A New Scheme of BACnet Protocol Based on HCPN Security Evaluation Method

Tao Feng, Xiao-yan Jiang, Jun-li Fang, and Xiang Gong
(Corresponding author: Xiao-yan Jiang)
School of Computer and Communication & Lanzhou University of Technology
Lanzhou,Gansu 730000,China
Email: 1848469146@qq.com
(Received Jan. 17, 2020; Revised and Accepted Oct. 9, 2022; First Online Oct. 15, 2022)

Abstract

They are building automation or management systems control services such as heating, air conditioning, and safe aisles in a facility. The standard protocol used to transmit data about the status of components is BACnet. To solve the security problem of BACnet protocol device authentication of intelligent building communication protocol [1], the attack vectors and security requirements of BACnet protocol device authentication are analyzed. First, this paper verifies the consistency of BACnet protocol device authentication based on Petri net theory and CPN Tools [14]. It introduces an improved Delov-Yao attack model to evaluate the protocol model security to verify whether there are other undiscovered attacks. Secondly, a new BACnet protocol device authentication model is proposed to solve the problems of session key leakage and message tampering during device authentication. This mechanism needs to change the key distribution method and introduce random numbers to complete BACnet protocol devices. Certified. The new scheme can use BACnet protocol devices to authenticate cryptographic primitives without significantly upgrading existing platforms. CPN Tools have verified the protocol; the results show that no intrusion path can ensure device certification's integrity, authenticity, freshness, and confidentiality.

Keywords: BACnet Protocol; CPN Tools; Formal Analysis

1 Introduction

With the rapid development of information technology, intelligent building to become "Internet +" and the construction industry and the direction of the depth of integration of a breakthrough, but the explosive growth of network security vulnerabilities, a large number of mobile Internet application of new technologies, automatic control, gave the introduction of intelligent building new information security risks. A growing number of cyber attacks show that the intelligent building is unsafe [2,13,19]. TCP / IP protocol data communications technology is widely used in intelligent building systems based, has been achieved despite the requirements for intelligent remote monitoring of construction equipment, but the original data communication protocol network face greater threat of attack.

The widespread use of the BACnet protocol in the field of intelligent building systems has proved to be unsafe [3, 5, 16]. Because of the BACnet protocol's Internet connectivity and the ability to find BACnet devices using the SHODAN search engine (cf.www.shodanhq.com), BACnet devices can also be remotely attacked, for example, by smoke detectors or other important BAS devices. Therefore, BACnet protocol must be studied and improved from the perspective of equipment authentication of both sides of communication to ensure the security of communication. The BACnet protocol standard defines network security services, which provide security mechanisms for communication equipment identification, data source identification, operator identification, and data confidentiality and integrity. However, few building automation system suppliers have implemented it. An attacker may exploit this vulnerability to intercept the session key and tamper with the message to modify the command of the communication device or perform an unauthorized service to attack remotely.

Literature [17] proposes a way to improve the reliability and security of networks and applications using traffic standardisers, but the tool does not implement prevention techniques. Literature [7] [10] made a detailed study on the identification problem, denial of service, eavesdropping and buffer overflow in the core functions of the protocol, and proposed a deterministic improvement on the BAS networking problem that was not taken into account at the beginning, and added the remote management technology of enterprise internal network and Internet connection. Literature [6] mainly discusses the limitations of secure communication and the security of data exchange in BAS. Holmberg *et al.* proposed corresponding

mitigation measures for some of the identified vulnerabilities in BACnet, such as BACnet firewall [23], which, however, required dedicated hardware due to its high computational complexity. Literature [8] determined the ability of legitimate malicious commands running within BACnet works to prevent them from transmitting data traffic through boundary firewalls. Literature [11, 21] focused on this problem and proposed a potential solution for BAS specific intrusion detection systems (IDS). Above the BACnet protocol security research mainly focus on its function and connect to the Internet after a series of problems, for internal data transmission security agreement did not put forward effective safety assessment methods, and puts forward improvement scheme couldn't resist the attacker as communications equipment for the session key and tampering with BACnet server and client attacking threat. Therefore, based on literature [9], guided by colored Petri net theory and DelovYao attack method, and based on CPN Tools model detection tool, this paper focused on the formal modeling and security assessment of the protocol, explored protocol vulnerabilities, proposed targeted security improvement schemes, and applied CPN detection Tools to verify the security of the proposed schemes.

This paper is organized as follows. In Section 3, based on Petri net theory and CPN Tools tool, we verify the consistency of the BACnet protocol device authentication. In Section 4, the improved Delov-Yao attack model of safety assessment protocol model is introduced, we verify that there are other attacks undiscovered. In Section 5, we propose a new protocol BACnet device authentication model, which needs to change the key distribution method. Meanwhile the random number is introduced to complete the BACnet protocol device authentication, then we use the CPN Tools tool to verify the security of the scheme and analyze its performance. Finally, In Section 6, we describe the general conclusions.

2 Preliminaries

2.1 BACnet Protocol Overview

BACnet is an object-oriented peer-to-peer network protocol, in order to ensure the efficiency of communication,we use the OSI-RM streamlined architecture model to define application layer, network layer, data link layer and physical layer. BACnet focus on the network layer and above, the goal of which is to run on any data link and physical media. The BACnet standard defines the data structure that represents the communications of devices on BACnet. The core data structure is an object with 54 standard types, as shown in the BACnet architecture hierarchy diagram in Figure 1.

BACnet standard defines six functional categories of services [12]: Object Access Service, file access service, alarm and event services, remote device management services, virtual terminal services and network security services. These services include all aspects of the building's

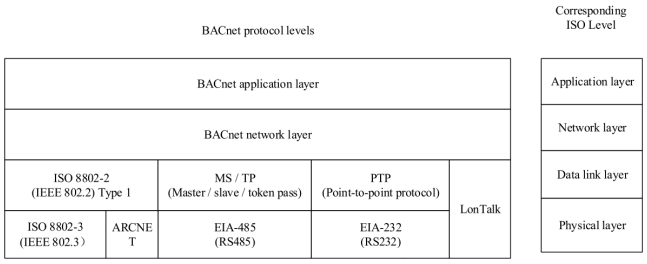

Figure 1: BACnet architecture hierarchical graph

automatic control network system. With the development of the protocol and the application of the network, new services will be added.

