Formal Security Evaluation and Improvement of BACnet/IP Protocol Based on HCPN Model

Tao Feng, Si-Meng Zhao, and Xiang Gong
(Corresponding author: Si-Meng Zhao)
School of Computer and Communication & Lanzhou University of Technology
Lanzhou, Gansu 730000,China
Email: 1078293826@qq.com
(Received Feb. 2, 2021; Revised and Accepted Dec. 8, 2021; First Online Feb. 19, 2022)

Abstract

The BACnet/IP protocol is widely used in building automation systems. However, while realizing remote monitoring of building equipment, it faces a more significant threat of cyber attacks. To solve the current situation of the building automation system being attacked, this paper takes the building automation protocol "BACnet/IP equipment authentication" as the research object and proposes a model detection method based on the colored Petri net theory and the Dolev-Yao attack method, and evaluates and improves the security of the protocol. First, the protocol's device authentication mechanism was verified for consistency based on the Petri net theory and CPN Tools model tools. Then the Dolev-Yao attack model was introduced to evaluate the security of the original model of the protocol. It was found that the protocol had replay, deception, and tampering 3 Man-in-the-middle attack vulnerability. Finally, a new solution is proposed for the loopholes in the protocol, which uses timestamps to enhance the security of the conversation between devices. It again uses the CPN model detection tool to verify the security of the new solution. Through verification, it can be found that the new solution improves the difficulty of the attack, thereby ensuring the ability of the BACnet/IP protocol to resist replay, deception, and tampering attacks.

KeyWords: BACnet/IP Protocol; Colored Petri Nets; Formal Analysis; Safety Assessment; Time Stamp

1 Introduction

Intelligent buildings provide people with a safe, efficient, comfortable and convenient building environment [26]. The development of building intelligence has always been closely related to the Internet. With the rapid development of Internet technology, Internet-based intelligent building application technologies and products have emerged in large numbers. In order to manage building equipment more efficiently and conveniently, the interconnection between the BACnet network [20] and the Internet has become an inevitable trend. However, because the BACnet protocol itself did not consider security issues at the beginning of its design, many common network attack methods can also threaten the BAS (Building Automation System) [15] connected to the Internet, directly attacking the BACnet server or building automation equipment, causing network paralysis.

In the field of smart buildings, the BACnet network has been proven to be insecure [12, 23]. Literature [18] designed a context-aware intrusion detection framework based on abnormal behavior analysis widely deployed in BACnet networks to accurately detect abnormal events triggered by network attacks or any functional failures. Literature [9] elaborated on the vulnerable types of BACnet and Internet connection and gave corresponding countermeasures under different attack methods. The literature [11, 16] conducted a detailed study on the identification and authentication, denial of service, eavesdropping, and buffer overflow in the core functions of the BACnet network, and added remote management technologies for corporate intranet and Internet connections. However, the above-mentioned documents have not done formal modeling analysis on the internal data transmission security of the protocol and proposed effective security assessment methods and improvement schemes.

Therefore, this article uses formal methods to conduct security modeling research on the BACnet/IP protocol, which is widely used in the field of building automation systems, but lacks effective security research. The main work includes the following three aspects:

1) A model detection method based on colored Petri net theory and Dolev-Yao attack method was proposed;

2) The BACnet/IP protocol equipment authentication mechanism was analyzed in detail and formalized description. The protocol is modeled by modeling tools, and the consistency of the model was verified. The Dolev-Yao attacker model was introduced to evalu-

ate the security of the protocol, and the loopholes in the protocol were found;

3) A new scheme for introducing a time stamp mechanism to enhance the strength of device authentication was proposed for the security vulnerabilities in the protocol, and the new scheme was also re-verified.

2 Related Theories and Concepts

2.1 Overview of BACnet/IP Protocol

At present, BACnet network has been widely used in intelligent buildings, however, in order to better realize the management and control of building equipment, it is extremely necessary to interconnect multiple different BACnet network equipment through the Internet to realize the interconnection and interoperability of equipment in different regions. The BACnet standard currently uses two technologies to realize the connection between the IP network and the BACnet network: One is the PAD technology, and the other is the BACnet/IP technology [21].

PAD technology is a relatively mature and developed BACnet network and Internet interconnection technology. However, this technology lacks flexibility in its use. First, when the configuration data of the network device is changed, all data and information of the PAD device must also be completely modified to maintain the correctness of the routing information. Second, when new devices are dynamically added to the BACnet network via the Internet, it is difficult and costly. In view of the shortcomings of PAD, the IP working group of the BACnet Standards Committee (SSPC135) developed a more scalable and flexible BACnet interconnection protocol [17]. The interconnection protocol is the BACnet protocol based on IP, referred to as the "BACnet/IP" standard for short. The main function of BACnet/IP is to directly encapsulate BACnet data packets into IP frames for data transmission. The BACnet/IP protocol mainly includes the following 7 parts:

1) Proposed and described in detail the concept of a BACnet network composed of one or more IP subnets.

2) Describes the use of BACnet non-confirmed services for the management of local, remote and global broadcasts between BACnet/IP networks and non-BACnet/IP networks.

3) A new device is defined, called BACnet Broadcast Management Device (BBMD), for broadcast management.

4) By defining a new protocol layer called BACnet Virtual Link Layer (BVLL), BACnet/IP communication is realized.

5) Provides a method for external devices to access the BACnet/IP network.

6) Provides routing between BACnet/IP networks and non-BACnet/IP networks.

7) Specifies the routing between multiple BACnet/IP networks. The BACnet architecture after joining the BACnet/IP protocol is shown in Figure 1.

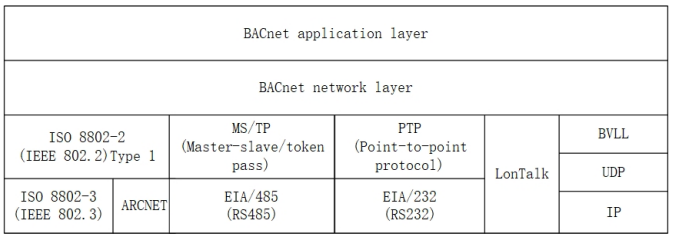

Figure 1: BACnet/IP architecture diagram

2.2 Colored Petri Nets and Modeling Tools

The concept of Petri net was first proposed by German scientist Carl Adam Petri, and then many expanded concepts appeared, such as time Petri net, stochastic Petri net, CPN, *etc.* [1, 22]. Colored Petri Net (Colored Petri Net, CPN) is an advanced form of basic Petri Net. It increases the ability of P/T net to simulate and describe the model. It also has strict formal definitions. In terms of formal analysis of security protocols, CPN, as a high-level network system, integrates the advantages of Petri nets and high-level programming language abstract mechanisms, has the ability to describe types and hierarchical structures, and can describe a complex system compactly and simplified [25]. It has a rich and flexible color set and function definition, suitable for the standardized definition of the message in the security protocol. CPN modeling can also perform incremental syntax checking and code generation, which to a certain extent also ensures the correctness of the model. The formal modeling tool CPN Tools has features such as editing, simulation, state space analysis and performance analysis, and can accurately locate errors generated through a feedback mechanism. This tool is developed by Aarhus University in Denmark based on Design/CPN. The user graphical interface (GUI) is designed using good man-machine interface technology. It can not only edit, simulate and analyze colored Petri nets, but also support time CPN and hierarchical CPN, with the help of CPN tools, users can not only model easily, but also simulate and analyze parallel systems [3, 4].

