Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security

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

Lin Wang, Richard Cheung
Ryerson University, Canada

Abstract — **Potential effectiveness of cyber-attacks against utility networks using protocol DNP3 would increase rapidly, when DNP3 is employed over TCP/IP, because attacks succeed on the Internet can be used against DNP3. This becomes a critical concern for DNP3 since an outstation may be accessed from multiple masters of external networks. However, commercial Internet security does not provide applicable security since they were not designed specifically for DNP3. This paper proposes a new efficient cyber-security specifically designed for DNP3 at its interface with TCP/IP to augment utility commercial security capability. Rule-based security is implemented for the proposed cyber-security for DNP3 over TCP/IP using the function codes, data objects, and data sets from DNP3 data link layer and application layer. The rule-based security is implemented on a connection basis so that detailed security rules are specifically defined for each connection to the device.**

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

I. Introduction

CYBER-SECURITY is implemented for Distributed Network Protocol (DNP3) over Transport Layer Protocol / Internet Protocol (TCP/IP) using DNP3 function codes and object headers from the application layer and the data-link layer at the interface between DNP3 and TCP/IP. Rule-base security is used to implement the cyber-security for incoming and outgoing data transmissions to a device. This DNP3 cyber-security is used to augment commercial firewall appliances that have not been designed specifically for DNP3 data communications. The DNP3 security in this paper therefore provides security coverage that commercial firewalls are unable to provide.

Ongoing power system automation is increasing the amount of computer network traffic in the power system, due to device replacement with electronic networked devices or introducing new devices such as smart-meters within the distribution system. As a consequence of increased computer network traffic, cyber-attackers have more opportunities to affect the power system utility operations through various cyber-attacks, i.e. data manipulation, manufacturing data, or denial-of-service attacks, which can be used to cause wide-area blackouts. For example, an advanced smart-meter may include a power cut-off safety switch to de-energize a premise, which can be used by a cyber-attacker to shutdown the distribution system for large residential areas. Security for DNP3 is critically required to prevent occurrences of such attacks.

Previously utility computer networks, such as those using DNP3, were not as vulnerable to security threats since only minimal numbers of trained utility staff had access to the computer networks. However, open-access under government imposed deregulation is increasing the utility computer network cyber-vulnerabilities due to more exposure to external networks. The increased exposure provides cyber-attackers with easier access into utility computer networks, such as from the corporate networks and Internet, as well as more locations from which to access power system devices. For example with distribution system smart-meters, device access will include the distribution system owner, the electricity retailer, premise owner, and possibly government regulatory organizations and the device manufacturer. As a consequence, there are not only more devices and data that can be affected from a cyber-attack, but more access to the utility network to facilitate the attacks.

With DNP3's capability to interface with TCP/IP [1], DNP3 has increased cyber-security vulnerabilities. Cyber-attackers are capable of using commonly exploited Internet vulnerabilities to attack DNP3 devices, critically requiring cyber-security be adopted for DNP3. Currently, DNP3 security requires the use of the Transport Layer Security (TLS) or Internet Protocol Security (IPsec) when used over TCP/IP [1]-[4], which may also be in addition to commercial firewall appliances. The TLS, IPSec, and commercial firewalls provide security for DNP3 over TCP/IP, such as confidentiality and authentication, but since they are designed for general commercial application they do not provide security designed specifically for DNP3, limiting their effectiveness for DNP3. For example, a commercial-off-the-shelf firewall appliance would not be capable of examining a received data-link link frame to detect and prevent an outstation from receiving a stop application command. In addition, TLS authentication would not be capable of preventing an outstation from receiving illegitimate control commands from a compromised master since the data would have been properly authenticated by the master.

