CSIT (June 2013) 1(2):135–141
DOI 10.1007/s40012-013-0013-5

ORIGINAL RESEARCH

SCADA communication protocols: vulnerabilities, attacks and possible mitigations

Durga Samanth Pidikiti · Rajesh Kalluri · R. K. Senthil Kumar · B. S. Bindhumadhava

Received: 31 October 2012 / Accepted: 26 March 2013 / Published online: 19 April 2013

Abstract Current hierarchical SCADA systems uses communication protocols which aren't having the inbuilt security mechanism. This lack of security mechanism will help attackers to sabotage the SCADA system. However, to cripple down the SCADA systems completely coordinated communication channel attacks can be performed. IEC 60870-5-101 and IEC 60870-5-104 protocols are widely used in current SCADA systems in power utilities sector. These protocols are lacking in the application layer and the data link layer security. Application layer security is necessary to protect the SCADA systems from Spoofing and Non-Repudiation attacks. Data link layer security is necessary to protect the systems from the Sniffing, Data modification and Replay attacks. IEC 60870-5-101 & 104 communication protocol vulnerabilities and their exploitation by coordinated attacks are explained in this paper. Proposed experimental research model can be used to mitigate the attacks at application layer and data link layer by adopting the IEC 62351 standards.

Keywords SCADA · MTU · RTU · Risk analysis · HMI

D. S. Pidikiti · R. Kalluri (✉) · R. K. S. Kumar · B. S. Bindhumadhava
Real Time Systems and Smart Grid Group, Centre for Development of Advanced Computing, C-DAC Knowledge Park, Bangalore, India
e-mail: rajeshk@cdac.in

D. S. Pidikiti
e-mail: pdsamanth@cdac.in

R. K. S. Kumar
e-mail: senthil@cdac.in

B. S. Bindhumadhava
e-mail: bindhu@cdac.in

Abbreviations

SCADA	Supervisory control and data acquisition
MTU	Master terminal unit
RTU	Remote terminal unit
HMI	Human machine interface
ICS	Industrial control systems

1 Introduction

SCADA system's operation completely depends on the data received from the RTU, based on which the control actions will be taken. So, if an attacker wants to cause damage to ICS systems which are using SCADA, the attacker mainly focuses on modifying the data or completely blocking the data transfer.

Since SCADA system's communication protocols were initially designed without security, they are luring the attackers now a day. There are two types of attackers, one is a targeted attacker and dumb attacker. The unskilled intellectuals perform the dumb attacks wherein many of them can be alleviated without much effort by the use of redundant systems and other security measures. The skilled intellectuals perform the targeted attacks which will be pretty hard to handle with the existing security measures of the SCADA systems. The coordinated attacks are difficult to handle due to their diverse attack origin nature [3–5]. Coordinated attacks can be modeled and analyzed to avoid detection [2, 8]. Coordinated attacks are difficult to differentiate between decoy and actual attacks [2]. There is a large variety of coordinated attacks [2]. These coordinated attacks are gaining a lot of attention from both amateur and professional attackers. The Coordinated communication

channel attacks if planned and executed with precision can break down all the existing SCADA systems. Coordinated communication channel attacks performed by the skilled intellectuals will be carried out only when they have performed a preliminary risk analysis. This preliminary risk analysis gives out all the possible loop-holes that exist in the system [1].

There is an old adage stating that, "Start thinking thyself as your enemy while implementing battle strategies to win a war". The same concept can be applied to this scenario also wherein the security providers of the critical systems should start thinking themselves as their attackers. So, the first step will be to perform the risk analysis over the communication channel to eliminate the possible coordinated communication channel attacks. Possible attacks can be represented using attack trees [7] and defense graphs [1].

One more advantage of using the risk analysis or vulnerability analysis [6] is that a particular industry may decide to completely implement the security to all the devices or apply it to particular selected critical areas. With this, a balance can be achieved between the implementation cost and the benefit of implementing security mechanisms [1].