3 BACnet/IP Protocol Equipment Certification HCPN Modeling

3.1 BACnet/IP Protocol Equipment Authentication Message Flow Model

The BACnet/IP protocol device authentication message flow (MSC) model is shown in Figure 2. RequestKey means requesting the session key from the key server, Ks means the session key distributed by the key server to devices A and B, IDA means the device number of A, IDB means the device number of B (the device number is unique), and Ka means The master key of device A, Kb represents the master key of device B (only shared with the key server). Authenticate represents the authentication request service between peer entities, Pseudo Random Number represents the pseudo-random number in the message, ComplexACK represents the complex response message, and Modified Random Number represents the modified random number in the response message.

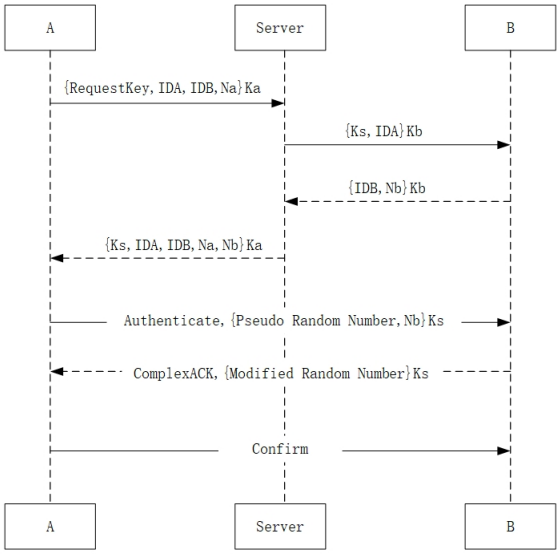

Figure 2: Authentication mode message flow model (MSC)

The equipment certification process is as follows:

1) Devices A and B run the DES algorithm to generate their own private keys Ka and Kb (only shared with the key server).

2) Device A initiates a "RequestKey" request to the key server to request the session key Ks for communication between devices A and B.

3) After receiving the request message from device A, the key server generates the session key Ks, uses the Kb of device B to encrypt Ks and IDA, and sends it to device B.

4) Device B uses Kb to encrypt and send its own device number IDB to the key distributor, and the key distributor verifies the device number of device B.

5) After decrypting using Kb, the key server first compares the obtained IDB with the one sent by device A. If they are consistent, use the Ka of device A to encrypt Ks and IDB and send them to device A.

6) Device A receives Ks and starts to authenticate device B. Device A initiates an Authenticate request. The protocol data part and Pseudo Random Number of this request are encrypted with Ks and sent to B.

7) Device B decodes the received authentication request of device A, changes the Pseudo Random Number to Modified Random Number, uses Ks to encrypt, and returns a ComplexACK message to device A.

8) Device A decrypts the received response message. If the ComplexACK packet contains the correct Modified Random Number, the device authentication is successful.

3.2 Message Analysis and Color Set Definition

The modeling process introduces multiple types of color set definitions. The color set ID defines the unique device numbers of devices A and B. The color set KEY defines the master keys (Ka and Kb) of the two devices and the session distributed by the key server. The key Ks, the color set NONCE defines the pseudo-random number Na and the modified random number Nb used in the equipment authentication phase. There are two encryption and decryption formats used in the communication process. One is that the key server uses the pre-shared master keys Ka and Kb of device A and device B to decrypt the data information obtained, and the other is device A and device B. B uses the master key Ka, Kb to encrypt its own device number and request information. According to the CPN ML language, use the product type color set definition to integrate the main information and the key according to a specific method to represent the encryption and decryption operations, thereby obtaining four message formats. On this basis, use the record (record) type color set definition for subsequent encrypted messages.Due to the complexity of the BACnet/IP protocol, there are many color sets defined. Here we only list some important related color set definitions, as shown in the Table 1.

3.3 HCPN Model Establishment

3.3.1 Top-Level Model

Based on the above analysis, the corresponding model diagram can be drawn, as shown in Figure 3. The double-

Table 1: Definition of color set for BACnet/IP protocol equipment certification

Category	Color set name	Color set definition
Preliminary preparation	ID	colset ID=with A— B;
	KEY	colset KEY=with Ka—Kb—Ks;
	NONCE	colset NONCE=with Na—Nb;
	CONFIG	colset CONFIG=product ID*ID;
	CRY1	colset CRY1=product KEY*KEY;
	CRY2	colset CRY2=product ID*KEY;
Key distribution	MSG1	colset MSG1=product CONFIG*KEY;
	MSG2	colset MSG2=product CRY2*KEY;
	MSG3	colset MSG3=product ID*KEY;
	MSG4	colset MSG4=product CRY2*KEY;
Equipment certification	ACK	colset ASK=record m:MSG*k:KEY;
	RSP	colset RSP=product NONCE*NONCE;
	RPL	colset RPL=record r:RSP*k:KEY;
	CFM	colset CFM=record n:NONCE*k:KEY;
Data	PACKET	colset PACKET=union MSG1+MSG2+MSG3+MSG4;

line rectangle in the figure is the alternative transition, and each substitution transition corresponds to a subpage of the physical layer. The three alternative transitions represent three different entities, from left to right: Device A, Key Server, and Device B. The places P1 to P7 represent the communication network. The top-level model completely simulates the BACnet/IP protocol device authentication session process, including the key distribution process and the device authentication process, as well as the communication data processing process.

3.3.2 Physical Layer Model

As shown in Figure 4, the model of entity A in BACnet/IP protocol equipment authentication includes 16 message places and 8 transitions. This model describes the sending and receiving process of the message initiator A requesting the key server Server to obtain the session key and initiating identity authentication to the message responder B. In the model, the indexAB and KEYA1 of the fusion place are used to configure the identity information and key generation parameters of the session initiator before the session occurs. Transition T1 integrates the message into MSG1 type and sends it to the port place p1;When the entity A initiates a session, the model is in the session participation state, and then the data will be sent to the responder, and the responder is entity B in the model;When the corresponding key server receives the message of entity B, it sends a message of type MSG4 to the port place p4. The initiator uses the shared key Ka with the key server to decrypt and obtain the session key Ks. Transition encA obtains the pseudo-random number Na from the place NumA and adds it to the data packet and integrates it into ACK format information and sends it to device B for identity authentication.

As shown in Figure 5, the model describes the receiving and processing process of entity B receiving the session key distributed by the key server and the data message that initiates identity authentication on entity A.When configuring the session participation mode, you need to introduce the index place, the specific function of the place is to set each entity and its identity information;After the data is sent to the message responder, that is, entity B participates in the session to perform Step 2, Step 3, and Step 6. Entity B in MSG2 decrypts the received data with the shared key Kb between the key server and obtains the session key Ks and the identity of the initiator entity A, and saves the obtained session key in the places KEYS2 and KEYS4. Then send an MSG3 type message to authenticate with the key server.

As shown in Figure 6, the model describes the process in which the key server Server distributes the session keys for identity authentication to entities A and B. The key server receives the message MSG1, judges the encryption key, if it is Ka, then performs a decryption operation to obtain the identity of the session initiator and the responder, and save it to the corresponding place indexB1. Then according to the identity of the responder in the message MSG1, synthesize and send the message MSG2, and send the session key Ks and the identity of the session initiator to the responder. The key server receives and uses the shared key Kb with the key server to decrypt the message MSG3 sent by the responder, and determine whether the responder's identity is correct.Finally, the server uses Ka to encrypt the session key Ks and responder identity according to the initiator identity in the message MSG1, synthesizes and sends the message MSG4.

