Exploitation of The Distributed Network Protocol in ICS with Improved D-Y Model Based on Petri Net

Ye Lu[1] and Wei-Bin Ou[2]

(Corresponding author: Wei-Bin Ou)

School of computer Science, Baoji University of Arts and Sciences[1]
Baoji Shaanxi 721000, China
College of Electronic and Electrical engineering, Baoji University of Arts and Sciences[2]
Email: luye528@126.com

(Received June 14, 2020; Revised and Accepted Feb. 11, 2021; First Online Aug. 8, 2021)

Abstract

Whether the communication protocol is safe or not is related to the stable and reliable operation of the industrial system. As a typical application layer protocol in the industrial field, Distributed Network Protocol has attracted much attention. We use CPN-Tool to present a formal study of DNP3 security, integrity, and authentication in this work. We introduce an improved Delov-Yao attacker model to reduce the size of the state space. Furthermore, we carry out the security evaluation of the protocol in the full attack state and give the vulnerability exploitation path according to the evaluation results. The exploited vulnerabilities reflect that the DNP3 protocol cannot resist three attacks listed in IEEE standards: replay, tampering, and spoofing. The CPN model developed provides a security assessment method for DNP3 that can clarify the methodology for achieving secrecy, integrity, and authentication for designers and developers interested in other protocols.

Keywords: Distributed Network Protocol; Exploitation; Delov-Yao; Petri-Net

1 Introduction

With the rapid development of intelligent manufacturing, big data of industry and the Internet of things, the communication protocols of industrial control systems tend to be open and standardized, especially the introduction of industrial Ethernet, TCP/IP and other open communication protocol standards, which greatly increase the risk of network attacks on industrial control systems. According to ICS-CERT Advisories, there had been 1350 cyber attacks on industrial control systems by May 2020, including critical infrastructure such as power grids, water conservancy facilities and transportation systems. According to the ICS-CNVD of CNCERT in China, a total of 1120 vulnerabilities were reported from 2018 to May 2020, accounting for 44 percent of the total number of vulnerabilities in the past.

In order to deal with more and more network security threats, researchers have proposed a series of security regulations and communication standards for industrial control system network protocols [13], such as CIP-Safety, OPC-UA, DNP3-Sec, DNP3-SA and so on. DNP3-SA protocol is the first industrial Ethernet security protocol with authentication attribute in industrial networked control systems, and it is widely used in DCS systems, although its security loopholes have been found. It is mainly used in industrial infrastructure fields such as electric power automation system, oil and gas system and so on. The protocol ensures the secure transmission of data by generating message authentication code (MAC).

The security of DNP3-SA protocol is described informally in IEEE Electrical Standard [10]. Although the informal description method can guide the design of DNP3-SA protocol, it has the following defects:

1) It is easy to cause ambiguity in the purpose of the agreement, difficult to understand and inaccurate description [12].

2) Security protocols run in an open environment, and attackers can attack protocol entities through replay, spoofing, denial of service and other methods, but manual identification of their threats has a large workload and low accuracy.

3) Due to the lack of formal verification methods, the accuracy of protocol security analysis is low.

Formal description and analysis methods can give the detailed model of the protocol, with the help of formal methods and tools to evaluate the security of the protocol and can ensure that the embedded security mechanism does not affect the functionality of the protocol itself, and can will not attract new errors. The formal method uses strict mathematical semantics to describe the protocol, and computer-aided verification tools are used to verify the availability and security of the protocol. For example, the typical Delov-Yao attack model [8] is a typical formal attack model. This model can help protocol designers to reduce the difficulty of manually finding protocol vulnerabilities. At present, a lot of research work [19, 24, 26] shows that formal methods can make protocol security improvement more effective.

At present, the main methods for security assessment of protocol state are functional verification based on protocol finite state machine model and security evaluation based on stochastic process model. However, in terms of protocol engineering modeling, protocol performance analysis based on two different models has the following shortcomings: First, the protocol model based on performance analysis is generally unable to accurately simulate the protocol behavior. Second, the use of two types of protocol formal models for protocol design and analysis will lead to too large state space of the model, and even lead to state space explosion. Colored Petri net [16] is a formal analysis theory that integrates protocol behavior verification and performance analysis. Based on this theory, the CPN behavior model of the protocol can be constructed to verify the functional consistency of the protocol, and the attacker model is added to analyze and evaluate the security, so as to overcome the above two kinds of defects and ensure that the state transition in the behavior CPN model can be associated with man-in-the-middle attacks.

Vulnerability disclosure is the basis for the formulation of defense strategy in Industrial Networked Control System, and its accuracy ultimately determines the stable operation of the system. Based on the research of literature [1], this paper further uses CPN modeling tools and state space analysis tools to formally describe the behavior process and security attributes of DNP3-SA protocol, and establish a security evaluation model of the protocol. The main improvements are about the Delov-Yao attacker model, which further reduces the state space, and three improved attacker models of replay, deception and tampering are introduced, and final vulnerability exploitation path of attack. This, in turn, can clarify the methodology for achieving secrecy, integrity, and authentication for designers and developers interested in these Distributed Network Protocols. We believe that our model and discussion of the protocol security properties are beneficial for both researchers and practitioners. To the best of our knowledge, this is the first work that presents vulnerability exploitation path of DNP3-SAv5.

The remainder of this paper is organized follows. section 2 reviews the research progress of DNP3 protocol security. Section 3 gives the adversary model and security attributes of the protocol according to the IEEE specifications. Section 4 reviews the improvement scheme of D-Y attacker model made by Bai, and further proposes an improved parameterized attack model based on CPN. Section 5 uses cpn tools to establish the attacker model of DNP3-SA protocol and verifies the consistency of the model behavior. Section 6 analyzes the attack behavior and excavates the vulnerability based on the state space tool, and gives the attack path. Finally, conclusions and future work are presented in Section 7.

2 Review the Security of DNP3 Protocol

DNP3 protocol has been running in industrial networked control systems (ICS) for decades, such as Supervisory Control And Data Acquisition systems (SCADA), Distributed Control Systems (DCS), and Process Control Systems (PCS). However, as revealed by a number of attacks on critical infrastructure in recent years, there are many security vulnerabilities in the protocols in these systems. A large number of protocols are transmitted in clear text without authentication and integrity checks, such as the shocking Stuxnet worm and Black-Energy. Therefore, for a long time, a large number of researchers have devoted themselves to propose secure TCP/IP-based transport protocols, which have certain authenticity, integrity, confidentiality and non-repudiation by using symmetric or asymmetric cryptography technology. Such as improved DNP3 protocol, DNP3-SA protocol, DNP3-SEC protocol, ICCP-SEC protocol and so on. However, these schemes have some limitations, which only focus on the implementation of the security function of the protocol, but lack of formal methods for the analysis and verification of protocol security. The formal method can study the security of the protocol based on the security strength of the encryption algorithm itself.

