Hindawi
Security and Communication Networks
Volume 2021, Article ID 8090547, 15 pages
https://doi.org/10.1155/2021/8090547

Research Article

Formal Security Evaluation and Improvement of Wireless HART Protocol in Industrial Wireless Network

Fuyuan Luo, Tao Feng, and Lu Zheng

School of Computer and Communication, Lanzhou University of Technology, LanZhou 730050, China

Correspondence should be addressed to Tao Feng; fengt@lut.cn

Received 6 August 2021; Revised 21 October 2021; Accepted 3 November 2021; Published 23 November 2021

Academic Editor: Chien Ming Chen

With the rapid development of wireless communication technology in the field of industrial control systems, Wireless HART is an international wireless standard, because of its low cost and strong scalability, as well as its wide range of applications in the industrial control field. However, it is more open communication so that the possibility of increased attacks by external. At present, there are many types of research on wireless protocol security at home and abroad, but they all focus on the realization of the security function of the protocol itself, which has certain limitations for the formal modeling of the protocol security assessment. Taking into account the aforementioned research status, this paper takes the Wireless HART protocol as the research object and adopts the model detection method combining eCK model theory and colored Petri net theory to evaluate and improve the security of the protocol. First, the colored Petri net theory and CPN Tools modeling tool were introduced to verify the consistency of the original model of the protocol. And the eCK model was used to evaluate the security of the original protocol model. It was found that the protocol has two types of man-in-the-middle attack vulnerabilities: tampering and deception. Aiming at the attack loopholes of the protocol, an improvement plan was proposed. After improving the original protocol, CPN Tools modeling tool was used for security verification. It was found that the new scheme improvement can effectively prevent the existing attacks and reasonably improve the security of the protocol.

1. Introduction

With the rapid development of industrial intelligence and Internet of Things technology [1], the field of traditional industrial control systems has entered a new stage of development. The industrial control system is interconnected with a large amount of external network equipment and ensuring information security problem has become increasingly serious. The traditional industrial control protocol design is mostly to meet the communication and control functions of industrial systems [2, 3]. The security of the protocol has not been paid enough attention and the necessary protection means are lacking to ensure information security, allowing attackers to use the security loopholes in the protocol to cause damage to the industrial control system [4]. As more and more wireless communication protocols expose security issues, it is of great significance to the security research of the protocol itself.

The main contributions of this article include three aspects:

(1) The security research of Wireless HART protocol adopted formal model detection based on colored Petri net theory and eCK model adversary.

(2) The Wireless HART protocol was described in detail, the CPN modeling tool is used to model the protocol, and the consistency of the model is verified. The eCK model was introduced to evaluate the security of the protocol, and the security loopholes in the protocol were found.

(3) A new improvement plan was proposed for the security vulnerabilities of the protocol, and the adversary attack model modeling was used to verify the security of the new scheme.

1.1. Related Work. In the current stage of research, the methods used in the security analysis of the protocol itself are different. There are security researches based on engineering methods under protocol-specific systems and

security assessment methods for theoretical methods under protocol simulation. Literature [5] proposed a Sybil attack tailored specifically to SCADA systems based on Wireless HART. The feature that internal attackers can cause harmful interference to the network completely isolates the wireless sensor and the SCADA network part, which confirms the feasibility of this attack and its potential dangers and proves that this kind of attack is easy to carry out and the time required to launch the attack is very short. Although this method can effectively prove that the protocol has such an attack, the engineering method used in the literature cannot explain the security problems of the protocol itself and it does not describe the detailed process of the attack. Literature [6] showed how internal attackers bypass the security mechanismand inject false commands into the network to detect the security problems of the Wireless HART protocol. By choosing the network key change command as the injected fake command to break the network manager's reception of data from wireless sensors, it indicated that an internal attacker can inject fake commands into the network. These false commands were verified as legitimate commands and executed by the receiving device, confirming the feasibility of the attack and its potential impact. Although the research method in the literature described the attack path of the internal attacker in more detail than the former, this research method still does not explain the interaction process of the security problem in the protocol communication. Literature [7] studied the different problems of the protocol by proposing a generalnonlinear and hybrid framework, a model of the key features of the protocol was established,and an overall hybrid model was proposed for multiple problems. Through these models, the behavior between samples, packet loss, and nonlinear equipment and controllers were captured, and simulation methods were used to analyze the protocol. However, in this analysis method, the emphasis was placed on the stability of frequent data transmission in the simulation environment under the influence of the outside world, and the modeling method was not used to focus on the security and unstable factors of the protocol itself. Literature [8] analyzed the security functions and security threats of the Wireless HART industrial wireless communication protocol standard. Through careful analysis of the problems of the standard itself and the security functions outside the user options and scope, the security functions and threats of each protocol stack were derived and some security requirements were put forward. In the literature, the security functions and threats of the protocol standards have been analyzed and deduced in detail, but the security functions and threats of the protocol stack are only obtained through derivation without strict formal analysis. Therefore, it is of great significance to study the security issues of the protocol interaction process through formal methods.

In summary, the security research work for wireless communication protocols is still in a single security assessment stage at present, and there is no more complete formal analysis plan for the agreement itself. The establishment of formal modeling and security assessment models for industrial wireless communication protocols is still being researched and investigated. In this paper, modeling research was used to assess the security of the Wireless HART protocol's interaction process, the colored Petri net theory and eCK model were used as theoretical guidance, and the CPN Tools modeling tool was used to conduct a security evaluation of the protocol. Through security analysis, the security loopholes were found in the protocol itself, then new solutions were proposed to improve the security vulnerabilities discovered, and the new scheme was remodeled for safety verification.

Compared to the existing research programs, this paper proposes a new formal model checking method to analyze the security of the protocol; the original model of the agreement was verified for consistency and the attacker model was also introduced to explore the security vulnerabilities of the protocol. For the discovered security vulnerabilities, targeted improvement methods were proposed and the security verification of the new scheme was carried out.

2. Research Foundation

2.1. Nonferrous Petri Net Theory and CPN Modeling Tool. Colored Petri nets are suitable for describing asynchronous and concurrent complex system models and have become a huge system after development [9]. The formal modeling tool CPNTools was used to edit, simulate,and analyze colored Petri nets and support temporal CPN and hierarchical CPN modeling [10]. It has incremental syntax checking and code generation functions when constructing the network, and its export state space function can generate and analyze state space. Through the state space report, the safety analysis and evaluation of the established model can be effectively carried out.

2.2. How the Wireless HART Protocol Works. The Wireless HART protocol is the first open international industrial wireless standard drafted and maintained by the HART Communication Foundation [11]. This protocol communication standard is based on existing international standards, including HART protocol (IEC 61158), EDDL (IEC 61804-3), IEEE 802.15.4 radio and frequency modulation, spread spectrum, and mesh network technology [12]. It has good usability and inheritance, and the openness of technology is relatively good, which is in accordance with the development requirements of today's industrial control field. As a wireless mesh network communication protocol for process automation [13], good wireless capability enhances the communication and control functions of the wireless mesh network in the process automation system. The working structure of the Wireless HART protocol is shown in Figure 1. During the point-to-point interaction of the Wireless HART protocol, the wireless communication device actively initiates a request. The data packet is sent by the communication device to the intermediate device in a standard data format. When passing through the routing and the central manager on the way, the corresponding data information in the data packet will be processed to a certain extent and then sent to the device that needs to be executed.

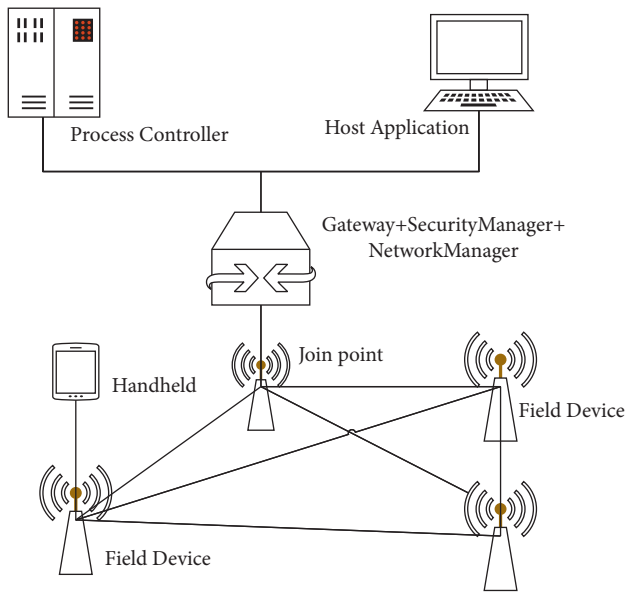

Figure 1: Working structure diagram of Wireless HART protocol.