The proposed cyber-security for DNP3 over TCP/IP is used to augment commercial security implementations, providing security specific to DNP3 and utility computer networks. The cyber-security is used to detect and block data transmissions that do not conform to the allowed DNP3 function code and object header usage for a device on a connection basis with multiple masters or outstations. The DNP3 function codes and

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

object headers rigorously define the data exchanged between devices, providing the capability to apply rule-based security to control which data can be accessed or transmitted for a device. The rule-based security allows both wide and narrow scope security rules to be implemented using DNP3 data-link layer function codes [5], DNP3 application layer function codes [6], DNP3 application layer data object types [6]-[7], and data sets [8]. The cyber-security limits the effectiveness of cyber-attacks due to manipulated data, data from compromised sources, and manufactured data. An extensive list of cyber-threats against power system utilities can be found in [9].

In Section II, the DNP3 characteristics used for the cyber-security proposed in this paper for DNP3 is discussed. Section III discusses the cyber-security operations. Section IV provides an example for the cyber-security and Section V provides the conclusion.

II. DNP3 Characteristics Used For The Cyber-Security

A. TCP/IP Interface

The DNP3 TCP/IP interface is located between the DNP3 data-link layer and the TCP layer, which provides various configuration options for a DNP3 device [1]. With DNP3 over TCP/IP, multiple logical devices can be defined for a single physical DNP3 device using different IP addresses [1]. As a consequence, security rules can be defined for the physical device or for the individual logical devices. In addition, it is simpler to implement multiple remote masters for an outstation using TCP/IP since the underlying network becomes abstract to the devices. The use of multiple devices and multiple masters for an outstation increases the number of connections that security rules have to be implemented for.

The cyber-security operations are not concerned with authentication or confidentiality since TLS or IPsec are used for the connection security. The cyber-security therefore assumes that the connection is legitimate and is only concerned with the DNP3 data. Although the connection may be legitimate to TLS or IPsec, the source device may have been compromised by a cyber-attacker allowing the cyber-attacker to manipulate the destination device if the cyber-security proposed in this paper is not used. For example without the cyber-security proposed in this paper, a master which typically only accesses monitoring data may be compromised to transmit control commands, altering the outstation's operations.

Unlike the cyber-security proposed in [10] which operates on the DNP3 data prior to fragmentation by the transport layer, the cyber-security proposed in this paper operates on the DNP3 data after fragmentation by the transport layer. In order for the cyber-security proposed in this paper to have the same degree of access to application layer fragments as was done in [10], the cyber-security would have to replicate much of the DNP3 protocol layer operations. For example, the cyber-security would have to remove the data-link layer Cyclic Redundancy Checks (CRCs), reassemble all of the transport layer fragments, and parse the application layer message fragment. Replicating the DNP3 protocol layer functionality would therefore result in an inefficient cyber-security design. In order to avoid the extraneous functionality of replicating the DNP3 protocol layer operations, the cyber-security places restrictions on the application layer without requiring alterations to the DNP3 specification. The cyber-security simply requires that each application layer message fragment contain only one object header. The cyber-security will therefore only have to examine the first data-link layer frame of the application layer fragment to obtain the function codes and the data object header. Within the data-link layer frame, the cyber-security also only has to examine the first user data block. Although this requirement may increase the number of data transmissions required to transmit the application data, the higher TCP/IP network speed may be able to compensate for the increased number of data transmissions.

B. Data-Link Layer

The cyber-security uses the following data-link layer header information to implement the security rules:

- Function code
- Source address
- Destination address

The data-link layer function code can be used to indicate link status information between devices and to pass link commands, such as reset link [5]. As a consequence, a cyber-attacker can alter the function code value for attacks in expectation of exposing vulnerabilities that may not have been handled by the device programmer, i.e. trying different header combinations to cause state errors. The cyber-security therefore must ensure that only valid function codes are used with a device.

Security for the DNP3 network addresses is not handled by the lower layer security, such as TLS or IPsec, since the DNP3 addresses appear as user data to TCP/IP. Therefore, a cyber-attacker could manipulate the DNP3 addresses and not be detected by TLS or IPsec if the data transmission was from a legitimate but compromised device. As a consequence, an attacker could masquerade as another device if the cyber-security is not used to confirm that the source IP address matches the source DNP3 address pairing.