2.2 Network Security Services

In the BACnet standard, network security services is an optional content [18]. BACnet network security mainly provides security mechanisms for equipment authentication, data source authentication, operator identity authentication, and data confidentiality and integrity [4], but does not provide communication security mechanisms such as access control and non-repudiation. This paper focuses on the analysis of equipment certification..

In the BACnet standard, there is a flaw in device authentication security, which is vulnerable to attacks such as man-in-the-middle ,replay attacks and other methods. For example, in the BACnet standard security service, BACnet's key distribution is a local method. Its keys are stored in the local device, there is no method for defining key updates, an attacker is able to crack an old session key and continue the session with that key. In network security services, key exchange, generation, distribution, storage, and erasure are critical to the security of the key. The BACnet standard has no systematic definition for this.

2.3 CPN Tools Modeling Tools

CPN [20] is a graphical language that plays an important role in modeling and verifying concurrency, distributed systems and other systems.CPN is a discrete behavioral model language combined with the capabilities of a high-level programming language, which provides basic graphical representation and the ability to model concurrent, communication, and synchronous. CPN's ML (Markup Language) [22] programming Language is based on the standard ML programming language. It provides basic data type definitions (complex data types can be combined through products, unions, etc.), a description of data manipulation, meanwhile, it can create a compact and parameterized model. CPN's model language is a general-purpose modeling language. It is not only applicable to a class of systems, but is oriented to a wide range of systems and can describe concurrent systems.

Its typical application fields include communication protocols, data networks, distributed algorithms, embedded systems, and many applications in the industrial field.

CPN Tools is a computer-aided design tool developed by Danish researchers for protocol modeling, analysis and validation. CPN tools can be used for CPN model editing, simulation, state space analysis, and performance analysis. CPN tools support tools the time and timeless level CPN models. CPN tools is a computer tool for industrialization. It can use simulation functions to investigate the behavior of model systems, and use state space methods and model detection methods to verify attributes. The interaction between the user and the CPN tools is based on the interactive technology that directly manipulates the graphical representation of the CPN model. Its representation is intuitive and has many industrial applications.

3 BACnet Protocol Modeling Device Authentication HCPN

3.1 BACnet Protocol Device Authentication Message Flow Model

Authentication Message Flow (MSC) model is shown in Figure 2. ReqKey represents a key request to the server, Ks represents the session key distributed by the server to devices A and B, IDa indicates the identity of device A, Kb denotes the master key of device B, IDb represents the identity of the device B, Ka represents device A master key. Authenticate represents peer entity requests the service identification, Pseudo Random Number represents a pseudo-random number in the packet, ComplexACK indicates a complex response message Modified Random Number response message indicates the modified random numbers.

Authentication mode as follows:

1) Run the initialization algorithm, devices A, B uses the DES algorithm to generate its own master key. Device A has the master key Ka and device B has the master key Kb (Shared only with the key Server);

2) A sends a "ReqKey" request to the server, requesting to obtain the session key Ks;

3) After receiving the request message from A, the key server Server generates a session key Ks, encrypts Ks and IDa using Kb of device B, and sends it to device B;

4) Device B uses Kb to encrypt its identity IDb and send it to the key server Server. The key server Server verifies the address of device B;

5) The key server Server then uses the Ka of the device A to encrypt Ks and IDb and sends it to the device A; server Server. The key server Server verifies the address of device B;

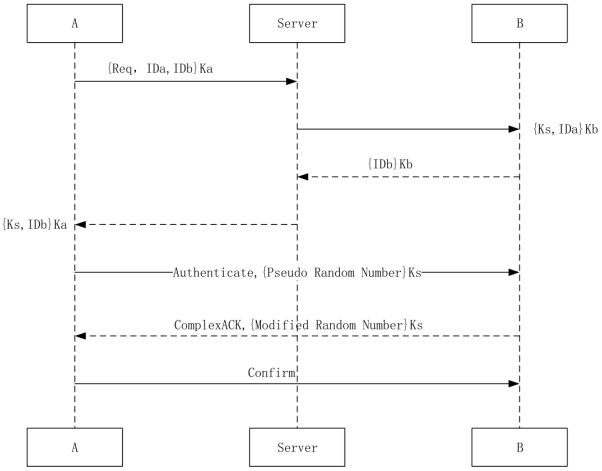

Figure 2: Authentication mode message flow model (MSC)

6) Device A receives Ks and begins to identify device B, device A generates an authenticate request, the protocol data portion of which and Pseudo Random Number are encrypted with Ks and sent to B;

7) Device B decodes the authentication request from A, modifies the Pseudo Random Number to Modified Random Number, and uses Ks to encrypt and return a ComplexACK message to device A;

8) Device A decrypts the message after receiving it, and if a ComplexACK message containing the correct Modified Random Number is received, device authentication succeeds.

3.2 BACnet Protocol Defined Color Set Device Authentication Message

First, analyze the four messages that the key is distributed. The information elements needed to establish the model include the identity of device A and device B, the master keys (Ka and Kb) of the two devices themselves, and the session key Ks of the key distributor; There are two formats for encryption and decryption. One is device A and device B use the master key Ka and Kb to encrypt their identity and request information, The other is that the key distributor uses the keys Ka and Kb of the device A and device B that are known in advance to decrypt the obtained information to verify the identity; We are combining basic information elements and cipher text into four message formats. Next, analyze the device authentication message, both messages are also ciphertext, and the content is differentand, Therefore, the task of cipher text is omitted when setting the color and the message is directly defined on the basis of the information elements. Finally, the main color collection as defined in Table 1.

Table 1: BACnet protocol devices certified color set statement

Category	Key element	Color set definition
Key distribution	MSG1	colset MSG1=product ID*CRY2
	MSG2	colset MSG2=product ID*CRY1
	MSG3	colset MSG3=CRY2
	MSG4	colset MSG4=MSG2
Equipment certification	ASK	colset ASK=record m:MSG*k:KEY
	RSP	colset MSG4=colset RSP=product NONCE*NONCE2
	RPL	colset RPL=record r:RSP*k:KEY
	CFM	colset MSG4=colset CFM=record n:NONCE*k:KEY2
Data	PACKET	colset MSG4=colset PACKET=union MSG1+MSG2+MSG3+MSG42

Here,ID represents the device, KEY represents the key that appears during the authentication process, and NONCE represents the pseudo random number Pseudo Random Number and the modified random number Modified Random Number. The data packet type (colset packet) is uniformly organized using the union type, and its elements are specific descriptions of different types of data packets. Among them, the MSG1 type is used to describe the message of Step 1 of the protocol operation of the data exchange between the session initiator and the key distributor; the MSG2 type is used to describe the message of Step 2 between the key distributor and the session responder; The MSG3 type is used to describe a message with a step of 3 between the session responder and the key distributor; the MSG4 type is used to describe a message with a step of 4 between the key distributor and the session initiator.The ASK record type is used to describe the protocol request message sent by the session initiator to the responder when the protocol runs in Step 5. The RPL record type is used to describe the response data message sent by the session responder to the initiator when the protocol runs in Step 6. The CFM record type is used to describe the data message that the session initiator confirms the received information when the protocol runs in Step 7.