After the execution device receives the data packet, it performs certain data reading and writing tasks, sends the completed state to the connection point through data, and finally returns the state information to the communication device through the transmission of each node.

In the work of the protocol standard Wireless HART, multiple devices are involved and the security guarantee of the interactive communication between each device is verified by the unique joining key of the device, confirming the legitimacy of the device through the initial device identity authentication. The use authority of the device guarantees the scope of the legal operation of the device, thereby allowing the operation request issued by the device. In the protocol standard, the main identity verification method is through the unique device identification code of the wireless device. After the initial authentication, various interaction processes are to ensure security by verifying the key distributed using the central manager. The provably secure three-factor authentication technique described in [14]makes use of the cloudcenter's tremendous computing and storage resources to achieve user anonymity and resistance to offline dictionary attacks while balancing security and performance. By using the computing and storage capabilities of the cloudcenter, the cost of computing on sensor nodes is relatively low. However, the protocol used in this article does not take into account the cloudcenter, and the system architecture does not conform to the protocol's usage scenarios nor can the cloudcenter's powerful capabilities be used to relieve the computational pressure on sensor nodes.

Literature [15] used the "fuzzyvalidator" technology to construct a fuzzy password validator and combined the concept of "honey talk" to design a protocol based on extended chaotic mapping and biometric recognition. However, the agreement in this article does not satisfy the three characteristic passwords, smart cards, and biometrics contained in any three-factor agreement, so this authentication scheme cannot use this agreement. Literature [16] has efficient privacy protection for user authentication schemes with forwarding secrecy. This scheme proposes a cloud-centric three-factor authentication and key agreement protocol. However, its cloud-centric three-factor authentication is still not applicable to this protocol. In summary, it is particularly important to propose an authentication protocol suitable for actual use scenarios and standards in this protocol.

3. Wireless HART Protocol Modeling

Because the Wireless HART protocol is a large and complex modeling system, the modularization idea was first used in the modeling process. The entire modeling was divided into different levels, and the alternative transition function of the CPN modeling tool was used to first establish the highest-level network and then split the alternative transition in the network like different substitution transition point to different subpages, whereby different subpages represent the interaction process of the underlying network. The process of gradually perfecting and refining each subpage model is the process of gradually completing the systematic modeling.

3.1. Protocol Message Flow Model

(1) The Wireless HART protocol contains two communication modes, namely, unicast communication mode and broadcast communication mode. What this article discusses is to ensure the unicast communication mode under the communication data through a simple encryption and verification mechanism. Figure 2 shows the communication interaction process of the protocol.

(2) The communication device sends a connection request to the central manager, including the connection key (uniquely owned by each device) and the ID that identifies the device information.

(3) After the central manager receives the information, it processes and verifies it. If the verification is successful, the session key and connection routing information are sent; otherwise, the connection request is rejected.

(4) After the connection is successful, secure communication can be carried out, and the device will divide the overall information into different fields before transmitting data information. The communication device will order information, and the data integrity verification code MIC and connection ID are sent to the central manager together. The central manager will verify the information after receiving it before sending it to the execution device.

(5) After the execution device receives the command information, it performs one-to-one conversation security key verification and MIC data integrity verification. If the verification is successful, the corresponding command operation will be executed and the execution success message will be returned. Otherwise, the requested command will be rejected.

The notations' description required in Figures 2 and 3 is shown in Table 1.

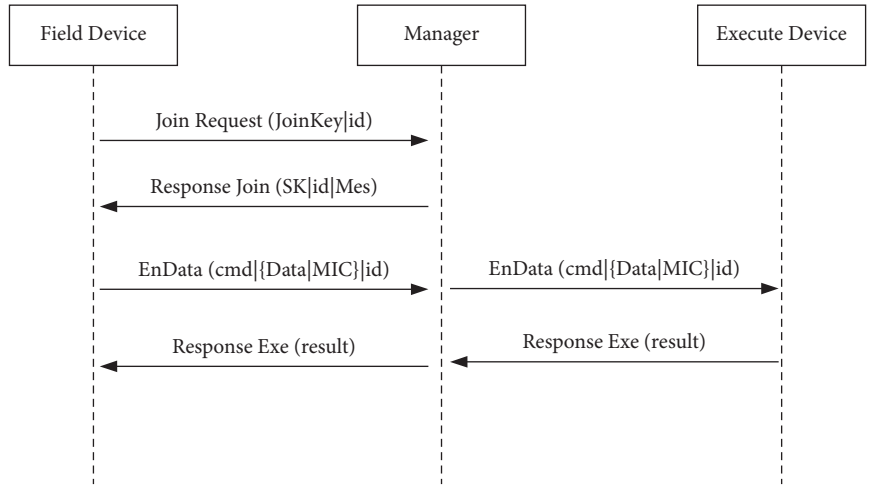

Figure 2: Message flow of Wireless HART protocol.

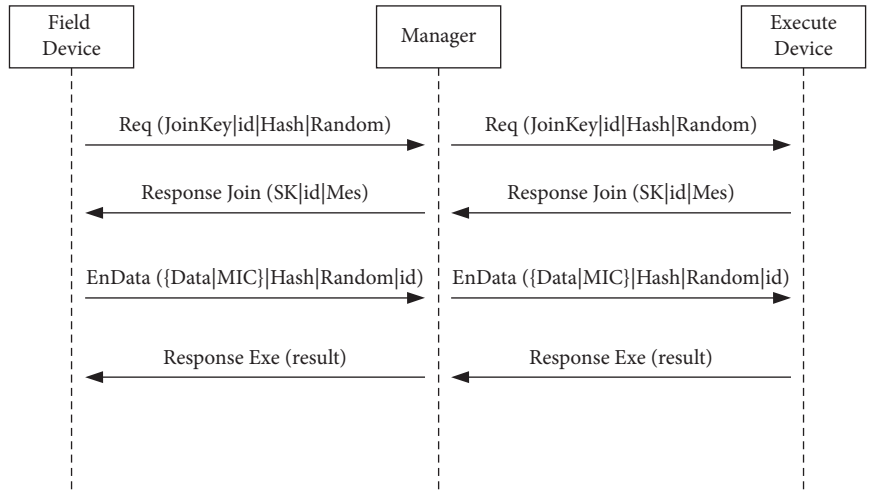

Figure 3: Flowchart of the new scheme agreement.

Table 1: Notations and description.

Notations	Description	Notations	Description
id	Device connection unique id	cmd	Command information
SK	Session key	Data	Necessary data after connection
Mes	Connect message	MIC	Integrity verification code
EnData	Secure data after connection	Result	Device execution return information
Hash	Hash value	|	Differentiate parallel segmented data
Random	Random value	{...}	Represents an integrated data package
Req	Connection request	(...)	Overall data sent

3.2. Modeling of CPN Model of Wireless HART Protocol. In the establishment of this protocol, there are mainly three parts: sender, receiver, and central manager network. Therefore, to simplify the model and minimize its complexity while accurately representing the network communication process, this article simplifies the protocol model into three layers, namely, the top, middle, and bottom layers. After subdividing each layer, the message flow of the protocol is described in detail.

