IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 22, 2019, accepted January 5, 2020, date of publication January 17, 2020, date of current version January 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2967469

An Internet of Things Roaming Authentication Protocol Based on Heterogeneous Fusion Mechanism

ZHIPING WAN[1], ZHIMING XU[1], SHAOJIANG LIU[1], WEICHUAN NI[2], AND SHITONG YE[3]

[1]Department of Information Science, Xinhua College of Sun Yat-sen University–Dongguan, Dongguan 523000, China
[2]Department of Equipment and Laboratory Management, Xinhua College of Sun Yat-sen University–Dongguan, Dongguan 523000, China
[3]Department of Data Science, Huashang College, Guangdong University of Finance and Economics, Guangzhou 510000, China

Corresponding author: Zhiping Wan (wzp888@xhsysu.edu.cn)

This work was supported by the 2017 School-level Scientific Research Startup Fund in Xinhua College of Sun Yat-sen University under Project 2017YB005.

ABSTRACT With the increasing and diversified Internet of Things (IoT) devices, more IoT heterogeneous wireless networks have emerged, providing more network services for IoT devices, especially mobile phones and other roaming devices. However, there are also some malicious users who use different means to attack the security of the network, so that more users begin to pay attention to the identity authentication and privacy protection of the Internet of Things. This paper designs an IoT node roaming authentication model, which is used to enhance the security authentication capability of the Internet of Things to roaming devices. In order to effectively prevent malicious nodes from connecting to the network, this paper proposes a roaming authentication protocol based on heterogeneous fusion mechanism (HFM-IoT). The authentication protocol uses the remote authentication server in the local and remote areas to perform interactive authentication on the roaming device, which increases the difficulty of attacking or infecting multiple network areas by malicious nodes. According to the security analysis, the protocol can protect against multiple network attacks, and it can be seen from the experimental simulation results that the protocol has lower energy burden and authentication delay.

INDEX TERMS Internet of things, heterogeneous network, node roaming, identity authentication.

I. INTRODUCTION

IoT mobile nodes with the development of mobile communication technologies and embedded technologies, IoT devices such as handheld mobile communication devices and wireless in-vehicle devices are widely used. More users expect to be able to get network services anytime and anywhere, and the security of network communication is guaranteed, which promotes the research on roaming authentication protocols in the IoT network environment [1]–[4]. Due to the rapid development of network information technology, wireless networks have gradually developed into all-IP heterogeneous wireless networks with multiple wireless access technologies. The heterogeneous wireless networks have the characteristics of dynamic topology changes and open links [5], [6]. It makes heterogeneous wireless networks more vulnerable to attackers than traditional networks, and will face security threats such as eavesdropping and replay attacks [7], [8]. The IoT network layer in many application scenarios is a network consisting of multiple access modes and consisting of multiple heterogeneous wireless access technologies. The network structure includes the sensing layer, the transport layer and the application layer. The sensing layer is composed of sensing nodes with small storage capacity and weak computing power, and is mainly used for data acquisition, information identification and coding. The transport layer is used to provide logical communication between different device processes. In the IoT environment, mobile devices can roam between different networks. In the application layer, the Internet of Things provides a variety of web application services for application interfaces on mobile devices. Although the Internet of Things is widely used, it is also vulnerable to hackers, especially through the use of malicious programs that access the Internet of Things to attack the Internet of Things server or other mobile devices in the Internet of Things. In order to effectively suppress the

The associate editor coordinating the review of this manuscript and approving it for publication was Honghao Gao.

intrusion of hackers, a roaming authentication protocol capable of verifying the legitimacy of mobile devices is needed. Therefore, the design of roaming authentication protocols in the IoT network environment is faced with higher security requirements [9], [10].

