Survey On Analysis Of Security Threats In DNP3 Protocol

Bhagyashri Sangewar, Dr. A. R. Buchade

Abstract— Industrial Automation and Control Systems (IACS) required facilitating the safer means of information communication between smart devices such as various Intelligent Electronic Devices (IEDs) or between IEDs and host systems. Security in Industrial Automation and Control Systems (IACS) is critical task as many of these devices are present in remote location and controlling critical plant processes. These IEDs and hosts use various protocols such as Modbus, DNP3, IEC 60870, IEC 61850 etc. Distributed network protocol version 3(DNP3) is non-proprietary protocol used in Supervisory Control and Data Acquisition (SCADA) system. SCADA is the key foundation for many critical industries. DNP3 protocol is de facto standard for water, sewage, and oil and gas industry. DNP3 is used in industrial automation but initially DNP3 was not covering security aspects. Due to the need for secure communication later secure authentication is added to the protocol. DNP3-SA is the authentication mechanism which ensures the integrity and confidentiality between communicating devices. This paper presents the survey on DNP3 protocol and what are various attacks possible in basic DNP3 without secure authentication and with secure authentication mainly on SAV2 (Secure Authentication Version 2) and SAV5 (Secure Authentication Version 5).

Index Terms— DNP3 protocol, IACS, SCADA, Secure authentication, SAV2, SAV5, Security.

INTRODUCTION:

DISRUPTING services in critical infrastructures is a very important issue to consider. This is because a disruption, either minor or major, deliberately or mistakenly caused to these infrastructures can lead to damaging highly sophisticated devices, degrade system performances and causes substantial economic losses. In addition, it could pose as life-threatening situations to the society. Unfortunately, this situation has now become the target area for many malicious attackers. The SCADA architecture has various components such as programmable logic controllers (PLC), Remote terminal units (RTU), intelligent electronic devices (IDEs) and human machine interface (HMI) etc. The control flow of every SCADA system is carried out by communication protocol used by master and outstation device to exchange data and for sending various commands. The most widely used SCADA protocols are MODBUS, DNP3 etc. SCADA systems initially designed for serial communication. But in last 10 years for taking advantage of modern technologies all the SCADA protocols such as MODBUS, DNP3 has been ported to TCP/IP communication stack. It has introduced the new complexity for reliable delivery of packets in real time constraints. Many industrial automation protocols are vulnerable to various attacks due to following conditions:

1. Do not have the mechanism for integrity checking of the packets between master to outstation or vice versa.
2. Do not provide any authentication mechanism.
3. Do not apply anti- replay and anti-repudiation mechanism

DNP3 (Distributed Network Protocol) is communication protocols used between components in process automation systems. It is used in communications between a master station and RTUs (remote terminal unit) or IEDs (Intelligent Electronic Device). In DNP3 three-layer Enhanced Performance Architecture (EPA) is created which includes data link, transport and application layer.

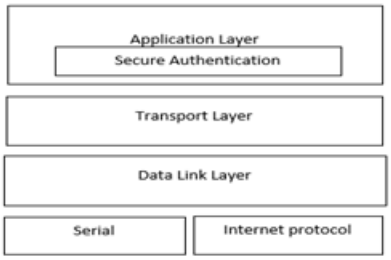

Fig 1. DNP3 Layer Architecture [1]

This paper is organized into 3 sections which contain DNP3 layer architecture, literature survey followed by attacks possible on DNP3 protocol.

2. DNP3 LAYER ARCHITECTURE

2.1 Application Layer

Application layer contains DNP3 request and response messages. The Request message contains the task outstation should perform. Request message contains various function codes which are used for either performing task or collecting and providing the data. Response message is sent from outstation to master. Outstation devices may send solicited or unsolicited messages. The message fragment size of application layer is between 2048 to 4096 bytes. Application control has one byte allocated. The FIN field is a single bit, which when set to 1 indicates that this is the final fragment of a message otherwise more fragments follows. The CON field is a single bit, which when set to 1 indicates that the receiver's Application Layer shall return an application confirmation message otherwise no confirmation is required. The UNS field is a single bit, which when set to 1 indicates the message contains an unsolicited response or a confirmation of an unsolicited response otherwise it is normal request or response message. The SEQ field is 4 bits wide. It is used for receiving fragments in correct order or to detect duplicate fragments. Following figures shows the request and