The destination address has special addressing modes for all-broadcast and self-testing [5]. These can be used to cause a cyber-attacker's data to be transmitted to all possible destinations or for the DNP3 device to enter a testing mode creating a denial-of-service attack. The cyber-security therefore must be able to block data transmissions using the special addressing modes.

C. Application Layer Security

The cyber-security proposed for DNP3 use the following information at the start of an application layer message fragment for implementing the security rules:

- Function code
- Object type (object group number and variation)
- Qualifier
- Object data (indexes and data sets)

Application layer function codes are used to indicate commands and requests to an outstation from a master and responses from an outstation to a master [6]. Since application layer function codes can be used to start, stop, or reconfigure a device they are a useful means to attack DNP3 devices that must be handled by the cyber-security. However, the security rules for the function codes may encompass too large of a scope for defining data transmission security rules. For example with a write command a master may be allowed to write to a certain point type but not to another point type, i.e. binary output and analog output. Therefore, the object header and data filled objects must be used to define finer security rules that the more encompassing function code security rules cannot handle.

The object type defines the type of data being used with the function code, such as writing or reading analog or binary values, altering device or application configurations, and accessing or altering data sets [6]-[8]. Using the object types, an attacker can control how a device operates, such as changing the binary output point type for turning on or off relays or altering the device attributes. However, the object type security rules may also encompass too large of a scope for the data transmission security rules and may require refinement based on the qualifier field point type index values and the data set indexes. For example, a master may be allowed to control only specific relays defined by different binary output point type indexes. However, without security rules defining which point type indexes are allowed to be manipulated by the master, a master could use the qualifier field value of 0x06 to control all of the relays in the DNP3 device.

Security rules for data sets are critical with their capability to use function codes within the data set, such as select and operate for the binary output point type [8]. Without security-rules for the data sets, a cyber-attacker could bypass the function code security rules and access or alter data directly through the data sets.

III. Cyber-Security Operations

A. Cyber-Security States

The cyber-security has three states, shown in Fig. 1, which are: idle, frame security, and data security. The cyber-security is in the idle state when there are no data transmissions to process. The frame security state is used to process the data-link layer header data and the data security state is used to process the user data from the application layer.

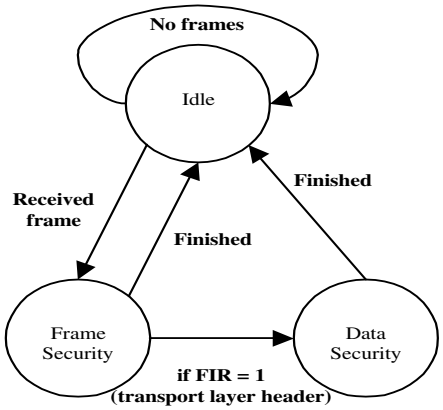

Fig. 1. Cyber-security states.

The idle state transitions to the frame security state for every data transmission that is received from either the TCP layer or the DNP3 data-link layer. The security rules for the data-link layer are applied, and if the frame does not conform to the rules, it is discarded. If the frame conforms to the rules, and it is the start of a new application layer message fragment as determined from the transport layer FIR bit [11], the cyber-security transitions to the data security state. Once the cyber-security finishes processing the frame and possibly the user data, it transitions into the idle state. If any data transmission does not conform to the allowed function code or data object usage, it is discarded by the cyber-security.

B. Frame Security State

For DNP3 over TCP/IP the types of function codes that can be used for a data transmission is limited [5]. The confirmed user data function code, and hence the NACK and ACK function codes, are not used for this configuration. Therefore, the cyber-security can implement simplified look-up tables for the security rather than implementing security rules that are used for the data security state. Basically only the unconfirmed user data, link status request, and link status function codes are needed to be defined for the cyber-security and therefore only a limited number of control field values, which includes the function code, need to be listed in the look-up table. The allowed control field values by the cyber security are shown in Table I. If a data transmission does contain one of these values, it is discarded by the cyber-security.