At present, there are two secure versions of DNP3 protocol, DNP3-Sec and DNP3-SAv5. The former focuses on link layer security, while the latter focuses on application layer security. Although authentication, encryption, authorization, integrity check and other security mechanisms are used in the two types of security protocols, they still face some security threats. Literature [6] uses a variety of attack scenarios for penetration testing in a simulated environment including DNP3 protocol. Vulnerability analysis and penetration testing show that there is a man-in-the-middle (MITM) attack. Literature [20] uses SCAPY to send a large number of forged data to DNP3 communication links, verifying that DNP3 protocol has security vulnerabilities such as data tampering, replay and spoofing. In the literature [18], the response behavior of DNP3 protocol under replay attack, rogue intrusion attack and flooding attack is studied, and its vulnerability is verified.

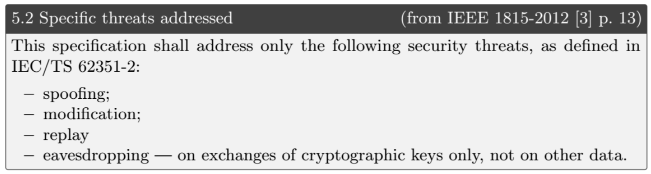
Literature [15] validates a series of attacks on a small test bed and proposes DNP3 improvement measures based on encryption and authentication. The literature [22] reviews some vulnerabilities that have been found in DNP3 and makes security improvements to the protocol in the application layer. Literature [23] analyzes a large number of industrial Ethernet protocols from the aspects of consistency, integrity and availability, and gives examples of the related studies of DNP3, DNP3SEC and dnp3sa, and gives some suggestions for security improvement. Literature [25] proposes an intrusion detection algorithm based on machine learning algorithm for smart grid to help dnp3 protocol detect attacks in time.

The literature [17] reviews the attacks in the smart grid, analyzes the protocols involved according to the types of attacks, and gives examples of possible improvements. Based on four supervised learning algorithms, Literature [9] has found a Peekaboo attack in a large number of substations running DNP3 protocol. Literature [14] analyzes the fragility of the transport layer of DNP3 protocol, proposes an intrusion detection technology of RNN, and describes the verification process of the proposed model through a DNP3 message of an actual substation. Literature [7] uses Bayesian analysis to model the likelihood distribution of Rttd of legitimate information and information attacked by hackers, and then proposes an intrusion detection model for DNP3 protocol. Based on the colored Petri net, literatures [1, 2] analyzes the security of the protocol, finds that replaying the previously authenticated commands can remotely control the slave station, and puts forward an improved scheme of the protocol. But literature [5] makes a complete analysis of the DNP3-SA protocol, and makes a complete state machine model for the complex behavior of the protocol.

Based on TAMARIN, it is proved that the security of the protocol is almost consistent with that declared by the standard. Literature [21] comprehensively analyzes the advantages and disadvantages and encryption structure of DNP3-SA protocol, and discusses the impact of encryption operation on the performance of the protocol. Literature [11] discusses all kinds of attacks in the application layer of DNP3 protocol. By extracting the traffic characteristics of four substations, a set of lightweight security improvement scheme is proposed. Literature [4] points out that the implementation complexity and analytical fuzziness of the protocol are related to the coupling state, and proposes a security enhancement scheme to avoid similar attacks. From the above literature, it can be concluded that DNP3 protocol and other variants mainly exist the following attack vectors: man-in-the-middle, replay, eavesdropping, data tampering, denial of service, buffer overflow and so on.

3 Adversary Model and Security Attributes

By checking whether unauthorized commands are executed by the slave station, we can verify whether the authentication mechanism of the DNP3-SA protocol achieves the security claimed in the standard. The DNP3-SA protocol complies with the requirements of the IEC62351 specification, which can ensure that the protocol is not affected by attacks such as spoofing, modification, replay and eavesdropping. For related descriptions, see the IEEE-1815-2012 and IEC62351 standards (Figures 1, 2, 3, and4).

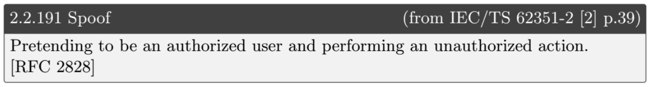

5.2 Specific threats addressed (from IEEE 1815-2012 [3] p. 13)

This specification shall address only the following security threats, as defined in IEC/TS 62351-2:

- spoofing;
- modification;
- replay
- eavesdropping — on exchanges of cryptographic keys only, not on other data.

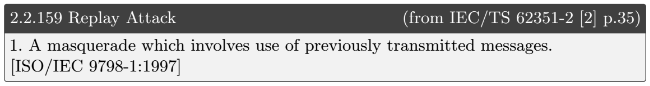
Figure 1: Types of attacks in the IEEE1815-2012 standard

The attack behaviors illustrated in Figures 1 are all described informally in the standard IEC62351. At the same time, the attack types such as masquerade and Perfect forward secrecy are further listed in the reference [5].


2.2.191 Spoof (from IEC/TS 62351-2 [2] p.39)

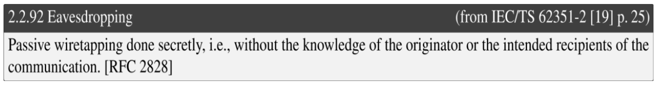
Pretending to be an authorized user and performing an unauthorized action. [RFC 2828]

Figure 2: Spoofing attack in the IEC62351 standard


2.2.159 Replay Attack (from IEC/TS 62351-2 [2] p.35)

1. A masquerade which involves use of previously transmitted messages. [ISO/IEC 9798-1:1997]

Figure 3: Replay attack in the IEC62351 standard


2.2.92 Eavesdropping (from IEC/TS 62351-2 [19] p. 25)

Passive wiretapping done secretly, i.e., without the knowledge of the originator or the intended recipients of the communication. [RFC 2828]

Figure 4: Eavesdropping attacks in the IEC62351 standard

However, for modification, the IEC62351 standard is not clearly stated. For the sake of integrity and with reference to other security standards, this paper defines tampering attacks that specifically refer to the ability of attackers to modify messages in transmission arbitrarily. The attacker models and capability assumptions of the above three man-in-the-middle attacks in our protocol attack-model are given below:

MD_ATK: Modify attack, the attacker has the ability to modify the messages in the NET subpages, including request messages and challenge messages.

