Challenges and Direction toward Secure Communication in the SCADA System

Sugwon Hong and Myongho Lee
Dept. of Computer Science and Engineering
Myongji University
Yongin, Korea
swhong@mju.ac.kr, myunghol@mju.ac.kr

Abstract—**In the past few years the security issues in the supervisory control and data acquisition (SCADA) system have been investigated, and many security mechanisms have been proposed from research communities. The international standard organizations also have published several standard documents for secured SCADA systems. In this paper we explain the technological challenges for the SCADA security and overview the approaches which address these challenges. Then we focus on the security protocol which has been proposed in the SCADA cyber security initiatives and implementation issues when the both security function and the communication function are implemented on the embedded system devices in future power grid including the SCADA network.**

Keywords-SCADA cyber security; security protocol; smart device; smart grid

I. INTRODUCTION

The main purpose of the supervisory control and data acquisition (SCADA) system is gathering real-time data, monitoring and controlling equipments and processes in the critical infrastructure. A SCADA network provides connection between servers which reside inside a control center and control devices which are located at fields, sometimes at remote locations.

Major concerns about cyber attack stem from the notion that the SCADA network is no longer an isolated network which prohibits outsiders from entering the network, nor is the specialized network based on private platforms and protocols, allowing only technical staffs with special knowledge to access to the resources. The reasons of claiming that the SCADA network is not a protected closed network is twofold. First, the communication architecture is more relying on the open standard communication protocols. The use of the open communication protocols renders the system more vulnerable to cyber attacks in many applications. Second, more importantly, the SCADA network is moving toward being connected to other networks including cooperate networks for convenience and other business reasons. Thus the SCADA network will open its doors to outsiders who can enter the networks maliciously. This trend will be all the more noticeable as the power grid is moving to the smart grid.

For this reason recently SCADA security issues have drawn attention in various levels, and some researches have been done on the SCADA security. Along with the works in the research community, the international standard bodies also have worked to derive the standard documents for the SCADA security [1.2].

In this paper we define the challenges for the secured SCADA system, and to overview the approaches that address the challenges. And we explain security protocols which can be adapted for secure communication between system devices in the SCADA network. Then we raise the implementation issues when both security function and the communication function are implemented on embedded system. Finally we introduce one possible alternative for implementing all the required functions on the embedded devices.

II. SCADA ARCHITECTURE

Main components of the SCADA system are intelligent electronic devices (IED), power equipments, and substation controller. The substation controller as a master station, located in a central site, monitors and supervises a large number of IEDs which are field devices located in physical environments. IEDs gather data from sensors which measure current and voltage, and send data to the substation controller. The actuator as a part of IED controls the operation of power equipments by commands issued by other IEDs. The substation controllers have a hierarchical structure. A high-level master station can control several sub-master stations.

The data and command transfer takes place between the substation controller and IEDs, between IEDs, or between IED and sensors (or switchgears). The transferred information is carried over the SCADA network. The SCADA network is based on various communication channels and network technologies including Ethernet, serial links, wireless communication, and so on. The IEC 61850 assumes the IEEE 802.3 LAN as an underlying communication network.

The communication between the devices is governed by the standard communication protocols. The most commonly used protocols are IEC 60870-5, DNP3 which is the derivative of IEC 60870-5, and Modbus [3]. Recently the International Electrotechnical Commission (IEC) is working

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (2009-0089793)

978-0-7695-4041-2/10 $26.00 © 2010 IEEE
DOI 10.1109/CNSR.2010.52

on the new protocol, IEC 61850, which not only defines a new structure for substation automation, but also can provide more enhanced communication functionalities [4].

Communication between IEDs and various power apparatuses has traditionally carried out over hardwired I/O logic to gather physical data and control circuit breakers and switchgears. IEC 61850 replaces this hardwired connection with communication lines such as serial unidirectional multi-drop point to point link or the IEEE 802.3 LAN. The generic SCADA communication architecture is shown in figure 1.