3.3 BACnet Protocol Device Authentication Model HCPN

This section will be established protocol BACnet device authentication HCPN hierarchical model, through the use of alternative high-level transitions in the network CPN tools tool to link it to a more detailed sub pages to hide the details of the top layer of the model , and a high-level description of a simplified model presented can be used broadly defined from the picture system. The hierarchical BACnet protocol model includes top-level and sub-pages of each entity-level model. Top model is an abstract description of the overall agreement, Entity layer model provides implementation details of the HCPN model.

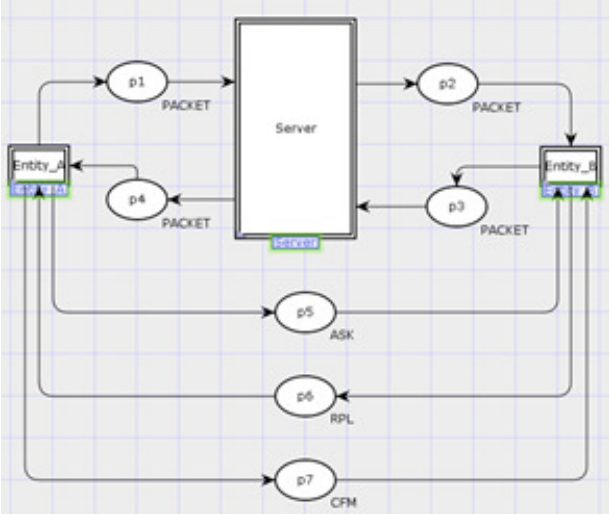

Figure 3: BACnet protocol device authentication CPN top level model

3.3.1 BACnet Protocol Device Certified Top Model

The CPN top-level model of the BACnet protocol device certification is an abstract description of the entire communication protocol, including the communicating parties, the communication network, and the messages passed. As shown in Figure 3, the double-line rectangle in the figure is an alternative change, and the oval is the message places.The left-hand alternative transition Entity_A represents the communication device A, the middle alternative transition Server represents the key distributor, and the right-most alternative transition Entity_B represents the communication device B.The top-level model completely simulates the BACnet protocol device authentication session process, including the key distribution process and device authentication process, and the processing of key information, which is a high degree of abstraction and generalization of the protocol MSC model.

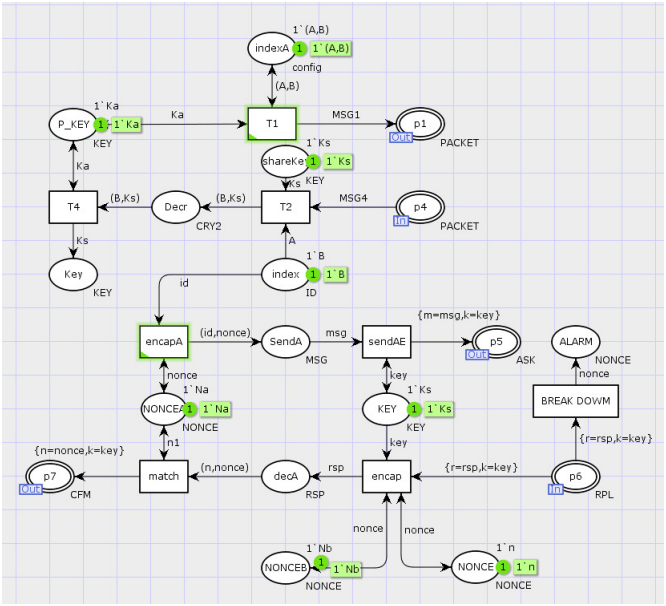

Figure 4: BACnet protocol CPN model device authentication entity A

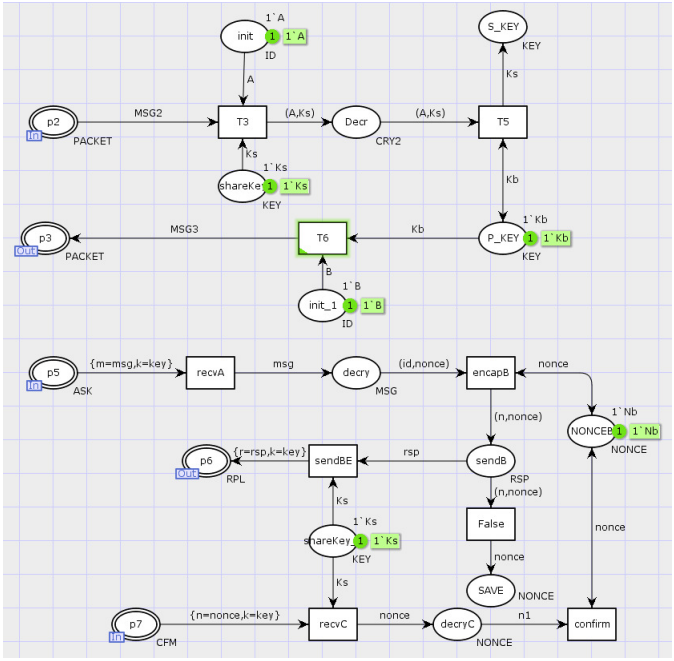

Figure 5: BACnet CPN model entity device authentication protocol B

3.3.2 BACnet Protocol Physical Layer Device Authentication Model

As shown in Figure 4, the model for entity A in the BACnet protocol device authentication for the protocol includes 16 message places and 7 transitions. The process of sending and receiving data packets where entity A requests a session from the key distributor and initiates identity authentication to entity B is described. In the model, the fusion place index is used to configure the session participation mode, and the protocol initiates the session and the role and identity information of each entity; For entity A, when participating in the process of session initiation (protocol execution Step 1), the session participation mode configuration controls the initiator and responder of the data it sends. Because entity A is an honest entity, its identity is A , And the respondent is entity B in this model, generate the shared keys Ka and Kb with the key distributor, and save them to the corresponding place P_KEY, organize and send MSG1 type data to the communication channel port place p1; the participating protocol executes Step 4. The key distributor sends data of type MSG4 to the communication channel port place p4 while receiving the data of entity B. the initiator uses the shared key Ka with the key distributor to decrypt to obtain the session key Ks. Fusion place index order of a session configuration settings, such changes in the entity performing the ignition operation of the respective step protocol.