RP_ATK: Replay attack, the attacker has the ability to intercept the message sent by the master station M and resend it to the slave station O.

SP_ATK: Spoofing attack, the attacker has the ability to impersonate the master station M to send messages to the slave station O.

MRS_ARK: Attackers launch Modify, Replay and Spoofing attacks at the same time.

0_ATK: An attacker cannot launch an attack without enabling any attack parameters.

4 Improved Attacker Model of Delov-Yao

Delov and Yao published an important paper [16] which has a profound impact on the research of protocol security. There are two main contributions: the first contribution is to discuss the security properties of the protocol itself on the assumption that the cryptosystem is "perfect", which can help researchers to concentrate on the inherent security properties of the protocol without discussing the security of cryptographic algorithms. The second contribution is that Delov and Yao proposed the attacker model and proposed that the attacker has stronger computing power than the real participants of the protocol. The attacker can eavesdrop, intercept, tamper, replay the information exchanged between real entities during the operation of the protocol, encrypt, decrypt, split and combine the original message, and forge the message content. However, the attacker model can combine "arbitrary" messages, which will cause a large increase of invalid messages, make the messages form an infinite loop, cause the model cannot be terminated normally, and finally cause the system state space to explode.

This section improves the Delov-Yao attacker model, on the one hand, applies the attack in the form of parameterization to the arc expression to reduce the state space; on the other hand, it effectively limits the messages that the attacker splits and combines, and only splits the key messages that are valid to prevent the attack from entering a disordered state and preventing the state space from exploding.

4.1 Review Bai's Study

In reference [3], Bai divides the Delov-Yao attacker model into message splitting stage and message combination stage. In the message splitting stage, the attacker splits all intercepted messages atomically, and stores the messages that need to be split and the split atoms in the element set DB. In the message composition phase, attackers extract the atomic information from DB and reassemble them into valid messages according to the protocol specification and store them in the set CB, which reduces the state space while maintaining the attack capability.

The buffer unit AB set of the basic elements is used as the pre-set of the composite element set CB, which is used to store the atomic information of all kinds of split. In order to avoid the cycle caused by split and combination operations, it is necessary to split the intercepted messages first, and then reassemble the messages according to the required capabilities of the attackers, and finally generate a set of combination elements CB, and send the generated elements to the communication link.

Compared with the original model, the biggest advantage of Bai's model is following two aspects. First, serialization defines the logical relationship between split and combination operations, while in the original model, split and combination operations occur randomly, which may lead to infinite loops and state explosions. Secondly, by limiting the data type and key fields, the generated message can not only be effectively received by the receiver, but also closely related to the security attributes, which effectively reduces the state space of the model.

Specifically, it is assumed that entity A and entity B are entity objects participating in the protocol interaction, and the original message transmitted by A and B is m. The encryption key used by both sides of the communication is k, the decryption key is k', and the communication link between the two parties is Channel. If "a" represents the basic elements obtained from the split of all the original messages, the formal description of the transformation rules for message splitting and message combination in the Delov-Yao attacker model in Bai's scheme is shown in Figure 5.

Split rule	
$\mathrm{channel}(A,m,B) \xrightarrow{resolve(A,m,B)} DB(m), DB(A), DB(B)$	(1)
$DB(m1 \bullet m2) \xrightarrow{resolve(m1,m2)} DB(m1), DB(m2)$	(2)
$DB(\{m\}k), AB(k') \xrightarrow{resolve(\{m1\}k,k')} DB(m), AB(k')$	(3)
Combination rule:	
$CB(m), AB(A), AB(B) \xrightarrow{\mathrm{assemble}(m,A,B)} channel(m, A, B)$	(4)
$CB(m), AB(A) \xrightarrow{\mathrm{assemble}(m,A)} channel(m, A)$	(5)
$CB(m1), CB(m2) \xrightarrow{\mathrm{assemble}(m1,m2)} CB(m1, m2)$	(6)
$CB(m), AB(k) \xrightarrow{\mathrm{assemble}(m,k)} CB(\{m\}k), AB(k)$	(7)
Transformation rule	
$DB(a) \xrightarrow{\mathrm{change}(a)} AB(a)$	(8)
$AB(a) \xrightarrow{\mathrm{change}(a)} CB(a)$	(9)
$DB(\{m\}k), \neg AB(k') \xrightarrow{\mathrm{change}(\{m\}k)} CB(\{m\}k)$	(10)

Figure 5: Formal description of message split and combination rules

Different from the random split or combination operation of the original model, the improved attacker model will be executed in three phases according to the above rules. Step 1, The split operation is performed in the order of Rules 1 to 3. Step 2, uses the combination operation in the order of Rules 4 to 7 to generate only the messages that can be effectively received by the recipient and with critical value to the security assessment. Step 3, converts according to Rules 8 to10. The improved attacker model can still generate messages output from the original attacker model, which can effectively reduce the state space without weakening the ability of the original Delov-Yao attacker.

4.2 An Extension of the Bai's Scheme

The CPN model checking tool has a parameterized method, through which researchers can build the response behavior of the protocol under different parameters according to their interests, which helps us to dynamically analyze the established model, and is especially suitable for studying the response behavior of the protocol under different attack parameters. Parameterization methods are usually implemented by arc expressions, transition guards and functions.

Enable or disable attack behavior by setting the true and false values of the above Boolean expression. Figure 6 shows an example of the parameterized attack model used later. When the arc expression is false, the attack function Mattack1 can tamper with the function code. In this paper, a variety of attack functions are defined to simulate tampering, spoofing and replay attacks on the protocol.

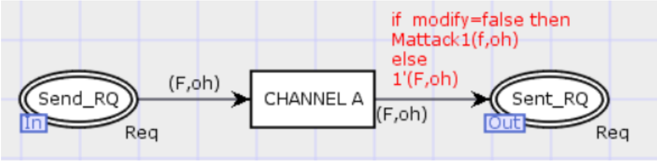


Figure 6: Example of parameterized attack model

4.3 Efficiency Analysis of Improved Attacker Model

This section takes Needham-Schroeder (NS) protocol as an example to verify the improved attacker model and analyze the actual effect of the scheme. As the first real authentication protocol, NS protocol is composed of initiator and responder and the network between them. Its security goal is to ensure that both sides of the communication can confirm each other's true identity and that the protocol entity will not be impersonated.