The IEC 61850 defines seven different types of messages which are exchanging between the substation nodes. The communication stacks depending on the message types are shown in figure 2.

Among the messages, the message of sampled values is intended to deliver samples of 960 Hz signal from measuring devices to IEDs. The General Object Oriented Substation Event (GOOSE) message is an urgent message which conveys protection information between IEDs and circuit breakers or other protection devices. Upon detecting an event, the IED multicasts GOOSE messages to notify other IEDs of the events, and cause an actuator to do protection action. The GOOSE message transmission has stringent performance requirement. No more than 3 ms is allowed to elapse from the time an event occurs to the time a message is transmitted. Collision is possible since the IEC 61850 is based on IEEE 802.3 network. So the GOOSE messages are retransmitted several times by IED.

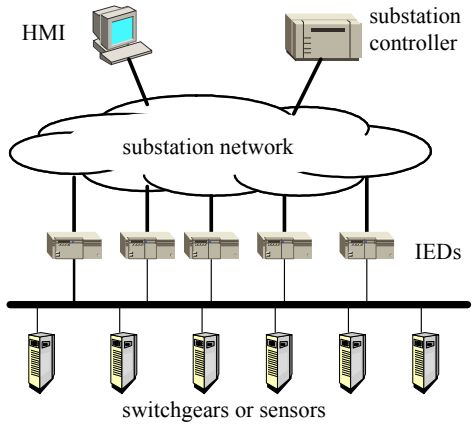


Figure 1. Substation communication architecture

The Manufacturing Message Specification (MMS) message is intended to configure and supervise the different devices in the substation. For this reason, unlike the other two messages, the MMS message has low or medium speed, consequently loose performance requirement.

There are two possible communication modes. The first one is the controller-IED communication mode where data transfer is done over a path between the substation controller and IEDs. The other one is the peer-to-peer mode where data can be delivered between IEDs directly. The current communication protocols only support the controller-IED communication mode, while the IEC 61850 protocol support the peer-to-peer mode too. In this paper we will consider the security protocols which can be applied to both modes.

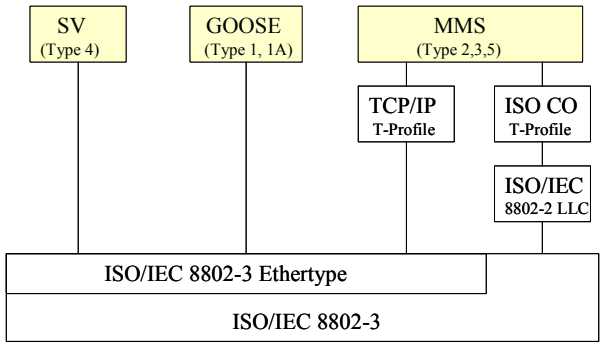


Figure 2. The protocol stacks for the IEC 61850 messages

III. SECURITY CHALLENGES

A. Key management

The building blocks of the security protocols are the existing cryptographic algorithms. Every security protocol is based on the underlying encryption/decryption or hash function keys. Thus, the key management including key establishment is an integral part of the security mechanisms proposed for the SCADA system. The big picture of the key management in the SCADA security mechanism is well summarized in the paper [5]. In this section we explain the key management schemes which are specified or assumed in the proposals, depending on the communication modes.

1) Master-to-IED communication mode

This is the typical mode which is encountered when the communication is based on the DNP3.0. The key establishment protocols proposed for this mode are based on the ISO/IEC 11770 Part2 server-less protocols [6].

In these protocols, a master station and an IED have a pre-shared symmetric key which is often called a long-term key in many literatures. Using this long-term key, two nodes establish an ephemeral key, which is also often called a session key and is used to encrypt and decrypt messages. The key establishment process takes 1 to 3 passes of message exchange, offering unilateral or bilateral authentication. In this procedure they use random number(nonce) and/or time stamp to protect the replay attack.

