Cyber Security for Supervisory Control and Data Acquisition

Reena Shinde[1], Dr. Magan P.Ghatule[2]
Department of Computer Science, Sinhgad College of Science, Pune-41 (MS, India)

Abstract- *SCADA stands for Supervisory Control and Data Acquisition, a communication technology which collects data from distant facilities and sends control signals to actuators. There are several factors which increase the risk associated with SCADA systems. SCADA components are considered to be profoundly privileged targets for cyber-attacks through which hackers can easily hit the nation's critical infrastructure and economy. This paper investigates security issues of SCADA communication protocols. In order to protect the SCADA networks, we focus on the protocols as they were not designed with inherent security features. Security system through protocol hardening is the main focus of this paper. The goal is to modify the structure of such protocols to provide more integrity and authentication. In the proposed structure, two algorithms are used to enhance the security and integrity of the payload. They are each discussed further in the next six sections.*

Keywords- SCADA, Data link layer protocol, CRC, Cyber security, Industrial Network.

I. INTRODUCTION

SCADA stands for Supervisory Control and Data Acquisition, is critical infrastructure to provide the services to real time system such as traffic control, electric power generation, power grid, waste treatment etc. It is a communication technology which collects data from distant facilities and sends control signals to actuators. SCADA systems [1] were introduced for local systems and its applications have been expanded to wide area networks as technology evolves. SCADA systems were somewhat secure as they had proprietary controls and limited security issues. Due to the increased connectivity to the internet and corporate network, SCADA network is no longer invulnerable to cyber-attacks. These systems were primarily designed with the thought for functionality and performance and little thought toward security.

Later on internet and corporate network have connected to SCADA systems [2] which introduces cyber security threats. It could pose a threat to economy of country and life of citizens. If intruders attack on SCADA components through which they can shaken the nation's critical infrastructure and economy. These types of attacks have a potential to obstruct. The essential operations of the nation such as disrupt financial service, shut down power systems.

While modern communication control systems and computing offer tremendous opportunities to improve electric power system response optimize generating station performance and offer resilience to failure, they also render the physical processes and systems vulnerable to intentional attacks from internal or external parties

II. INDUSTRIAL NETWORK

Compared to IT systems, SCADA systems have higher requirement concerning reliability, latency, and uptime, so it is not always feasible to apply IT security measures deployed in IT system. Confidentiality, Integrity and Availability is the main concern for both IT systems and SCADA systems. Availability is the top priority for SCADA systems whereas Confidentiality is the major concern for IT system. It is required to analyze various threats and vulnerability that effects the SCDA system operation.

Supervisory Control and Data Acquisition (SCADA) systems are the core of automation and Industrial networks that constitute Critical National Infrastructure. Traditionally, such systems were installed standalone and did not interface with the outside world. These systems are now increasingly being connected to the internet and corporate network therefore are vulnerable to cyber security threats. SCADA [3] components are considered to be privileged targets for cyber-attacks through which hackers can easily hit the nation's critical infrastructure and economy. Such attacks can potentially shut down power systems, interrupt financial service and therefore obstruct the essential operations of the nation. While modern communications, control systems and computing offer tremendous opportunities to improve electric power system response, optimize generating station performance and offer resilience to failure, they also render the physical processes and systems vulnerable to intentional attacks from internal or external parties.

Protecting the SCADA systems which perform the monitoring and control functions of utility infrastructure, such as electricity, gas, water etc. is critical for national security. Any vulnerability in these systems can pose serious threats and can bring down operations of a utility. In critical applications, the appropriate control strategy to block execution and any unknown or malicious behavior.

In order to better understand how to protect SCADA systems, it is important to analyze the security risk of these systems and develop appropriate security solutions to protect them from cyber-attacks.

The protocols used in SCADA [4][5] systems traditionally have built with little thought given to security. Security of SCADA system by means of protocol hardening is a plausible solution to address such threats.

DNP3 protocol is used to communicate between the Master and Outstation by critical infrastructure. Securing DNP3 is an active research topic. DNP3 is acronym of the Distributed Network Protocol Version 3 used by SCADA systems to communicate between the Master and Outstation. DNP3 protocol is designed to optimize the transmission of data acquisition and control commands between the master and slave units. It is not general purpose protocol like those found on the Internet for transmitting electronic mail, hypertext documents, SQL queries. It is highly suitable for SCADA applications.

