario is given in (4) and represents the average number attempts for an attacker to locate and obtain the user data.

$$T = A \times ET = \frac{\sum_{i=1}^{N} i}{N} \times ET \approx \frac{N}{2} \times ET \tag{4}$$

where T is the total time to break the frame encryption, A is the average number of attempts to locate frame containing the user data in the frame transmission group, ET is the time to break the security layer frame encryption dependent on factors such as cipher, cipher mode, key size, and currently available cryptanalysis attack techniques, N is the number of frames in the transmission group, and i is the frame position within the group.

The FTG security therefore on average provides *N/2* times greater security than the padding security mode. In order for the FTG mode to provide more effective security than the padding security mode, the transmission group size must be larger than 2. Therefore FTG at least requires a bandwidth three times greater than what would be required if security was not used or if the padding security mode was used.

The FTG security mode also favors smaller transmission group sizes, which limits the required additional bandwidth for this security mode. Since (4) indicates that the average amount of time to break the security is half of the transmission group size, large transmission groups do not

provide as much security for the data transmissions in comparison to the amount of time it would take to manufacture and transmit the frames.

For the FTG security mode to be effective, each of the frames in the transmission group must be using different encryption, as was proposed for the security layer. If the same encryption was used for each of the transmission group frames, the security would be equivalent to (3), which is no security improvement compared to the padding security mode. The FTG security mode is also still vulnerable to the traffic analysis attack where the total number of frames transmitted within a period of time is counted to determine the type of data being transmitted, i.e. control or monitoring data.

C. Split Frame Transmission Group

The SFTG security mode increases the overall processing for the security layer in comparison to the FTG mode with the security layer generating *N* frames, where *N* is the size of the frame transmission group. In addition, the destination requires more processing capability for the SFTG modes since it must reassemble the user data-link layer frame from the manufactured frames. The SFTG security mode therefore requires a bandwidth increase by a factor of *N* to provide the same performance as a device that did not use the security layer due to the additional manufactured frames. The bandwidth may not be an issue for LANs or for networks using fiber-optics as the transmission medium since the DNP3 frames are much smaller than the available bandwidth.

The strength of the SFTG security mode is given by (5) in comparison to the padding mode.

$$T = (N+1)ET \tag{5}$$

where *T* is the total time to break the frame encryption, *N* is the number of frames in the transmission group, and *ET* is the time to break the security layer frame encryption dependent on factors such as cipher, cipher mode, key size, and currently available cryptanalysis attack techniques.

The SFTG security therefore provides *(N+1)* times greater security than the padding security mode. The SFTG mode provides stronger security with its minimum transmission group size (*N*=2) than the FTG mode does with its minimum transmission group size (*N*=3). The SFTG security mode requires a bandwidth at least two times greater than what would be required if security was not used or if the padding mode was used. Since the SFTG security mode provides as much security as the size of the transmission group, larger transmission groups provide greater security. The limiting factor for the SFTG security mode is the bandwidth limitations, the delays associated in reassembling the user data from all the manufactured frames, and the increased processing requirements.

For the SFTG security mode to be effective, as was the case for the FTG security mode, each of the frames in the transmission group must be using different encryption, as was proposed for the security layer. The SFTG security mode is also still vulnerable to the traffic analysis attack where the total number of frames transmitted within a period of time is counted to determine the type of data being transmitted, i.e. control or monitoring data.

The SFTG security mode is slightly less vulnerable to replay attacks than the other security modes since the frames in the transmission group are not independent of each other. If an attacker inserts a frame into the sequence, the reassembled frame by the security layer is unlikely to have valid DNP3 data-link layer CRC values, and will therefore be discarded by the data-link layer. Valid CRC values are very unlikely since the user data segments are random in size and will therefore not match the user block(s) CRC values.

D. Performance

The three security-mode operations were tested using non-optimized code complied for Windows 2000 on a Pentium 550 MHz machine using a commercial visual-based compiler and commercial software encryption components. Therefore higher performance would be expected for an optimized real-system device.