When modeling the Wireless HART protocol, the specific interaction process was expressed in the form of a model. The top-level model modeling of the Wireless HART protocol is shown in Figure 4. The top-level model represents the conversion process of the protocol as a whole, simulating the communication equipment of the protocol, communication management center, and network, and the double-line rectangle represents the substitution changes. The ellipse represents the message place, the communication

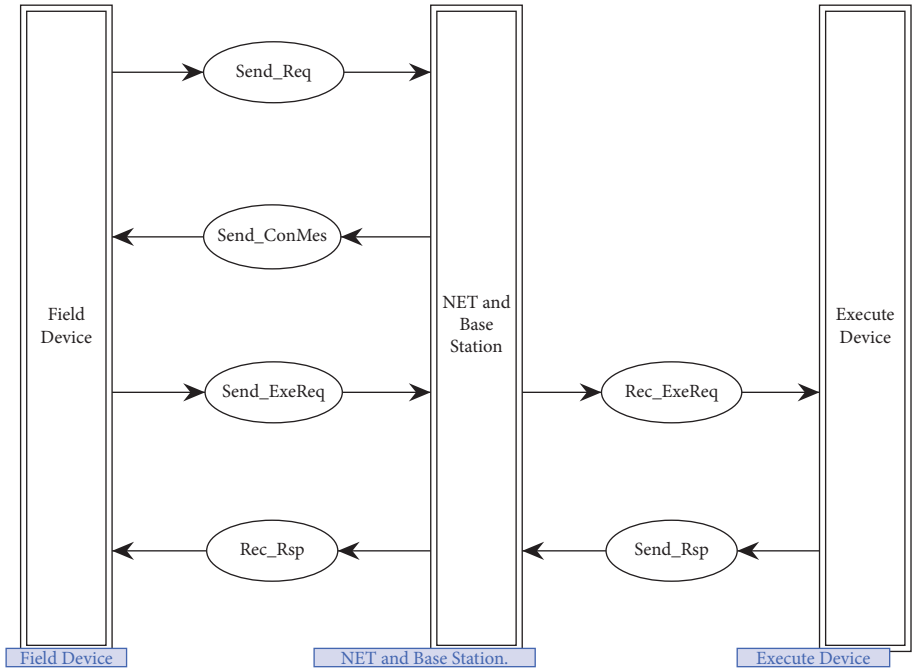

Figure 4: Top-level model of the Wireless HART protocol.

area equipment is represented by Field Device while the communication execution device is represented by Execute Device, and the communication network and base station center manager are represented by NET and BaseStation.

Figure 5 shows the middle-level model of the protocol, which consists of 4 alternative transitions and 7 message places. The message process of the communication device requesting connection is represented by the alternative transition Connection, the process of sending commands for safe transmission is represented by the alternative transition SafeComm after the connection is successful, and the command execution and response process after successful verification is represented by the alternative transition SafeComm'.

The underlying model of the protocol consists of 4 parts and the communication network and base station central manager was first described in detail. Then, according to the interactive mode of the communication parties, the session connection process and the command data transmission process were explained in detail.

Figure 6 shows a detailed description of the internal model of the alternative transition NET and BaseStation. The request connection process and the connection success process are represented by the transition SendRequsetMes and the transition TransmitConMes. The transmission path of the initiation request connection and the transmission of the response information of the successful connection are simulated, respectively. The transition TransmitExecuteMes and the transition SendResResult represent the transmission process of the communication device sending the execution command request after the secure connection, and executing the process of replying information after the device receives the command information.

Figure 7 shows the internal model of the alternative transition Connection. The information synthesis and transmission mode in the connection process are simulated through transition and place. The transition Join_Conn combines the connection information header and the connection ID into a request information packet and sends the connection request information to the network center manager through the transition Req_Conn, and transition Res_Conn receives the reply message after processing by the network center manager. If the verification fails during verification, the transition Reset will perform the reset operation; otherwise, the connection ID will be sent to the next SafeCommtransition through the place JoinID.

Figure 8 shows a detailed description of the internal model of SafeComm, which is an alternative transition. After a successful connection, the communication equipment requests the transmission process of command information and the final response information reception process. The transition combination connects ID, security control, and counting information are merged, while transition MIC_Payload performs MIC information integrity verification on local load security data. Finally, this information is sent to the network center manager by Send_ExeReq of the place; the command execution response information is received by the place Rec_Rspand stored in the placeRsp_Count.

Figure 9 shows a detailed description of the internal model of SafeComm's alternative transition and describes the processing and response process after the execution device receives the request command information. Place Rec_ExeReq accepts the request information sent by the communication device, and then transition SafeComm' decomposes the received request information. First, the local device performs local MIC verification on the request information

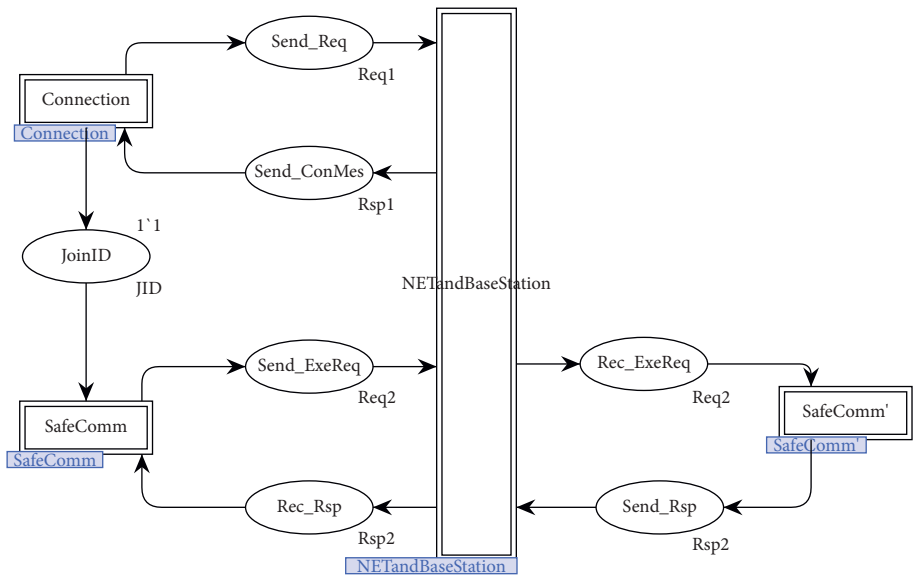

Figure 5: The middle-level model of the Wireless HART protocol.

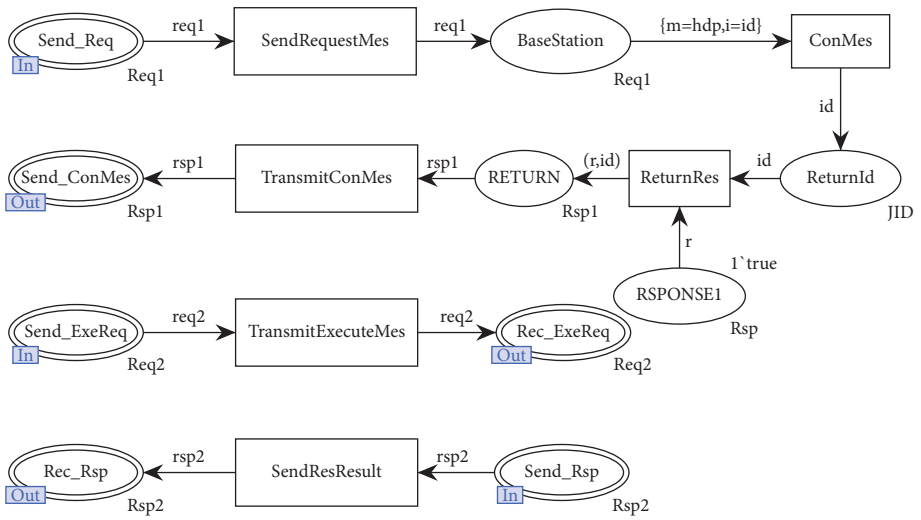

Figure 6: Alternative transition NET and BaseStation internal model.