3.3.3 Functional Consistency Verification of the Original Model

The State Space tool component in the CPN Tools tool can calculate the original model state space and generate a state space report. The details are shown in the

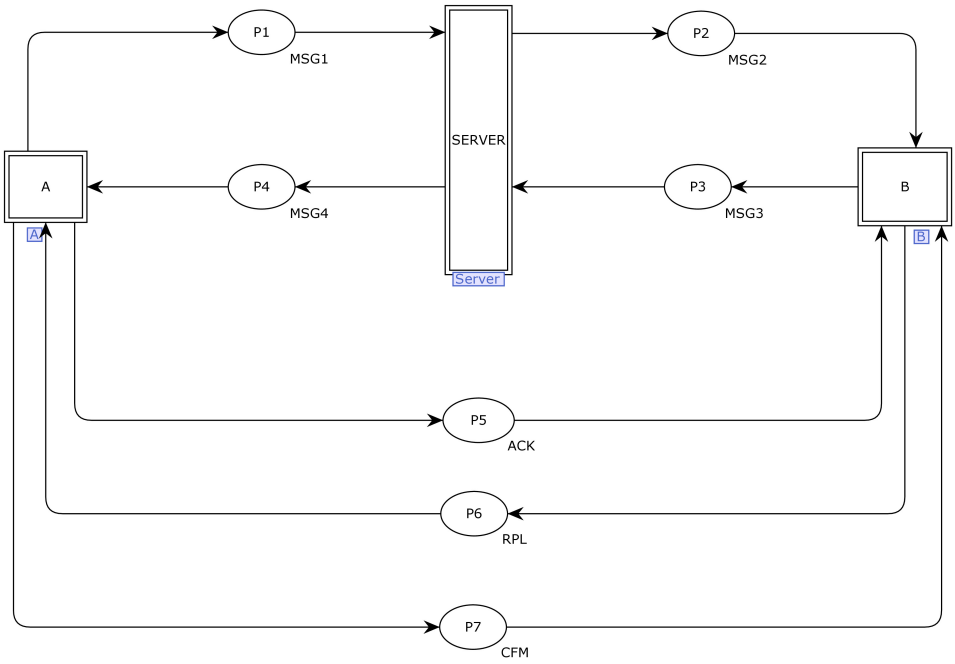

Figure 3: CPN top-level model of BACnet/IP protocol equipment certification

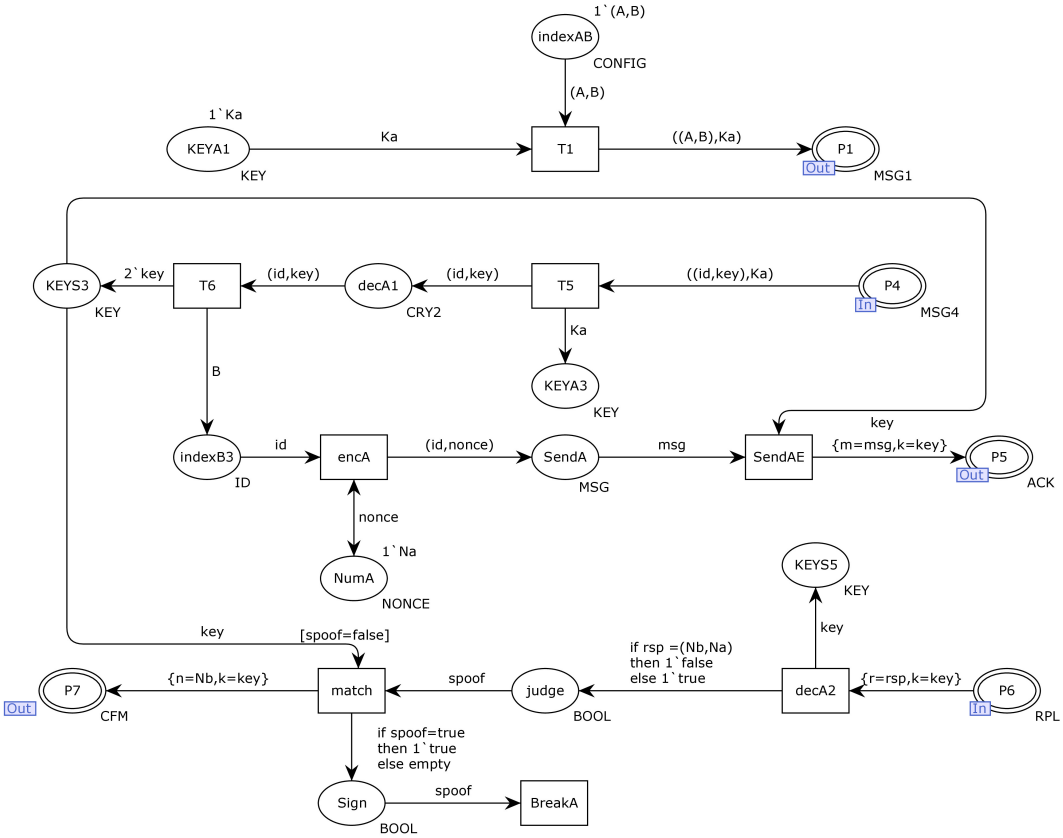

Figure 4: CPN model of entity A certified by BACnet/IP protocol equipment

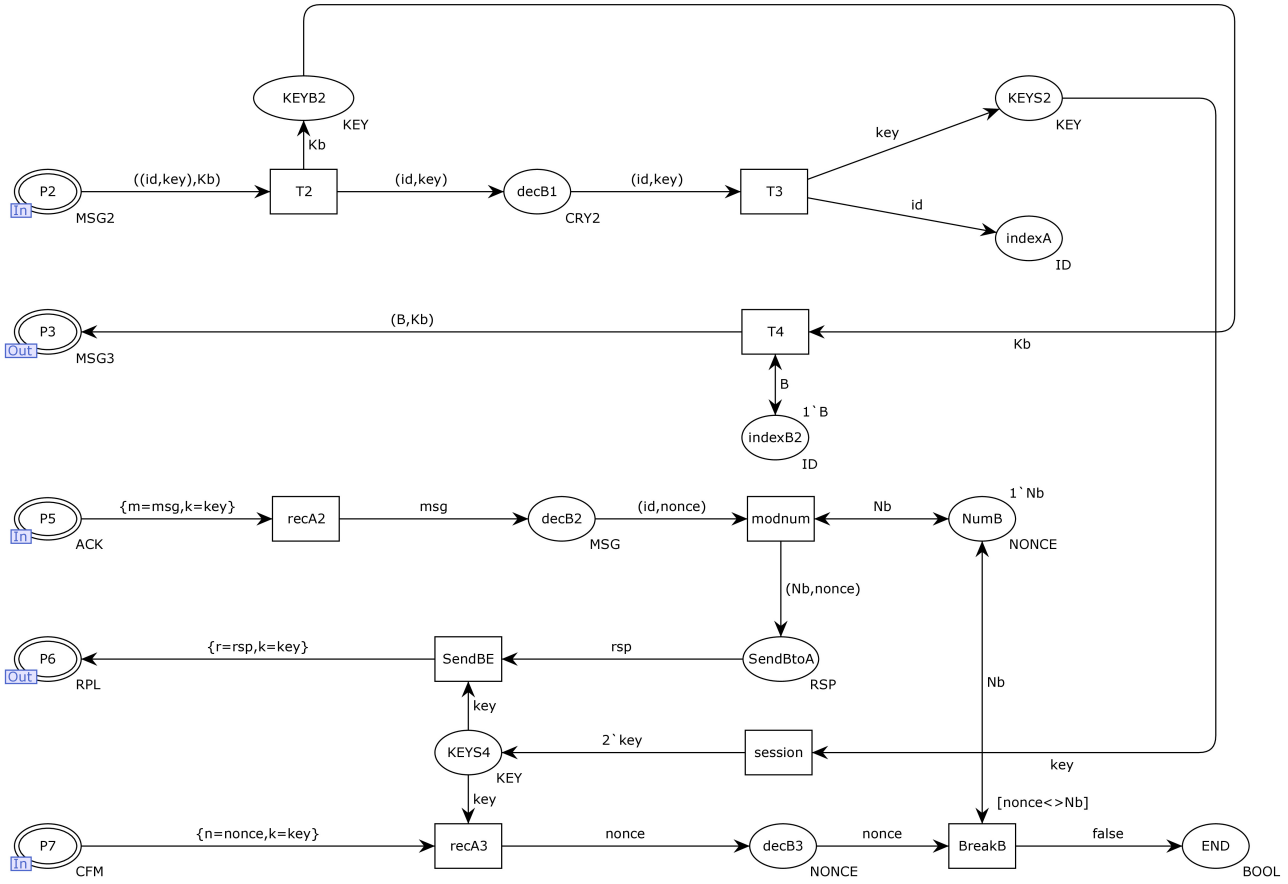

Figure 5: CPN model of entity B certified by BACnet/IP protocol equipment

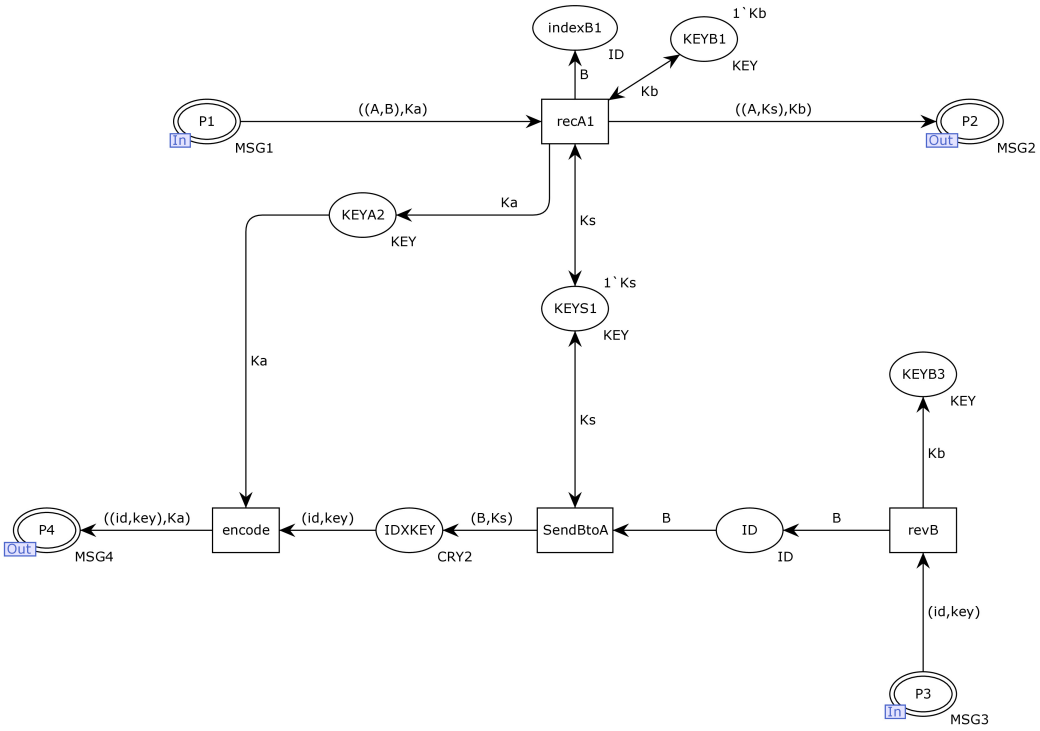

Figure 6: The CPN model of the key server for BACnet/IP protocol device authentication

Table 2: State space query results of HCPN model certified by BACnet/IP protocol equipment

Categorys	No.	Name
State space node	40	/
Directed arc	59	/
Strongly connected node	40	/
Strongly connected arc	59	/
Master state node	0	/
Dead node	1	[40]
Death transition	2	BreakA/BreakB
Live transition	0	/

following Table 2.

Perform state analysis on the CPN model, focusing on investigating the node statistics, bounded data, and liveness data, *etc.*, and then compare the survey results with the expected state to determine whether the model is consistent with expectations and whether it meets the protocol specifications. According to the BACnet/IP protocol device certification specification, when a device initiates an authentication request, the data packet will carry the generated pseudo-random number. Whether the device can be successfully authenticated depends on whether the modified random number in the response data packet meets expectations.When the device is successfully authenticated, device A will trigger the transitions decA2 and match instead of BreakA, and device B will trigger the transitions recA and decB3, but not the transition BreakB, so it can be predicted that the transitions BreakA and BreakB are two death transitions of the model. The model automatically ends after the certification request is completed. According to this feature, it can also be judged that there should be no live transitions when the model is in the terminated state.

4 Protocol Security Evaluation Based on Attacker Model

4.1 Dolev-Yao Attack Model