As shown in Figure 5, the model of entity B in the BACnet protocol device authentication of the protocol includes 16 message places and 8 transitions. It describes the entity B receives the key distributor session key distribution, and data packets received authentication entity A initiates a transmission and reception process. Fusion places used in the model for the session participation mode configuration index, set the protocol to initiate the session, and where the role of each entity's identity information and the like taken; For entity B, the session participation Step 2, Step 3 and Step 6. In MSG2, entity B decrypts the received data with the shared key Kb with the key distributor and obtains the session key Ks and the identity of the initiator entity A, and saves the obtained session key in a specific repository. The identity of the corresponding entity in S_KEY is stored in the place init. It will then send MSG3 type and key distributor for authentication. Fusion place index order of a session configuration settings, such changes in the entity performing the ignition operation of the respective step protocol.

As shown in Figure 6, the model of the key distributor in the BACnet protocol device authentication of the protocol includes 10 message places and 3 transitions. This model describes the process by which the key distributor Server distributes the session keys for identity authentication for entities A and B. Step 1: Receive the message MSG1, determine whether the encryption key is Ka, use Ka to decrypt it, obtain the identity of the session initiator and the identity of the responder, and save it to the corresponding place init, Step 2: according to the identity of the responder in the message MSG1, organize and send MSG2, and send the session key Ks and the identity of the session initiator to the responder; Step 3: the key distributor receives and uses the shared key Kb with the key distributor to decrypt the message MSG3 sent by the responder, and determines whether the identity of the responder is correct. Step 4: according to the

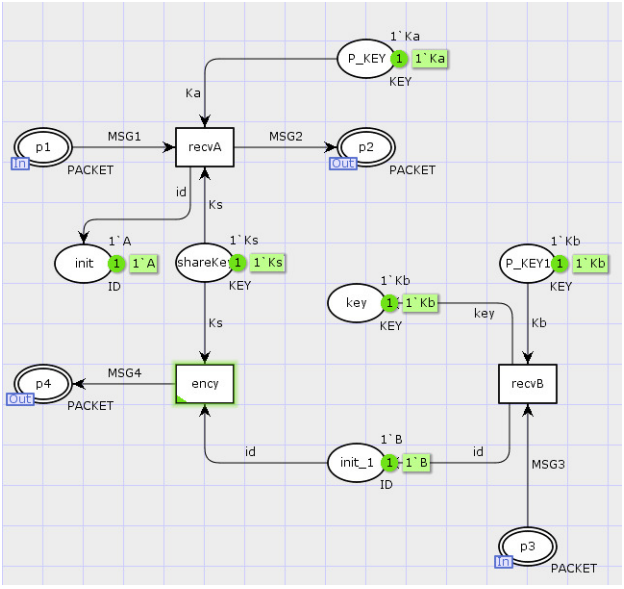

Figure 6: BACnet protocol CPN model device authentication key dispenser

identity of the initiator in the message MSG1, use Ka to encrypt the session key Ks and the identity of the responder, and organize and send the message MSG4.

3.4 Features the Original Model of Consistency Verification

Whether the original model accurately reflects the functionality required by protocol specification to determine the effectiveness of subsequent security assessment model. In this section, a state space analysis tool will be used to verify the functional consistency of the HCPN model of the original BACnet protocol device certification described above. During the verification process, it is mainly verified whether the behavior of the key distribution process and the device authentication process conforms to the authentication behavior attributes described in the protocol specification. It should be noted that the original HCPN model did not introduce network attacks.

3.4.1 Analysis of Results Expected

For any CPN model state analysis, researchers mainly investigate the activity of their state nodes, state master nodes, andtransitions, so as to compare with the expected system state, determine whether the model is consistent with expectations, and meet the protocol's behavior specifications. As shown in figures 4 and 5, according to the BACnet protocol device authentication specifications, when a device initiates an authentication request, it will also generate a pseudo-random number of the desired data packet. Whether the device can successfully authenticate depends on the encrypted data verification, When authentication is successful, device A will trigger the transition encap and match without triggering the transition BREAK DOWN, and device B will trigger the transition recvC and confirm without triggering the transition False, so the transition BREAK DOWN and False can be predicted in the model Two dead transitions. In addition, the original model will finish running after the authentication request is completed, so it can be predicted that there is no live transition of the model termination state and there is only one dead state node. Table 2 gives the expected performance results of the original model.

3.4.2 Analysis of the Results of the State Space

This section is mainly used for state space analysis tool for behavioral attributes protocol model for analysis. SML includes the following query: SccReachable (). Nodes exist in the model for determining the size, and determining the possibility of deadlock in the model; InitialHomeMarking (). Means for determining whether there is always reachable from any other accessible STATUS This state is a state of the main model; ListDeadMarkings (). Model used to determine the final state; ListDeadTIs (). Used to determine whether a given change is not up to the state to enable; TisLive (). For determining whether changes always occurring or being performed; Reachable (x, y) for determining whether the marker M (y) up to the path from the marker M (x). Table 3 shows the state space model of the original agreement query results.

4 BACnet Protocol Device Authentication Security Assessment

4.1 Based on BACnet Protocol Attacker Model of Device Authentication Security Assessment

This paper makes full use of the advantages of CPN visual modeling, dynamic model execution, and state space analysis of system operation. Based on the improved solution of the Delov-Yao [15] attacker model, the attacker is introduced into the HCPN model of BACnet protocol device certification. The model evaluates the security of the protocol and analyzes the loopholes in the protocol.