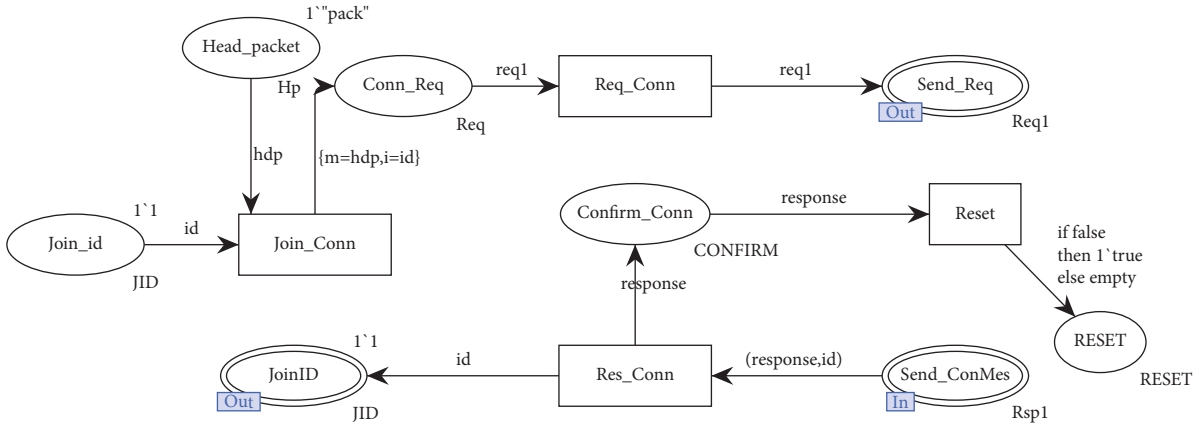

Figure 7: The internal model of the alternative transition Connection.

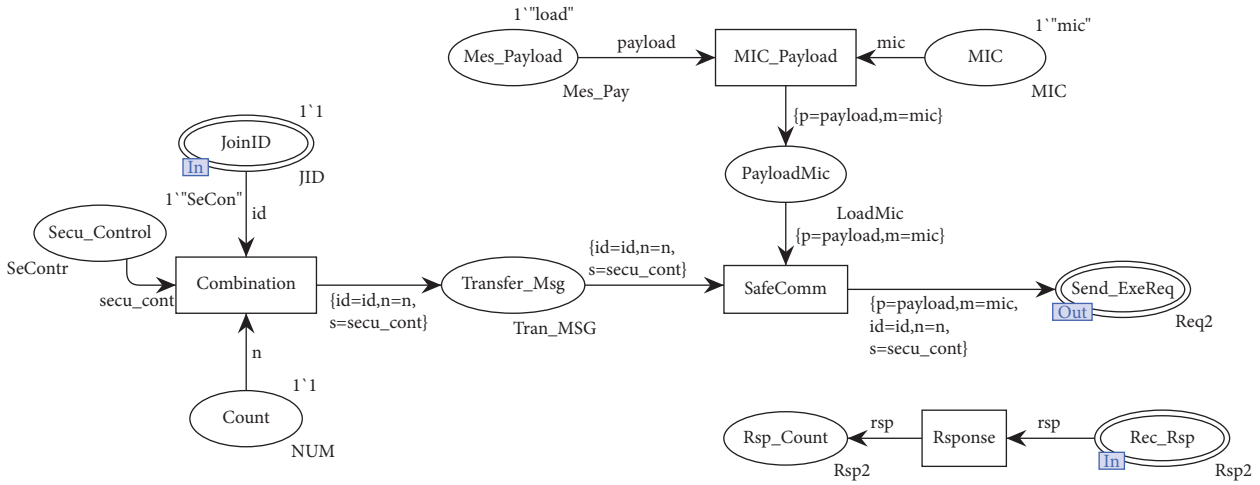

Figure 8: The internal model of the alternative transition SafeComm.

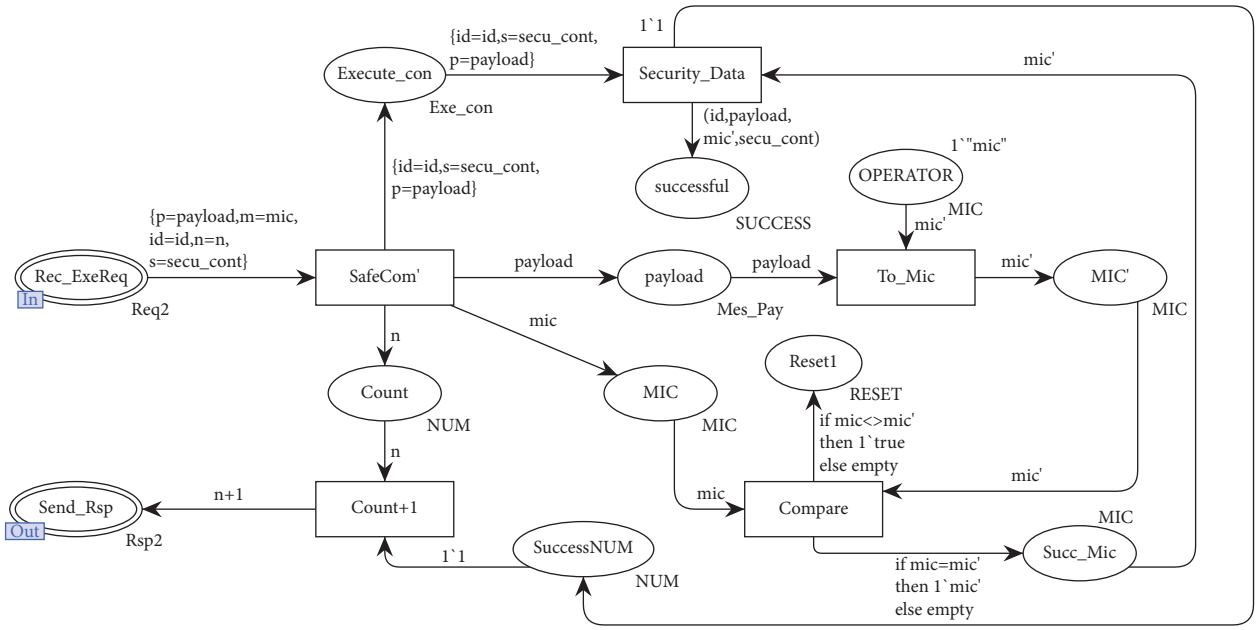

Figure 9: The internal model of the alternative transition SafeComm'.

and then compares it with the received verification data. If they are the same, it performs the corresponding command execution operation and returns the execution success response message; otherwise, it resets the request.

3.3. Wireless HART Protocol Model Consistency Verification. The consistency of Wireless HART protocol modeling is verified by using state space analysis tools [17]. In the establishment of the model, the expected result is obtained through theoretical analysis. During the entire session interaction process of the model, the state of each transition is reachable, and all reasonable requests are executable and the session endpoint is unique. By analyzing the data in Table 2, it can be seen that the number of state space nodes, directed arcs, and strongly connected nodes and the number of strongly connected arcs is the same, which shows that there is no state infinite loop and iterative behavior in the model we built. The number of dead nodes is 1, which means that all requests are executable, and the end point of the protocol is uniquely determined no matter what the situation is during the session interaction process of the protocol. The absence of dead transition instances and live transition

Table 2: State space analysis of Wireless HART original model.

Type	Number/state
State space nodes	117
State space arc	221
SCC graph node	117
SCC graph arc	221
Dead marking	1
Live transition instances	0
Dead transition instances	0

instances means that the model has no unreachable nodes and nodes that are always active. Through the analysis of the data in the table, it can be verified that the results are the same as our expected results.

3.4. Introducing eCK Adversary Model Modeling Evaluation. Scholars LaMacchia, Lauter, and Mityagin [18] proposed an extended CK model based on the CK model, namely, the eCK model. The eCK model is considered to be a fairly strong model and is currently receiving more and more attention. Many new authentication key agreement proposals have been designed and analyzed under the framework of this model. This model requires a two-party authentication key agreement protocol to be secure. As long as each party still has at least one secret that has not been leaked, a unique and independent secret session key should be generated for each run. Even if the adversary already knows the session key other than the current session, it will not affect the security of the current session key. Among them, the adversary has simulated a multiprobability polynomial time Turing machine, which controls all communication on the network and can modify, discard, or forge communication messages at will, as well as arranging the order of message sending or modifying the recipient of the message. In addition, adversaries can also obtain long-term keys, temporary keys, session keys, etc. [19]. In this model, the adversary's behavior ability is powerful enough to meet the requirements of the attacker's ability in the model we established.