In the IoT environment, the user's communication equipment can spontaneously and automatically interact with other objects or the outside world through certain technical means, but the trust problem between the Internet of Things devices must be solved [11]. In the traditional centralized system, the trust mechanism is relatively easy to establish, and there is a trusted third party to manage the identity information of all devices. During the operation of the network, the communication request of the legal device is allowed, and the illegal identity device is denied access to the network, but the identity information of all devices needs to be recorded in advance to the management center [12], [13]. In today's IoT communication system, due to the popularity of mobile communication devices, more wireless roaming requirements are proposed for the Internet of Things. Many roaming target domains of mobile communication devices are usually random, so identity information cannot be recorded in advance. Network Management Center [14], [15]. In order to ensure the security of the Internet of Things while satisfying the wireless roaming requirements of legitimate mobile communication devices, it is necessary to use an authentication protocol in the Internet of Things to verify the identity information of the device requesting communication.

Safkhani et al. proposes an Internet of Things ultra-light authentication protocol, which protects against the privacy protection of IoT devices during communication and prevents passive privacy breach attacks [16]. Li et al. proposed an IoT mutual authentication protocol based on key change. The protocol uses an integrated random number generator. The calculation of secret parameters uses a one-way hash function. And the protocol has a key backup mechanism to enhance the security defense mechanism of the Internet of Things [17]. Wu et al. proposes a privacy-protected user authentication scheme based on Internet of Things security, which addresses some shortcomings of the Internet of Things network authentication scheme, such as no session key, lack of mutual authentication and internal attacks, offline guessing attacks, user forgery attacks and sensor capture attacks. The defense mechanism, etc., proposes a more secure IoT identity authentication system to reduce the security loopholes in the Internet of Things [18]. Jang et al. proposes an IoT effective device authentication protocol without a certification authority, which improves the authentication efficiency by minimizing the number of message exchanges. The protocol is based on a key hash algorithm, so no authorization certificate is required, which can reduce the resource consumption of the device [19]. In [20], an attribute-based IoT authentication protocol is proposed by Liu et al., which uses attribute-based encryption instead of traditional identity-based encryption (IBE), and then uses BAN logic to formally analyze the security of the protocol. The effectiveness of the protocol in enhancing encryption performance is proved by simulation experiments.

In the second section of the thesis, the IoT node roaming authentication model is introduced, and the possible roaming of the node is analyzed. In the third section, the roaming authentication protocol based on heterogeneous fusion mechanism is introduced, and the encryption mechanism of the protocol is analyzed. The security analysis of the protocol was carried out in the fourth section. In the fifth section, the experimental simulation is introduced, and the experimental results are compared with other protocols.

II. DESIGN OF IOT NODE ROAMING AUTHENTICATION MODEL

The security strategy of the IoT node roaming authentication model designed in this paper is: when the roaming node moves to a certain area, if the node needs to access the network service, the remote authentication server detects the identity legality of the roaming node, and the detected roaming node can access the network service in the area. When a roaming node wants to communicate with a node in the remote area, it needs to pass the security authentication of the remote domain authentication server in the local and remote areas at the same time.

Figure 1 shows the Internet of Things roaming authentication network model, which includes the Internet of Things Management Center CA-IoT. Remote Authentication Server (RAS), and various types of IoT roaming nodes. The roaming node is assumed to be a variety of IoT handheld mobile communication devices, such as mobile phones, iPads, etc. [21]–[24]. The Internet of Things Management Center CA-IoT is responsible for the management of all remote authentication servers, including security monitoring of remote authentication servers and open authentication of roaming nodes for cross-regional communications. The remote authentication server mainly authenticates the roaming node in its responsible area, and as the base station enables the roaming node to access the network service provided by the regional network [25]–[27], which acts as a gateway node of the regional subnet in the network model. Features. Under the management of CA-IoT, roaming nodes in different areas can be interconnected through a remote authentication server [28]–[30].

In the network model of the IoT roaming node constructed, the authentication process of the network mainly includes two scenarios. The first case is local authentication: an IoT node roams into a heterogeneous network area and requests network services within the area. Assume that the Node 2 node in Figure 2 roams into the A area. In order to access the network service of the A area, the remote authentication server in the A area needs to authenticate the Node2. After the verification, the Node2 node can access the service in the A area. The second case is cross-region point-to-point communication: It is assumed that when the Node 2 node needs to communicate with the Node 3 node of the area B, the Node 2 transmits the information to the remote authentication server RSA in