Figure 7 shows the security assessment model of the Server subpage of the HCPN model server authentication based on the BACnet protocol. The server subpage simulates the key distributor to distribute the session keys for devices A and B. According to the assumption of the Delov-Yao attack, the attacker has eavesdropping, tampering, and packet loss, and can disguise as the session initiator and responder, but not as the trust third-party servers. As shown in the figure, the transitions in the red annotation and the place simulate the replay attack. The transition t0 intercepts the message sent by the protocol in the first step, defines the color set of the place

Table 2: expected performance of the original model results

Types	Death changes	Live changes	The master node	Dead state
Numbers	2	0	0	1
Name	BREAK DOWN,False	/	/	/

Table 3: expected performance of the original model BACnet protocol device authentication HCPN state space model results

Types	Numbers	Name
State space node	5806	/
State Space arcs	15767	/
Scc Graph node	5806	/
Scc Graph arcs	15767	/
Home Markings	0	/
Live Transition	0	/
Dead Markings	1	/
Dead Transition	2	BREAK DOWN,False

resovle as DB, stores the decomposition and messages to be decomposed; defines the place The color set of P5‘ is CB, which stores synthesized and band-synthesized messages; defines the color set of element in the place as AB, and stores atomic messages. Transition t11 uses the rules of the attacker to save the messages that cannot be decrypted to the place P5‘ using excessive rules. Transition t3: uses the attacker's composition rule to synthesize the atomic message and save it to the place P5‘. The concurrency control place SP is used to limit the transition t3 corresponding to the composition rule. The transition t4 sends the attacker's synthesis message to the channel p2 port place. Purple section marked transition guard simulated spoofing attacks, including transitions recvA, ency, recvB. The arc expression labeled in the blue part of the transition At simulates a tampering attack.

4.2 BACnet Protocol Device Authentication Security Property Validation Analysis

When the model is successful and there is no semantic errors, you can run "into the state space" tool. Then run the "Calculate State Space" tool and the "Calculate Strongly Connected Component Diagram" tool in order. If the operation is successful, it means that a state space for the protocol model has been generated. You can now save a Standard State Space Report file. The model status query results are shown in Table 4.

Security evaluation model with the introduction of improved Delov-Yao attacker model lead to a substantial increase compared to the original model state space of nodes and the number of arcs, is in line with expecta-

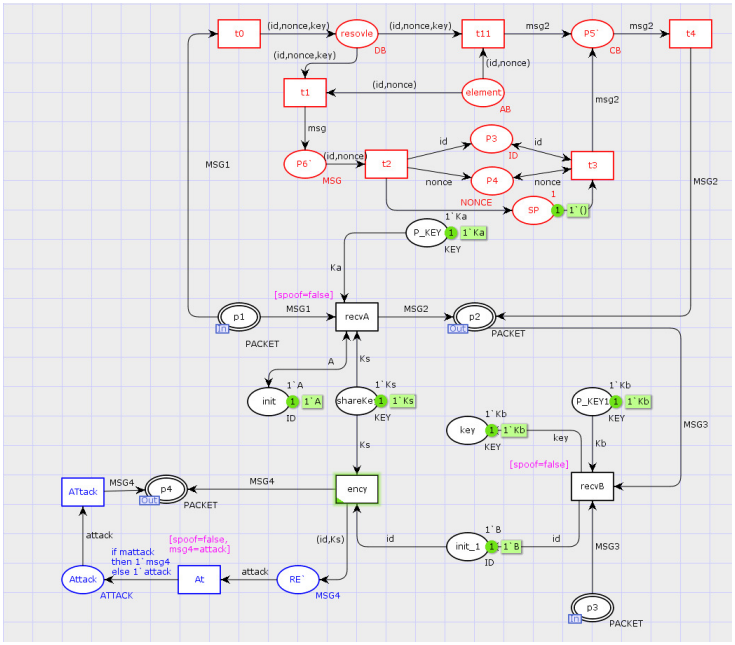

Figure 7: BACnet protocol device authentication model attacker

Table 4: BACnet protocol device authentication model introduced HCPN attacker's state-space search results

Types	Numbers
State space node	18751
State Space arcs	50922
Scc Graph node	18751
Scc Graph arcs	50922
Home Markings	27

tions, and the number of state space arc, the number of nodes and the number of strong connectivity arc, the same number of nodes, indicating safety assessment model for all state nodes are reachable lead to the occurrence of the state of infinite loop iterations and behavior do not exist, which further illustrate the improved Delov-Yao attacker model is valid.

As can be seen from the report, the CPC model generates a 18,751 node state space where the dead node 27, the results show that the addition of three kinds under attack mode security assessment occurred unpredictable behavior. Use ListDeadMarking () to determine the number of 27 dead nodes. After checking the status of all dead nodes, it was found that the messages received by the key distributor Server in nodes 164 and 184 were sent by the intruder, and then the intruder tricked the key distributor Server to obtain the session key and tampered with the correct message Send false messages; it is found in node 549 and node 572 that the message received by responder B has been changed by the intruder, and the intruder can send the same message to responder B repeatedly.

5 BACnet Device Authentication Protocol of The New Program

According to the security assessment of the above method, it can be known that the security result of the BACnet protocol device authentication actually does not meet the authentication requirements in the specification, and it cannot resist two attacks of replay and tampering. In view of the above security threats, this article proposes a method that introduces the generation of random numbers and changes the distribution method of session keys, including the security improvements in the key distribution phase and the device authentication phase, and using HCPN again The model verifies the performance and security of the improved protocol.

5.1 BACnet Protocol Device Authentication Security Scheme Based on New Modeling HCPN

The results of the security assessment of the BACnet protocol reflect that the protocol does not actually meet the authentication requirements claimed in the BACnet standard and cannot withstand replay and tampering attacks. Aiming at the above security threats, this section introduces methods for adding random numbers and changing the session key distribution process. This paper proposes an improved protocol and verifies the improved performance security.

The improved authentication message flow (MSC) model is shown in Figure 8. ReqKey indicates requesting a key from the server, Ks indicates the session key distributed by the server to devices A and B, IDa indicates the identity of device A, Kb indicates the master key of device B, IDb indicates the identity of device B, and Ka indicates the identity of device A Master key. Authenticate indicates that the peer entity requests the service, Pseudo Random Number indicates the pseudo random number in the message, ComplexACK indicates the complex response message, Modified Random Number indicates the modified random number of the response message, and Na and Nb are random numbers added by the improved protocol .