TABLE I
ALLOWED DATA-LINK LAYER CONTROL FIELD VALUES

Function Code	Primary	Master	Control Field
Unconfirmed user data	✓	✓	0xC4
			0x44
Request link status	✓	✓	0xC9
			0x49
Link status		✓	0x8B
			0x0B

In Table I, the function code column lists the allowed function codes, the primary column indicates if the function code is from a primary station or a secondary station, the master column indicates if the data transmission is from a

master or an outstation, and the control field column lists the allowed values for the control field.

For incoming data transmissions to the DNP3 device, the cyber-security uses a look-up table to match the source IP address with the DNP3 source address. The cyber-security also confirms that the DNP3 destination address is less than 0XFFF0, which is the start of the special address mode address range. No security is applied to the address fields for the data transmissions from the device since the TCP/IP interface will provide the operations for controlling outgoing data transmissions, i.e. looking-up the destination IP address paired with the DNP3 destination address.

C. Data Security State

Since the IP addresses can used to create multiple logical devices within a single physical device, the number of security rules used for the data security state have to be minimized in order to increase efficiency. The cyber-security therefore discards any data transmissions that do not have a matching security rule. Function codes, object headers, and data have to have explicit rules defined for each connection in order to be allowed by the cyber-security. The data security state security rules are applied four stages: function code, object type, qualifier field, and data sets. A data transmission is discarded if it does not conform to the usage rules.

1) Function Codes

The security rules for the function codes define encompassing rules for data transmissions that allow them to be discarded or passed on to either the DNP3 data-link layer or TCP layer with minimal processing. The security rules for the function codes use the following parameters: source IP address, destination IP address, rule applicability, function code, unconditional permission, and object type link.

Source IP address: provides the IP addresses of the logical devices within the single physical device. This parameter is unnecessary for DNP3 devices that have a single logical device.

Destination IP address: provides the IP address of the connecting device. This value represents the source IP address for data transmissions incoming to the DNP3 device and the destination IP address for data transmissions outgoing from the DNP3 device.

Rule applicability: indicates if the security rule is to be applied to data transmissions leaving the DNP3 device or being received by the DNP3 device for a specific connection defined by the destination IP address parameter.

Function code: provides the allowed function code values for the connection between the DNP3 devices and for a particular data transmission direction.

Unconditional permission: provides the scope of the function code security rule. If unconditional permission is given, all data transmissions using the function code are allowed regardless of the object header or the data. Otherwise, the cyber-security has to proceed to the next stage of security rules dealing with the object type.

Object type link: provides a reference link to the security rules used for the object type if the unconditional permission parameter is not set. The object type link provides a unique reference to the object types for each function code allowing a finer security rule scope. However, some function codes may share the same object type security rules and therefore have the same object type link parameter. For example with an outstation, the read function code security rules may have the same object type link parameter as the response and unsolicited response function codes security rules.

The cyber-security will search the function code security rules for a matching entry for the received data or data that is being transmitted for a particular connection and direction. If no matching entry is located, the data transmission is discarded. If an entry is found and the unconditional permission parameter is set, the data transmission is allowed and the data security set transitions back to the idle state. If an entry is located and the unconditional permission parameter is not set, the cyber-security proceeds to the object type security rules.

2) Object Type

The security rules for the object types define encompassing rules for object headers and the data filled objects that allow them to be discarded or passed on to either the DNP3 data-link layer or TCP layer with minimal processing. The object type field in an application layer object header is composed of both the object group and the variation values. The object group indicates the type of the data, i.e. binary and analog input and output values, time values, and file operations [6]. The variation represents the data type used for the object data, such as floating point, integer, and flags [6]. The security rules for the object type use the following parameters: object type link, object group, unconditional permission, unconditional variation permission, variation list, unconditional index permission, and index list. The last two parameters are used for the qualifier field and data set security rules that are dealt with in following subsections.

Object type link: provides the reference link from the function code security rules to the object type security rules. The same object type security rule may be referenced from multiple function code security rules.

Object group: provides the allowed object group values for a particular connection, function code, and transmission direction.