The rest of the paper is organized as follows: Sect. 2 discusses about the vulnerabilities of communication protocols IEC60870-5-101 and IEC60870-5-104. Section 3 discusses about an in-depth view of exploiting vulnerabilities. Section 4 discusses, uncoordinated and coordinated attacks using the existing vulnerabilities. Section 5 discusses application layer security for IEC 60870-5 series protocols based on IEC 62351. Section 6 discusses experimental research model. Section 7 discusses additional security mechanism. Section 8 discusses observed results. Section 9 discusses future work. Conclusion of this paper is expressed in Sect. 10 by examining some important properties of the proposed paper.

2 Vulnerabilities of communication protocols IEC 60870-5-101, IEC 60870-5-104

Before going in through the attacks, an attacker first tries to espial the weak links of the communicating protocols and then tries to figure out their usage to cause maximum chaos. Some of the weak links present in the communication protocols IEC 60870-5-101 and IEC 60870-5-104 are as follows:

1. One byte checksum in the case of IEC 60870-5-101 protocol and absence of checksum field in IEC 60870-5-104 protocol, as it is completely dependent on lower layers for data integrity.
2. Lack of inbuilt security mechanisms in both the protocols for providing security at application layer and data link layer.
3. The communication vulnerabilities at data transit level are
    a. Limited bandwidth, this leads to limited frame length of data being transferred (Example: Only 255 octets can be transmitted both by IEC 60870-5-101 & IEC 60870-5-104 protocols at a time).
    b. Unreliable media of communication (The communication medium may or may not have security mechanisms implemented).

The possible attacks due to lack of the application layer security are

a. Spoofing [3–5].
b. Non-Repudiation [3–5].

The possible attacks due to the lack of data link layer security are

a. Sniffing [3–5].
b. Data modification [3–5].
c. Replay [3–5].

These vulnerabilities are also discussed along with few other vulnerabilities in IEC 62351 security document. These vulnerabilities are acting as crevices for the IEC 60870-5-101 and IEC 60870-5-104 protocols wherein the attackers are prowling into plunder them.

The possible areas for communication channel attacks in a SCADA environment are

1. Communication between MTU and RTU, wherein the IEC 60870-5-101 and IEC 60870-5-104 protocols are used for data transmission.
2. Communication between MTU and HMI.

These are the major areas of communication of data wherein the modification of data may lead to wrong control decisions which will cause chaos.

3 An indepth view of exploiting vulnerabilities

The checksum vulnerability which was stated earlier is having two problems.

A. Insufficient size of checksum.
B. Checksum alone is unreliable for data integrity.

3.1 Insufficient checksum size

The size of checksum in the IEC 60870-5-101 protocol is just one byte, here there is always a possibility of overflow

of the checksum. The preliminary research in the SCADA industry showed some supporting results for this.

An example of the above statement is consider a case where the maximum value of the checksum is 100 and the sum of all the data is 130 or 230 or 330 and so on, then the checksum value will be shown as 30. This is revealing that the exact value of checksum cannot be determined by the use of a single byte checksum.

3.2 Checksum alone is unreliable for data integrity

Purely relying on the checksum alone for checking the data integrity is not appreciated. A smart attacker can play a hoax on the operator by changing both the data value and the corresponding checksum value. An example for this mechanism is shown in Sect. 5.

3.2.1 Communication vulnerabilities at data transit level

The limited bandwidth for data transmission is acting as an obstacle for the packet frame length. Due to this limited bandwidth only 255 octets can be transmitted at a time by using both the IEC 60870-5-101 and IEC 60870-5-104 protocols. This is indirectly acting as a barricade on the security bits to be added during data transmission.

The unreliable medium of communication which is not having security mechanisms is also adding insult to the injury. Generally the medium of communication will be radio waves or the twisted cable (Fiber optic also). If radio waves are used as a communication medium then frequency interference can be created by producing a different signal apart from intended communication signal with same frequency range.

The IEC 62351 security standard is provided for adding the security mechanism to the IEC 60870-5 series protocols. The IEC 62351 is providing security mechanisms at the application layer level but it is not dealing with the Data link layer security mechanisms. Thus, by the use of IEC 62351 document alone complete security to the communication protocols of SCADA systems can't be provided.