Research shows that attackers'attack methods include attacks on cryptographic algorithms, attacks on the protocol itself, and attacks on both cryptographic algorithms and the protocol itself.Under the premise of the perfect password assumption, the attacker can also launch passive or active attacks on the protocol itself. Passive attacks include eavesdropping and traffic analysis, but the attacker only passively detects the data stream transmitted in the network, and it is difficult to detect passive attacks on the protocol. Therefore, passive attacks can only collect effective information, prepare for active attacks, and will not conduct malicious attacks against the protocol. Active attacks on the protocol include interception attacks [27], replay attacks [13], integrity violation attacks [10], type error attacks, concurrent session attacks, and denial of service attacks [2], *etc.*

In 1983, Dolev and Yao published an important document in the history of security protocol development [5]. In this paper, Dolev and Yao proposed to distinguish the security protocol itself from the specific cryptographic algorithm used by the security protocol, and analyze the correctness, security and redundancy of the security protocol itself based on the assumption of a complete cryptographic system [8]. As a result, the analysis of security protocols is clearly divided into two different levels:First study the security nature of the security protocol itself, and then discuss the specific details of the implementation level and the specific cryptographic algorithm used. Dolev and Yao also established the corresponding attacker model to accurately describe the attacker's behavior:

1) Attackers can eavesdrop and intercept all messages passing through the network;

2) Attackers can store intercepted or self-constructed messages [6];

3) Attackers can send intercepted or self-constructed messages;

4) The attacker can participate in the operation of the protocol as a legal subject [24].

4.2 Protocol Security Evaluation Model Establishment

Since the Delov-Yao attacker model will generate a large number of repeated messages, it is easy to cause the state space to explode, which limits the use of the model to a certain extent, so this article adopts an improved Delov-Yao attacker model. On the one hand, the attack is applied to the arc expression in a parameterized form to reduce the state space;On the other hand, it restricts the messages that the attacker can split and combine, and only split and combine key messages that are effective to organize the attack into a disordered state to prevent the explosion of state space [19].