Unconditional permission: provides the scope of the object type security rule. If unconditional permission is given, all data transmissions using the object group are allowed regardless of the variant, qualifier field, and data sets. Otherwise, the cyber-security proceeds to the security rules dealing with the variant values.

Unconditional variant permission: indicates if security rules are applied to the object type variant values. If unconditional permission is given, there are no restrictions on the variant. Otherwise, the variant value for the data transmission must be located in the variant list parameter.

Variant list: contains a listing of allowed variant values for the object group for a particular connection, function code, and data transmission direction.

The cyber-security will search the object type security rules for a matching object group entry and object type link for a particular connection. If no matching entry is located, the data transmission is discarded. If an entry is found and the unconditional permission parameter is set, the data transmission is allowed and the data security set transitions back to the idle state. If an entry is located and the unconditional permission parameter is not set, the cyber-security examines the unconditional variant permission parameter. If this parameter is not set, the variant list is examined for a matching variant value. If the matching variant value is not located the data transmission is discarded. Otherwise, the cyber-security goes to the qualifier field security rules if the object group is not a data set or the data set security rules if the object group is a data set.

3) Qualifier Field

The qualifier field defines how the data is organized in the data-filled object, i.e. whether the data is packed by indexes or by object size [6]. Although security rules can be created for the qualifier field values, the cyber-security assumes that only the recommended qualifier field values [6] are allowed by the application layer in order to simplify the application of the security rules and increase the efficiency of the cyber-security. Associated with the qualifier field are the point type arrays, which is an index of data points for a particular point type such as one analog input point for each phase voltage. Security rules are critical for the qualifier field in allowing which point type indexes are allowed to be accessed. Without security rules for the qualifier field a cyber-attacker would be able to access any index for a particular point type. For example, a compromised master would be able to alter all of the binary output data points instead of the binary output data point that it should only be allowed to access. The qualifier field security rules use following parameters from the object type security rule parameters: unconditional index permission and index list.

Unconditional index permission: indicates if there are any restrictions on which index values for the point type are allowed for the connection. If unconditional permission is given, there are no restrictions on the indexes. Otherwise, the cyber-security determines which index points are allowed for the data transmission using the index list parameter.

Index list: contains a listing of allowed data points for the object group for a particular connection, function code, and data transmission direction.

The qualifier field security rules will discard a data transmission if the unconditional index permission is not set and the index value for the data point is not located within the index list parameter, i.e. if the qualifier field has a value of 0x06 for all data points. The unconditional index permission parameter is unlikely to be set in most cases since if unconditional permission cannot be granted for an object type, there will be restrictions on which data points that can be accessed, such as preventing a device from altering relay block values in the binary output object group (g12v3). The cyber-security will transition back to the idle state after this data security state stage.

4) Data Sets

Data sets provide the means to group related data, but possibly in unrelated point types, together. Since the data sets can contain various combinations of point types and points within a specific point type and use function codes, data sets can be used to bypass the security rules implemented for the function codes, object types, and qualifier fields. Therefore, cyber-security rules are necessary to control the use of data sets from being transmitted and received by a device. For example if security rules were not used for data sets, a master that was blocked from using select and operate function codes may bypass this security if an outstation data set contained the select and operate function codes. The data set security rules use following parameters from the object type security rule parameters: unconditional index permission and index list. These are the same parameters that are used by the qualifier field security rules. The cyber-security can distinguish if these parameters are to be used for the data sets by the object group numbers that are used for the data sets (groups 85 through 87).

Unconditional index permission: indicates if there are any restrictions on which data sets are allowed for the connection. If unconditional permission is given, there are no restrictions on the data sets. Otherwise, the cyber-security determines which data sets are allowed for the data transmission using the index list parameter.

Index list: contains a listing of allowed data sets for a particular connection, function code, and data transmission direction.

The data set security rules will discard a data transmission if the unconditional index permission is not set and the index value for the data set is not located within the index list parameter. The unconditional index permission parameter is unlikely to be set since data sets can be varied by an outstation after reset for both ordering, structure, and number of supported data sets. The cyber-security will transition back to the idle state after this data security state stage.