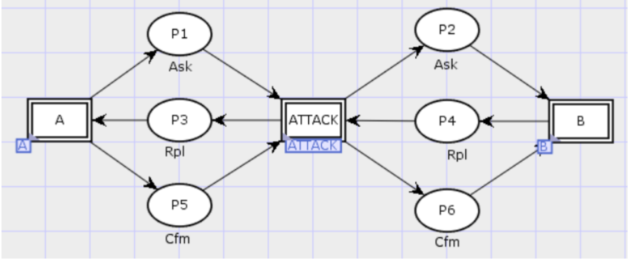


Figure 7: Top-level CPN model of the NS protocol

Figure 7 shows the top-level CPN model of the NS protocol. The layer model consists of entities A and B involved in communication and the attacker "ATTACK". The hierarchical method of the HCPN model uses alternative transitions to simulate each participating entity of the protocol, and the internal model of the transition simulates the detailed behavior of each function in the entity layer. Other message repositories in the top-level model simulate the communication channel of the network. The attacker in the communication channel can intercept all the data packets in the communication network and attack according to the improved attacker model.

Figure 8 shows the entity layer model of NS protocol replacing transition "ATTACK" without attack. In this model, according to the requirements of the implementation specification of NS protocol, the attack behavior of each stage of the protocol is simulated by alternative transition Int_Ask, Int_Rpl and Int_Cfm, respectively. The subscript of the place is used to assign the type of port place, In is the input port place and OUT is the output port place. Taking the Int_ ask subpage as an example, the original Delov-Yao attacker model and the improved Delov-Yao attacker model are analyzed. Considering that the introduction of the attacker model will lead to a large state space of the protocol model, the attacker is limited to attack the protocol only as a middleman, and the replay attack is taken as an example to simulate the execution of a single session of the protocol.

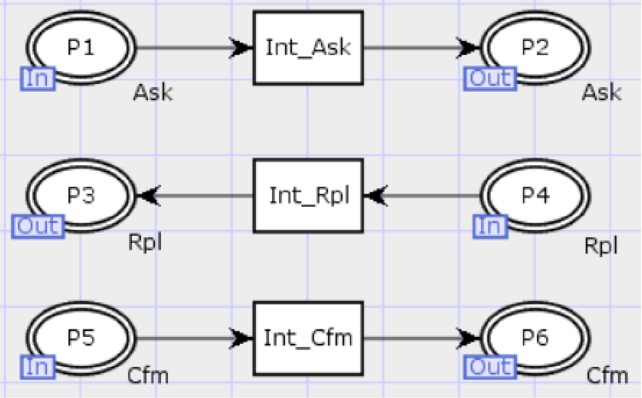


Figure 8: The CPN Model of substituting transition "ATTACK"

Figure 9 shows the subpage model corresponding to the transition Int_Ask under the original Delov-Yao attack model. The knowledge possessed by the attacker is stored in repository P3'. The transition T1 is used to simulate the decryption of the intercepted cipher text by the attacker attack. Transition T2 simulates the process that the message sequence msg obtained after decryption in the previous step is divided into random number n and identity element id. The library P3' is used to store the split and reassembled message sequence; the message sequence is finally replayed to the library P2 through transition T1.

Figure 10 depicts the attacker subpage "Int_Ask" based on the improved attacker model. The red part of the graph is the transition guard and arc expression, which constitutes the parameterized attack model. The request message sent by the protocol entity is intercepted by tran-

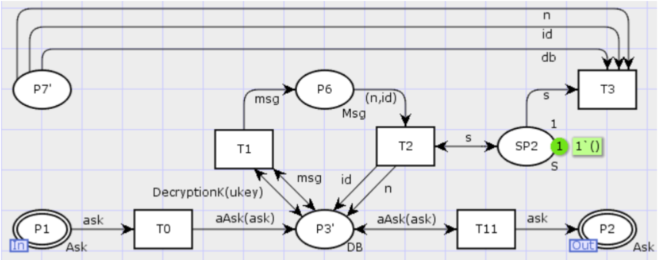


Figure 9: CPN model of the original Int_Ask

sition T0, and the intercepted message is split and stored in the repository "resolve". Transition T11 applies the transition rules defined in Figure 5 to store undecrypted, to be combined and combined messages in the repository P5'. Transition T2 decomposes the message based on the splitting rules listed in Figure 5 and obtains the key message elements and stores them in the repository "element". Transition T3 simulates the combined operation and generates valid data messages that can be identified by the receiver, then stores them in the message repository P5'. The function of SP is to restrict the combination function of transition T3 and prevent multiple messages from concurrency. Transition T4 finally sends the generated attack message to the port library P2 connected to the network channel.

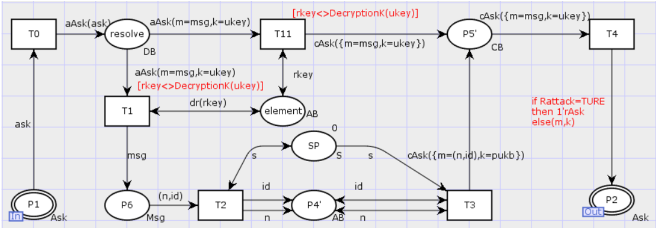


Figure 10: Int_Ask attackers model based on improved Delov-Yao model

Table 1 makes statistics on the state space according to the state space analysis report of the above two models. Within 50 seconds of computing time, the number of state space nodes and directed arcs of NS protocol under the original attacker model far exceeds the state space formed by the improved attacker model under the same assumption. In addition, the original attacker model does not have dead nodes and dead transitions in the simulation time, which violates common sense and may lead to an infinite cycle of protocol behavior. The above comparison results show that the improved attacker model can avoid generating a large number of message data that are not recognized by the receiver. On the premise of ensuring the attack ability, it can significantly improve the efficiency of the attack model and reduce the size of state space nodes.