Since the Wireless HART protocol is real-time communication, the time for data to be transmitted through each communication entity during the communication process is relatively short, and the encryption, decryption, and verification processes of the protocol are implemented by hardware, so when the eCK model was introduced in this article, an attacker was added to the network channel.

Based on the powerful attack capability that the adversary of the eCK model can launch against the network channel, the man-in-the-middle attacks of replay, deception, and tampering were introduced to the network level of the original model established. As shown in Figure 10, the purple part simulates a spoofing attack, including the changes in the transmission processes SendRequsetMes, TransmitConMes, TransmitExecuteMes, and SendResResult. The expressions, transition, and place in the red part simulate tampering attacks, while the introduced attacker mattack launches an attack through the transition Attack. The transition and place marked in blue represent replay attacks. The place P1 receives and stores the data information in the process of intercepting the protocol request connection, transition Separate can break down information, the places PACKET and JID store the decomposed atomic information, transition Combin uses the attacker's decomposition rules to store the decomposed atomic information in the place DB, transition TransID transmits the decomposed atomic information whenever decomposition information is generated, and transitions ATTRsp and ATTSend synthesize the attacker's information and send it to the attacked channel place.

3.5. Security Evaluation of Wireless HART Protocol Model. In the state space report shown in the adversary model in Table 3, the numbers of state space nodes, directed arcs, and strongly connected nodes and strongly connected arcs are the same. This shows that all state space nodes in the eCK adversary model of the Wireless HART protocol are reachable. Compared with the state space in the original model,it was found that the number of state spaces is within an acceptable range after the adversary model is introduced and there is no situation that the state space is too large or exploded. The credibility of the attack model is ensured based on the attacker's ability in the adversary model, which further illustrates the effectiveness of introducing the adversary model.

Comparing the state space of the original model with that of the adversary model [20], it can be found that the number of dead nodes has changed from one to four. Through the query analysis of transition, it was found that there are 2 dead nodes because the request transmission connection cannot be enabled after the introduction of a spoofing attack and the unpredictable end-state during the protocol connection process. One dead marking is due to the introduction of tampering attacks during the interaction of the protocol, resulting in a command request,and a valid response message cannot be generated. Through the comparative analysis of the state space of the original model and the adversary model, it was found that the introduced adversary model has effectively attacked the connection process of the original model and the request command information transmission process, reflecting the existence of the man-in-the-middle attack vulnerability of tampering and deception in the original protocol.

4. Wireless HART Protocol Improvement and Reinforcement

4.1. Protocol Reinforcement Scheme. By introducing the attacker model to evaluate the security of the original model, it was discovered that the original protocol had man-in-the-middle attack vulnerabilities such as tampering and deception. In response to the results of the security assessment and analysis, we perform reinforcement processing during the session connection authentication and secure data transmission process. In order to verify the security between the communication device and the execution device, the point-to-point security authentication between the two was added when the session is connected, instead of the authentication of only the network central manager in the original protocol. The random value and hash value were added in the data information transmission process toensurethe safe transmission of data information. While adding reinforcement methods, it also retains the good security features of the protocol, including security features for internal opponents. After the central manager verifies that the device is legitimate, if it is hijacked as an internal adversary, because each device has its legal operation authority, as long as the internal adversary device has some attack behavior, it will be detected by other node devices or the central manager. Once an illegal attack is detected, the

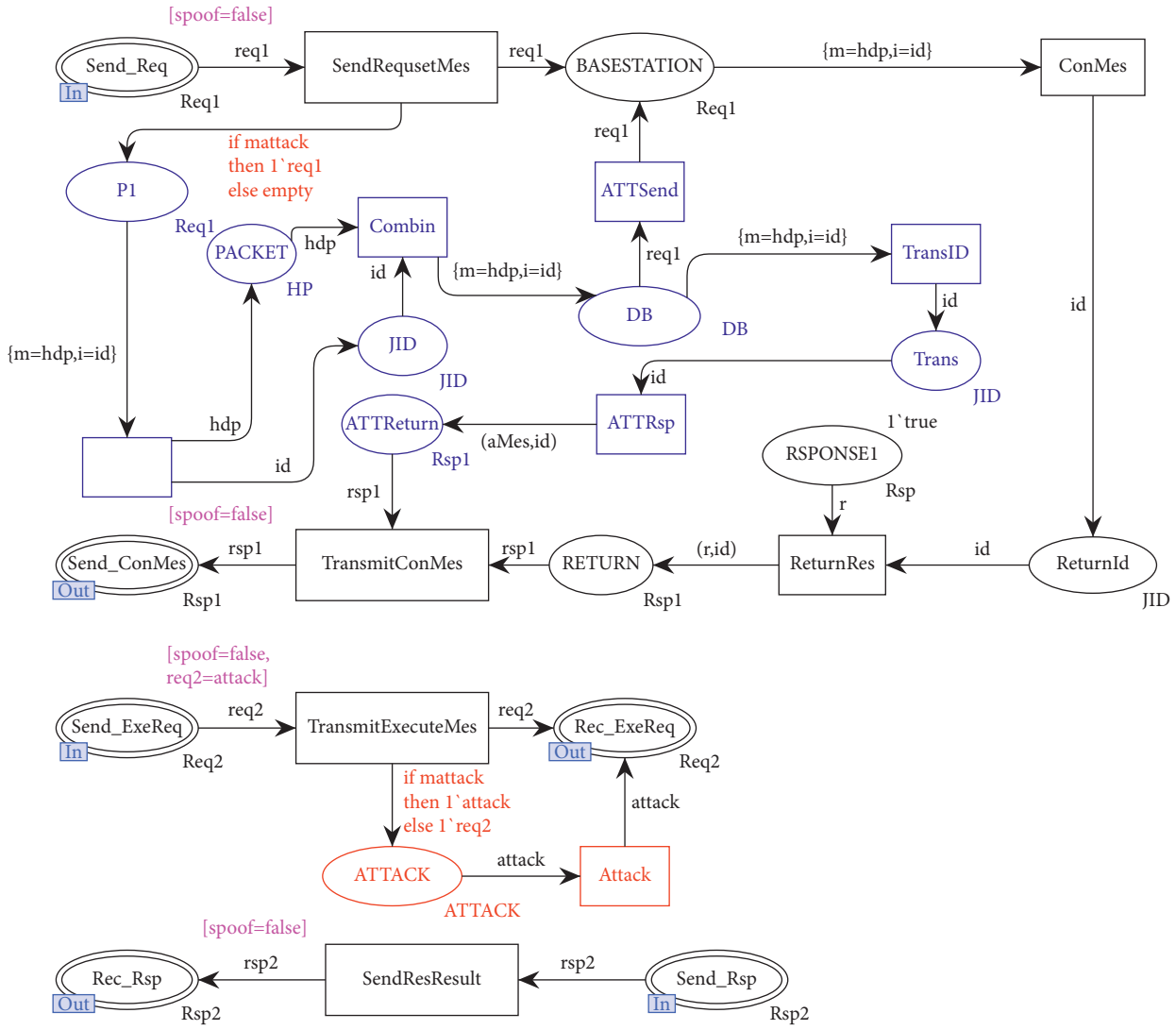

Figure 10: The original protocol attacker model.

Table 3: Comparison of model state space.

Type	Original model	Attack model
State space nodes	117	896
State space arc	221	2576
SCC graph node	117	896
SCC graph arc	221	2576
Dead marking	1	4
Dead transition instances	0	0

device will be excluded from the list of legitimate devices by the central manager, to protect against the security threats caused by the verified device being hijacked.

Figure 3 shows the improved message flow diagram of the new scheme. The improved transmission process of the message flow diagram isas follows:

(1) The communication device sends a connection request to the network center manager, including the connection key, connection ID, a random value, and hash value.

(2) The network center manager processes the received connection information and verifies whether the connection request sent by the communication device is legal through encryption and decryption. After the verification, the key information and the received connection request information are combined and sent to the execution device.

(3) The execution device receives the connection request information of the communication device from the network center manager and verifies the legitimacy of the connection request through key decryption, and finally, the connection response result is sent to the network central manager.