The security assessment model of the protocol security assessment model constructed based on the improved Delov-Yao attack model, as shown in Figure 7. According to Delov-Yao's attack hypothesis, the attacker has the ability to eavesdrop, tamper, and replay. It can pretend to be the initiator and responder of the session, but not a trusted third-party server. As shown in the figure, the blue-labeled arc expression of the transition AT simulates tampering attacks and replay attacks, and the transitions in the purple-labeled part and the library simulate spoofing attacks.Different definition places correspond to different color sets, and their functions are also different.For example, the color set of resovle is defined as DB, whose function is to store the intercepted information;The main function of the definition place CB1 is to store and split the original message.Different types of transitions play

Table 3: State space query results of BACnet/IP protocol equipment certification security evaluation model

Categorys	Numbers
State space node	248
Directed arc	495
Strongly connected node	248
Strongly connected arc	495
Dead node	3
Death transition	2

different roles. For example, the transition CB saves the decrypted message and key to the places CB1 and CB2 respectively. In the process of changing AB to synthesize messages, it is also necessary to introduce concurrency control place SP to restrict and regulate.

4.3 Analysis of State Space Table of Safety Assessment Model

When the three attacks are launched at the same time, the corresponding state space report of the security assessment model is shown in Table 3. The static characteristics of the system are represented by statistical data, which have two attributes, namely: state space attributes and strongly connected graph attributes. The model includes a variety of elements, such as node identifiers, arc connecting nodes, the former is represented by nodes. The result of the state is full, which means that the corresponding appearance graph is complete. The space state table provides a variety of operating tools. By performing Home Properties and Live Properties operations, you can see the model's identification name, live transition name, *etc.*Through the above method, the state space query result can be obtained.

4.4 Protocol Security Analysis

The number of arcs of the security evaluation model has increased significantly compared with the original model, which meets the research needs. In addition, because the number of arcs and the number of nodes are the same, it can be seen that there is no iterative behavior in the security evaluation model, and the added Delov-Yao attack is also verified. The author model is effective. It can be seen from the report that the model generates a total of 248 state space nodes, including 3 dead nodes, which shows that unexpected behaviors have occurred in the security assessment.Use ListDeadMarking() to determine the serial numbers of 3 dead nodes. Through the NodeDescriptor() function to check the status of all dead nodes, it is found that the attacker at node 236 has successfully forged a legitimate participant to tamper with the session key between devices A and B to Kt and initiate a replay attack;Node 244 is caused by an unexpected final state of the protocol due to a spoofing attack.

5 Protocol Improvement and Analysis

5.1 A New BACnet/IP Protocol Equipment Authentication Security Scheme Based on HCPN Modeling

Through the evaluation test of the security evaluation model, it can be seen that the BACnet/IP protocol device authentication mechanism does not meet the design requirements of device authentication in the protocol specification, and does not have the ability to resist tampering, replay and other attacks. In response to the above-mentioned security threats, this article proposes a protocol improvement scheme that introduces time stamps to strengthen the device authentication strength, which specifically includes security improvements in the key distribution phase and device authentication phase, and uses the security evaluation model again to improve the security of the protocol. Verified. The improved authentication message flow (MSC) model is shown in Figure 8. Timestamp adds time stamp information for the improved protocol.

The improved equipment certification process is as follows:

1) Devices A and B run the DES algorithm to generate their own private keys. Device A has a key Ka, and device B has a key Kb (only shared with the key server).

2) Device A sends a "RequestKey" request to the key server, requesting a session key to ensure the security of the logical connection to device B. The message contains the transmitted time stamp information and the identity of device A and device B.

3) After receiving the message from device A, the key server Server uses Ka to perform the data source identification process, determines whether the request is issued by device A, and then determines whether the timestamp meets the security requirements. If not, discard the data packet to stop the authentication process, and continue to use the DES algorithm to generate the session key Ks and use the master key Kb of device B to encrypt the session key Ks, IDA and time stamp information, and send it to device B.

4) After device B receives the message sent by the key server Server, it uses Kb to perform the data source identification process to determine whether it is sent by the key server Server and whether the timestamp meets security standards.Device B decrypts and stores the session key Ks to be used later, and uses Kb to encrypt the device number IDB and time information and send it to the key server. The key server verifies the device number of device B.

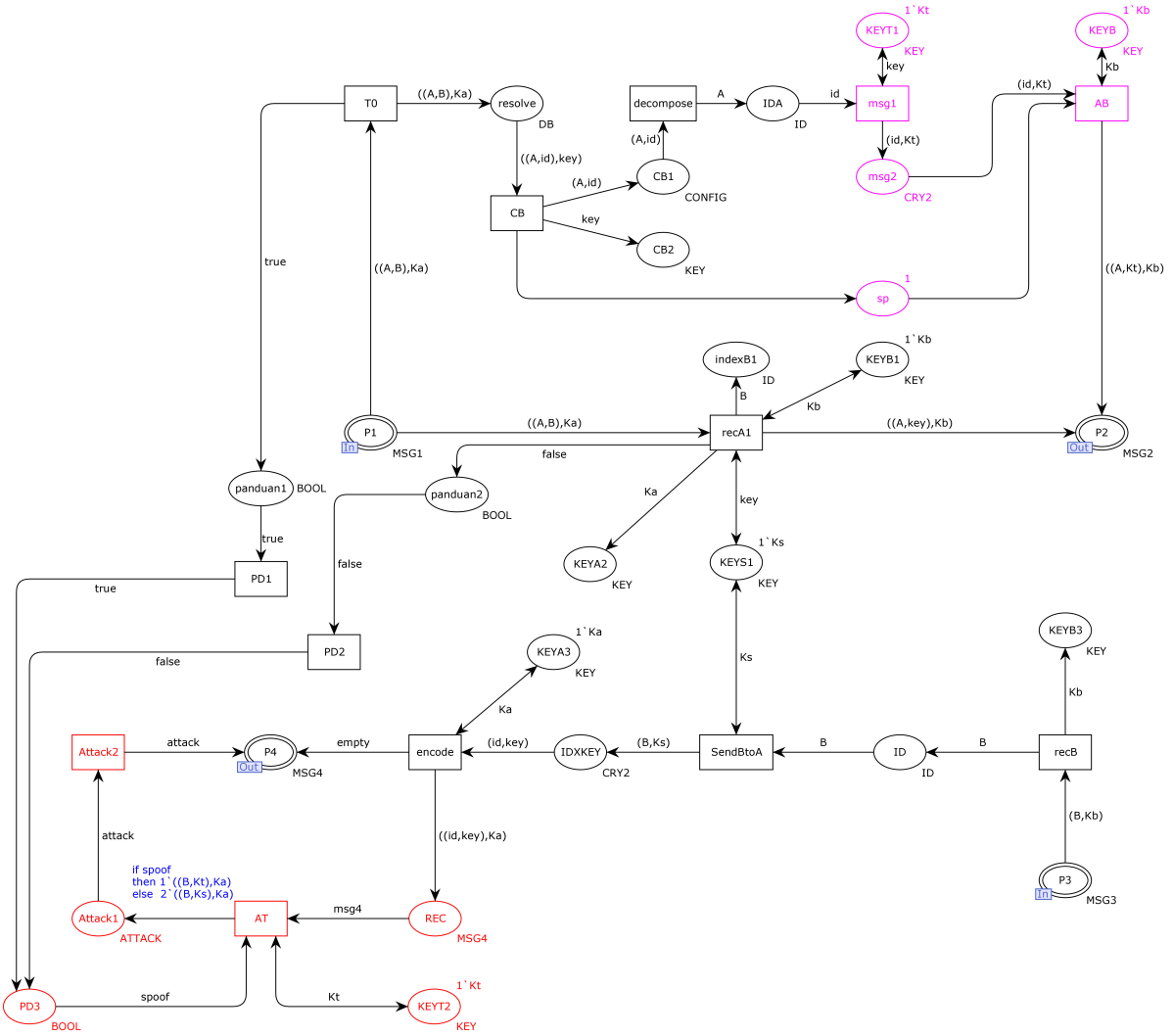

Figure 7: The security assessment model of BACnet/IP protocol equipment certification