The secure DNP standard protocol has two kinds of modes: challenge-response mode and aggressive mode [3]. The challenge-response mode is the typical example based on the common key establishment protocol. Figure 3 shows the typical two-pass key establishment protocol. In this figure K_{AS} is a pre-shared secret key and K'_{AS} is a newly established session key between A and S. N_A denotes nonce generated by A and T is a timestamp. $\{M\}_K$ means that M is encrypted by the key K.

2) Peer-to-peer communication mode

There are no specific remarks about any key establishment protocol in the standard documents for the peer-to-peer model. But some researchers have proposed key establishment protocols based on the symmetric

cryptographic algorithm [7]. These protocols are variants of the Kerberos protocol or the ISO/IEC 11770-2 server-based protocols [9, 10].

In these protocols, two nodes A and B assume the trusted third party(TTP) which distributes the shared secret key between A and B. When the TTP generates the shared key, the TTP acts as the key distribution center(KDC). On the other hand, when the shared key is generated by an initiating node, the TTP will be the key translation center(KTC). Since random number generation requires complex computation, it is desirable for the master station to generate the key rather than an IED which normally has limited computer power.

The nodes A and B have the pre-shared keys with the TTP respectively. When a newly generated shared key between A and B(session key) is distributed, the session key is encrypted by the pre-shared key. The additional information such as nonce or time stamp or sequence number may be transmitted together with the key for verifying message freshness or preventing the Man-In-The-Middle attack. Normally the master station can act as the KDC or KTC. But the KDC can be located separately from the master station. One of the proposed protocols, SKMA, maintains a separate KDC, and treats the master-to-RTU and peer-to-peer in a unified way, i.e. the server-based three party key establishment cases[7].

The key distribution procedure may take several passes of message exchange depending on the complexity. Figure 4 shows the basic Kerberos protocol where the server is acting as KDC. This protocol is a simplified version of the complete protocol, involving 3 passes of message exchange. In this figure, A and B denote each node ID, and L denotes an expiration time of the session key, K_{AB}.

The asymmetric key cryptographic algorithm can also be used for the peer-to-peer model. The difficulty in implementing the public key cryptographic algorithm lies in maintaining the private certificate authority(CA) and processing the public-key certificates at each node. Few researchers propose the protocol using the public-key cryptography [8].

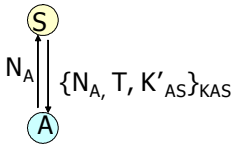


Figure 3. two-pass authentication protocol

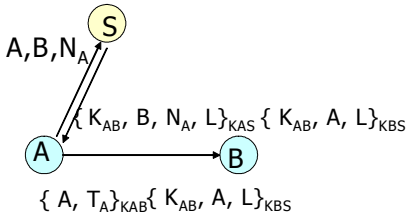


Figure 4. Basic Kerberos protocol

3) Broadcast communication mode

As long as the underlying communication network in the SCADA system is multi-access, especially wireless, we can exploit the advantage of the broadcast communication. The most convincing rationale for using broadcast channels in the SCADA system is that the master station can reach all IEDs by propagating a single message. If an emergent shutdown happen, it would not be desirable for the master station to send a message individually [11].

Another reason to mention the broadcast in the SCADA system is that sensors will be deployed in the SCADA network rapidly in the near future. Researchers on the wireless sensor networks(WSN) have produced numerous protocols [12]. And the constraints of the WSN are very similar to the SCADA system as explained in the section 2.2. For this reason, the proposed key establishment protocol for broadcast channel can borrow the ideas in the sensor networks [11].

B. Intrusion Detection

Recently some information in the SCADA system is allowed to be accessed from the corporate servers for providing efficient database management and enhanced services. Thus the servers in the SCADA system should be protected from intruder's attacks. The protection measures for servers are the same as the typical approaches carried out in the traditional IT industry. The servers with shared information are located in the demilitarized zones(DMZ) which is a buffer between the protected SCADA network and the cooperate network, and separates two networks through firewalls and additional routers.