III. INDUSTRIAL NETWORK PROTOCOL (DISTRIBUTED NETWORK PROTOCOL VERSION 3-DNP3)

DNP3 [6][7] is an open, robust, efficient modern SCADA protocol. DNP3 uses the term outstation to denote remote computers as are found in the field. The term master is used for the computers in the control centers. It is designed to optimize the transmission of data acquisition information and control commands between the master and slave units.

DNP3 [8] is a simplified 3 layer standard (application layer, data link layer, physical layer) initially proposed by the International Electro technical Commission but later on Enhanced Performance Architecture (EPA) enhanced the architecture of DNP3 by adding a fourth layer, a pseudo transport layer that allows for message segmentation.

3.1 Application layer

The Application Layer provides standardized functions, data formats, and procedures for the efficient transmission of data acquisition values, attributes, and control commands [11]. Application Layer‘s services are used to send messages to DNP3 devices and receive messages from, another DNP3 device. A fragment is a block of octets containing request or response information transported between a master and an outstation. Application layer fragment structure is of two types:

- Request fragment
- Response fragment

In request fragment, the application request header is of 2 bytes: Application control (1 byte), Function code (1 byte).

In response fragment, the application response header is of 4 bytes: Application control (1 byte), Function code (1 byte), and Internal Indication (2 byte).

3.2 Pseudo Transport layer

This layer allows message segmentation. It breaks down the long fragment of Application layer into Data Link layer sized data unit (Transport function) at transmission time and amalgamate it at receiving site. The Transport function adheres header (1 octet) and application data (1 to 249 octets).

3.3 Data Link layer

Data link layer transport data across communication channel to destination device bi directionally. This layer performs several functions like encapsulation, error detection, source and destination addressing. It encodes data section containing data passed down from the pseudo transport application layers with fixed length data link header.

The encoded data is sent over communication channel for transmission. The DNP3 data link frame has fixed length header block (10 octets) followed by optional data blocks. Each block ends with a 16bit CRC. Frame length may be long as 292 octets.

3.4 Physical Layer

The physical layer is top most layer which responsible for transmitting messages over physical media

IV. SECURITY ISSUES IN INDUSTRIAL NETWORK

4.1 Issues related to Device Security MTU/RTU

Device in industrial networks are sometimes located in remote places and therefore device security takes a high priority in design and deployment of these devices

4.2 Issues related to Protocol Security

Integrity and authentication are of utmost importance in industrial network as unauthorized data manipulation by adversaries can have disastrous consequences. Man in the middle attacks and replay attacks can be directed on these networks in the absence of integrity & authentication measures.

4.3 Model based Security

The overwhelming growth of vulnerabilities has become one of the key challenges facing operational security personnel who must not only consider an increasing number of attacks, but how these attacks can be combined in complex ways. Clearly a methodology is needed to A threat may be known to exist, but not significant. For instance, a company may know of industrial spies targeting them from a competitor, but the company may deem the threat as non-existent for specific portions of their infrastructure. For example, risk analysis may reveal that an outlying control station that is operating with 20 year old technology is not a likely target. It is unlikely that the competition would target this facility. Assigning additional security resources to the remote control station is unwarranted. Therefore, in order to properly assign resources, the severity of the threat must be determined.

Some industry experts speculate that since SCADA systems are typically custom made for specific sector applications, that it requires a great deal of specific knowledge on a particular system and the specific industry in order to attack it. Furthermore, that the - specialized knowledge‖ requirement will limit the number of attackers perhaps explains why SCADA attacks are not nearly as common as attacks on other computer networks. Although successful SCADA attacks are infrequent to date, there are indications of increased interest by adversaries.

There are a number of ways using which we can perform security analysis of a given network based on protocol application and topology.

Fault Tree Analysis (FTA) is a tool used for safety and reliability evaluations to analyse and visually display failure paths in a system. It provides a means for systems level risk evaluations via a tree structure. FTA is about 50 years old as of this writing and is widely used around the world. The failure behaviour of the system is modelled in a visual fault tree. The simple set of logic rules and symbols within the tree structure make qualitative and quantitative evaluation of very complex systems possible. The construction of fault trees is simple, but if the tree becomes too complex, they become much more difficult to solve. Attack trees take advantage of all of the features of fault trees plus additional capabilities.