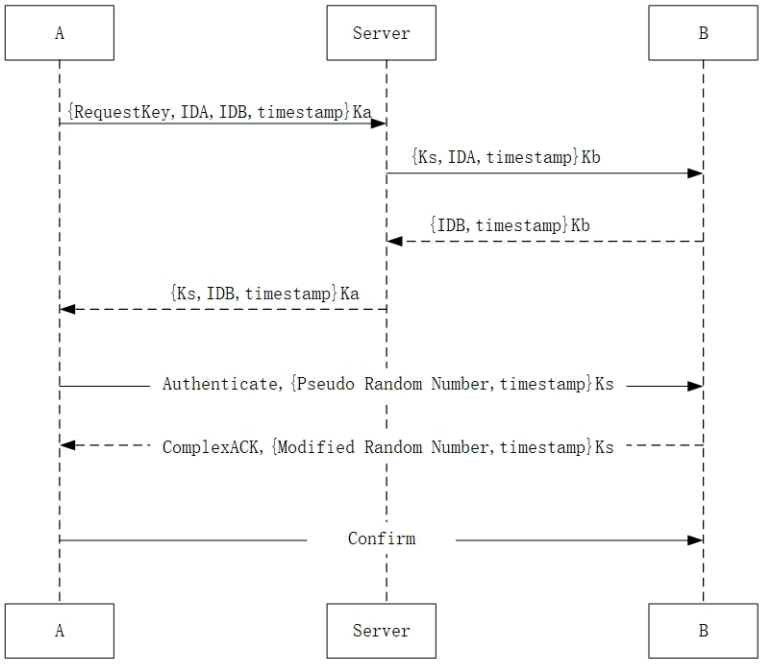

Figure 8: Improved authentication mode message flow model (MSC)

5) After the key server uses Kb for identification and decryption again, it first compares the obtained IDB with the one sent by device A. If they are the same, it uses the Ka of device A to encrypt Ks, IDB and the time stamp information, and sends it to device A.

6) Device A receives Ks and starts to identify device B. Device A generates an Authenticate service request. The protocol data part, Pseudo Random Number and time information of this request are encrypted with the session key Ks and sent to device B.

7) Device B decodes the received authentication request of device A, changes the Pseudo Random Number to Modified Random Number, uses Ks to encrypt, and returns a ComplexACK message to device A.

8) Device A decodes the received response message and checks whether the ComplexACK packet contains the correct "Modified Random Number". If it is correct, the device is successfully authenticated and can start communication.

5.2 Improved CPN Physical Layer Model for Equipment Certification

5.2.1 Improved CPN Model of Equipment Certification Entity A

Based on the modeling of the original entity A, a new color set T representing time stamp information and two constant definitions representing time delay are added. The constant Prdelay represents the operation delay of the places in the model to the data, and the constant Trdelay represents the maximum possible time for normal message transmission in the BACnet network. If this limit is exceeded, the message is lost or the system has been invaded. In order to fully verify the relevant security properties, the message recipient should check the time value before decrypting the message for processing. Figure 9 shows the improved CPN model of device authentication entity A.

5.2.2 Improved CPN Model of Device Authentication Entity B

Figure 10 shows the improved CPN model of the device authentication entity B. Its behavior includes receiving the session key Ks sent by the key server Server, responding to the device A with a modified random number for identity verification, and verifying the time stamp information and calculations. The new place Timestamp2 is used to store and calculate the current timestamp information of the device.

Table 4: Comparison of state space of security evaluation model before and after BACnet/IP protocol equipment certification improvement

Categorys	Before	After
State space node	248	1475
Directed arc	495	4193
Strongly connected node	248	1475
Strongly connected arc	495	4193
Dead node	2	5
Death transition	2	2

5.2.3 Improved CPN Model of Device Authentication Key Server Server

The behavior of the key server Server mainly includes identifying and decrypting messages from device A, and obtaining the device numbers of devices A and B, and then encrypting the session key Ks in two messages and distributing them to devices A and B. In the CPN model of the key server with the attacker, two Timestamp places are also added to store and calculate timestamp information, which enriches the attacker's ability to split combined messages. Figure 11 shows the improved BACnet/IP protocol device authentication key server server CPN model.

5.3 State Space Analysis of Improved CPN Model

Table 4 shows the comparison of the state space results of the improved BACnet/IP protocol equipment certification security evaluation model with that before the improvement. Due to the introduction of timestamps and the addition of related color definitions, the model correspondingly increases the number of transitions and places, and the number of states and directed arcs after the improvement are significantly increased compared to before the improvement.

In the security evaluation phase, add attack parameters to the arc expression to verify whether the improved BACnet/IP protocol device authentication can resist both tampering and replay attacks. The SML statement investigation of the dead state in the above state space report shows that at node 35, because the attacker's decomposition and synthesis message time exceeds the threshold, device B discards data packets, making subsequent attacks invalid, and nodes 1441, 1452, and 1474 are sent to ports. The message MSG4 of the library P4 was intercepted and replayed by the attacker, which caused the system token to be exhausted and the final authentication could not be completed. The improved BACnet/IP protocol equipment authentication can resist information tampering and message replay attacks, and meet the authentication attribute requirements defined by the BACnet/IP protocol equipment authentication specification.