Table 1: State space comparison of two attacker models

Attack Model	Node	Arc	Dead Node	Dead Transition	Live Transition
Bai's	337	482	0	0	0
Ours	108	170	1	T4	0

5 Attacker Model

5.1 The Establishment of Attacker Model

The CPN model of the protocol is a concrete simulation of the whole communication protocol, including the communication sides of the protocol, the communication network and the messages transmitted. As shown in Figures 11, the double-line rectangle in the diagram is the alternative transition and the ellipse is the message repository. The left alternative transition M represents the communication master station Master Station, while the middle alternative transition NET subpage represents the communication network, and the rightmost alternative transition O represents the communication slave OutStation. The top-level model completely simulates the session process of the protocol, including request-reply mode (NACR) and active mode (AGM), and the process of dealing with key information.

Figure 12 shows the NET subpage attacker model based on the top-level model of the protocol, where all simulated attacks will be carried out. The NET subpage simulates the network channel. According to the assumption of the Delov-Yao attack, the attacker has the powerful ability to eavesdrop, replay and tamper with the messages in the network channel, and then launch all kinds of man-in-the-middle attacksAs shown in Figures 12, the red part of the transition and place simulates RP_ATK attacks, including transition REPLAY, port place send_AGRQ and related transformation rules. The arc expression marked in blue simulates the MD_ATK attack, including the functions: mattack (), attackseq1 () and attackseq2 () in the arc expression on transition CHANNEL A, CHANNEL C and CHANNEL C'. The transition guard of purple part tags simulates SP_ATK attacks, including transition CHANNEL A, CHANNEL B, CHANNEL C, CHANNEL C', CHANNEL D, CHANNEL AGM.

5.2 State Space Analysis of Attacker Model

The running environment of the attacker model: CPU is i5-6200u, main frequency is 2.3GHz, memory is 8GB. By the environment,the state space report (Figures 13) of three full attack modes of man-in-the-middle attack at the same time shows that the number of nodes in the state space is 63344, the number of connecting arcs is 911557, and the time to construct the state space is 3194 seconds.

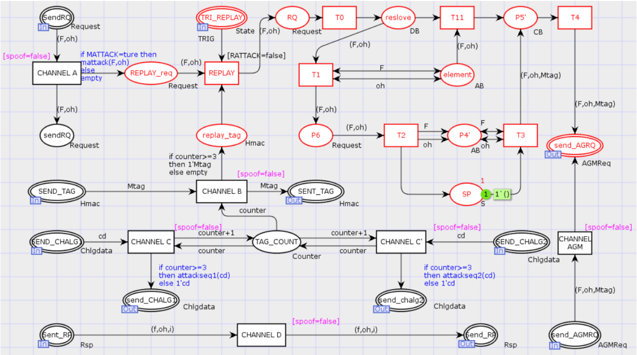


Figure 11: Top-level CPN model of the protocol

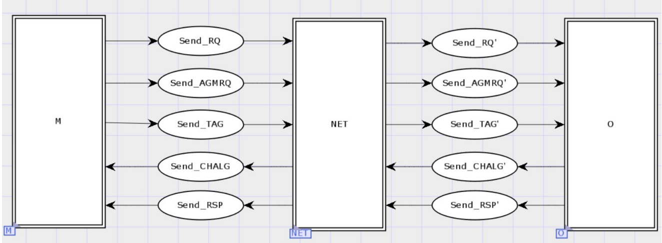
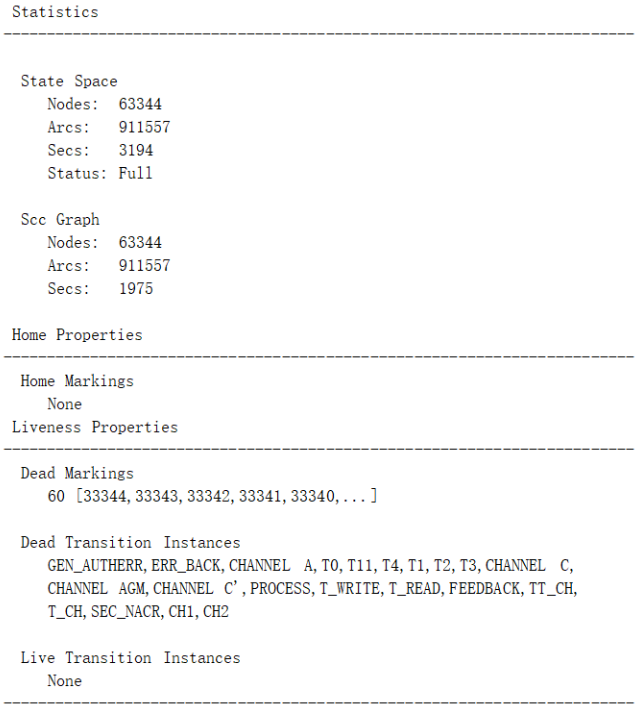


Figure 12: Attacker model in NET subpage


```
Statistics
------------------------------------------------------------------------

 State Space
    Nodes:  63344
    Arcs:   911557
    Secs:   3194
    Status: Full

 Scc Graph
    Nodes:  63344
    Arcs:   911557
    Secs:   1975

Home Properties
------------------------------------------------------------------------

 Home Markings
    None
Liveness Properties
------------------------------------------------------------------------

 Dead Markings
    60 [33344,33343,33342,33341,33340,...]

 Dead Transition Instances
    GEN_AUTHERR,ERR_BACK,CHANNEL  A,T0,T11,T4,T1,T2,T3,CHANNEL  C,
    CHANNEL  AGM,CHANNEL  C',PROCESS,T_WRITE,T_READ,FEEDBACK,TT_CH,
    T_CH,SEC_NACR,CH1,CH2

 Live Transition Instances
    None
------------------------------------------------------------------------
```

Figure 13: State space report of protocols in full attack mode

The number of nodes and directed arcs obtained by the strongly connected graph is consistent with the results given by the state space, which shows that all state nodes of the protocol model are reachable and will not lead to infinite state occurrence and behavior iteration. There are 60 dead mark states in the model. There are 21 dead transitions in the model, and dead transitions refer to the transitions that can not be triggered in the model. Usually due to the defects in the design of the model, there are many dead transitions. However, due to the introduction of the attacker model, the 21 dead transitions in this model have a special meaning. The living transition in the model refers to the transition that can be triggered during the operation of the model. Because there is a dead mark state in the model established in this paper, that is, all the changes can not be triggered under the dead mark state, that is to say, the dead mark indicates the termination state of the completion of data transmission. therefore, the report shows that there is no living transition in the model established in this paper. This paper will conduct an in-depth analysis of the state space report to verify whether the protocol function is completed and whether the security is satisfied.