4 Uncoordinated and coordinated attacks using the existing vulnerabilities

The succeeding part will deal with the impact of the uncoordinated and coordinated attacks based on the vulnerabilities stated in the previous sections.

4.1 Uncoordinated attacks

It is again classified into two types

a. Dumb way.
b. Smart way.

Dumb way of performing an uncoordinated attack is a very simple attack here the attackers doesn't need any prior knowledge about the communication protocol structure. In this attack the attacker simply modifies some bytes of data and transmits it to the destination station. An experiment has been conducted to show this attack but the drawback of this attack is the MTU simulator has detected the modification based on the checksum and popped out a message stating "Checksum mismatch". So, this attack will not have any serious impact on the systems.

Smart way of performing an uncoordinated attack requires knowledge about the communication protocol in use. The frame format of IEC 60870-5-101 protocol is explained in the Fig. 1.

The CF (Control Field) 8 bits classification table is shown in the Fig. 1. In this ACD bit is transmitted from the slave (controlled station) system to the master (controlling station) system. The purpose of this bit is to inform the master that the slave station is having the digital data with it. Then if the master system wants to read the digital data it would send the digital data request. Generally digital data is considered to be the data regarding circuit breakers, switches and so on. This digital data is considered as the critical data in most cases. So, keeping this in mind an intelligent attacker will modify this bit value and the checksum correspondingly and misguides the master station and makes the digital data unavailable to it.

One more bit DFC is also transmitted from slave (controlled station) system to the master system. The purpose of this bit is to indicate the master (controlling station) system that if it further sends the requests it will lead to overflow. Based on this the master will decide whether to transmit further requests or not. A smart attacker will modify this bit and the corresponding checksum value. By this the attacker fulfills in making the master station wait continuously.

The bits common address of ASDU (CAASDU) and link address (LA) consists of the station address and link address respectively. A smart attacker will change these bits and the corresponding checksum value. The result of this modification is the intended control operation will not take place at the desired RTU. The other bits in the frame format like type identification (TI), variable structure qualifier (VSQ), cause of transmission (COT) can also be modified. But, the affect of these attacks will be very minimal as these modifications can be very easily detected by the operator.

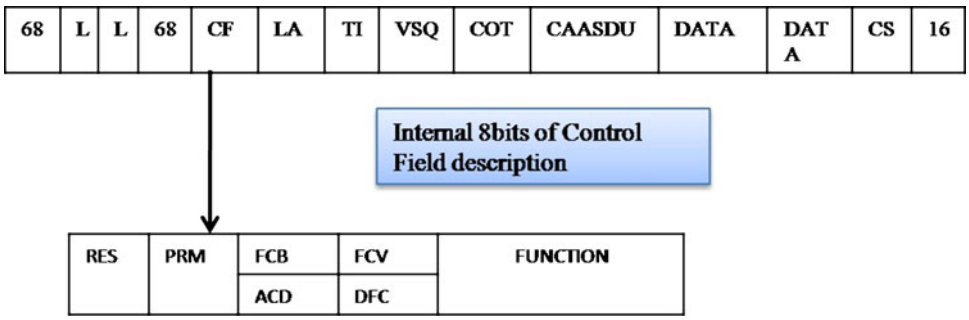

Fig. 1 Frame format of IEC 60870-5-101 & 104 communication protocols Legend: *CF* control field, *LA* link address, *TI* type identification, *VSQ* variable structure qualifier, *COT* cause of transmission, *CAASDU* common address of application service data unit, *CS* checksum, *L* length, *RES* reserved, *PRM* primary message, *FCB* frame count bit, *FCV* frame count bit valid, *DFC* data flow control, *ACD* access demand

4.1.1 Attack's intention

The attacker can mislead the control center operator.

4.1.2 Loophole of this attack

Control center operator can detect this attack after cross checking the tag values and ranges.

4.2 Coordinated attacks

Coordinated attacks are generally practiced by the people who wanted to cause maximum damage to a particular organization or a nation. These attacks are also known as targeted coordinated attacks. The targeted coordinated attacks will not be carried by a single person instead they are carried by a group of professionals in different areas. The network access and access credentials are obtained just like any normal communication channel attack but, the variation here is in the collection of details of communication protocols and the field details. The attackers here will study the communication protocols and figure out the possible vulnerabilities which will be exploited to cause a maximum damage.