In addition to the separation of two networks, the intrusion detection system(IDS) can bestow some intelligence on the edge devices in the DMZ. An IDS is a tool that can interpret the contents of a log file in the edge devices and patterns of incoming traffic. If the current traffic pattern matches the known attack signature, it can detect attacks.

The use of any SCAD-tailored IDS depends on whether we can find any special traffic patterns which is peculiar to the SCADA system. Some papers proposed model-based monitoring intrusion detection techniques [13, 14].

C. Developing smart devices

Current system devices basically have two functions: electrical measuring and/or control function, and communication function. For secure communication each device is also required to have security function on top of them. Moreover these functions should be implemented on embedded system devices. Dealing with incoming packets is not critical burden to the devices so far because traffic volume is so light that even serial communication links can treat the traffic. We can tell how much traffic the devices have to process yet, but some devices will have to accommodate much heavier traffic in the smart grid than they are encountering in the current grid.

In the smart grid the devices should be smart enough to have high performance communication function and security function as well as the basic electrical function. To provide

those smart grids with reasonable cost will be one of major practical issues in realizing the smart grid.

D. Transition

The biggest challenge when we build the secured SCADA system is a migration issue. The power systems have been built extending for a long time and it is not feasible to replace all the system components overnight. The systems are said to have lifetime between 7 to 20 years and it is too expensive to replace them for the sole purpose of applying security. System devices have been installed over the long period of time, so old devices, which are based on old microprocessors, have very limited computing powers and memories to process the security logic. For quite a long time it is expected that applying security to the legacy SCADA systems require retrofitting existing insecure devices.

There are two transition scenarios for achieving security: "bump-in-the wire"(BITW) solution and "bump-in-the-stack"(BITS) solution. In a BITW solution, two hardware modules are inserted into the communication link, one next to each of the communicating devices. These BITW modules transparently provide the devices with the necessary security functions.

IEEE P1689 and P1711 as well as AGA 12 are the trial use standard for retrofitting existing SCADA devices. In such an effort, some papers propose the BITW solutions that retrofit security into time-critical communications over bandwidth-limited serial links between devices [15, 16].

IV. SECURITY PROTOCOL

Up until now several organizations have taken different SCADA cyber security initiatives. Among them IEC TC57, DNP3 User Group, IEEE Power Engineering Society Substation Committee, and the American Gas Association(AGA) have produced some proposals which are noteworthy considering their impacts on the industry [17, 18, 19, 20]

In this section we overview the security measures against possible cyber attacks on the SCADA networks which are proposed in IEC 62351-5 and Secure DNP3.0 because these two proposals are more relevant in our context. For clarification we explain security procedures for message sender's authenticity and message integrity which are the primary goals, maybe the only goals addressed until now in the SCADA communication, in generic terms without sticking to the details of the documents.

As for the key management, the proposals assume the pre-shared long-term keys between server and nodes, and establish the session keys between nodes as explained in section 3.1. But they do not specify any key management structure and leave detailed implementation to user responsibility.

A. Security goal

We focus on secure transfer of the messages. In the IEC 61850 terminology the sample value message and the GOOSE message are typical example. The secure transmission of these two messages plays a critical role for normal protection operation in the substation. Receivers need to verify that messages are sent from claimed senders. Attackers can inject malicious messages to the IEDs or breakers, consequently causing system malfunctions. To authenticate the owner of messages is one of the most important security requirements in many applications in the SCADA system.

Receivers also need to make sure that the messages they receive are not altered on the way by attackers. In particular, sample values are used for the IEDs to decide whether voltage, current, or frequency anomalies happen. If these values are modified, the IEDs are mistaken to understand the current status. For this reason we consider the security protocol to guarantee the message authenticity and integrity.