5.3 Behavior Consistency Analysis

This section verifies whether the behavior of the attacker model is consistent with that of the original protocol model when the attack is not enabled, The statistics of the state space reports of the protocol model in various modes are shown in Table 2.

The 0_ATK column only introduces the attacker model, but does not enable any attacks. RP_ATK is listed as the status space report obtained after the enable replay attack. MD_ATK is listed as a status space report obtained after enabling tampering attacks. SP_ATK is listed as a status space report obtained after enabling spoofing attacks. MRS_ATK is listed as the status space report obtained after enabling the above three attacks. In the attacker model, due to the introduction of the improved Delov-Yao attacker model, the number of state space nodes and arcs increases significantly compared with the original model, which is in line with expectations. And the number of arcs and nodes in state space is the same as that of strongly connected arcs and nodes, which shows that all state nodes in the attacker model are reachable, and there is no loop and iterative behavior that leads to the infinite occurrence of states, which further shows that the improved Delov-Yao attacker model is effective.

In 0_ATK mode, the number of dead nodes in the attacker model is the same as that in the original model, which indicates that all requests are successfully authenticated and executed by slave O, which is consistent with the expected behavior of the protocol without enabling any attack parameters. However, the number of dead transitions increases to 14, which indicates that many transitions in the model have not occurred. Furthermore, we use the ListDead Transitions () function to query the state space and find that the dead transition GEN_AUTHERR and ERR_BACK, are consistent with the original model, indicating that because the attack mode is not turned on, there is no request message of authentication failure in the model, which is consistent with the expected behavior. The other 12 dead transitions reflect that the transition in the attacker model including the red part (replay attack), the blue part (tamper attack) and the purple part (spoofing attack) in Figure 12 failed to occur. Due to the lack of enabling attack parameters, these dead transitions are still consistent with the expected behavior of the protocol. The above analysis shows that when the attack parameters are not enabled, the attacker model does not change the behavior of the protocol, and the identity authentication function of the master station in the protocol specification can still be realized.

6 Attack Analysis and Vulnerability Mining

6.1 Attack Analysis

This section will enable all attacks, including RP_ATK (replay attack), MD_ATK (tamper attack), and SP_ATK (spoofing attack), to form the final attacker model MRS_ATK. For tampering attacks, it is necessary to set the initial token value of the library TAG_COUNT in the NET subpage model to 1, and the tamper attack flag MATTACK on the transition CHANNEL output arc to be ”ture” to manipulate the challenge information received from the slave station O (Figure 12). The above settings enable the attacker to obtain enough challenge information issued by the slave station in NACR mode, so as to obtain the latest challenge information, which is used to forge the request information of the master station in AGM mode.

As shown in Table 2, MRS_ATK lists 60 dead nodes and 21 dead transitions, which indicates that unexpected behavior has occurred in the attacker model in full-state attack mode. Furthermore, the above 60 dead nodes are classified and analyzed by using SML query statements, including ListDeadMarkings(), SearchNodes(), Reachable $(M1, m2)$. The ListDeadMarkings() function is used to determine all the dead node sequence numbers of the model. The SearchNodes() function is used to determine whether a state contains an attack sequence. The Reachable() function is used to determine whether there is a path to the protocol security state, that is, the request initiated by the attacker is not authenticated by the slave O. S0-7 is used to classify the state points satisfied under different conditions. The number and meaning of states in each category are shown in Table 3.

In order to further analyze the authentication attributes of the protocol, the dead nodes are classified into expected and unexpected types. The expected dead node refers to the state node when the first two NACR requests are successful and the third AGM attack request fails. The unexpected dead node is the state node other than the expected dead node. The classification basis of the expected dead nodes is that the attacker model in this paper assumes that the AGM mode is used in the third communication, and the attacker expects to use the latest challenge information intercepted to launch three types of man-in-the-middle attacks in the third communication. According to the above description of unexpected dead nodes, it can be seen that the result of S4 query reflects the number of such dead nodes.

Further, the SML statement is used to query the status of the above dead nodes, and the process and results are as follows:

1) Using the above SML function AttackallInstaces query, the result shows that there are 36 unexpected dead nodes;

2) Use the SearchNodes statement to find all the states that contain the attacker request message, and get the status node 173;

3) The reachability from the node containing the attack request status to all unexpected dead nodes is verified by using the Reachable (M1-M2) statement.

The return value of the Reachable (M1-M2) statement is ”ture”. According to the definition of the authentication attribute of the protocol in section 3, the behavior of the attacker leads to the unexpected termination of the protocol, violating the authentication attribute of the protocol. Moreover, the attacker can still control the slave station to execute the key request message without obtaining the session key and without a valid message authentication code. Therefore, the protocol does not meet the authentication requirements claimed in IEC62351 and IEEE-1815-2012 specifications.

6.2 Attack Path Analysis

The attack results in the full attack state show that the attacker can send valid AGM messages to the slave station O without knowing the session key, and be executed by the slave station, including read and write registers, and even restart the application service. Considering the plaintext transmission of protocol messages, legitimate request and challenge information can be intercepted and tampered with, thus preventing the formation of legitimate message sequences. This results in the following attack threats:

1) The first kind of protocol loophole: in NACR mode, randomly changing the value of message sequence number Ksn and random number will make the protocol lose synchronization and cause unexpected authentication failure. By observing the challenge information of the slave station in continuous NACR mode, the attacker can find that whenever there is a new NACR request, the message sequence number Ksn will be increased by 1. Therefore, the attacker can modify the sequence number in the challenge information from the slave station O to form a new

Table 2: Comparison of the state space of each model

Types	Original model	Attack model				
		0_ATK	RP_ATK	MD_ATK	SP_ATK	MRS_ATK
State Space Nodes	11829	13327	12979	12674	12708	63344
State Space Arcs	129394	135602	177604	145866	124450	911557
SCC Graph Nodes	11829	13327	12979	12674	12708	63344
SCC Graph Arcs	129394	135602	177604	145866	124450	911557
Dead Markings	1	1	1	1	9	60
Dead Transitions	2	14	16	16	19	21

Table 3: SML functions mainly used in the classification of dead nodes

Item()	Description
S0(60)	The number of DeadMarking for the entire model
S1(60)	Contains the number of successful or failed DeadMarking
S2(0)	Contains the number of successful and failed DeadMarking
S3(24)	Number of DeadMarking which authentication failed
S4(36)	Number of DeadMarking which authentication successful
S5(16)	Number of DeadMarking caused by replay attack
S7(18)	Number of DeadMarking caused by tampering attack
S7(26)	Number of DeadMarking caused by spoofing attacks

challenge information and send it to the master station M, so as to induce the master station to send the wrong message authentication code, resulting in the failure of message authentication. Figure 14 shows the MSC model of this attack.