Authentication modes for improved as follows:

1) Run the initialization algorithm. Devices A and B use the DES algorithm to generate their own master keys. Device A has a master key Ka, and device B has a master key Kb(shared only with the key server Server);

2) Device A sends a message(ReqKey = IDa,IDb,Na)to the key server Server, requesting a session key to secure the logical connection to device B. This message contains the random number Na and the device A for this transmission. And the identity of device B;

3) After receiving the message from device A, the key server Server uses Ka to perform the data source identification process, determine whether the request is issued by device A, and then use the DES algorithm to generate the session key Ks. The key server Server uses the master key Ka of the device A to encrypt the one-time session key Ks for the session and the previous request information, and uses the master key Kb of the device B to encrypt the one-time session key Ks and The identity of device A is encrypted and sent to device A, which is (E (Ka,[Ks,IDa,IDb,Na])E(Kb,[Ks,IDa]));

4) After receiving the message sent by the key server Server, device A uses Ka to perform the data source identification process to determine whether it is sent by the key server Server. Decrypt and store the session key Ks to be used, and send the information from the key server Server to device B, which is E(Kb,[Ks,IDa]);

5) After receiving the message, device B decrypts and obtains the session key Ks and the device A (IDa) of the other party who wants to establish a connection. Device B uses the new session key Ks to encrypt the random number Nb of the transmission and sets the result. Send to device A, namely E,(Ks,Nb);

6) After receiving the message from device B, device A starts to authenticate device B. Device A uses the session key Ks to encrypt the Authenticate service request, that is, it contains the data part of the request protocol, Pseudo Random Number, and random number Nb, and sends it to device B;

7) Device B decodes after receiving the authentication service from device A. First verify whether the received random number Nb is the same as the previous one. If it is the same, then reverse the highest

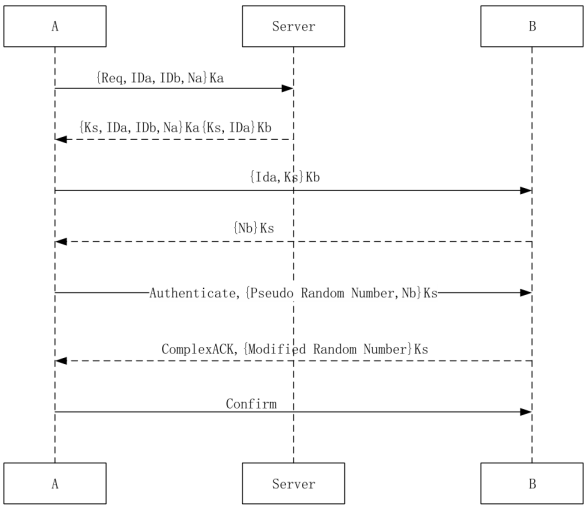

Figure 8: Improved authentication mode message flow model (MSC)

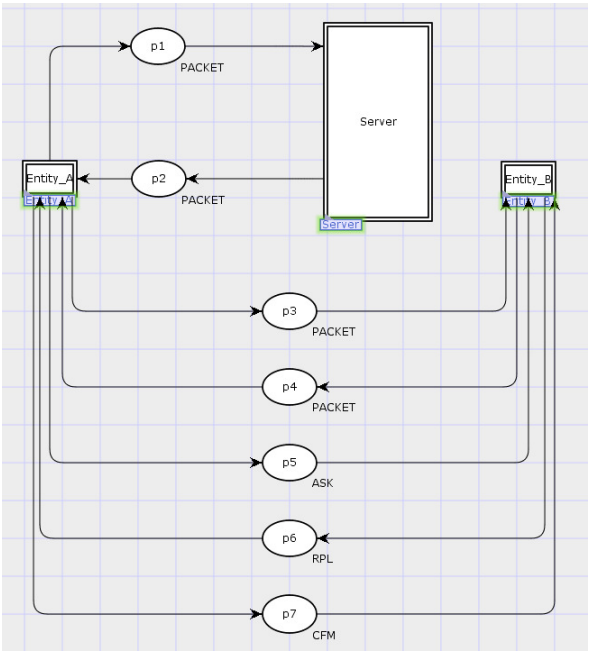

Figure 9: the improved device authentication BACnet protocol CPN top level model

and lowest bits of each byte of this parameter, modify the Pseudo Random Number to Modified Random Number, and return a ComplexACK (Transfer service request has been successfully executed) message;

8) Device A decodes the received response message to check whether the ComplexACK message contains the correct "Modified Random Number". If it is correct, then device B completes the identity authentication.

5.2 The New BACnet Protocol Device Authentication Model HCPN

This section will establish the improved HCPN hierarchical model for BACnet protocol device authentication, which mainly includes the top-level model, device A model, device B model, and key distributor Serves model.

1) Equipment Certification of improved CPN top model

Figure 9 shows the improved top-level model of the CPN. The model includes both parties to the communication, the communication network, and the passed messages. It consists of 3 alternative transitions and 7 places. It completely simulates the complete communication process of key distribution and device authentication. The left-hand alternative transition Entity_A represents the communication device A, the middle alternative transition Server represents the key distributor, and the right-most alternative transition Entity_B represents the communication device B.

2) CPN model entity A device authentication improved

The behavior of entity a mainly includes sending session key request message to key distributor servers, including random number Na and device ID; for entity B, entity a first has the function of distributing key, after authenticating that both sides of the device have session key KS, entity a sends an identity verification request to B, and verifies the correctness of identity by verifying protocol data part and complex message complexack Sex. Figure 10 shows the CPN model of entity a of the improved device authentication.

3) CPN model of device authentication entity B improved

Figure 11 shows the CPN model of the improved device authentication entity B, which includes 7 transitions, 4 places ports and 11 general places. Its behavior includes receiving the session key KS sent by device a, sending the random number Na for authentication to device a, and finally receiving the data authentication of the device authentication request. Among them, the functions of transition recvb, encapa and the model before improvement are similar.

4) Improved device authentication key distributor of CPN model Servers

The behavior of key distributor services mainly includes decrypting the message from device a, obtaining the identity ID and random number Na of device a and B, and then encrypting the session key KS in two messages to device a. Figure 12 shows the CPN model of the improved BACnet device authentication key distributor services, which includes three transitions, two places ports and five common places.