B. Message Authentication and Integrity

The message authentication code (MAC) is a common method used to verify the authenticity of the sender and the integrity of the message. Since it can avoid the encrypting/decrypting computation, this method is preferable when we apply the authentication algorithm to the devices which have limited computing resources.

The Keyed-Hashing (HMAC) is the most widely used algorithm for computing MAC [21]. In the HMAC, first, the sender A concatenates the Sync Code C, the original message M_A, and the (session) authentication key, K_{AB}, then computes MAC by applying a one-way hash function, H, to the concatenated message. The detailed procedures are explained in [22]. Next, the sender replaces the authentication key by the MAC and finally delivers the message.

The node B applies the same hash function to obtain new MAC on the message it received with the authentication key. If these two MACs are the same, B can trust that the message was sent by the claimed sender A, and also the message was not modified on the way.

The authentication key can be of any length. But it is recommended that the key length should not be less than L bytes which is the byte-length of the hash function output, since it would decrease the security strength. Keys longer than L bytes are acceptable but the extra length would not provide significant increase of security [21]. The implementation in [22] uses L=16 as a default secrete key length since the default keyed hash function is MD5 [23].

The Sync Code is used to verify the freshness of the message. Since the Sync Code is a non-decreasing number, the value of a new message should be bigger than the one of an old message. Comparing these two values reveals whether the message was resent or not, thus ensuring that no attackers replay old messages. The whole procedure is as follows.

$$MAC = H(C \mid M_A \mid K_{AB})$$
$$A \rightarrow B : <C \mid M_A \mid MAC>$$

V. DIRECTION FOR DEVELOPING SMART DEVICES

Devices in the future power grid are expected to have electrical control function, communication function, and security function, all harnessed in a single box. Since the security functions eventually should be applied to most,

though not all, incoming packets to guarantee secure operation in the power grid including the SCADA system. More demanding requirement is that these functions should be implemented mostly on the embedded, microprocessor-based platform. For this reason finding any feasible and economic way of implementing the security functions as well as handling incoming packets in the embedded system will pose very daunting task to any researcher concerned in this area.

Figure 5 shows the basic functional blocks inside a device in the future power grid. First the device should capture all incoming packets without any loss. Unfortunately capturing packets is not an easy task due to the kernel livelock in which the system spends all its time processing interrupts [24]. Over the past few years many efforts have been tried to improve the performance of packet capture and transmission, eliminating Kernel livelock while processing interrupts [25, 26, 27]. But the capabilities and limitations of the current capturing systems have not been examined in the recent past [28].

For capturing packets, especially high-rate arriving packets, one alternative is to use specialized hardware such as network processors in the monitoring cards. This expensive alternative is mostly adapted in developing network devices in real-life.

We face the same challenge in implementing cryptographic functionality these days. The security function on heavy traffic load is intimidating task to enterprise servers. To overcome the limitation of pure software implementation, some dedicated hardware, which may be FPGA-based co-processors or hardware accelerators or graphic processor (GPU), are used only for security functions.

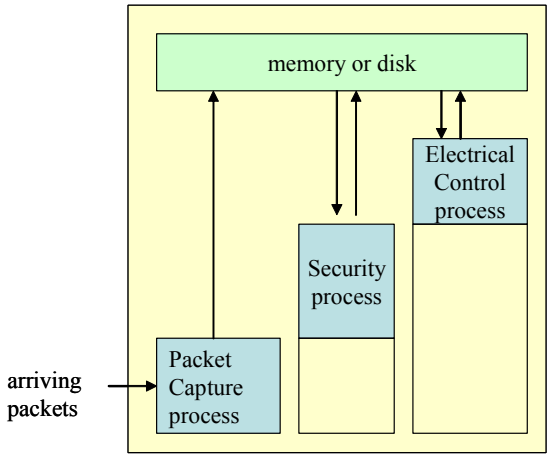
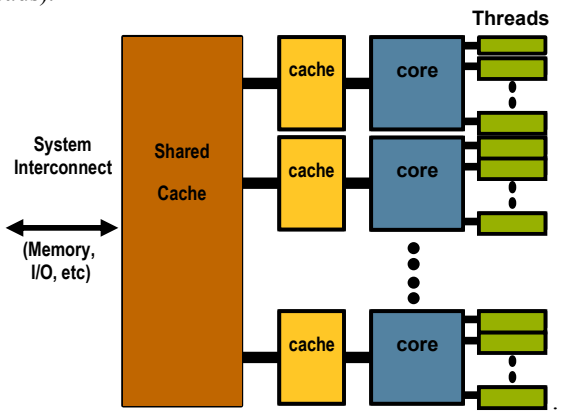