2) The second kind of protocol vulnerability: through the observation of a large number of plaintext challenge information, when an attacker finds challenge information with the same message sequence number Ksn and random number, he can replay the message authentication code tag_old intercepted in previous sessions to the slave O, thus causing the slave station to execute false commands. Prented_RSP is a false response message defined by an attacker based on a bogus request message. Figure 15 shows the MSC model of this attack.

3) The third kind of protocol vulnerability: by observing a large number of plaintext challenge messages, when an attacker finds challenge information with the

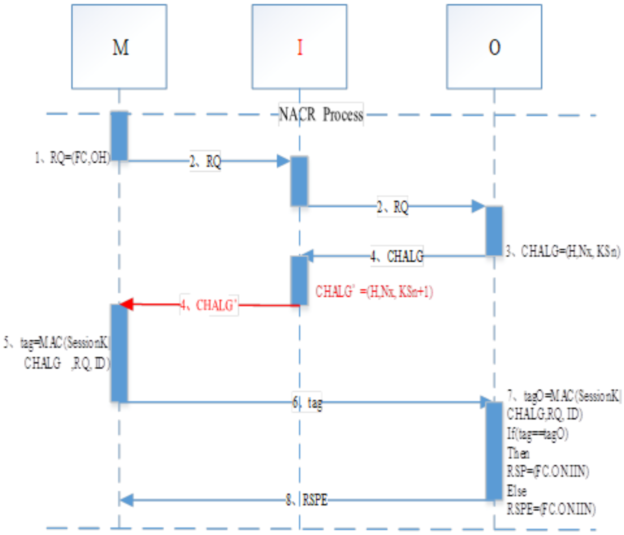


Figure 14: The first type of attack path

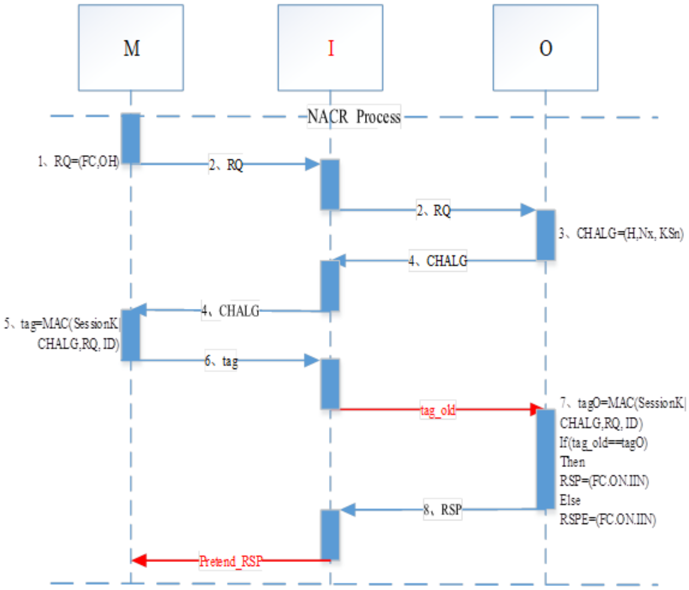


Figure 15: The second type of attack path

same message sequence number Ksn, he can replay the active request message Old_AGMRQ in AGM mode intercepted in previous sessions to the slave station, which causes the slave station to mistakenly assume that the master station will initiate an AGM session later, which in turn causes the slave station to perform unauthorized operations. Through the analysis of the state space of the model in the full attack state, it is concluded that in the attack mode, the transition T_WRITE in the O_EXE_RQ sub-page is triggered, and the slave station O still executes the false request command, resulting in 12 dead transitions in the model. Figure 16 shows the MSC model of this attack.

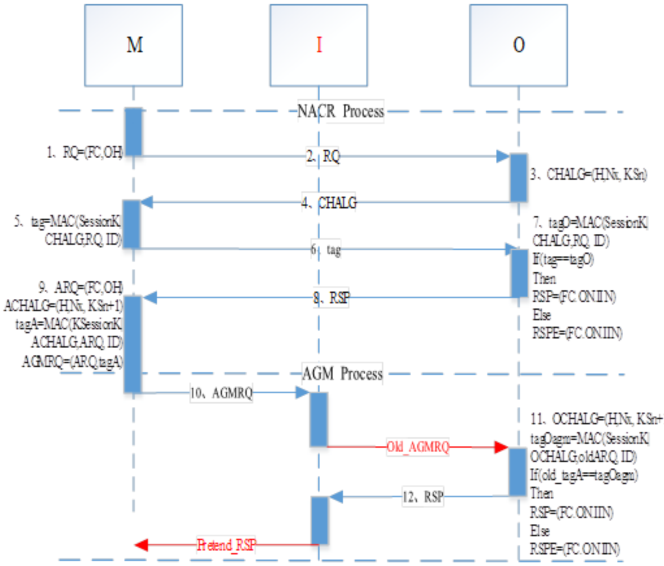


Figure 16: The third type of attack path

7 Conclusion

In This paper, we introduces an improved Delov-Yao attacker model to the DNP3-SA protocol, establishes a parameterized CPN attacker model of the protocol, and verifies the authentication attribute of the protocol and its ability to resist man-in-the-middle attacks. Firstly, the improved Dolov-Yao attacker model is studied, including message splitting and combination and parameterization. The advantage of the improved attacker model is verified by the application example of NS protocol. Secondly, the improved attacker model is applied to the NET subpage of the protocol, and three kinds of attacks such as replay, tampering and spoofing attack are introduced, the state space report of the attacker model is generated, and the functional consistency of the attacker model is analyzed. Finally, the vulnerability mining in the full attack state of the protocol is carried out, and the vulnerability exploitation path is given according to the results of SML query.

The running results of the protocol attacker model proposed in this paper show that the protocol actually does not meet the authentication requirements claimed in the IEC62351 and IEEE-1815-2012 specifications, and can not resist the three attacks listed in the specification: replay, tampering and spoofing.

Acknowledgments

This work is funded by the Shaanxi Provincial Department of Education Scientific Research Project (19JK0040), Science and Technology Project of Shaanxi Province (NO.2020GY-041), Doctoral research project of Baoji College of Arts and Sciences (209040080). The authors would like to thank the anonymous reviewers and the editors for their suggestions.