Attack trees (AT), just like fault trees are models of reality. They provide a simplified representation of complex real world drivers. The accuracy underlying the drivers and future analysis depend on time/effort spent studying them and assumptions made.

In an attack tree, the attacks against the target are represented by an upside down tree structure with the goal as the root node and different ways of achieving that goal as sub-goals and leaf nodes as the lowest level tasks. The leaf nodes contain user-definable values called indicator values to store attributes of that leaf node.

It is possible to assign multiple user-defined variables in the form of Boolean, continuous, or explicitly specified values to the leaf nodes. For instance, a Boolean value could take the form of breach of trust, either true or false, a continuous value such as cost, from zero to potentially millions of dollars and explicitly specified values such as 1 for low to 4 for high. There are many other possibilities for continuous node values to include, but not limited to - technical difficulty, technical ability, notice ability, impact of attack, probability of apprehension, likelihood of attack success, site conditions and installed countermeasures. This research uses, in part, publically available attack data as a source to populate indicator values in the attack tree. For a large attack tree there can be thousands of potential attack scenarios if all possible paths are followed in order to read the root goal. In order to narrow down the number of attacks to better match the potential threat, a threat agent profile is applied to the tree. The attack tree includes both physical and cyber-attacks for completeness. It shows the touch points between the two and how they affect one another

V. PROPOSED SOLUTION INDUSTRIAL NETWORK SECURITY

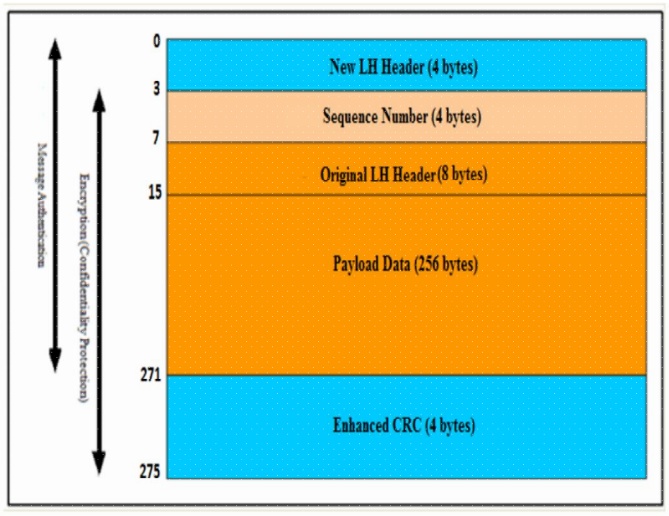
This work deals with communication security aspects of DNP3/ SCADA. Our work enhances security of the DNP3 protocol to alleviate the threats. Most important focus is on the redistributes the bytes of the protocol, on the augmentation of the CRC algorithm and Blowfish algorithm for better security aspect. Traditionally DNP3 pro-tocol has only CRC is used for detecting transmission error [14][15]. We provide the security through following ways:

- Encrypting DNP3 Packet.
- Modify the internal structure of protocol.

It uses 34 bytes out of 292 bytes of the DNP3 link protocol data unit for integrity and security. We redistribute these bytes to enhance the payload range and security of the DNP3 protocol with the help of following rearranges fields:

- New LH Header (4 bytes)
- Key Sequence Number (4 bytes)
- Original LH Header (8 bytes)
- Payload Data (256 bytes)
- Enhanced CRC (4 bytes)

In this proposal the message is protected by encryption using Blowfish and our al-gorithm for authentication as shown in Fig. 1.



- In this ZA protocol, the message is protected by the following two algorithms:
- Blowfish encryption algorithm: Blowfish provides the confidentiality to the data by encrypting the data.
- Enhanced CRC algorithm for data authentication in the protocol: CRC helps in the authentication of the data at both sides. In the enhanced CRC technique, it uses only 4 bytes of DNP3 protocol.