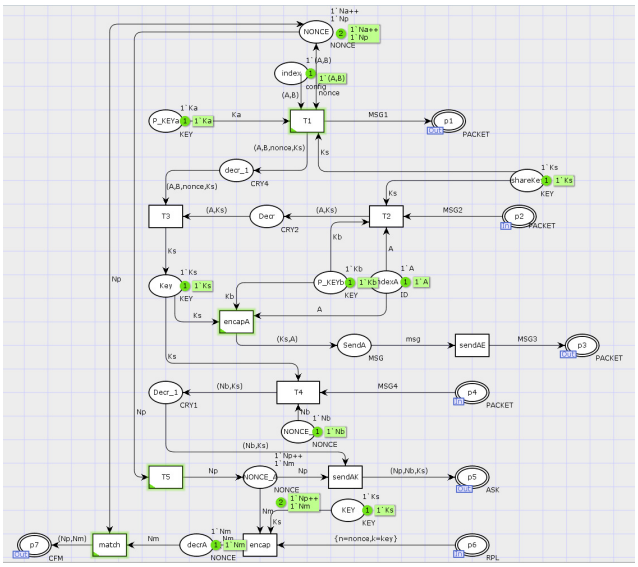

Figure 10: CPN model BACnet protocol entity A device authentication improved

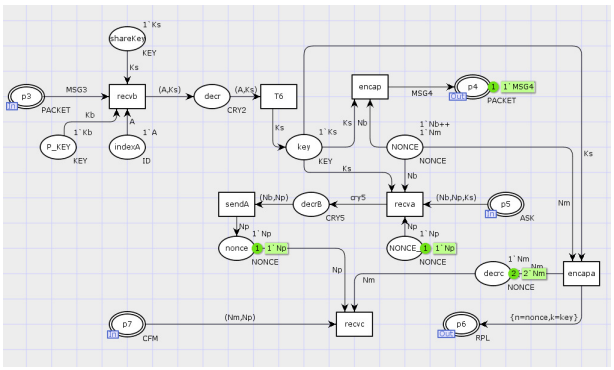

Figure 11: CPN model entity B improved BACnet protocol authentication device

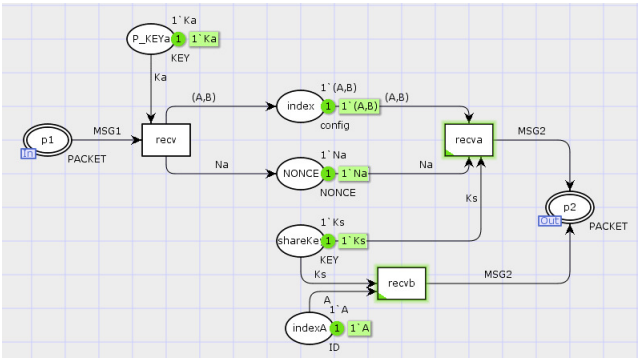

Figure 12: BACnet protocol device authentication key distribution is improved Serves the CPN model

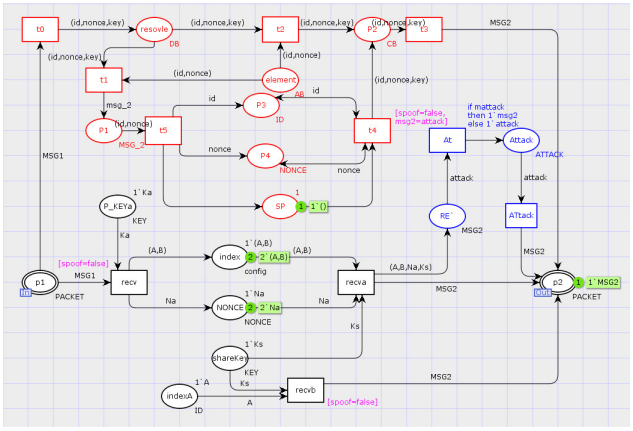

Figure 13: Equipment Certification of improved security evaluation model CPN

5) New equipment certified CPN security evaluation model

Figure 13 shows the security evaluation model of the improved BACnet protocol device authentication HCPN model server sub page. Server sub page simulation key distributor mainly distributes session key for device a, and the improved servers will no longer have data interaction with device B. According to the Delov-Yao attack hypothesis, the attacker has eavesdropping, tampering, packet loss, and can disguise as a session initiator and responder, but not as a trusted third-party server. As shown in the figure, the transitions of the red part and the places simulate replay attack, the transitions of the purple part simulate deception attack, including transitions recv, recvb, recva, and the blue part simulate tamper attack, including transitions At and ATtack.

5.3 The New BACnet Protocol Device Authentication Security Assessment

Table 5 shows the comparison of the state results of the BACnet protocol device authentication security evaluation model after the improvement and before the improvement. Due to the introduction of random Numbers and the change of the key distributor and the way of distributing keys, the model increases the number of transitions and places. Compared with that before the improvement, the number of states and arcs is significantly increased.

In the safety assessment phase, add parameters to verify the BACnet protocol attacks Equipment Certification improved tampering and replay can withstand two attacks. Table with the improved die before improvement number of nodes is reduced from 42 to 5, the above statement SML attacks investigations have found that all dead attack state causes nodes, reducing the number of dead nodes showed increased change key distribution random number and after manner, an attacker can not get the

Table 5: Comparative state space model before and after authentication security assessment improved apparatus BACnet protocol

Types	Improved ago	The improved
State space node	18751	112506
State Space arcs	50922	305532
Scc Graph node	18751	112506
Scc Graph arcs	50922	305532
Home Markings	27	5

full details of the message, including the session key, devices a, B of the master key and the random number, the device authentication BACnet protocol improved to overcome information message tampering and replay attacks, to meet the BACnet protocol apparatus certification certification requirements specification defines the property.

5.4 New Security Analysis Program

1) To prevent tampering with information

   The program information can effectively prevent tampering. Server A server key to return the device information, the device comprising two parts A wants to acquire, i.e. the request message and session key Ks before. Thus, the device A can know whether it's the original information is changed before the key server Server receives.

2) To prevent replay attacks

   The program can effectively prevent replay attacks. The random number Na key distribution stage may know whether the device A previous request information is reproduced. Random number Nb equipment can ensure the authentication stage device B session information has not been received replay attacks.

5.5 New Program Performance Analysis and Program Comparison

This section analyzes the performance of the new BACnet protocol device authentication. In the information interaction stage of the device, key distribution and identity authentication must be initiated. The new scheme not only USES the method of adding random Numbers to encrypt and verify messages, but also changes the way of key distribution. Therefore, the performance consumption of this part of the protocol has a great impact on the time cost of the whole communication. Most of the encryption methods used in key distribution and authentication use the cryptographic primitives in the BACnet specification, which do not require major upgrades to existing platforms, but do add some communication, computing, and storage overhead.