(4) After the network central manager receives the response information sent by the executing device, the session key, session ID, and routing information are combined and sent to the communication device.

(5) After the session connection is established, the communication device initiates a secure command to

request information. First, it performs a local Hash operation on the data information, uses the session key to encrypt data information, combines the local hash, random value, data information, and session ID, and sends them to the network center manager.

(6) After receiving the command request information, the network center manager performs split verification, and comparison of key encryption and decryption, and the consistency of data such as random values. After the verification is successful, the command data information is sent to the execution device.

(7) After the execution device receives the command data information, it uses the session key to decrypt the relevant information and performs local data verification. If the verification is successful, the relevant command is executed, and finally, the execution result is sent to the communication device through the network central manager. At this point, the interactive process of session connection and execution command information ends.

4.2. CPN Modeling of New Scheme. In response to the discovered protocol security vulnerabilities, the original protocol was strengthened with a new scheme, and CPN modeling verification was carried out. The improved middle-level model of the new scheme is shown in Figure 11, whichis composed of 5 alternative transitions and 9 message places. The middle-level model of the new scheme describes the protocol connection request process and the transmission process of command request information as a whole. The request connection process of the communication device is represented by the alternative transition Connection, the connection authentication process of the performing device is represented by the alternative transition Connection, and the transmission process and message data authentication process of the network central manager are represented by the alternative transitions NET and BaseStaion. After the communication device is connected, the command information request process is represented by the alternative transition SendCommand, and the verification execution and result response process of the executing device is represented by the alternative change SendCommand.

Figure 12 shows a detailed description of the internal model of the alternative transition Connection. Transition HASH combines the calculated hash value and random number, while transition MIC is used to transmit local integrity verification data. The transition combination combines the first two data and the connection ID and then sends them through Send_Req in the place. The place Rece_Con receives the sessionconnection information returned from the execution device and the network central manager. If the session connection is successful, the place Join_Conn will send the ID and session key information after the session connection to the next transition.

Figure 13 shows a detailed description of the internal model of the alternative transition Connection', where the transition Rece_Req accepts the session connection request information from the communication device. The place Separate decomposes the request information into atomic messages, the ConfirmH of the place is used to verify the local Hash operation data and the decomposed Hash value, and the ConfirmM of the place is used to verify the local data integrity check value and the decomposed MIC check value. If the session key is generated after successful verification, then the place Send_Sess combines the generated session key and connection ID and sends them together; the transition Send_Con sends the synthesized information to the communication device through the network central manager.

Figure 14 shows a detailed description of the internal model of the alternative transition SendCommand. This alternative transition describes the interaction process of the command request message after the connection is successful. Among them, the place HashDt combines the locally generated Hash value and the command message load, transition assemble merges the message combination, command message load, and Hash of the successful connection of the previous session. It is sent by the transition REQ2 to the place Send_CMD and then sent by the place Send_CMD to the network central manager. The network central manager verifies the integrity and legitimacy of the received messages one by one; the message place Rece_Rspreceives and stores the execution response information returned from the execution device.

Figure 15 shows a detailed description of the internal model of SendCommand's alternative transition, which describes the verification and execution process after the execution device receives the command message as a whole. The message place Rece_CMD receives the command request message from the communication device, and transition Separate1 decomposes the request message into an atomic message. The transitions confirmH and ConfirmSK are used to verify the correctness of the local operation Hash value and the decomposed Hash value and session key encryption and decryption, respectively. The place Send_Rsp combines the response result information to be returned by the executing device and sent to the communication equipment through the network central manager.

4.3. Modeling the New Scheme Attacker Evaluation Model. We use the same method as the original protocol attacker model, introduce the eCK adversary model, and add man-in-the-middle attacks to the network channel of the improved new solution model, including tampering, deception, and replay attacks. As shown in Figure 16, the blue part of transition and place simulates a replay attack. The expression, transition, and place in the red part simulate a tampering attack, and the purple part simulates a spoofing attack.

4.4. Comparison of Safety Assessment of New Scheme Models. Comparison of the security assessment state space of the adversary model of the new scheme with the state space of the original adversary model is shown in Table 4. The established adversary model of the new scheme well controls the number of nodes and arcs in the state space, effectively prevents the state space explosion that may occur, and uses the man-in-the-middle attack of the previous protocol to

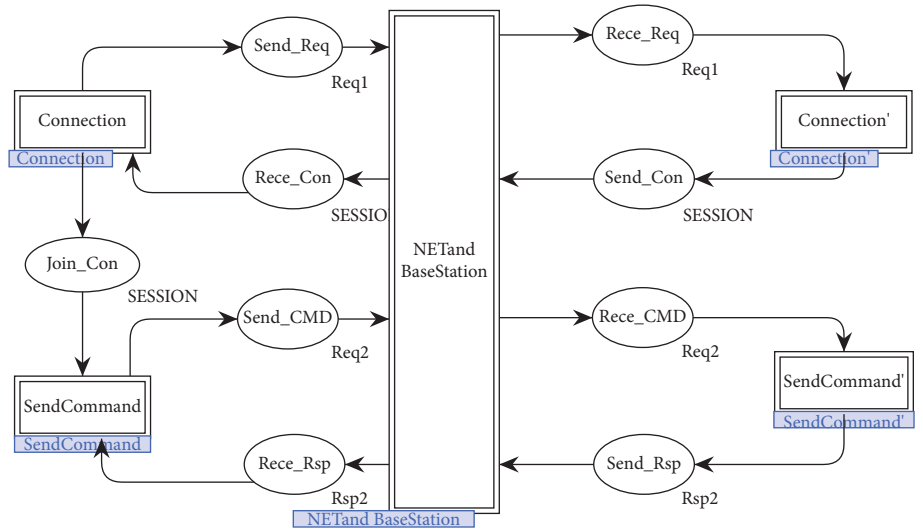

Figure 11: The midlevel model of the new scheme.

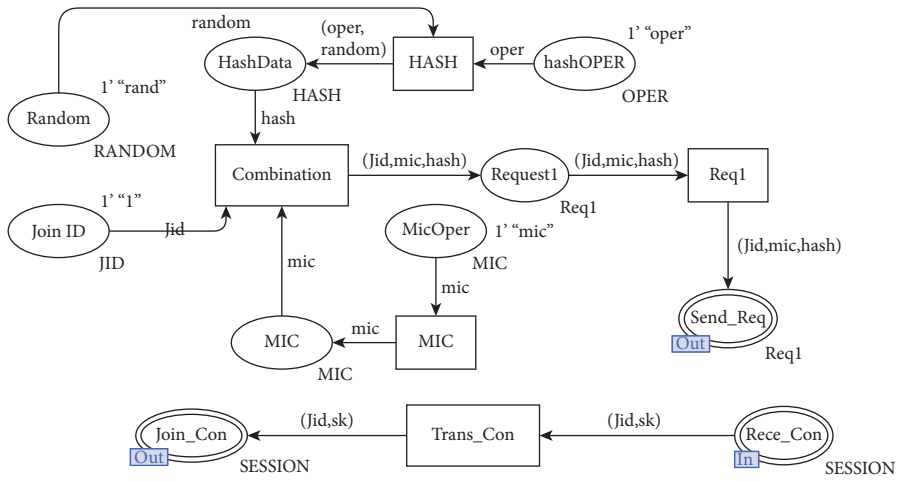

Figure 12: The internal model of the new scheme to alternative transition Connection.

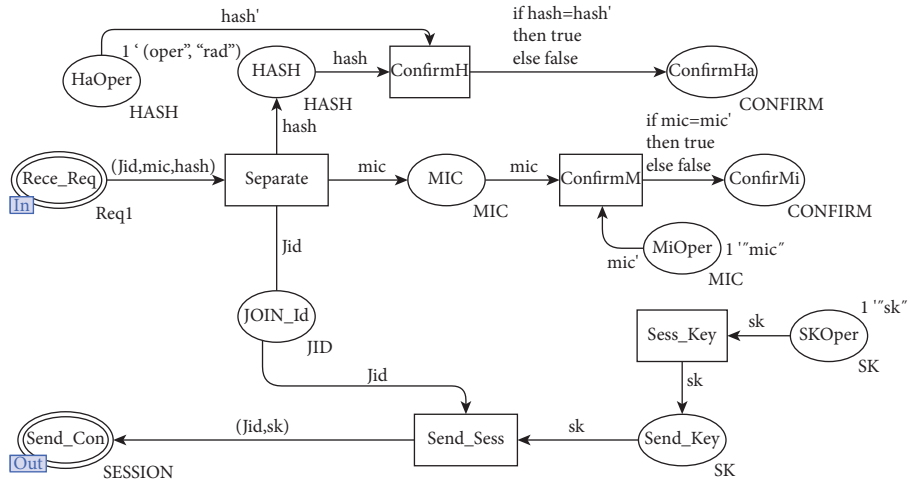

Figure 13: The internal model of the new scheme to alternative transition Connection'.