- *Bhagyashri Sangewar, Computer Engineering, Pune Institute of computer technology, Pune, India. bhagyashrisangewar@gmail.com*
- *Dr. A. R. Buchade, Computer Engineering, Pune Institute of Computer Technology, Pune, India. arbuchade@pict.edu*

response message structure. DNP3 have various function codes for both request and response. This function code indicates the action targeted device should perform. Some of these function codes are given in the table 1.

Table 1: Function codes

Type	Function Code	Name
Request	0x01	Read
Request	0x02	Write
Request	0x03	Select
Request	0x04	Operate
Request	0x05	Direct Operate
Request	0x0D	Cold Restart
Request	0x0E	Warm Restart
Request	0x11	Start Application
Request	0x12	Stop Application
Request	0x14	Enabled Unsolicited
Request	0x15	Disable Unsolicited
Response	0x81	Response message
Response	0x82	Unsolicited Response
Response	0x83	Authentication Response

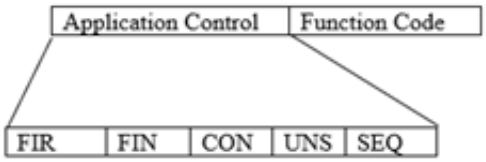

Fig2. Application Request

DNP3 secure authentication has provided the way to check the authenticity of the device by using challenge response mechanism. But DNP3 basic version has no such facility available.

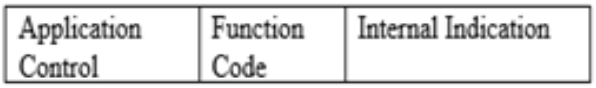

Fig3. Application Response

Internal indication has 2 octets. It is provided in the response message which indicates certain states and error conditions within the outstation. Some of these internal indications are provided in table 2.

Table 2: Internal Indications

Bit	Name	Description
IIN1.0	Broadcast	Broadcast message has received
IIN1.4	Need Time	Time synchronization required
IIN1.6	Device Trouble	Abnormal device condition exists
IIN1.7	Device Restart	Outstation restarted.
IIN2.0	No_func_code_support	Outstation does not support this function code.
IIN2.3	Event_Buffer_overflow	Event buffer overflow condition exists in the outstation

2.2 Transport Layer

The main task for transport layer is message fragmentation and reassembly. It divides the application layer message in multiple frames having size more than data link layer frames.

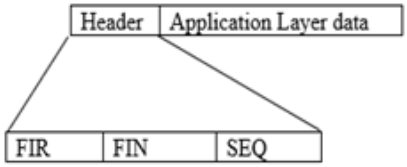

Fig4. Transport header

2.3 Data Link Layer

The logical link between master and outstation is provided at data link layer. The maximum frame size is 292 bytes. The payload of it contains data from application and transport layer.

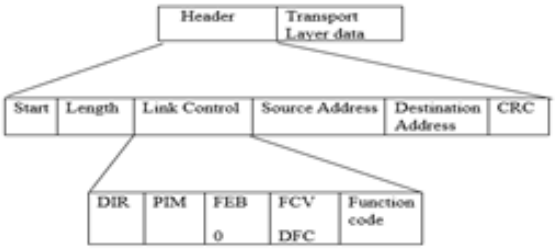

Fig5. Data Link Layer header

Start field is 2 bytes where first byte is 0x05 and second byte is 0x64. The length field gives the count of octets of header and data block expect CRC field. DIR bit when set to 1 indicates frame from master otherwise it indicates frame from outstation. PRM bit when set to 1 indicates transaction is being initiated by either master or outstation otherwise transaction is being completed by either a master or outstation.

FCB (Frame Count bit) and FCV (Frame Count Valid) bits works in synchronization. When FCV bit set to 1 indicates that state of the FCB bit is valid otherwise state of the FCB bit should be ignored. DFC (Data Flow control) is present in every response message. When DFC field is set to 1 indicates that receiver buffer is not available.