IV. Security Example

A. Overview

An example is presented for illustrating the application of the cyber-security proposed in this paper for the distribution system using a residential property. The residential property has a smart-meter, dispersed generation such as solar or wind, and an electricity storage device such as fuel cells for uninterruptible power supply (UPS) and electricity back-up operations. The smart-meter, generator, and electricity storage device are part of a single logical DNP3 device that is connected into the Internet shown in Fig. 2.

The DNP3 device has Internet connections to the distribution system owner, the electricity retailer, and the residential consumer shown in Fig. 2. The example assumes

that the security dealing with the Internet connections are dealt with by either the TCP interface or the TLS.

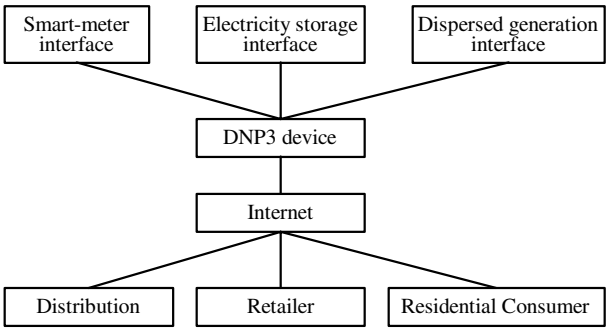

Fig. 3. Cyber-security example of a single DNP3 outstation device with multiple masters.

The distribution system owner in this example requires full access to all of the DNP3 device's point types and data points to ensure reliable distribution system operation, for control, protection and monitoring operations.

The electricity retailer is an independent company from the distribution system owner that purchases bulk electricity from generation companies and sells the electricity to residential consumers. The electricity retailer therefore requires access to the residential consumer's consumption records for billing purposes.

The residential consumer requires access to the device for monitoring their electricity consumption, which allows them to control their electricity usage and minimize their electricity costs. The residential consumer also requires control over the DNP3 device. For example, the residential consumer can decide how much of their generation capacity to sell to the distribution system owner from both the dispersed generation and the electricity storage device dependent on the current electricity rates, their current consumption, and their current capacity.

B. Device Point Types and Data Points

The cyber-security example is simplified by considering only a few point types and data points. In addition, the cyber-security example is simplified by not including security rules for the object type variations. The point types used in this example are binary output, counter, analog input, analog output, and data set [6]-[8].

Binary Output:

Index 0 is used to disconnect the home entirely from the distribution system although the dispersed generation and the electricity storage will still be operational within the home.

Index 1 is a master override to disconnect the dispersed generation from the electricity system within the home and the distribution system.

Index 2 is a master override to disconnect the electricity storage from the electricity system within the home and the distribution system.

Index 3 is a local override to disconnect the dispersed generation from the electricity system within the home and the distribution system for maintenance.

Index 4 is a local override to disconnect the electricity storage from the electricity system within the home and the distribution system for maintenance.

Index 5 is used to initiate device diagnostics for troubleshooting and maintenance.

Counter:

Indexes 0 through 2 are used to provide the power consumption information (KWh for current price rate, KWh for current day, and KWh from last billing date) to the distribution system owner, the electricity retailer, and the residential consumer. These indexes provide all of the parties with billing parameters to the residential consumer and the electricity retailer.

Indexes 3 through 5 provide power generation billing information (KWh for current price rate, KWh for current day, and KWh from last billing date) to the distribution system from the residential consumer.

Analog Input:

Index 0 is used to monitor the power consumption from the distribution system.

Index 1 monitors the total power generation by the residential consumer into the distribution system.

Index 2 is the total power generation of the dispersed generation.

Index 3 is the total power being generated or stored by the electricity storage device.

Index 4 is the current power generation capacity of the electrical storage device to allow the residential consumer to determine if they should store or generate electricity for the electricity storage device.

Analog Output:

Index 0 is used by the residential consumer to control how much electricity the electricity storage device is allowed to generate for selling to the distribution system.