The comparison between the proposed scheme and the related BACnet protocol scheme is shown in table 6. Literature [8] made a detailed study on the identification problem, denial of service, eavesdropping and buffer overflow in the core functions of the protocol, and proposed deterministic improvement for BAS networking problems that were not taken into account at the beginning, and added the remote management technology of enterprise internal network and Internet connection. Literature [10] mainly discusses the limitations of secure communication and the security of data exchange in BAS. Holmberg *et al.* proposed mitigation measures for some of the identified vulnerabilities in BACnet, such as the BACnet firewall, which is computatively complex and requires dedicated hardware. Literature [13] identified the ability of legitimate malicious commands running within BACnet works to prevent them from transmitting data traffic through boundary firewalls, and proposed a potential solution for BAS specific intrusion detection systems (IDS).

Table 6: comparison table of this scheme and other BACnet protocol schemes

Attributes	[8]	[10]	[13]	Our scheme
DOS	✓	✓	✓	✓
Hacking	✓	-	-	✓
IDS	✓	-	✓	x
Information to	×	✓	×	✓
tamper with				
Replay attack	×	-	×	✓

6 Conclusion

In this paper, BACnet protocol device certification process as an object, to colored Petri net theory and Delov-Yao attack as a guide, based on CPN Tools model checking tools, focusing on formal modeling and safety assessment of the agreement, the agreement loophole mining is proposed targeted safety improvement program, and proposed a new program model checker application CPN tools for safety verification. BACnet protocol BACnet device authentication is only an agreement in the security services, other security services are lack of formal modeling and safety assessment. The next step, consider other security services are also studied.

Acknowledgments

This research is supported by The National Natural Science Foundation of China (No.61462060,No. 61762060) and The Network and Information Security Innovation Team of GansuProvincial Department of Education Lanzhou University of Technology (No.2017C-05). Tao Feng is the corresponding author.

References

[1] M. Bayat and M. R. Aref, "An attribute based key agreement protocol resilient to kci attack," *International Journal of Electronics & Information Engineering*, vol. 2, 2015.

[2] R. Casado-Vara, F. D. L. Prieta, S. Rodriguez, J. L. Calvo-Rolle, and J. Prieto, "Adaptive fault-tolerant tracking control algorithm for iot systems: Smart building case study," in *14th International Conference on Soft Computing Models in Industrial and Environmental Applications*, 2019.

[3] D. Fauri, M. Kapsalakis, D. R. dos Santos, E. Costante, and S. Etalle, "Leveraging semantics for actionable intrusion detection in building automation systems," in *13th International Conference on Critical Information Infrastructures Security*, 2018.

[4] R. Gansner, H. Reppy, "The standard ml basis manual," in *AT Corporation and Lucent Technologies Inc*, 2004.

[5] O. Gasser, Q. Scheitle, C. Denis, N. Schricker, and G. Carle, "Security implications of publicly reachable building automation systems," in *IEEE Security & Privacy Workshops*, 2017.

[6] W. Granzer and W. Kastner, "Communication services for secure building automation networks," in *IEEE International Symposium on Industrial Electronics*, 2010.

[7] D. G. Holmberg, "Bacnet wide area network security threat assessment," 2011.

[8] D. G. Holmberg, J. Bender, and M. Galler, "Using the bacnet; firewall router," *Ashrae Journal*, vol. 48, no. 11, pp. B10–B14, 2006.

[9] S. Hyun, J. Kim, H. Kim, J. Jeong, S. Hares, L. Dunbar, A. Farrel, "Interface to network security functions for cloud-based security services," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 171–178, 2018.

[10] W. Kastner, G. Neugschwandtner, S. Soucek, and H. M. Newman, "Communication systems for building automation and control," pp. 1178–1203, 2005.

[11] J. Kaur, J. Tonejc, S. Wendzel, and M. Meier, *Securing BACnet's pitfalls*, Springer, 2016.

[12] S. E. Kim, J. P. Jeong, H. Ko, and H. Kim, "A flexible architecture for orchestrating network security functions to support high-level security policies," in *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*, p. 5, 2017.

[13] N. Li, L. Chen, M.Chen, and Z. Lu, "A method of building safety rule base for power mobile terminals," pp. 72–75, 2018.

[14] L. Liu, L. Wang, and Z. Cao, "A note on one protocol for subset sum problem," *International Journal of Electronics & Information Engineering*, vol. 2, pp. 103–119, 2019.

[15] W. Mao, "A structured operational modelling of the dolev-yao threat model," in *Security Protocols*, pp. 34–46, 2004.

[16] H. M. Newman, "Bacnet; the global standard for building automation and control networks," *Business Expert Press*, 2013.

[17] M. Peacock, M. N. Johnstone, and J. I. D. Hartog, "Timing attack detection on bacnet via a machine learning approach," in *Australian Information Security Management Conference*, 2015.

[18] A. V. Ratzer, L. Wells, H. M. Lassen, M. Laursen, J. F. Qvortrup, M. S. Stissing, M. Westergaard, S. Christensen, and K. Jensen, "CPN tools for editing, simulating, and analysing coloured petri nets," in *Applications and Theory of Petri Nets*, pp. 450–462, 2003.

[19] O. N. Samijayani, L. Addien, I. Fauzi, and M. Zasyi, "Multi-sensing wireless sensor network for smart building system," *Journal of Computational & Theoretical Nanoscience*, vol. 23, no. 4, pp. 3660–3664, 2017.

[20] M. Weber, E. Kindler, "The petri net markup language," *Acta Simulata Systematica Sinica*, 2003.

[21] S. Wendzel, B.Kahler, and T.Rist, "Covert channels and their prevention in building automation protocols: A prototype exemplified using bacnet," in *IEEE International Conference on Green Computing and Communications*, pp. 731–736, 2012.

[22] H. Xinya, L. Jianhua, and L. Hao, "Construction and analysis of network security situation awareness model based on colored petri nets," *Computer and Digital Engineering*, vol. 47, no. 2, 2019.

[23] P. Čeleda, R. Krejčí, V. Krmíček, "Flow-based security issue detection in building automation and control networks," in *Information and Communication Technologies*, pp. 64–75, 2012.

Biography

FENG Tao, was born in 1970, researcher/PhD supervisor, CCF senior member, IEEE and ACM member. He graduated from Xidian University,and then worked at school of computer and communication in Lanzhou University of Technology. His research interests include Cryptography and information security. words.

Jiang Xiao-yan, was born in 1993, CCF member.She is a master's student at lanzhou university of technology. Her research interests include technical information security and industrial control systems.

Fang Jun-li, was born in 1985, CCF member. She is a doctor's student at lanzhou university of technology. Her research interests include technical information security and industrial control systems.

Gong Xiang, was born in 1986, CCF member. He is a doctor's student at lanzhou university of technology. His research interests include technical information security and industrial control systems.