Data Flow Control (DFC) bit appears in every response from a Secondary Station regardless of the function code in the control octet. It is used to report an insufficient number of Data Link Layer buffers to hold a receive frame. It is also used to indicate that the Secondary Station's Data Link Layer is busy. DFC = 1 indicates receive buffers were not available or that the Secondary Station's Data Link Layer was busy. DFC = 0 indicates receive buffers were available and the Secondary Station's Data Link Layer was ready.

Function code field indicates function or services associated with data link layer frames. The values are depending on whether message is sent from master to outstation or outstation to master.

Destination and source address fields are 2 octets in size each. The fields indicate source and destination address of the frame.

CRC is the 2-octet cyclic redundancy check appended to each frame. It calculates the CRC of start, length, control, destination, source, destination fields.

3. DNP3 SECURE AUTHENTICATION

DNP3 secure authentication is based on challenge-response mechanism and HMAC (key hashed message authentication code). In challenge response algorithm whenever a user tries to perform any critical function, receiver of the message can initiate the challenge object containing random data. The challenge data is being hashed by session key which is already shared between communicating devices.

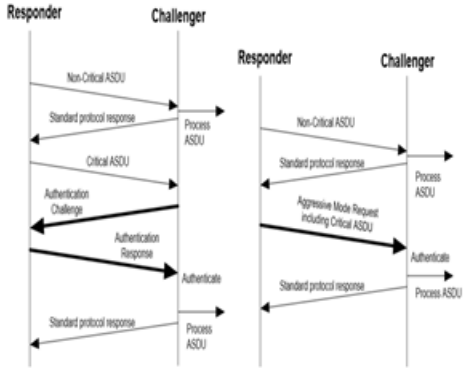

Fig6. Challenge response sequence and aggressive mode challenge response

The request of the challenge data will be processed only if sender of the request replies correctly to the challenge data having correct MAC (message authentication code). This process can take place in any direction either from master to outstation or outstation to master.

HMAC is used to ensure that message is not getting altered in transit. It contains cryptographic hash and session key to calculate the message authentication code. A HMAC algorithm used by DNP3-SA includes SHA-HMAC (secure hash algorithm) and AES (advanced Encryption Algorithm).

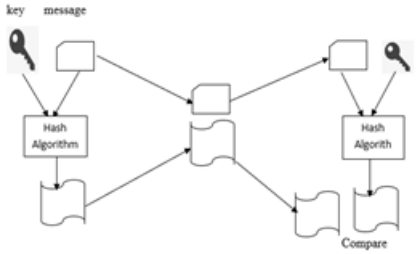

Fig7. Message Authentication

4. LITERATURE SURVEY

Ihab Darwish et.al [2] highlights different security threats and vulnerabilities that is being challenged in smart-grid utilizing Distributed Network Protocol (DNP3) as a real time communication protocol. Two attack scenarios have been demonstrated: 1. unsolicited message attack 2. Data set injection. The experiments were run on a computer virtual environment and then simulated in DETER testbed platform. Intrusion detection system is used to identify different attacks which can target parts of smart grid infrastructure.

Ihab Darwish et.al [3] In this research paper they have created an attack detection model based on the Round-Trip Time Delay (RTTD) for DNP3 transactions. They have used host-based intrusion detection technique and Naïve Bayes estimator was used to categorize network traffic by application. Likelihood distributions for both legitimate and hacked transactions are modeled using Bayesian analysis. Both Maximum A Posterior probability (MAP) and the loss functions are utilized to optimize our threshold to ensure an improved attack detection accuracy.

Raphael Amoah et.al [4] presents DNP3 Secure Authentication for Broadcast (DNP3-SAB), a new lightweight security scheme for broadcast mode communication. The DNP3 protocol standard only gives the use of broadcast permission but does not specify its security. This paper is the first to present DNP3 Secure Authentication for Broadcast (DNP3-SAB. One of the advantages of this mode is that it reduces delay and overhead in large-scale systems.