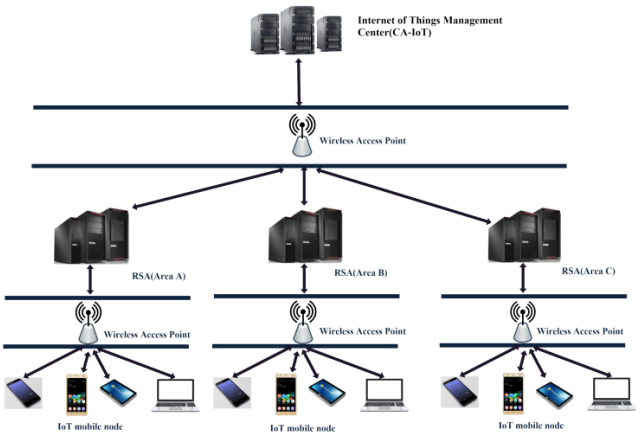

FIGURE 1. Internet of things roaming node network model.

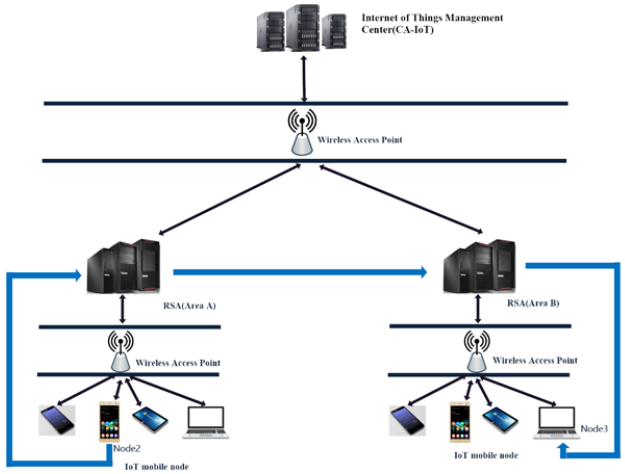

FIGURE 2. Internet of things node roaming situation.

the area. After the CA-IoT verifies the RSA of the area A, the RSA of the area A is allowed to transmit the message to the RSA of the area B. After receiving the information, after the RSA of the area B verifies the identity of the Node 2, it agrees to communicate between the Node 2 and the Node 3.

III. ROAMING AUTHENTICATION PROTOCOL BASED ON HETEROGENEOUS FUSION MECHANISM

In the roaming authentication protocol, the roaming device needs to register with the local RSA to obtain the authorization credential in the network before acquiring the local network service. Only registered roaming devices can apply for network services to RSA within the local network area. A roaming device that has been registered and obtained authorization credentials can apply for network services in the local roaming area, and can also communicate with roaming devices in other network areas with the assistance of the local RSA. The content of this section focuses on the registration process and roaming authentication process for mobile devices.

A. REGISTRATION PHASE

It is assumed that there is a node Node* that roams into a certain network area. In order to apply for network services in the area, the Node* node submits its device information PI and registered account $\mathrm{ID_{node}}$ to RSA. After receiving the {PI,$\mathrm{ID_{node}}$}, the RSA sends the message {PI $\|\mathrm{ID_{node}}\|T_*$ } to the CA-IoT according to the current timestamp T_*, and the CA-IoT decides whether to agree to the registration. In the case that the CA-IoT agrees to register, the CA-IoT uses its private key x to calculate the secret value R, get:

$$R = \mathrm{H}\left(\mathrm{ID_{node}} \| x \| T_* \right) \oplus \mathrm{ID_{CA\text{-}IoT}} \tag{1}$$

And generate the current timestamp T_D, and send the confirmation message $\{\mathrm{ID_{node}} \| R \| T_D\}$ to the RSA through the secure channel.

After receiving the confirmation message sent by CA-IoT, RSA randomly selects the secret number r_1 to generate registration authorization information:

$$RA = R + r_1 \mathrm{ID_{node}} \tag{2}$$

Then randomly select the secret number r_2 to form a temporary password:

$$PD = H\left(\mathrm{ID_{node}}, r_2\right) \tag{3}$$

Then issue the authorization credentials for the Node*:

$$\mathrm{CERTIFICATE} = \{\mathrm{ID_{node}} \| RA \| t_S, PD, G_{RSA}\} \tag{4}$$

t_S indicates the effective duration of the voucher, and G_{RSA} indicates the private key of the RSA. After receiving the authorization credential information, the Node* node decrypts the message through the RSA public key PK_{RSA} to verify whether the information is sent by the real RSA.