Enhanced CRC algorithm for message authentication and Blowfish encryption algorithm

CRC helps in the authentication of the data at both sides. In the enhanced CRC technique, it uses only 4 bytes. Blowfish helps in confidentiality of the payload.

Blowfish [10] is a variable length keyed symmetric block cipher. It is designed by Bruce Schneier in 1993. Blowfish algorithm contains two parts: Key Expansion part and Data Encryption Part. In key Expansion part, inputted key of up to 448 bit is converted into several sub array keys of total 4168 bytes. Data Encryption contains a feistel network consist of sixteen rounds. Each round contains a key dependent permutation and key and data dependent substitution.

In this scenario, the key sequence number, the original header, payload data and enhanced CRC are encrypted with the help of Blowfish encryption algorithm as shown in Fig.2. The total 272 bytes are under Blowfish encryption algorithm. It is a symmetric block cipher and each block is 64 bits. The secret key of Blowfish cryp-tography ranges from 32 bits to 448 bits. It is a strong encryption algorithm to provide security in the SCADA protocols use the generator polynomial. The ge-nerator polynomial is used to divide the message to find out the remainder as CRC [9][12]. The generator polynomial must be of degree r, to compute an r -bit CRC checksum.

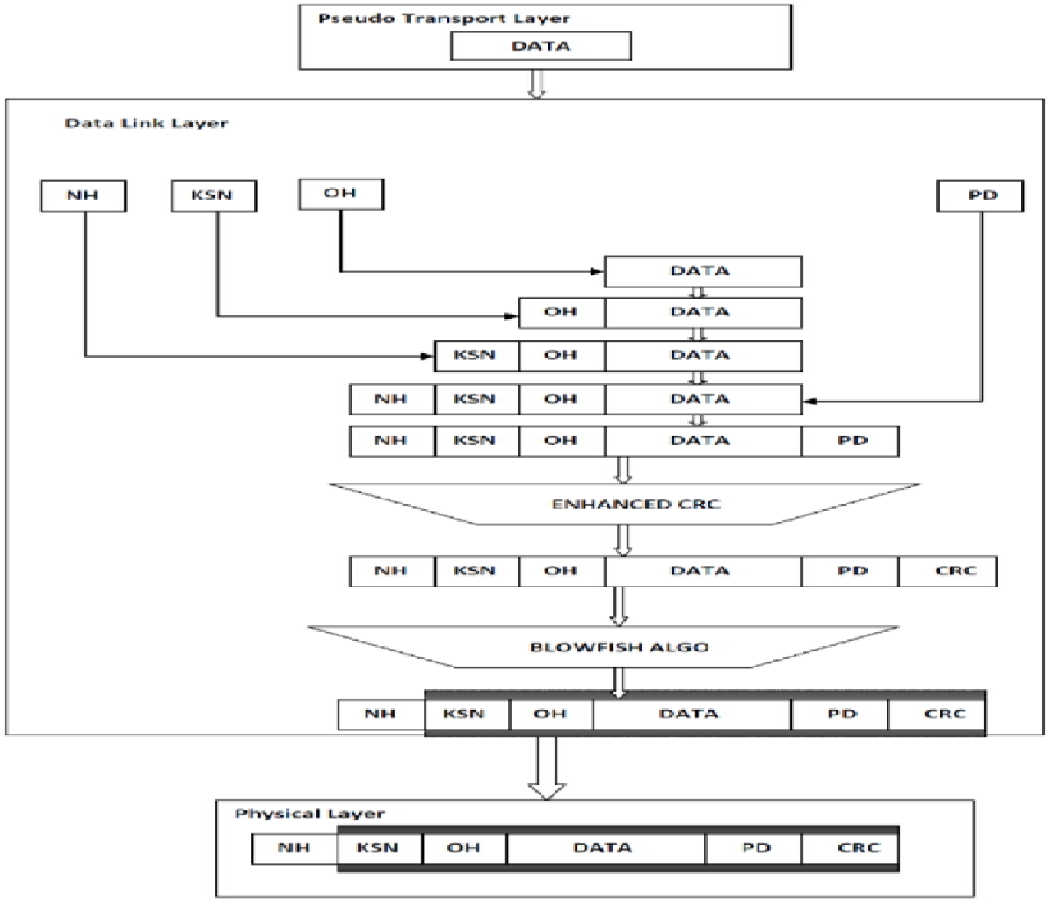


Fig. 2. Internal Structure of ZA Protocol

The remainder polynomial is generated when sender appends r 0-bits to the m-bit message and divides the resulting polynomial by the generator polynomial. The data transmitted is the original m-bit message followed by the r bit CRC. The CRC [13][16] method treats the message as a polynomial in GF (2). At receiver side, the receiver uses the same generator polynomial to divide received message. If the remainder generated after dividing the received message is zero, then no error occurred in the message, otherwise, error occurred.
In ZA protocol, the original message can be represented in a polynomial:

P (x) = aN-1xN-1 + aN-2xN-2+..... a0

Original message is represented in a binary form

[aN-1 aN-2 ...a0]

here aN-1 denotes the MSB and a0 is LSB.

For CRC computation generator polynomial is always associated and we use generator polynomial G(x) of M degree can be represented in a polynomial:

G(x) = gM xM + gM-1 xM-1+..... +g0

And binary representation is

[gM, gM-1... g0].

In our enhance algorithm we divide the original message of N bits

[aN-1 aN-2 aN-3 ..... a0] into n chunks of M size

Without loss of generality, N= nM, where original message of N bits, M bits size of chunk, n is integer. For example message of 272 bytes is divided 68 chunks of 4 bytes as shown in fig 3.

Here Wi (x) = a(i+1)M-1xM-1+.....+aiM. Then original message will be

P (x) = W n-1 xN-1 + W n-2 xN-2 +.....+W0 …… (1)

And Wi (x) is the ith chunk of the original message

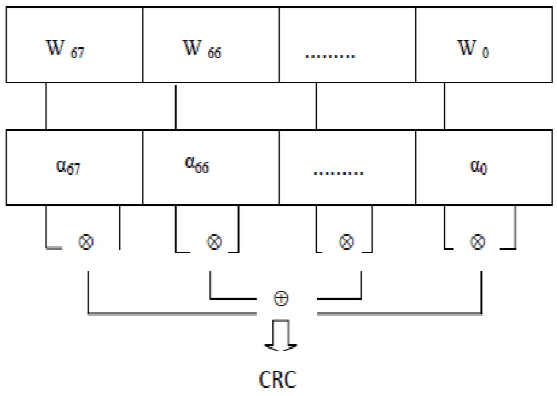


Fig 3: Enhanced CRC

Given the original message is P(x) and generator polynomial G(x), we can compute the CRC by appending M zeros after the LSB and then dividing the appended message by G(x). Then equivalently is:

CRC [P(x)] = (P(x)xM) mod G(x)……..(2)

From the equation (2) and congruence property, CRC computation on chunked message (1) by:

CRC [P(x)]=Wn-1 (x) nM modG(x) +....+ W0xMmodG(x).

Here, the modulo of Wi(x) by G(x) will be Wi(X) i.e. Wi (x) mod G(x) = Wi(x).

Wi(x)x(i+1)MmodG(x)=Wi(x)modG(x)x(i+1)MmodG(x), for i = 0,1, 2…..n-1.

Note degree of each polynomial Wi (x) for each chunk is less than M.

Let us define α coefficient,

αi = x(i+1)M mod G(x) for i= 0 ,1,....., n-1.

Now CRC can be computed as:

CRC [P(x)] = Wn-1 ⊗ αn-1 ⊗ W0 ⊗ α0 ⊗

By the help of the generator polynomial G(x), we compute α. To compute the α factor, we have

$\alpha 0 = x^M \mod G(x) = \{g_{M-1}+..... +g_0]$

α1 = x2M mod G(x) = [α0 ⊗ α0]

.....

αn = xnM mod G(x) = α0n

After (α_0 α_1... α_n) is computed, then CRC is computed as

CRC (β (x)) =W n-1 ⊗ αn-1 ⊗ ..... ⊗ W0 ⊗ α0

The operation ⊗ , ⊕ in the above equation is Galois Field multiplication, addition over GF (2^M), respectively.