Ihab Darwish et.al [5] analyzes vulnerabilities and performing penetration testing using man-in-the-middle (MITM) attack to identify possible threats associated with smart grid. Game theory is used by utilizing theoretical modeling of smart grid attacks, they can analyze the outcomes of MITM for DNP3 environment. Intrusion detection system (IDS) is used to identify attackers targeting different part of the smart grid infrastructure and mitigation strategies will ensure a healthy check of the network**.**

Jeyasingam Nivethan et.al [6] proposed the Linux based firewall for DNP3 protocol. They have added the fileting rules which are used to identify the common attacks on DNP3 protocol. The testing is done at scaled down electric power station between DNP3 master and DNP3 slave. They use the iptables open source firewall facility. The experimental results show that the proposed approach succeeded in blocking most of the DNP3 attack traffic.

Jin Bai, Salim Hariri et.al [7] find out the fact that security was not the goal while designing DNP3 protocol so attacker can easily target the device which is part of critical infrastructure. They have proposed the automatic network protection framework to detect the attacks on DNP3 over TCP/IP. They have focused on ruled based anomaly intrusion detection. The testing result shows that the system has high positive rates and very low false positive rates. As well as for testing they have used both offline and online testing.

Y. Xu et.al [11] studied and analyzed various communication protocols such as DNP3, Modbus, IEC 60870-5-104, IEC 61850, IEC 61400-25 as well as IEEE C37.118. They have also given attacks possible on these protocols and its mitigation techniques. Most of these protocols lack any of the authentication, authorization, encryption, availability, integrity, confidentiality. Due to lack of network security features man-in-the-middle, Denial of service, replay, injection, spoofing, eavesdropping and modification all these attacks are possible on the protocol. They have provided the solutions such as risk assessment, encryption, authentication and intrusion detection techniques.

H. Li et.al [12] analyzes the DNP3 protocol and snort rules are used to detect the abnormal behavior in the system. Due to lack of authentication and authorization features in DNP3 protocol attacker can easily manipulate the data specifically function codes. The paper specifies that abuse of function code in DNP3 is the main reason of attacks. They have provided snort rules for identifying the anomalous behavior of the system.

R. Amoah et.al [13] used Colored Petri Nets (CPN) model to check the correctness of DNP3 protocol. This model specifically focused on non-aggressive challenge response feature of DNP3 protocol. The model analyzes the protocol which ensures that protocol will behave as expected. It also validates the behavior of the protocol using state space tool to check whether there are any insecure states in it. This approach is used to identify Denial of Service attack.

A. Carcano et.al [14] proposed work considered the set of different states which when consider in isolation might not be considered as anomalous behavior. The have designed the IDS system which will focused on two protocols for communication mainly DNP3 and Modbus. They have presented how the general behavior of such protocols can lead to vulnerabilities and causes various malicious attack scenarios. They have provided the firewall implementation for identifying those attacks by using various rules.

5. ATTACKS ON DNP3 AND MITIGATION TECHNIQUES:

DNP3 faces various threats which includes eavesdropping(secretly listens the message), man-in-the-middle attack (attacker not only listens to the messages between two unsuspecting parties but can also modify, delete, and replay the messages), spoof (attacker pretends to be authorized user)and replay (an attack that attempts to trick the system by retransmitting a legitimate message)[10].

DNP3 SAV2 of the mechanism addresses four threats: spoofing, modification, replay and eavesdropping. However, some minor flaws still exists in this version of secure authentication. The full method needs Update Key that must be pre-shared by each device. In version 2, update key should not be transmitted via the protocol. This was the weakness if large no of remote devices are being used. By adding remote update key exchange mechanism version 5 of secure authentication addresses this issue.

Following are the list of attacks and mitigation techniques to overcome those:

1. **Man-in-the-middle Attack:** This attack Sniff or capture the traffic passing between the master and slave device. The attacker can also modify the packet and transmit to the respective devices. DNP3 without secure authentication will not be able to overcome this attack. But DNP3-SA has provided mitigation technique by providing challenge and response mechanism. Because of this mechanism the authenticity that message is coming from intended sender will be preserved.