B. NODE ROAMING AUTHENTICATION PHASE

In the node roaming authentication phase, the authentication process of the roaming device is discussed in the models of Figure.1 and Figure.2 mainly including two scenarios, namely, authentication of the roaming node in the local area and authentication of the remote point-to-point communication. The two certification scenarios will be introduced separately below.

1) LOCAL NETWORK AREA AUTHENTICATION

A discussion of the first scenario is made in this section, it is about the authentication process of local roaming devices when applying for network services. It is assumed that the Node 2 node passes through the A area and needs to accept the roaming service from the A area. Before providing the service, the RSA of the A area needs to perform roaming authentication on the Node2 node first, and then allows the Node2 to enjoy the network service in the area after the authentication is passed.

First, the RSA of the A area exposes the system parameters as the system public key. Suppose Node2 enters account

ID_2 and temporary password PD_2 in area A, and randomly generates a secret number r_2 and calculates:

$$NB_2 = (RA \oplus PD_2) \oplus r_2 \tag{5}$$

Then, Node2 generates a message $Message = (\text{CERTIFICATE}, ID_2, PD_2, NB_2)$ according to the existing authorization information, and sends the verification information $Enc\{PK_{RSA} \| ID_2 \| Message \| T_2\}$ to the RSA according to the current timestamp T_2. After receiving the verification information, RSA first detects the freshness of the timestamp T_2, then decrypts the information with the public key, verifies the legitimacy of Node2, and randomly selects the secret number r_A, calculates $Y = rPK_{RSA} + r_A PK_{RSA}$, and then calculates $G_A = H(ID_2, Y)$. At this time, the RSA of the B area will save the information $\{ID_2, G_A\}$, and retain the account information of the Node2 in the database, and send the information $CTK_A = \{ID_{A,RSA}, ID_2, Y, T_c\}$ to the Node2 through the secure channel, and T_c indicates the current timestamp.

After receiving the information sent by the RSA in the A area, the Node2 will verify the source of the information and detect the freshness of the time stamp T_c and retain the information. When accessing the network, Node2 uses the registered account ID_2 and password PD_2 to log in to access the network service of the A area.

2) REMOTE PEER-TO-PEER COMMUNICATION AUTHENTICATION

A discussion of the second scenario is made in this section, that is, the authentication process taken when peer-to-peer communication between two different roaming devices in two different network regions. It is assumed that the Node2 node needs to communicate with the Node3 node in the area B. First, it is necessary to obtain the permission of the RSA of the area B, so that the Node 2 can transmit the information to the RSA of the B area through the gateway RSA node of the area A. Then, the information is transmitted to the Node3 node through the RSA of the B area, thereby establishing a communication channel between the Node2 and the Node3.

The Node2 node randomly generates a secret number r_2^*, and sends the login request message $Message_2 = \{Session_2, r_2*, ID_2, ID_{A,RSA}\}$ to the RSA of the A area, and then sends the information to the RSA of the B area through the RSA of the A area, and $ID_{A,RSA}$ represents the ID information of the RSA in the A area. $Session_2$ denotes a new secure session established between the Node 2 node and the RSA of the B area. When the RSA of the B area receives the message $Message_2$, the RSA stores the secret number r_2^* and generates a new secret number $r_{B,RSA}$, and sends a delegation verification message $Message_{B,RSA} = \{\text{verification request}, r_{B,RSA}, ID_{B,RSA}\}$, verification request is a request prompt message, prompting the RSA of the area A to perform the Node 2 Authentication.