Index 1 indicates the current electricity rate for purchasing electricity in the free-market.

Index 2 indicates the current electricity rate for the residential consumer to sell electricity to the distribution system.

Index 3 indicates the current contractual electricity rate for the residential consumer to purchase the electricity from the electricity retailer.

Data Sets:

Index 0 is used to provide all of the current KWh counter values while index 1 provides all of the current power readings from the analog input point type.

C. Security Rules

Since the example is simplified by omitting security for the variation, the unconditional permission (U.P.) for the group object is equivalent to the unconditional index permission.

1) Distribution System Owner

Since the distribution system owner requires full access to the DNP3 device, there are no restrictions on device access. Therefore, all of the function codes have unconditional

permission. Since all of the function codes have unconditional permission, there are no security rules for the data objects.

2) Electricity Retailer

The electricity retailer requires information for billing purposes and therefore does not need access to as much data from the DNP3 device. For data transmissions received by the device, the security rules will allow the following function codes: confirm, read, and write. For data transmissions transmitted by the device, the security rules will allow the following function codes: response and unsolicited response. Only the confirm function code has unconditional permission with the rest of the function codes requiring object type security rules.

For the read function code, the electricity retailer will require access to the binary output point type to determine the home's connection status to the distribution system. The electricity retailer will require access to the counter point type to determine electricity billing for the residential consumer. Access to the analog input point type is used to monitor the power consumption by the residential consumer, which requires access to all of indexes for each of the analog input group objects except the deadband. The electricity retailer also requires access to the analog output point type for monitoring the electricity rates, i.e. determining when the distribution system owner has increased penalties on the residential consumer not conserving electricity. The electricity retailer is not allowed to access any of the data sets since they contain information that the retailer does not need to access. For the read function code, the security rules for the object groups are listed in Table II.

TABLE II
ELECTRICITY RETAILER READ FUNCTION CODE SECURITY RULES

Point	Object Type	Group	U.P.	Index List
Binary Output	Present Value	10	N	0
	Report Changes	11	N	0
Counter	Present Value	20	N	0, 1, 2
	Frozen Value	21	N	0, 1, 2
	Event Value	22	N	0
	Frozen Event Value	23	N	0
Analog Input	Present Value	30	N	0
	Frozen Value	31	N	0
	Event Value	32	N	0
	Frozen Event Value	33	N	0
Analog Output	Present Value	40	N	1, 3
	Report Changes	42	N	1, 3

For the write function code, shown in Table III, the electricity retailer requires the capability alter the residential consumer's pricing information.

TABLE III
ELECTRICITY RETAILER WRITE FUNCTION CODE SECURITY RULES

Point	Object	Object	U.P.	Index List
Analog Output	Alter Value	41	N	3

The response and unsolicited response function codes have the same group object rules as the read function code since the device will only respond with the same indexes that were allowed for the read requests.

3) Residential Consumer

The residential consumer requires information for billing purposes and device operations, including the capability to shut down the device. For data transmissions received by the device, the security rules will allow the following function codes: confirm, read, and write, select, operate, direct operate, and direct operate no response. For data transmissions transmitted by the device, the security rules will allow the following function codes: response and unsolicited response. Only the confirm function code has unconditional permission with the rest of the function codes requiring object type security rules.

For the read function code, the residential consumer will require access to the binary output point type to determine the status of the device. The residential consumer also requires all data regarding the electricity rates in order to make decisions regarding their generation capacity, i.e. whether to sell or store electricity. The analog input point type is used to monitor consumption and generation for the home, requiring access to all data points except for some indexes dealing with deadbands that are used by the distribution system owner. The residential consumer also requires full access to all electricity rate information in the analog output point type and the data sets. For the read function code, the security rules for the object groups are listed in Table IV.