In Fig. 5, the padding security mode operations are shown with various sized data-link frames, from the minimum 10 octets to the maximum 292 octets. The data transmission size axis is marked for the user data sizes from the transport layer, and therefore range from 0 octets (frame size = 10 octets) to 250 octets (frame size = 292 octets). The encryption used with the padding mode was the 256-bit Advanced Encryption Standard (AES) using the chain blocking cipher (CBC) mode with no authentication.

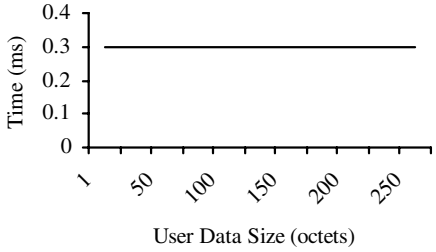

Fig. 5. Padding mode operation performance for various user data sizes.

As can been seen from Fig. 5, the padding operations (rounded to the nearest tenth of a millisecond) have negligible effects on the encryption operations. Therefore, only the FTG and SFTG security modes require consideration performance wise for the DNP3. The same test was performed for the padding mode decryption operations, with negligible differences between encryption and decryption operations.

In Fig. 6, the FTG and SFTG security mode encryption operations are shown compared to each other for various transmission group sizes. The minimum FTG transmission group size was *N*=3 while the SFTG minimum transmission group size was *N*=2. Transmission group sizes was limited to ten since large transmission group sizes are not practical for DNP3 devices, due to the overhead in manufacturing frames and the delays associated with the destination receiving the data, especially with the SFTG mode where the data is divided across all of the frames in the transmission group. The same encryption was used for the FTG and SFTG modes as the padding mode.

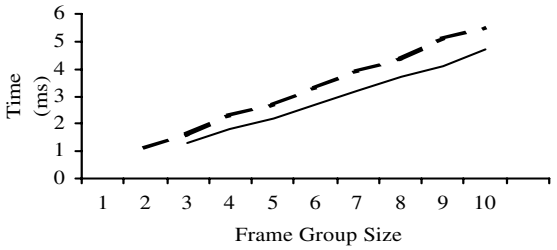

Fig. 6. FTG and SFTG modes encryption operation performance for various frame group sizes. FTG is the solid line and SFTG is the dashed line.

Fig. 7 shows the FTG and SFTG security mode decryption operations compared to each other for the same transmission group sizes as given in Fig.5. Fig. 7 shows that the decryption operations are quicker than the encryption operations since there is less data manipulation. The FTG decryption performance was better than the SFTG decryption performance since there was less data manipulation.

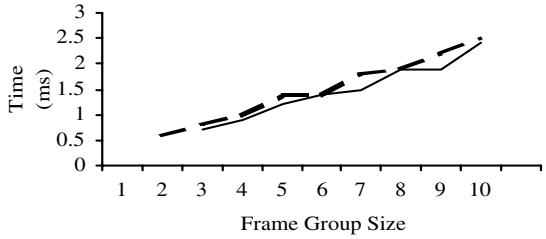

Fig. 7. FTG and SFTG modes decryption operation performance for various frame group sizes. FTG is the solid line and SFTG is the dashed line.

Table I provides the numeric results for the FTG and SFTG mode for a more detailed comparison of values, with a transmission group size of (*N=3*) which is the minimum group size for the FTG mode.

Table I
FTG and SFTG Performance for (*N=3*)

Security Mode	Encryption	Decryption
FTG	1.3 ms	0.7 ms
SFTG	1.6 ms	0.8 ms

Based on the results from Table I, and the padding mode operation performance, Table II indicates the overall performance for each of the security modes based on a single user data-link layer frame. In Table II, the bandwidth transmission time (*TT*) is given in relationship to the padding mode since the other security modes are multiples of this value.

Table II
Overall Mode Performance for a Link with (*N=3*)

Security Mode	Overall Performance
Padding	0.3 ms + *TT*
FTG	1.6 ms + *TT* ≤ FTG ≤ 2.0 ms + 3*TT*
SFTG	2.4 ms + 3*TT*

In Table II, the FTG has a range of values for the overall performance, since the user data-link frame will be between the first and last frames in the transmission group. If the user data-link layer frame is the first frame, the decryption operations are equivalent to the padding decryption operation.