After receiving the data of $Message_{B,RSA}$, the RSA of the area A first sends a message $\{ID_{A,RSA}, ID_{B,RSA}\}$ to the CA-IoT, and the CA-IoT confirms whether the two areas are in a cooperative communication relationship. If the CA-IoT confirms that the area A and the area B can cooperate, it will respond to a message to the RSA of the area A. After receiving the message, the RSA randomly generates a secret number $r_{A,RSA}$ and sends the message $Message_{A,RSA} = \{r_{A,RSA}, ID_{A,RSA}\}$ to the RSA of the B area.

After receiving the message $Message_{A,RSA}$, the RSA of the B area sends the message $\{r_{A,RSA}, r_{B,RSA}, ID_{A,RSA}, ID_{B,RSA}\}$ to the Node2 node. After receiving the information, anonymous roaming identity authentication starts between Node 2 and the RSA of the B area.

After receiving the message $\{r_{A,RSA}, r_{B,RSA}, ID_{A,RSA}, ID_{B,RSA}\}$, Node2 starts calculating CID:

$$CID = ID_{A,RSA} \oplus h\left(ID_2 \left\| r_2^*\right.\right) \tag{6}$$

And calculate the session key:

$$KD = h\left(ID_2 \| h\left(ID_{A,RSA} \left\| r_{A,RSA}\right.\right) \right\| h\left(ID_{B,RSA} \left\| r_{B,RSA}\right.\right)) \tag{7}$$

Calculate parameters based on the session key:

$$F_1 = H\left(KD \left\| r_2^* \right\| r_{B,RSA}\right) \tag{8}$$

Node2 then sends a message $Message_1 = \{KD, r_2^*, ID_{A,RSA}, F_1, \}$ to the RSA of the B area. When the RSA of the B area receives the message $Message_{KD}$, the RSA checks F_1 and calculates the parameter value F_2:

$$F_2 = H\left(KD \left\| r_2^* \right\| r_{A,RSA} \left\| G_{A,B}\right.\right) \tag{9}$$

$G_{A,B}$ indicates the shared key between the RSA of the A zone and the B zone.

After calculating F_2, the RSA of the B area will send a message $Message_2 = \{KD, r_2^*, ID_{B,RSA}, F_2\}$ to the RSA of the A area. When the RSA of the A area receives $Message_2$, it will detect the identity information $ID_{B,RSA}$ of the RSA of the B area and the parameter F_2. Then, the RSA of the A area starts to authenticate the identity of the Node2, and according to the credential information of the Node2 node reserved by the RSA, it can accurately authenticate whether the Node2 is a registered legal user. If the authentication is a legitimate user, then the RSA of the A area sends the message $Message_2 = \{\text{validation verification}, ID_{A,RSA}, r_{A,RSA}, ID_2, r_2^*\}$ to the RSA of the B area, validation verification is the message header.

IV. PROTOCOL SECURITY ANALYSIS

Replay attack. Replay attack refers to an attacker deceiving the target system by sending a packet that the destination host has received. It is mainly used in the identity authentication process and destroys the correctness of the authentication. Assume that in this system, a malicious roaming node roams into a heterogeneous network area and steals the authentication credentials of other legitimate roaming nodes through network monitoring or other methods. When a malicious node sends authentication credentials to the RSA in this area, because the anonymous roaming authentication protocol of

the Internet of Things in this article has the security negotiation and secret number of the session key, it uses a time stamp mechanism, so it can prevent unauthorized users from using replay attacks. And the two-way identity authentication between local and remote RSA and Node can also resist replay attacks by unauthorized users.

Resistant to replacement attacks. The replacement attack is to intercept normal network communication data, and perform data tampering and sniffing, but the two sides of the communication are unaware of it. Assume that in this system, roaming malicious nodes roam to a heterogeneous network. In this protocol, Node needs to register before accessing network services. RSA issues credentials and records. Even if a malicious node uses a replacement attack to intercept the login information of other nodes, it will still be recognized by the RSA when the identity credentials do not match, and it will be refused to provide services. Therefore, using a replacement attack is not effective.

Resist counterfeiting attacks. In this protocol, when a roaming malicious node roams into the system area and uses forged login information for verification, because the attacker cannot fake the RSA master key, any forged credentials of the attacker cannot pass the authentication server's legal Sexual verification.