TABLE IV
RESIDENTIAL CONSUMER READ FUNCTION CODE SECURITY RULES

Point	Object	Object	U.P.	Index List
Binary Output	Present Value	10	Y	-
	Report Changes	11	Y	-
Counter	Present Value	20	Y	-
	Frozen Value	21	Y	-
	Event Value	22	Y	-
	Frozen Event Value	23	Y	-
Analog Input	Present Value	30	Y	-
	Frozen Value	31	Y	-
	Event Value	32	Y	-
	Frozen Event Value	33	Y	-
	Deadband	34	N	2, 3, 4
Analog Output	Present Value	40	Y	-
	Report Changes	42	Y	-
Data Set	Static	87	Y	-
	Event	88	Y	-

For the write function code, the residential consumer will require access to the analog input deadband values for controlling events for the dispersed generation and the electricity storage devices. In addition, the residential consumer must be able to control the electricity storage device using the output analog point type. For the write function code, the security rules for the object groups are listed in Table V.

TABLE V
RESIDENTIAL CONSUMER WRITE FUNCTION CODE SECURITY RULES

Point	Object Type	Group	U.P.	Index List
Analog Input	Deadbands	34	N	2, 3, 4
Analog Output	Altering Value	41	N	0

For the select/operate group of function codes, the residential consumer will require access to the binary output point type to control the operations of the DNP3 device such as shutting down the dispersed generation, the electricity storage, and disconnecting the home from the distribution system for maintenance. For the select/operate group of function codes, the security rules for the object groups are listed in Table VI.

TABLE VI
RESIDENTIAL CONSUMER SELECT/OPERATE FUNCTION CODES SECURITY RULES

Point	Object	Object	U.P.	Index List
Binary Output	Altering	12	N	3, 4

The response and unsolicited response function codes have the same group object rules as the read function code. If the electricity retailer is allowed to read the index for a particular object, then the device must be able to transmit the data for those points.

V. CONCLUSION

The cyber-vulnerabilities of utility computer networks are increasing due to more network-capable devices arising from utility automaton and open-access under government imposed deregulation. Cyber-vulnerability is increased since the networked devices are exposed to external networks, such as from corporate computer networks, and from unsecured sites, such as smart-meters within residential premises. This paper has proposed a new cyber-security for DNP3 over TCP/IP to augment commercial security implementations, providing security specific to DNP3 and utility computer networks.

The proposed cyber-security uses the function codes, object type (object group and variation), qualifier field and data point index values and data sets from the DNP3 data-link layer and application layer headers to implement security rules for the data transmissions which are not handled by TLS, IPsec, or firewall appliances. The cyber-security ensures that a device can only receive or transmit data that is allowed for a particular connection to a master or outstation. The cyber-security prevents a compromised master from being capable of transmitting control data to a device when it should only be allowed to access monitoring data. Security rules are used to implement the cyber-security for both incoming and outgoing data transmissions to a device. The security rules provide both coarse and fine rules so that the coarse rules minimize the number of rules that need to be implemented increasing efficiency while the fine rules allow precise application of the security to data transmissions. Coarse rules are defined through the function codes while fine rules are defined through the object type, qualifier field, and the data sets such as ensuring that only analog input values are read for the monitoring data rather than the binary output values used for device operations.

With the proposed cyber-security potential threats from cyber-attackers manipulating or manufacturing data are minimized, such as altering configuration settings to disrupt the power system through wide-area blackouts.

VI. REFERENCES

[1] *DNP3 Specification Volume 7: IP Networking*, DNP User's Group, December 2004.

[2] "Security Update", DNP User's Group, February 2006.

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

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

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

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

[7] *DNP3 Specification Volume 6: DNP3 Object Library*, DNP User's Group, January 2006.

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

[9] F. Cleveland, "IEC TC57 Security Standards for the Power System's Information Infrastructure-Beyond Simple Encryption", IEC TC57 WG15 Security Standard, October 2005.

[10] T. Mander, R. Cheung, and F. Nabhani, "Power System Peer-to-Peer Networking Data Object Based Security," in *Proc. 2006 IEEE Large Engineering Systems Conference on Power Engineering (LESCOPE 2006) Conf.*, pp. 90-94.

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

VII. 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 at the same university. 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.