Figure 5. basic functions in a smart device

Recently, microprocessor designers have been considering many design choices to efficiently utilize the ever increasing effective chip area with the increase of transistor density. Instead of employing a complicated processor pipeline on a chip with an emphasis on improving single thread's performance, incorporating multiple processor cores on a single chip (or multi-core Processor) has become a main stream microprocessor design trend [29]. As a Chip Multi-Processor (CMP), it can execute multiple software threads on a single chip at the same time. Thus a multi-core processor provides a larger capacity of computations performed per chip for a given time interval (or throughput) [30]. All the CPU vendors including Intel, AMD, IBM, Sun, among others have introduced multi-core processors in the market. It is also adopted in embedded systems such as ARM11 MPcore (quad-core) based systems introduced lately.

The current main design for multi-core processors is based on CMP's such as quad-core Intel Xeon, AMD Opteron, among others. Some multi-core processors go one step further to incorporate Simultaneous MultiThreading (SMT) or similar technologies on a processor core. Figure 6 shows the architecture of an advanced multi-core processor.. On each processor chip, there are N-processor cores, with each core having its own cache on chip. The N-cores share a larger cache on or off the processor chip. Each core also has M hardware threads performing SMT or similar features. Thus it supports two levels of parallelism. Also, it has a cache hierarchy of private (to each core) and shared (among threads).



~~Figure 6.~~ Architecture of an advanced multi-core processors

One less expensive alternative for developing the so called smart devices in the future power grid is to use the Chip-level MultiThreading(CMT) processor. We can improve tremendously the performance of packet capture and security function on a general purpose microprocessor, avoiding any specialized hardware, and consequently reducing development costs significantly.

Although multi-core processors promise to deliver higher chip-level throughput performance than the traditional single-core processors, resources on the multi-core processors such as cache(s), cache/memory bus, functional units, etc., are shared among the cores on the same chip. Software processes or threads running on the cores of the same processor chip compete for the shared resources, which can cause conflicts and hurt performance. Thus exploiting the full performance potential of multi-core processors is still a challenging task.

VI. CONCLUSION

The SCADA system is not immune to cyber attacks any more, especially when we are moving into the smart grid. Most devices in the smart grid are required to have security function with communication function as basic capability. How to implement these functions on embedded system is as important as what to do for secure communication. Still we can not predict how much traffic the device has to accommodate in the future grid. One sure thing is that one daunting task lies ahead in constructing the future power grid.

REFERENCES

[1] V. M. Igure, S. A. Laugher, and R. D. Williams, "Security issues in SCADA networks," Computers & Security Vol. 25, pp. 498-506, 2006.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clar IEC technical committee 57, "Part 1: Communication network and system security - Introduction to security issues," IEC 62351-1, May 2007.

[3] DNP User Group, http://www.dnp.org.

[4] IEC, "Communication networks and systems in substations- Part 1: introduction and overview," IEC TR 61850-1, 2003.

[5] L. Pietre-Cambacedes and P. Sitbon, "Cryptographic key management for SCADA systems – issues and perspectives," International Conference on Information Security and Assurance, 2008.

[6] ISO, Information Technology – Security Techniques – Key Management – Part 2: Mechanisms Using Symmetric Techniques, ISO/IEC 11770-2, 1996.