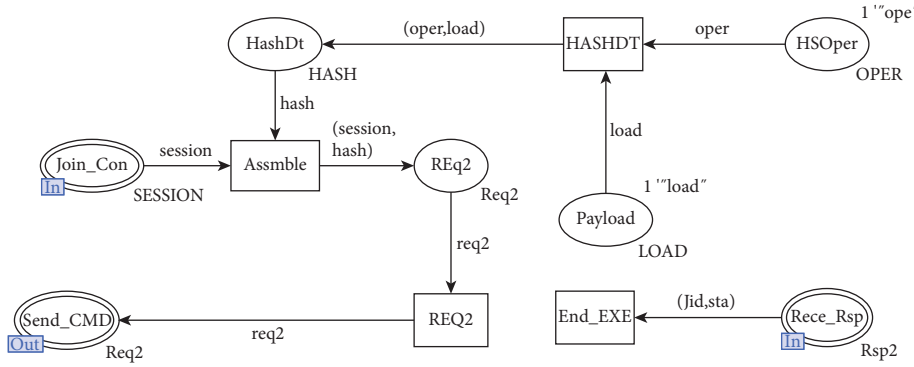

Figure 14: The internal model of the new scheme to alternative transition SendCommand.

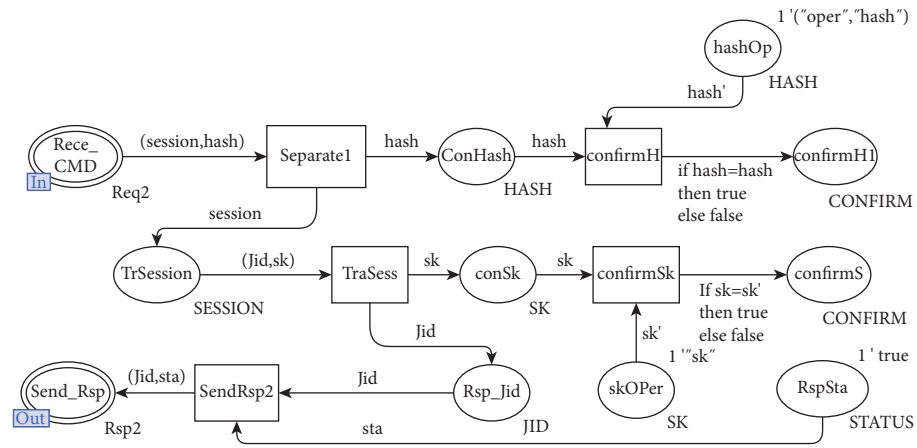

Figure 15: The internal model of the new scheme to alternative transition SendCommand'.

verify the security of the new scheme. It can be easily found through the state space comparison results in Table 4 that the dead node of the state space of the adversary model of the new scheme becomes 1, which is a significant change compared with the original adversary model. Through further analysis and query, a dead node in the new scheme can be found to be the final state after the protocol runs. Multiple dead nodes in the original adversary model are caused by the attack state after joining the attack, indicating that the adversary model of the new scheme has not been attacked.

Further analysis found that the attacker cannot launch an effective attack in the new scheme. In the new scheme, a random value was added and a Hash operation was performed on the transmission message of the protocol. These security reinforcement methods ensured that the protocol can effectively prevent tampering and spoofing attacks that have been discovered and retain the MIC message integrity verification method in the original protocol to prevent replay attacks. The implementation of the device authentication process added during the connection phase of the protocol request also further enhances the security of the protocol. Therefore, the attacker cannot launch an effective attack on the new scheme. Through a comprehensive analysis, it can be concluded that the security reinforcement method of the new scheme is effective for the security protection of the protocol.

4.5. New Solution Performance Analysis. In this section, the performance of the new scheme was analyzed, random value and Hash operation were added to the new protocol improvement scheme, and one step is added to perform the authentication connection of the device at the beginning of the protocol interaction request connection. A large number of computing operations were completed by hardware devices and network center managers, so the overall calculation and time consumption are within an acceptable range. Compared with the original agreement, the cost of interaction is slightly increased, and there is no excessive consumption gap, while the random value and Hash calculation methods only increase the cost of calculation, communication, and data storage. There is no need to upgrade and improve the original overall structure too much, the increase in the authentication connection method of the implementation device will have an impact on the connection request time. However, in the subsequent execution request of the new scheme agreement, the overhead of the agreement operation is not large; while enhancing the overall security of the protocol, it will slightly affect the real-time performance of the protocol.

To compare the analysis scheme used in this article with other analysis methods, several typical documents were selected to compare the safety analysis methods. Each analysis method has different safety verifications and, in

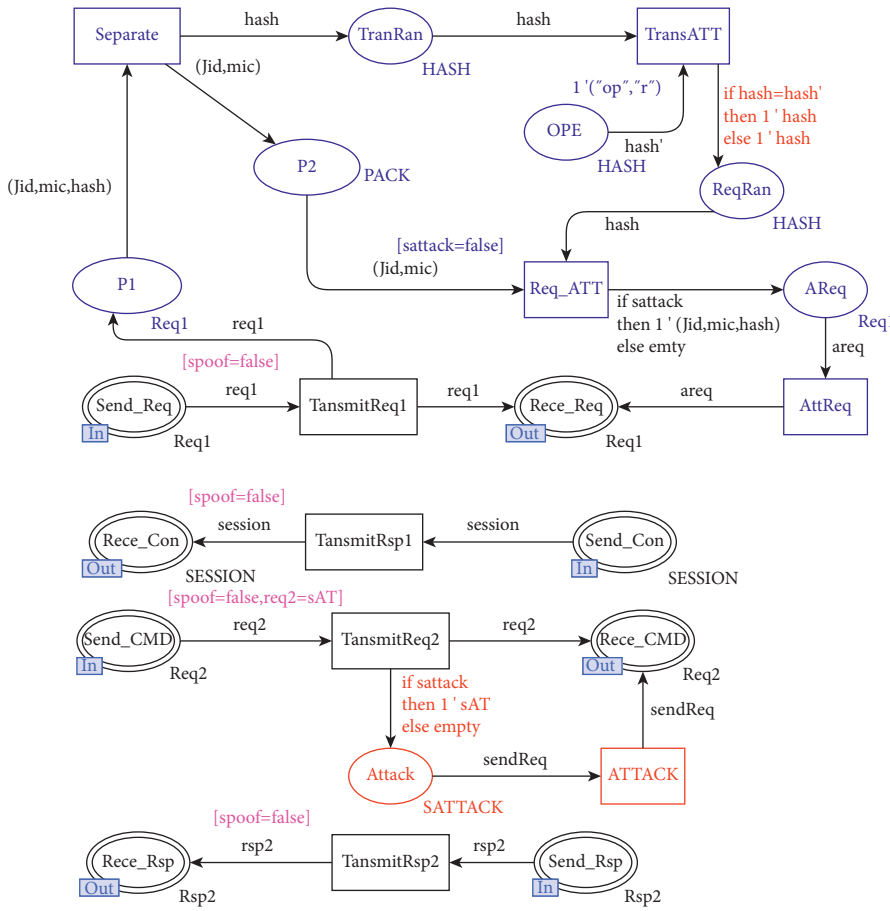

Figure 16: Attacker model of the new scheme.

Table 4: Comparison of state space of security assessment models.