References

[1] R. Amoah, S. Camtepe, E. Foo, "Formal modelling and analysis of DNP3 secure authentication," *Journal of Network & Computer Applications*, no. 59, pp. 345-360, 2016.

[2] R. Amoah, S. Camtepe, E. Foo, "Securing DNP3 broadcast communications in SCADA systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1474-1485, 2016.

[3] Y. Bai, *Research on Security Protocol Formal Method Based on Colored Petri Nets Model*, Inner Mongolia University, 2013.

[4] J. A. Crain, S. Bratus, "Bolt-on security extensions for industrial control system protocols: A case study of DNP3 SAv5," *Security & Privacy IEEE*, vol. 13, no. 3, pp. 74-79, 2015.

[5] C. Cremers, M. Dehnel-Wild, K. Milner, "Secure authentication in the grid: A formal analysis of DNP3: SAv5," in *Proceedings of European Symposium on Research in Computer Security*, pp. 389-407, 2017.

[6] I. Darwish, O. Igbe, T. Saadawi, "Vulnerability assessment and experimentation of smart grid DNP3," *Journal of Cyber Security*, vol. 5, no. 1, pp. 23-54, 2016.

[7] I. Darwish, T. Saadawi, "Attack detection and mitigation techniques in industrial control system - Smart grid DNP3," in *Proceedings of International Conference on Data Intelligence & Security*, 2018. DOI: 10.1109/ICDIS.2018.00028.

[8] D. Delov, A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198-208, 1983.

[9] T. R. de Toledo, N. M. Torrisi, "Encrypted DNP3 traffic classification using supervised machine learning algorithms," *Machine Learning and Knowledge Extraction*, vol. 1, pp. 384-399, 2019.

[10] IEEE, "1815-2012 - IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)," *IEEE*, 2012. DOI: 10.1109/IEEESTD.2012.6327578.

[11] C. Irvene, T. Shekari, D. Formby, and R. Beyah, "If I knew then what I know now: On reevaluating DNP3 security using power substation traffic," in *Proceedings of the Fifth Annual Industrial Control System Security Workshop (ICSS'19)*, pp. 48-59, 2019.

[12] J. Jiang, H. Mao, R. Shao, *et al.*, "Formal verification and improvement of the PKMv3 protocol using CSP," in *Proceedings of IEEE Computer Software & Applications Conference*, 2018. DOI: 10.1109/COMPSAC.2018.10318.

[13] O. S. Kidege, S. P. Maj, "Industrial network security – A critical review," *Modern Applied Science*, vol. 11, no. 6, pp. 24-32, 2017.

[14] S. Kwon, H. Yoo and T. Shon, "RNN-based anomaly detection in DNP3 transport layer," in *Proceedings of IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*, 2019. DOI: 10.1109/SmartGridComm.2019.8909701.

[15] D. Lee, H, Kim, K, Kim, P. D. Yoo, "Simulated attack on DNP3 protocol in SCADA system," in *Proceedings of the 31th Symposium on Cryptography and Information Security*, 2014. (https://caislab.kaist.ac.kr/publication/paper_files/2014/SCIS2014_DS.pdf)

[16] F. Liu, M. Heiner, D. Gilbert, "Coloured Petri nets for multilevel, multiscale and multidimensional modelling of biological systems," *Briefings in Bioinformatics*, vol. 20, no. 3, pp. 877–886, 2019.

[17] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469-482, 2018.

[18] T. C. Pramod, N. R. Sunitha, "SCADA: Analysis of attacks on communication protocols," in *Proceedings of International Symposium on Sensor Networks, Systems and Security*, pp. 219-234, 2018.

[19] M. A. Rahman and A. Datta, "Impact of stealthy attacks on optimal power flow: A simulink-driven formal analysis," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 3, pp. 451-464, 2020.

[20] N. R. Rodofile, K. Radke, E. Foo, "Real-time and interactive attacks on DNP3 critical infrastructure using scapy," in *Proceedings of the 13th Australasian Information Security Conference*, 2015. (https://eprints.qut.edu.au/81587/21/Vol161_AISC2015_paper09.pdf)

[21] C. Rosborough, "Colin gordon and brian waldron, all about eve: Comparing DNP3 secure authentication with standard security technologies for SCADA communications," in *Proceedings of Power and Energy Automation Conference Spokane*, 2019. (https://ccaps.umn.edu/documents/CPE-Conferences/MIPSYCON-Papers/2019/AllAboutEve.pdf)

[22] A. Shahzad, M. Lee, S. Kim, K. Kim, J. Y. Choi, Y. Cho, K. K. Lee, "Design and development of layered security: Future enhancements and directions in transmission," *Sensors*, vol. 16, no. 1, pp. 37-52, 2016.

[23] A. Volkova, M. Niedermeier, R. Basmadjian and H. de Meer, "Security challenges in control network protocols: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 619-639, 2019.

[24] M. Xiao, W. Li, X. Zhong, K. Yang And J. Chen, "Formal analysis and improvement on ultralightweight mutual authentication protocols of RFID," *Chinese Journal of Electronics*, vol. 28, no. 5, pp. 1025-1032, 2019.

[25] X. C. Yin, Z. G. Liu, L. Nkenyereye, B. Ndibanje, "Toward an applied cyber security solution in IoT-based smart grids: An intrusion detection system approach," *Sensors*, vol. 19, no. 22, pp. 4952, 2019.

[26] J. Zhang, L. Yang, W. Cao and Q. Wang, "Formal analysis of 5G EAP-TLS authentication protocol using proverif," *IEEE Access*, vol. 8, pp. 23674-23688, 2020.

Biography

Dr. Ye Lu was born in Shannxi, China in 1986. He received his Bachelor's degree from The Beijing Institute of Technology, China in 2008 and Ph.D degree degree in Lanzhou University of Technology, Lanzhou City, China. He is currently a lecturer at Baoji College of Arts and Sciences, Baoji, China. His research interests are in the areas of Blockchain, Internet of things and protocol security.

Wei-Bin Ou was born in Shannxi, China in 1977. He received his Bachelor's degree and Ph.D degree from Xi'an Technological University, Xi'an City, China. He is currently a lecturer at Baoji College of Arts and Sciences, Baoji, China. His research interests are in the areas of Industrial networked control system and industrial fieldbus.