[7] R. Dawson, C. Boyd, E. Dawson, and J.M.G. Nieto, "SKMA-A Key Management Architecture for SCADA Systems," Proceedings of the Australasian workshops on Grid computing and e-research, 2006.

[8] C. Beaver, D. Gallup, W. Neuman, and M. Torgerson, "Key management for SCADA," Technical Report, SANDIA, 2002.

[9] B. Clifford Neuman and T. Tso, "Kerberos: An authentication service for computer networks", IEEE Communications Magazine, Vol. 32, No. 9, pp33-28, September 1994.

[10] ISO, Information Technology – Security Techniques – Key Management – Part 2: Mechanisms Using Symmetric Techniques, ISO/IEC 11770-2, 1996.

[11] Y. Wang and B.-T. Chu, "sSCADA: Securing SCADA Infrastructure Communications," http://eprint.iacr.org/2004/265.pdf.

[12] S.A. Camtepe and B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey," TR-05-07, Dept. of Computer Science, Rensselaer Polytechnic Institute, 2005.

[13] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, and K. Skinner, "Using Model-based Intrusion Detection for SCADA Networks," SCADA Security Scientific Symposium, 2007.

[14] J.L. Rrushi and R. H. Campbell, "Detecting Attacks in Power Plant Interfacing Substations through Probabilistic Validation of Attack-Effect Bindings," SCADA Security Scientific Symposium, 2008.

[15] P.P. Tsang and S.W. Smith, "YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems," The IFIP TC 11 23rd International Information Security Conference, 2008.

[16] A. K. Wright, J. A. Kinast, and J. McCarty, "Low-Latency Cryptographic Protection for SCADA Communications," Applied Cryptography and Network Security, 2004.

[17] IEC technical committee 57, "Data and Communications Security, Part 5: Security for IEC 60870-5 and derivatives," IEC 62351-5 Second Committee Draft, December 2005.

[18] DNP User Group, Secure DNP3 specification, www.dnp.org, 2007.

[19] IEEE, Trial Use Std. for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access, P1689, 2007.

[20] AGA Report No. 12, Cryptographic Protection of SCADA Communications: General Recommendations, Draft2, 2004.

[21] H. Krawcryk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[22] I. H. Lim, S. Hong, M. S. Choi, S.J. Lee, T. W. Kim, S. W. Lee, and B. N. Ha, "Security Protocols Against Cyber Attacks in the Distribution Automation System," IEEE Tran. on Power Delivery, Vol. 25, No 1, Jan. 2010.

[23] R. Rivest, "The MD5 Message-Digest Algorithms", RFC 1321, April 1992.

[24] J. C. Mogul and K. K. Ramakrishnanl "Eliminating receive livelock in an interrupted-driven kernel," ACM Trans. On Computer System, Vol. 15, No 3, pp217-252, 1997.

[25] L. Rizzo, "Device Polling support for FreeBSD," the EuroBSDCon 2001.

[26] L. Deri, "Improving passive packet packet capture: Beyond device polling," the 4th Int. System Administration and Network Engineering Conference 2004.

[27] L. Deri, "nCap: Wire-speed packet capture and transmission," the IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services 2005.

[28] F. Schneider, J. Wallerich, and A. Feldmann, "Packet Capture in 10-Gigabit Ethernet Environments Using Contemporary Commodity Hardware," LNCS 4427, pp207-217, 2007.

[29] L. Spracklen and S. Abraham, Chip MultiThreading: Opportunities and Challenges, 11th International Symposium on High-Performance Computer Architecture (HPCA-11), pp 248-252, 2005.

[30] Y. Li, D. Brooks, Z. Hu, K. Shadron, "Performance, Energy, and Thermal Considerations for SMT and CMP Architectures," 11th International Symposium on High-Performance Computer Architecture, 2005.endon, 1892, pp.68–73.

.