An experiment has been conducted to prove this attack's severity.

4.2.1 Attack's intention

The maximum damage can be caused when the attacker knew about the field details like tag ids and tag values and ranges of field devices like actuators and circuit breakers. Based on those details the attacker can send control commands for malfunctioning of the field devices. The smart coordinated attacks are considered as the brutal attacks over any control system because they cannot be detected and controlled easily.

5 Application layer security for IEC 60870-5 series protocols based on IEC 62351

Authentication mechanism is considered as a critical security measure at the application layer level. Here authentication is of two types.

1. Operator authentication.
2. MTU/RTU authentication.

Non-Repudiation attack can be eradicated by the use of operator authentication. In operator authentication mechanism each and every operator possesses a unique authentication credentials. Some operator privileges can also be set. Thus by the use of operator authentication operators are made accountable.

Spoofing attack or masquerade attack can be eradicated by the use of the MTU/RTU authentication. IEC 62351 stated a mechanism wherein only critical data request will be authenticated and non critical data will not be authenticated. This is to reduce the bandwidth and processing requirements. There is one more mechanism specified in IEC 62351 called as aggressive mode wherein the challenge response mechanism is eliminated. But, the aggressive mode is less secure than the challenge response mechanism. The IEC 62351 also specified key exchange mechanism for changing/managing of the authentication credentials.

6 Experimental research model

One major problem in implementing these security mechanisms to the existing SCADA systems is that, the RTU and MTU software is a third party software which is not revealed to outsiders. The design of the security model should be in such a way that it should not affect the existing SCADA systems technically and economically. Therefore, the security mechanism for application layer

security should be provided externally to the systems without disturbing the existing SCADA system's working. This can be implemented by the use of the single board computers (SBCs). These SBCs will act as an extra layer; wherein the data to be transmitted will be wrapped up within this extra security layer. Keeping this as foundation logic, following security design model shown in Fig. 2 was developed for IEC 60870-5-101 protocol. The Security Hardener shown in the Fig. 2 is a SBC.

The above security model was designed with full compliance of IEC 62351 security standard. In this model authentication of critical data alone is performed to optimize the bandwidth utilization and the processing power.

6.1 Calculation for supporting the bandwidth and processing power optimization

Let us consider the normal Application Service Data Unit (ASDU) of IEC 60870-5-101 protocol is of length 25 bytes. The processing power required for computing the same 25 bytes is say 100 ms. Now as we are including the challenge response mechanism for providing the application layer security by the SBCs. The challenge message consists of 112 bits (23 bytes) and response message consists of 72 bits (9 bytes). The critical ASDU request and critical ASDU response will occupy 50 bytes. Then the total number of bytes that are getting transferred with the security mechanism included for critical data are 82 bytes (23 bytes challenge + 9 bytes response + 50 bytes of challenge request and response).

Now the increase in number of bytes leads to increase in the bandwidth consumption. The processing power will also be incremented by some factor "X". So, the new processing power will be "100 ms + X".

Note: the "X" value will be less than 100 ms.

If we have chosen an aggressive mode request instead of challenge response mechanism then the number of extra bytes added will be 57 bytes (7 bytes of aggressive mode request + 50 bytes of normal data transfer).