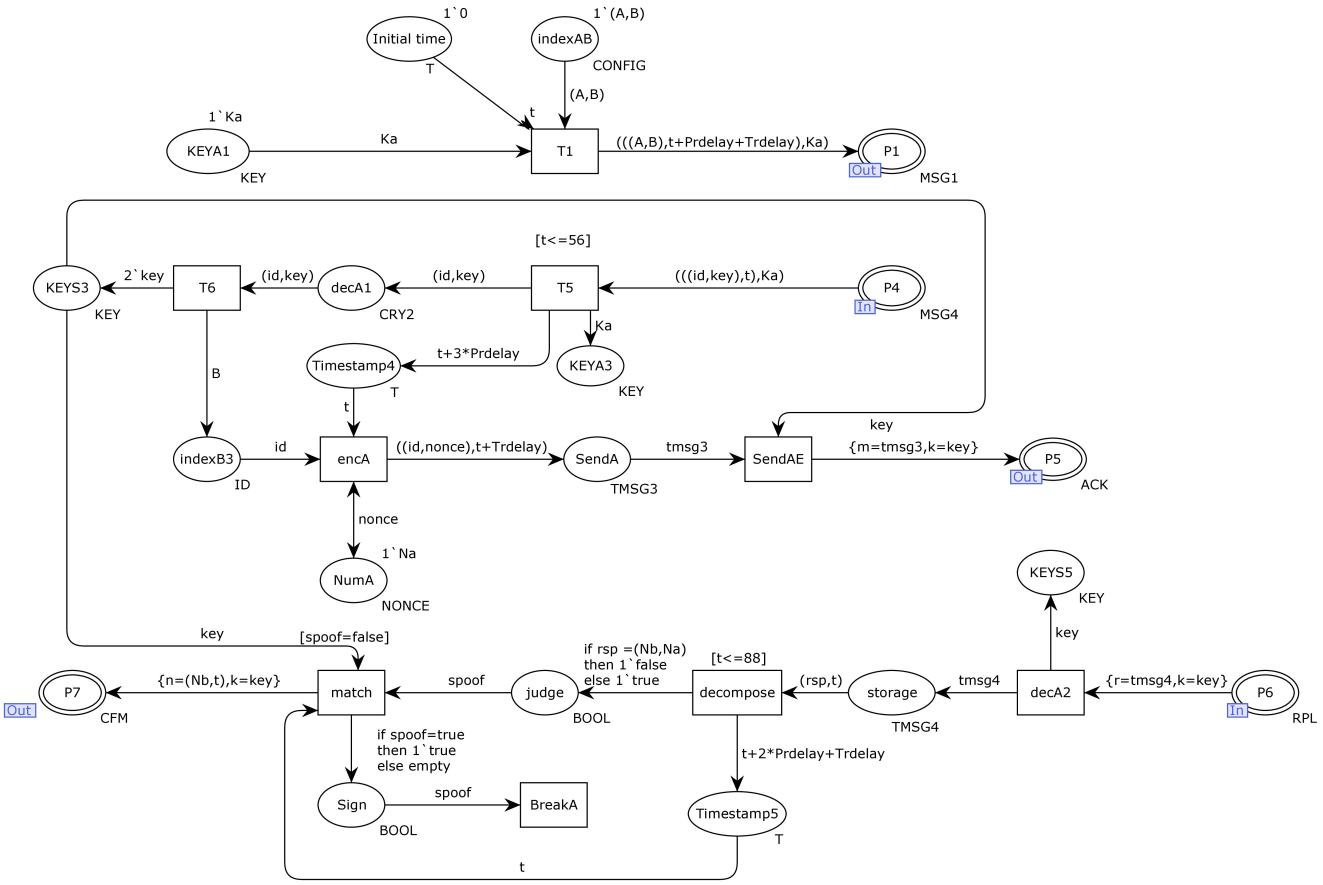

Figure 9: The improved BACnet/IP protocol device authentication entity A's CPN model

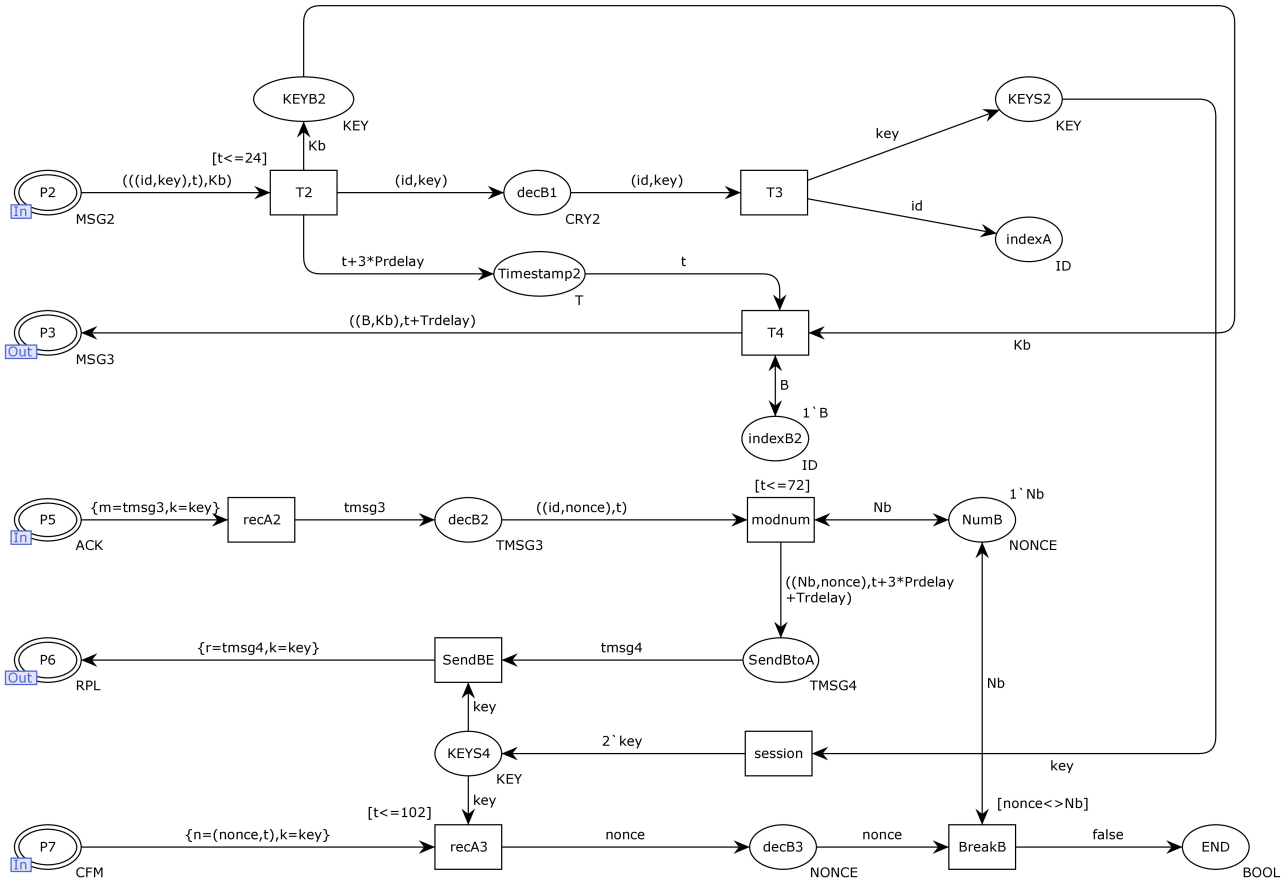

Figure 10: CPN model of entity B for improved BACnet/IP protocol equipment authentication