Type	Original attack model	New scheme
State space nodes	896	536
State space arc	2576	1732
SCC graph node	896	536
SCC graph arc	2576	1732
Dead marking	4	1
Dead transition instances	0	0

Table 5: Comparison of protocol security analysis methods.

Scheme	Multiscenario attack	Specific attack	Standard itself	Improvement advice	State space	Smart selective attacks
Reference [12]		√				
Reference [13]	√			√		√
Reference [8]		√				√
Reference [21]		√		√		
Reference [22]			√	√		
Our scheme	√	√	√	√	√	√

this article, a security verification analysis was conducted based on the advantages of various current analyses. Through the comparative analysis in Table 5, it can be seen that the formal model detection method based on colored Petri nets combined with eCK model theory in this paper [23] can not only have an intuitive and accurate graphical description in protocol security research Method and protocol consistency verification but also analyze the types of attacks that exist in the attack model. While discovering problems through anomaly detection and evaluation in the attacker model of the protocol, it can also effectively improve the reinforcement methods for the analyzed security vulnerabilities and adopt effective verification methods for the improved reinforcement methods. In

summary, the solution in this article effectively solves the problem of state space explosion in traditional model detection methods. This research scheme can be used in the security analysis and research of industrial wireless protocols in the future.

5. Summary and Outlook

This article focuses on the security of the widely used international wireless industry standard Wireless HART protocol. First, the interaction process of the protocol message flow was analyzed, the CPN modeling of the protocol was carried out through the CPN modeling tool, the adversary model was introduced based on the original protocol model, and the state space tool was used to obtain the data and compare the state space of the original model and the adversary model. It was found that the protocol has man-in-the-middle attacks such as tampering and deception, and then new solutions were implemented to improve the security of the protocol for the existing attack types. CPN was modeled again for the new scheme. After modeling, the adversary model was introduced to verify whether the attack method was effective. Finally, by comparing the state space table of the original protocol adversary model and the adversary model of the new scheme, it was found that the security improvement of the new scheme effectively prevented the previous existence of two types of man-in-the-middle attacks. However, in the research process of this article, the focus was on the security of the protocol itself. The real-time nature of the protocol is not considered enough, and the introduction of the adversary model of the protocol is only the man-in-the-middle attack on the network channel. And other methods of attack were not considered. In future research work, the need to ensure the real-time performance of the protocol will be considered while enhancing the security and exploring whether other attack methods can be used to discover other different types of security problems in the protocol. In addition, the performance of the new program and the improvement of other identity verification features will be the focus of our future work. In this research, we focused on security and did not optimize performance well; hence, finding a balance between security and performance in the next work will be one of the focuses of our research work. With the advent of Industry 4.0, this protocol will involve more application scenarios [24, 25], such as cloud center-based device data transmission and computing migration, which requires multifeature authentication (such as biometrics, smart cards) verification. Protocol security solutions based on these application scenarios need to consider the actual environment and development trends [26]. Adding cloud center modeling and multifeature authentication to future solutions will also be the focus of our next research work.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] C. Zhang and Y. Chen, "A review of research relevant to the emerging industry trends: industry 4.0, IoT, blockchain, and business analytics," *Journal of Industrial Integration and Management*, vol. 05, no. 1, pp. 165–180, 2020.

[2] I. Jamai, L. B. Azzouz, and L. A. Saïdane, "Security issues in industry 4.0," in *Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 481–488, Limassol, Cyprus, June 2020.

[3] M. Alrashidi, N. Nasri, S. Khediri, and A. Kachouri, "Energy-efficiency clustering and data collection for wireless sensor networks in industry 4.0," *Journal of Ambient Intelligence and Humanized Computing*, vol. 51, no. 1, pp. 224–256, 2020.

[4] S. S. Sokolov, O. M. Alimov, P. S. Nekrashevich, A. I. Moiseev, and A. V. Degtyarev, "Security issues and IoT integration for in Russian Industry," in *Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 517–520, St. Petersburg and Moscow, Russia, January 2020.

[5] L. Bayou, D. Espes, and N. B. Cuppens, "Security Issue of WirelessHART Based SCADA Systems," in *Proceedings of the International Conference on Risks and Security of Internet and Systems*, pp. 225–241, Nanyang Executive Centre, Singapore, November 2016.

[6] L. Bayou, D. Espes, and B. Cuppens, "Security analysis of wirelesshart communication scheme," in *Proceedings of the International Symposium on Foundations and Practice of Security*, pp. 223–238, Montreal, Canada, November 2018.

[7] M. Martinez and A. Ignacio, "Modelling and analysis of networked control systems implemented over," *WirelessHART*, vol. 25, no. 7, pp. 3214–3222, 2019.

[8] X. Cheng, J. Shi, M. Sha, and L. Guo, "Launching smart selective jamming attacks in wirelesshart networks," in *Proceedings of the IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, pp. 1–10, Vancouver, BC, Canada, May 2021.

[9] W. Michael, "Cpn tools 4: multi-formalism and extensibility," in *Proceedings of the International Conference on Applications and Theory of Petri Nets and Concurrency*, pp. 400–409, Milan, Italy, June 2013.

[10] O. I. Bokova, S. V. Kanavin, V. A. Meshcheryakov, and N. S. Khokhlov, "Information security system model in the automated system developed in the simulation software environment CPN Tools," *Journal of Physics: Conference Series*, vol. 1479, no. 1, pp. 12–21, 2020.

[11] A. Samaddar, A. Easwaran, and R. Tan, "SlotSwapper," *ACM SIGBED Review*, vol. 16, no. 4, pp. 32–37, 2020.

[12] Q. Huang, J. Jiang, and Y. Q. Deng, "Comparative evaluation of three wireless sensor network transceivers in a high radiation environment," *EPJ web of Conferences*, vol. 225, pp. 5–10, 2020.

[13] S. Siddiqui and M. Darbari, D. Yagyasen, Modeling and simulation of queuing models through the concept of Petri nets," *Advances in Distributed Computing and Artificial Intelligence Journal*, vol. 9, no. 3, pp. 2255–2863, 2020.

[14] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor Authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, p. 1, 2020.

[15] Q. Jiang, Z. Ning, J. Ni, J. Ma, X. Ma, and K. K. R. Cho, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous

vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, 2020.

[16] C. Wang, D. Wang, D. He, and G. Xu, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," *SCIENCE CHINA: Information Sciences*, vol. 65, 2020.

[17] M. Xiao, *Formal Analysis and Verification of Security protocols*, pp. 1–161, Science Press, Beijing, China, 2020.

[18] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *Proceedings of the International Conference on Provable Security*, pp. 1–16, Springer, Wollongong, NSW, Australia, November 2007.

[19] H. Zhang, Q. Wen, and Z. Jin, *Provable Security Algorithm and Pro- tocol*, Science Press, Beijing, China, 2012.

[20] S. Liu, M. Caporin, and S. Paterlini, "Estimating time-varying networks with a state-space model[J]," *University of Padova - Department of Statistical Sciences*, vol. 51, no. 32, pp. 33–67, 2020.

[21] A. Samaddar, A. Easwaran, and R. Tan, "A schedule randomization policy to mitigate timing attacks in WirelessHART networks," *Real-Time Systems*, vol. 56, no. 4, pp. 452–489, 2020.

[22] J. H. Jeong, S. M. S. Kwon, and S. Tea, "Security threats analysis and security requirement for industrial wireless protocols isa 100," *11a and WirelessHART*, vol. 29, no. 5, pp. 1063–1075, 2019.

[23] Ye Lu, *Formal Security Assessment and Improvement of DNP3-SA Protocol Based on HCPN Model detection*, Lanzhou University of Technology, Lanzhou, China, 2018.

[24] i. Bütün, "Security Implications of Underlying Network Technologies on Industrial Internet of Things," *Politeknik Dergisi*, vol. 24, no. 2, p. 1, 2022.

[25] M. T. Khan and I. Tomic, "Securing industrial cyber-physical systems: a run-time multilayer monitoring," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 6251–6259, 2021.

[26] G. Chen, X. Cao, and J. Jin, "Joint scheduling and channel allocation for kalman filtering over multihop WirelessHART networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3555–3565, 2021.