2. Packet Modification and Injection Attack: The attacker can capture the packet passing between master and slave device and can modify its contents. This attack is possible in DNP3 without secure authentication. The mitigation technique is provided in DNP3-SA as the message is being hashed by the session key and hashing algorithm such as SHA-256.This hash value will change with even small change in the message.

3. Denial of Service Attack: The attacker attempts to make a service or a network resource unavailable to its intended users or it can temporarily interrupt or suspend services of a host connected to the network by randomly sending the unexpected messages. This attack is possible on DNP3-SA (SAV2) as well. DNP3 SAV5 has mitigation techniques for following scenarios:

a. When the attacker intentionally sends the unexpected message to the device the device is forced to change the session key. The key is being reset every time attacker sends unexpected message which causes normal communication to halt. SAV5 provides the threshold on no of reset session key request permitted between two devices.

b. The device waits for the reply message, but attacker intentionally delays the replay so that the device will not be able to take the further requests.SAV5 discard the request after certain timeout period.

4. Replay Attack: In this form of network attacker can maliciously repeat or delay the valid message. This attack is possible on DNP3 without secure authentication. DNP3 SAV2 has mitigated it using challenge response mechanism as the receiver can any time check the authenticity of the attacker.

5. Spoofing: In this attack to gain an illegitimate advantage the attacker can falsify the data. This attack is possible on DNP3 without secure authentication. DNP3 SAV5 mitigates it using challenge and response mechanism as only authenticated users can communicate with each other.

6. Eavesdropping: In this attack the attacker steal information that computers send and receive without incurring any harm to the system. This attack is possible on all versions as secure authentication as it can only mitigate it for securing the session keys. The original message can be read by the attacker but will not be able to modify it as hashing prevents modification of data.

Following are the list of attacks which are possible on DNP3 layers in DNP3 without secure authentication:

A. Length Overflow Attack: The length field in the DNP3 data link header can be modified by incorrect value which causes data corruption, unexpected actions or device crash.

B. DFC Flag Attack: DFC flag bit is set in response message which indicates outstation buffer is full and will not be able to process the request therefore request should be sent later. This attack causes an outstation device to appear busy to the master.

C. Reset Function Attack: Attacker sends request message to the outstation device with function code 1 (reset user process). This leads outstation device to restore it to the inconsistent state or make it unavailable for certain period of time.

D. Unavailable Function Attack: Attacker sends response message to the master with function code 14 or 15 which indicates either service is not functioning or does not available in the outstation device. This attack causes the master not to send requests to the outstation as it assumes that service is not available in the device.

E. Destination Address Alteration: The attacker can reroute the message by changing the destination address field in DNP3 header. The attacker can also send erroneous request in the broadcast message which causes all the outstation devices to execute the erroneous broadcast request as it is very difficult to detect such attacks.

F. Fragmented Message Interruption: The FIR flag indicates the first and FIN flag indicates the last frame of the fragmented message. The attacker can maliciously insert the packet with FIR flag set which disrupt the reassembly of valid message frames. Malicious insertion of

FIN flag leads to error while processing the partially completed message.

G. Transport Sequence Modification: The sequence field is used to reassemble the message in correct sequence. The sequence numbers are increments for each fragment so that predicting the next sequence no is easier. Attacker can insert any malicious fragment which causes the processing error.

H. Outstation Write Attack: The attacker sends the message with function code 2 (write request) which writes data to the outstation. This attack causes error or overflow condition due to corrupt values stored in the device.

I. Clear Objects Attack: The attacker sends a function code 9 or 10 in the DNP3 request message to freeze or clear the data objects. This attack can cause the outstation device to malfunction or crash by clearing critical data in the outstation device.

J. Outstation Data Reset: The attacker sends a DNP3 message with Function Code 15. The attack causes an outstation device to reinitialize data objects to values inconsistent with the state of the system.

K. Outstation Application Termination: The attacker sends a DNP3 message with Function Code 18 (terminate applications running on outstations). A message with this function code causes a device to become unresponsive to normal requests from the master.

L. Configuration Capture Attack: In the response message from the outstation fifth bit in the second byte of IIN is set to 1 maliciously which indicates that the configuration file is corrupted. This causes the master to transmit a new configuration file again which is intercepted by the attacker.