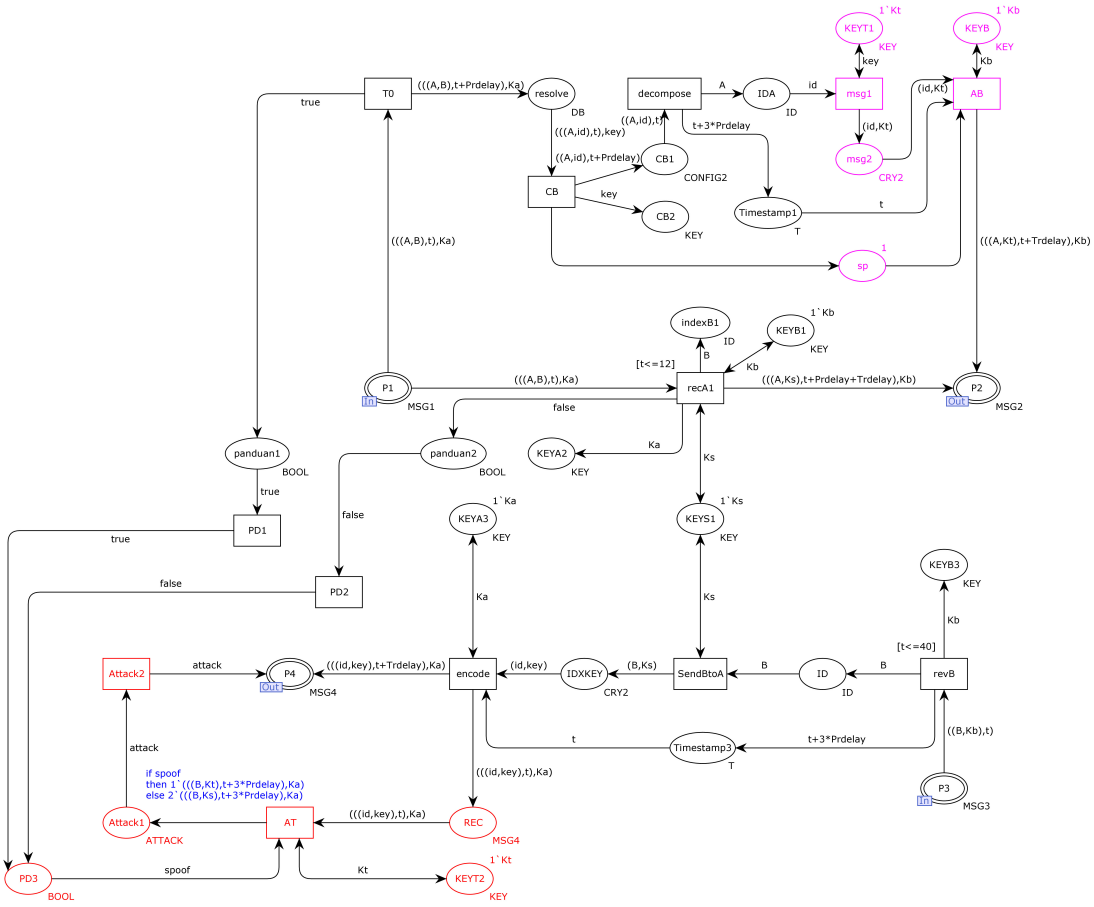

Figure 11: The improved BACnet/IP protocol device authentication key distributor Server CPN model

6 Conclusion

This paper, guided by colored Petri net theory and the Delov-Yao attack method, takes the building automation network communication protocol, BACnet/IP equipment certification, as the research object and uses the CPN Tools model detection tool to formalize the BACnet/IP protocol modeling and safety assessment. By modeling and analyzing the equipment authentication mechanism of the protocol, mining and verifying security vulnerabilities, a security improvement plan that uses timestamps to enhance the authentication strength between devices is proposed. The security of the proposed scheme is verified using CPN model detection tools. The next step is to improve the fine-grained protocol modeling based on the current research and verify the security of other protocol services and other forms of attacks.

References

[1] M. Abbaszadeh, S. Saeedvand, "Weak consistency model in distributed systems using hierarchical colored petri net," *Journal of Computers*, vol. 13, no. 2, pp. 236-243, 2018.

[2] L. An, G. H. Yang, "Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks," *IEEE Transactions on Cybernetics*, no. 99, pp. 1-12, 2018.

[3] D. Arena, F. Criscione, N. Trapani, "Risk assessment in a chemical plant with a CPN-HAZOP tool," *IFAC-Papers OnLine*, vol. 51, no. 11, pp. 939-944, 2018.

[4] I. V. Artamonov, A. P. Sukhodolov, "CPN tools-based software solution for reliability an alysis of processes in microservice environments," *International Journal of Simulation: Systems,Scienceand Technology*, vol. 19, no. 6, 2018.

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

[6] Y. Fang, "Research on automatic verification method of security protocol based on model checking,"Hunan University,2015.

[7] O. Gasser, Q. Scheitle, C. Denis, *et al.*, "Security implications of publicly reachable building automation systems," *IEEE Security and Privacy Workshops (SPW'17)*, 2017. DOI: 10.1109/SPW.2017.13.

[8] J. A. Herzog, "Computational interpretation of Dolev–Yao adversaries," *Theoretical Computer Science*, vol. 340, no. 1, pp. 57-81, 2005.

[9] T. Hong, "Research on the security problems and countermeasures of BACnet network," Chongqing University,2006.

[10] Information Technology - Data Integrity; Reports on Data Integrity from North China Electric Power University Provide New Insights (Data Integrity

Attack Detection for Node Voltage In Cyber-physical Power System)[J]. Information Technology Newsweekly,2020.

[11] W. Kastner, G. Neugschwandtner, S. Soucek, "Communication systems for building automation and control," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1178-1203, 2005.

[12] J. Kaur, J. Tonejc, S. Wendzel, "Securing BACnet's pitfalls," in *The 30th International Information Security and Privacy Conference*, pp. 616-629, 2016.

[13] J. Kim, J. S. Song, "A simple and efficient replay attack prevention scheme for LoRaWAN," in *The 7th International Conference*, pp. 32-36, 2017.

[14] L. Li, F. Basile, Z. Li, "An approach to improve permissiveness of supervisors for GMECs in time petri net systems," *IEEE Transactions on Automatic Control*, no. 99, pp. 1-1, 2019.

[15] K. Lohia, Y. Jain, C. Patel, "Open communication protocols for building automation systems," *Procedia Computer Science*, vol. 160, pp. 723-727, 2019.

[16] M. Mylrea, S. N. G. Gourisetti, "Cybersecurity and optimization in smart "Autonomous" buildings," in *Autonomy and Artificial Intelligence: A Threat or Savior?*, pp. 263-294, 2017.

[17] M. Nast, B. Butzin, F. Golatowski, *et al.*, "Performance analysis of a secured BACnet/IP network," *The 15th IEEE International Workshop on Factory Communication Systems (WFCS'19)*, 2019. DOI: 10.1109/WFCS.2019.8758009.

[18] Z. Pan, S. Hariri, J. Pacheco, "Context aware intrusion detection for building automation systems," *Computers & Security*, vol. 85, pp. 181-201, 2019.

[19] M. Peacock, M. N. Johnstone, C. Valli, "An exploration of some security issues within the BACnet protocol," in *Information Systems Security and Privacy*, pp. 252-272, 2018.

[20] Z. Qing, D. Shiyun, "Building equipment management system based on BACnet protocol," *Intelligent Building*, no. 06, pp. 58-60, 2020.

[21] A. G. Siemens Schweiz, Patent Issued for System And Method For Isolating Device Communications In A BACnet/IP Building Automation Network (USPTO 10,812,287)[J]. Internet Weekly News,2020.

[22] M. Simon, D. Moldt, D. Schmitz, *et al.*, "Tools for curry-coloured petri nets," in *Application and Theory of Petri Nets and Concurrency*, pp. 101-110, 2019.

[23] J. Xiaoyan, "Formal security assessment and improvement of BACnet protocol based on HCPN model checking method," Lanzhou University of Technology,2020.

[24] W. Xiong, L. Robert, "Threat modeling–A systematic literature review," *Computers & Security*, vol. 84, pp. 53-69, 2019.

[25] T. Xuecheng, "Security analysis of EtherNet/IP protocol in industrial control system," Lanzhou University of Technology,2020.

[26] J. Yuzheng, "Application of PKI technology in information security protection of military intelligent buildings," Shan Dong University,2006.

[27] H. Zhou, W. Yang, C. Yang, "Privacy preserving consensus under interception attacks," *The 36th Chinese Control Conference (CCCC'17)*, 2017. DOI: 10.23919/ChiCC.2017.8028702.

Acknowledgments

This research is supported by The National Natural Science Foundation of China (Grant No. 61762060), Educational Commission of Gansu Province, China (Grant No.2017C-05), Foundation for the Key Research and Development Program of Gansu Province, China (Grant No.20YF3GA016). Tao Feng is the corresponding author.

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.

Zhao Si-Meng, was born in 1996, CCF member.He is a master's student at lanzhou university of technology.His 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.