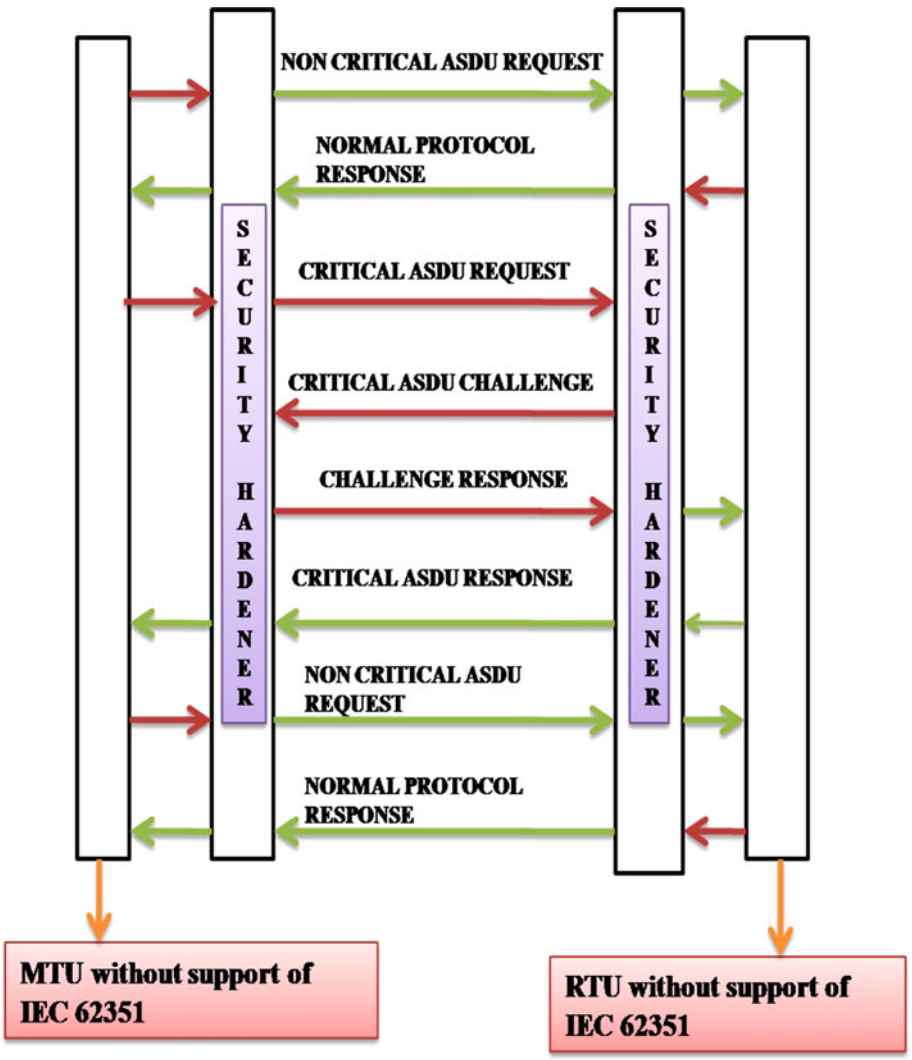

Fig. 2 Authentication security model for IEC 60870-5-101 protocol

Note: the challenge and response mechanism data length taken is with only minimum values (mentioned in IEC 62351) required so, there is always a possibility that the data length may increase.

The design diagram of IEC 60870-5-104 protocol for implementing authentication layer security is shown in the Fig. 3.

The IEC 60870-5-104 protocol is an IP based protocol so, the design model for it is different from the design model of the IEC 60870-5-101 protocol to some extent but, the data transfer mechanism is almost similar.

This design model is also in full compliance with the IEC 62351 security document. In these models only the challenge response mechanisms alone are shown. The aggressive mode of authentication is not shown as it is less secure when compared to the challenge response mechanism. This aggressive mode is very important in time critical scenarios but the scenarios where we are working are allowing the delay caused by the challenge response mechanism.

7 Additional security mechanism

IEC 62351 document provides only the application layer security. But in SCADA, application layer security alone can't guarantee the data integrity which is critical. So, to provide the data integrity security encryption mechanisms should be included. As MTU and RTU are third parties software, we have implemented the data link layer security mechanism also by the bump in wire mechanism.

After completely analyzing the packet structure of IEC 60870-5-101 protocol it was observed that there are actually 2 sizes of packets which are getting transmitted in between MTU and RTU. Some ASDU packets are <16 bytes size and some are >16bytes size. The ASDUs which are <16 bytes are completely encrypted and are transmitted in between the boards and only 16 bytes (which includes checksum byte also to provide greater level of security) of the ASDUs which are >16 bytes will be encrypted and is transmitted in between the boards along with remaining data. To provide a strong security mechanism AES-128 bit encryption algorithm (block cipher) was used. This technique was implemented and tested on SCADA TESTBED in our simulation lab.