All the above attacks which are possible in DNP3 without secure authentication on different layer and can be overcome in DNP-SA as payload is being encrypted by session keys and session keys are being encrypted by pre-shared update key. Hashing algorithms applied on payload generates the HMAC (message authentication code) and it is impossible to identify the key from the given HMAC.

Table 3: Comparison table of DNP3 protocol with and without secure authentication

Sr. No	Protocol Features	DNP3 without secure authent-ication	DNP 3 SAV2	DNP3 SAV5
1.	Man-in-the middle attack protection	No	Yes	Yes
2.	Eavesdropping	No	No	No(yes for key updates only)
3.	Symmetric key support	No	Yes	Yes
4.	Asymmetric key support	No	No	Yes
5.	Message replay protection	No	Yes	Yes
6.	Denial of service attack protection	No	No	Yes

6. CONCLUSION

From the above survey we conclude that DNP3-SA has provided various security solutions and many of the attacks are overcome due to the challenge-response and HMAC technique. The secure authentication technique still has one drawback that is they have provided confidentiality for key exchanges only. All operations which are carried out are transferred clearly. This choice was made by DNP3 working groups developing the standard. They stated that extra overhead of confidentiality is not required if authentication is provided. But by just looking at the data which is being transmitted attacker can gain lot of information. This issue needs to be considered.

7. REFERENCES

[1] Rosborough, C., Gordon, C., Waldron, B. (2019). All About Eve: Comparing DNP3 Secure Authentication With Standard Security Technologies for SCADA Communications. Power and Energy Automation Conference. W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[2] Darwish, I., Igbe, O., Celebi, T. (2005). Smart Grid DNP3 Vulnerability Analysis and Experimentation. IEEE 2nd International Conference on

[3] Cyber Security and Cloud Computing

[4] Darwish, I., Saadawi, T. (2018). Attack Detection and Mitigation Techniques in Industrial Control System - Smart Grid DNP3. International Conference on Data Intelligence and Security.

[5] Amoah, R., Camtepe, S., Foo, E. (2016). Securing DNP3 Broadcast Communications in SCADA Systems. IEEE Transactions On Industrial Informatics. Vol. 12, No. 4

[6] Darwish, I., Igbe, O., Saadawi, T. (2015). Experimental and Theoretical Modeling of DNP3 Attacks in Smart Grids. IEEE sarnoff symposium.

[7] Nivethan, J., Papa, M. (2016. A Linux-based firewall for the DNP3 protocol. IEEE Symposium on Technologies for Homeland Security.

[8] Bai, J., Hariri, S., Al-Nashif Y. (2014). A Network Protection Framework for DNP3 Over TCP/IP Protocol. IEEE/ACS 11th International Conference on Computer Systems and Applications.

[9] Thibodeau, E., Gilchrist, G. (2012). Introducing Secure Authentication Version 5 for DNP3. 2012 CIGR´E Canada Conference Hilton Montr´eal Bonaventure, September 24-26, 2012.

[10] DNP Users Group. “Distributed Network Protocol (DNP3)” (DNP3-2012, 2012, 839 pages).

[11] 10. IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol(DNP3).2012.doi:10.1109/IEEESTD.2012.6327578 ISBN 978-0-7381-7292-7.

[12] 11. Xu ,Y., Yang ,Y., Li ,T., Ju ,J. (2017). Review on cyber vulnerabilities of communication protocols in industrial control systems . 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2).

[13] 12. Li , H., Liu ,G., Jiang , W., Dai, Y. (2015). Designing Snort Rules to Detect Abnormal DNP3 Network Data. 2015 International Conference on Control, Automation and Information Sciences (ICCAIS).

[14] 13.Amoah , R., Suriadi , S., Camtepe ,S., Foo, E. (2014). Security analysis of the non-aggressive challenge response of the DNP3 protocol using a CPN model. 2014 IEEE International Conference on Communications (ICC).

[15] 14.Carcano , A., Fovino , I., Masera, M. (2010). Modbus/DNP3 State-based Filtering System. 2010 IEEE International Symposium on Industrial Electronics.