Now enhanced CRC algorithm is presented as:

i. Put original message of N bits and divide it into n chunks

[Wn-1Wn-2 .....W1 W0] and each chunk size is M bit (N= nM).

ii. Initially take generator polynomial G(x) and its degree M at the same time calculate α coefficient (as discussed above).

iii. Now perform n-pair Galois field multiplication in parallel and then XOR the products. This generates the CRC result.

Here the original message is now divided into small 68 chunks of 4 bytes. These chunks are under going to CRC algorithms to provide message authentication. In Fig: 3 the illustration of the enhanced CRC. In the CRC algorithm is used to provide integrity of the message in SCADA protocol. Here 4 bytes are used in the CRC out of 20bytes and the remaining bytes are reserved for future work. So the protocol is providing authentication and integrity by using blowfish and enhanced CRC. Through this approach we are rearranged bytes of the DNP3 protocol to enables confidentiality, integrity, and authenticity. In this protocol we have done modification in the protocol to reserve the bytes and provide security. The original LH header and Payload data is encrypted by the Blowfish algorithm to provide the confidentiality to the message. The 4 bytes of our proposed CRC is used to provide message authentication.

VII. CONCLUSION

This paper investigates security issues of network communication protocols. In order to protect the SCADA networks, we focus on the protocols as they were not designed with inherent security features. The aim is to modify the structure of such protocols to provide more integrity and authentication. In the proposed structure, two algorithms are used to enhance the security and integrity of the payload. We have freed 16 bytes in the frame for future enhancements and possible modifications. The aim is to increase the security of such protocol to alleviate threats.

REFERENCES

[1] Zia Saquib, D. Patel, R. Rajrajan ―A configurable and efficient keymanagement scheme for SCADA‖ International Journal of Research and Reviews 2011.

[2] Anupam Saxena, Om Pal, Zia Saquib, Dhiren Patel ―Customized PKI for SCADA Systems Network‖ Int. J. of Advanced Networking and Applications. 282. Volume: 01, Issue: 05, Pages: 282-289 , 2010.

[3] Athar Mahboob, Junaid Zubairi ―Intrusion Avoidance for SCADA Security in Industrial Plants‖ Collaborative Technologies and Systems (CTS)‖ 2010.

[4] S. Bhagaria, S B Prabhakar, Z Saquib ―Flexi-DNP3: Flexible distributed network protocol version 3(DNP3) for SCADA security‖,Recent Trends in Information System 2011.

[5] S Saiwan, P Jain, Z Saquib, D Patel ―Cryptography key Management for SCADA System An Architectural Framework‖, Advances in Computing Control, & Telecommunication 2011.

[6] Robert Dawson ―Secure Communication for Critical Infrastructure Control System‖ University of Queensland 1997.

[7] Munir Majdalawieh, Francesco Parisi- Presicce, Duminda Wijesekera (2006)_ DNPSec Distributed Network Protocol Version 3 (DNP3)', Security Framework Advances in Computer, Information and Systems Sciences and Engineering 2006.

[8] DNP3 Application Note AN2003-001, http://www.dnp.org.[9]H. Michael Ji, Earl Killian ―Fast Parallel CRC Algorithm and Implementation on a Configurable Processor‖ IEEE 2002 vol3. [10] Bruce Schneier ―Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), Fast Software Encryption‖ Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag pp. 191-204 1994.

[11] Distributed Network Protocol (DNP3) IEEE Standard for Electric Power Systems Communications 2012.

[12] David C. Feldmeier‖ Fast Software Implementation of Error Detection code‖IEEE/ACM Transactions on networking, December 1995.

[13] Sanjay M.Joshi, Pradeep K. Dubey, Marc A. Kalpan ―A new parallel algorithm for CRC Generation, Communication‖ ICC IEEE International Conference 2000.

[14] P. Rogaway, M. Bellare, J. Black ―OCB A block –cipher mode of operation for efficient authenticated‖ ACM Trans. Inf. Syst. Secure 2006.

[15] M. Bellare, P. Rogaway ―Entity authentication and Key distribution‖ in Advances in cryptology-CRYPTO 93, Lecturenotes in computer Science, Springer 1994.

[16] D. V. Sarwate ―Computation of Cyclic Redundancy Checks via Table Lookup‖ Communications of the ACM, vol. 31, no. 8 1988.