IV. Security Operation for Power distribution system stability Control Application

The proposed security operations have been successfully applied for enhancement of laboratory prototype power 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 [11], a novel generator control based on step-ahead predictive control methodology and state-of-the-art real-time digital signal processing 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 security operations 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 [12], an equivalent-circuit for the power distribution system at the point of connection for the generator GEN-1, as shown in Fig.8, 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 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 security operations 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.

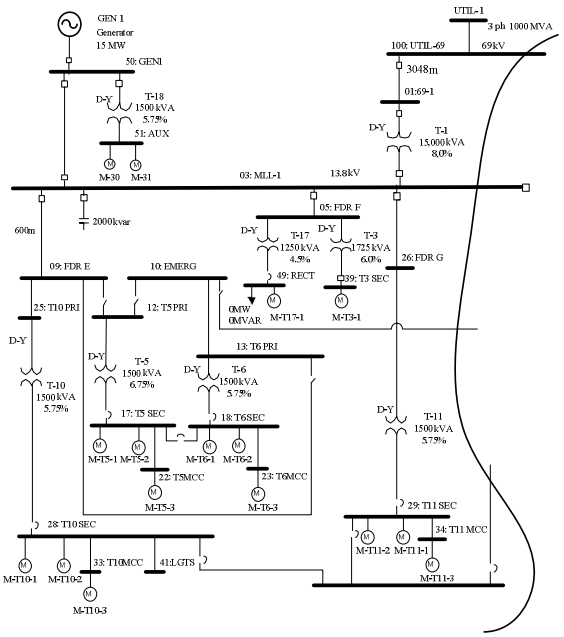

Fig.8 Simplified one-line diagram for IEEE power system

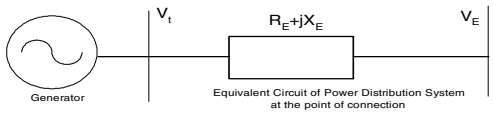

Fig.9 Equivalent circuit for the power distribution system shown in Fig. 8

V. Conclusion

Three security operation modes of the security layer located below the DNP3 data-link layer, which are padding security mode, the FTG security mode, and the SFTG security mode, have been proposed to enhance the security of power system computer networks in this paper.

The padding mode provides improved security beyond simply only using encryption with negligible effects on performance. The padding mode is therefore suited for lower security demands. The FTG security mode provides much higher security than the padding mode, but with increased processing overhead. The SFTG security mode provided much higher security than the FTG mode, but with higher processing demand. The FTG and SFTG modes are recommended for links requiring high security or for links that temporarily require higher security during cyber-attacks. The transition between modes is highly flexible, allowing links that require temporary higher levels of security to easily transition to a higher security mode and then back to the normal mode afterwards. The transitions between modes can occur immediately without prior information exchanges and independently, such as one mode for each link or an outstation transitioning modes without request from a master.

The results from the performance analysis for the three security modes show that these three security operation modes can provide additional strength to encryption and authentication operations in limiting the effectiveness and applicability of traffic analysis and cryptanalysis attacks for power system data transmissions. Since the security layer modes are independent of specific encryption ciphers and authentication operations, the paper does not provide constraints on the types of encryption ciphers or authentications used for the data transmissions.

The security operations proposed in this paper have been successfully applied to enhance power system security controls.

VI. References

[1] "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.

[2] Masoud Amin "Balancing Market Priorities with Security Issues", *IEEE Power & Energy Magazine,* July/August 2004. pgs. 30-38.

[3] J. Kumagai "Nine Cautionary Tales", *IEEE Spectrum*, September 2006, vol. 43, no. 9, pp. 36-45.

[4] "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.

[5] *DNP3 Technical Bulletin TB2005-003: Plans to Implement Authentication Security Draft*, DNP User's Group, November 2005.

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

[7] Xinwen Fu, Bryan Graham, Riccardo Bettati, Wei Zhao "On the Effectiveness on Link Padding For Statistical Traffic Analysis Attacks", IEEE Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS'03), 2003.

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

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

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

[11] 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.

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

VII. Biographies

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.

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.

Helen Cheung is currently an engineering student at Ryerson University as well as Research Assistant in Ryerson Power Engineering Laboratory.

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.

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.