Data modification attack, replay attack and Sniffing attack can be eradicated by using the encryption techniques. The replay attack can also be eradicated by the use of the time stamping techniques in the data transmission protocols.

8 Observed results

Time delay involved by implementing

S. No.	Mechanism	Time taken (at MTU)
1.	Challenge-response	1258 ms
2.	Challenge-response with key change	1263 ms
3.	Challenge-response with key change and data link layer security	1365 ms

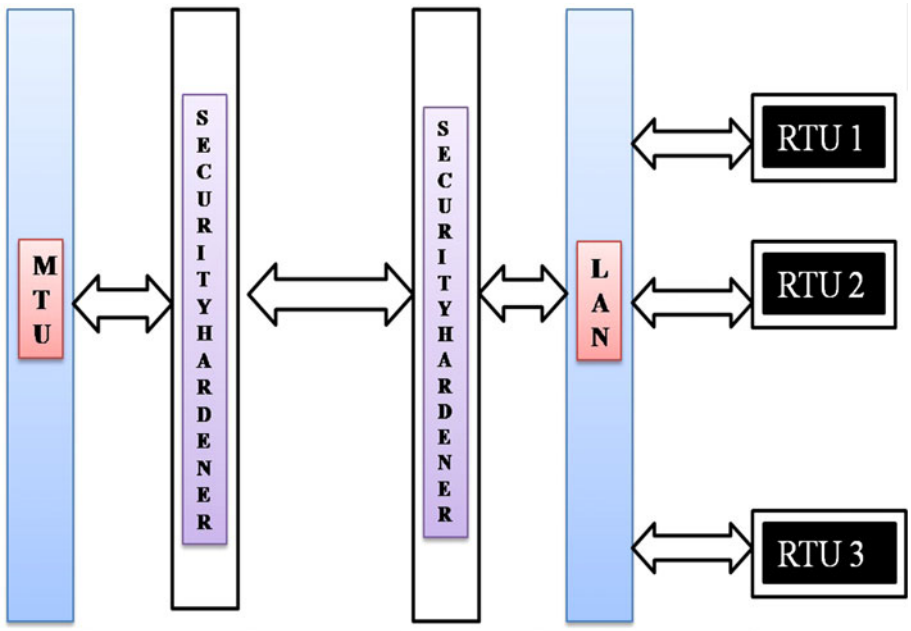

Fig. 3 Authentication security model for IEC 60870-5-104 protocol

9 Future work

Future work is to implement the security mechanism for IEC 60870-5-104 protocol.

10 Conclusion

The lack of security mechanisms both at application layer level and the data link layer level are pushing the legacy SCADA systems into mire of cyber attacks. These cyber attacks are being launched as a means of cyber warfare by criminals to cause damage to the organization or nation. By adopting proposed experimental research model, these attacks can be eradicated and security at both application & data link layer will be provided for the SCADA systems. This research model is in compliance with IEC 62351 standards also.

References

1. Bindhumadhava BS, Senthil Kumar RK, Kalluri R, Pidikiti DS (2012) SCADA systems security-threat analysis using defense graphs. In: International conference on cyber, physical and system security
2. Braynov S, Jadliwala M (2003) Representation and analysis of coordinated attacks. In: FMSE '03 Proceedings of the 2003 ACM workshop on formal methods in security engineering, pp 43–51
3. Gregg M (2007) Certified ethical hacker guide. Que Publication
4. http://csrc.nist.gov/. Accessed 22 Oct 2012
5. http://www.cert-in.org.in/. Accessed 23 Oct 2012
6. http://www.cert.org/. Accessed 23 Oct 2012
7. Ten C-W, Manimaran G, Liu C-C (2010) Cybersecurity for critical infrastructures: attack and defense modeling. IEEE Trans Syst Man Cybern Part A Syst Hum 40(4):853–865
8. Xh Li, Sh Xu (2007) A stochastic modeling of coordinated internal and external attacks