Anti-distributed denial of service attacks. A distributed denial of service attack is when multiple attackers in different locations simultaneously launch attacks on one or several targets. Because the attack points are distributed in different places, such attacks are called distributed denial of service attacks. Due to the existence of the IoT management center, even if the RSA of a certain network is attacked by an attacker using a distributed denial of service attack, it will not affect the surrounding network. When an attacker wants to attack other network areas across the network, the Internet of Things Center It is found that traffic anomalies can abort the connection between RSAs in each area.

Two-way interactive authentication. In the roaming phase, it is assumed that the node 1 in the A area needs to communicate with the node in the B area. In addition to the authentication legality of the RSA in the A area, the RSA of the B area needs to be allowed with the consent of the Internet of Things management center. The RSA in the A area cooperates, so that the RSA of the B area entrusts the RSA of the A area to perform verification, and then the RSA of the B area receives the verification information. This two-way interactive authentication method can improve the reliability of authentication and prevent malicious nodes from spreading attacks.

Forward security analysis. The mobile roaming node sends the authentication message to the RSA in a confidential situation, and the authentication information includes a timestamp, and the freshness of the authentication message can be determined by the timestamp, even if the attacker obtains the old private key or the old one. The authentication message does not analyze the plaintext corresponding to the new authentication message.

Anti-managin attack. The attacker cannot obtain the roaming proof information $Message = (\text{CERTIFICATE}, ID_3, PD_3, NB_3)$ through the application information of the roaming node. If an attacker uses fake roaming proof information to apply for authentication to RSA, the attacker cannot pass the RSA verification due to the spoofing of the fake roaming proof information. Therefore, the use of man-in-the-middle attacks in this protocol has no effect.

Anonymity. Since the roaming device uses the validity of the roaming proof information as the authentication credential during the roaming authentication process, the roaming proof information does not include the privacy information of the user and the device, and the RSA and the roaming device adopt a randomly generated process in the mutual authentication process. The secret number guarantees the anonymity and security of the verification process.

V. EXPERIMENTAL SIMULATION AND ANALYSIS

In order to verify the performance of the IoT roaming authentication protocol proposed in this article, this paper uses experimental simulation and comparative analysis methods to compare this protocol with some roaming authentication protocols under the same simulation conditions, such as the protocol of literature [31] and [32]. Literature [31] adopted a mobile communication device identity roaming verification scheme. After experimental verification, this scheme is more secure than the traditional mobile device identity authentication protocol in the roaming stage. Literature [32] adopted a wireless roaming protocol based on single identity authentication. The protocol implements mutual authentication between the roaming server and the roaming device and generates a session key through a single channel of information, improving the security of the roaming device's identity authentication.

TABLE 1. Total network energy consumption under different security protocols.

Network running time(s)	Total network energy consumption(J)		
	HFM-IoT	Literature [31]	Literature [32]
100	132	142	150
200	213	232	241
300	295	315	326
400	377	395	410
500	456	478	498
600	521	546	562
700	581	602	618
800	642	665	684

Table 1 shows the comparison of energy consumption between the IoT roaming authentication protocol and the comparison protocol proposed in this paper. From the results in Table 1, it can be seen that the total network energy consumption results obtained by using the protocols in this article, [31] and [32] are different. Among them, using the HFM-IoT authentication protocol proposed in this article in

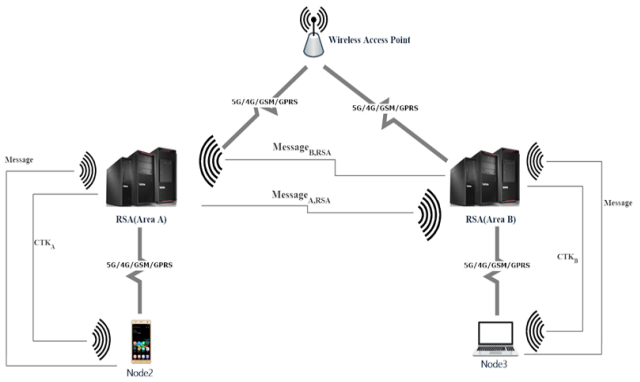

FIGURE 3. Roaming authentication structure graphic.

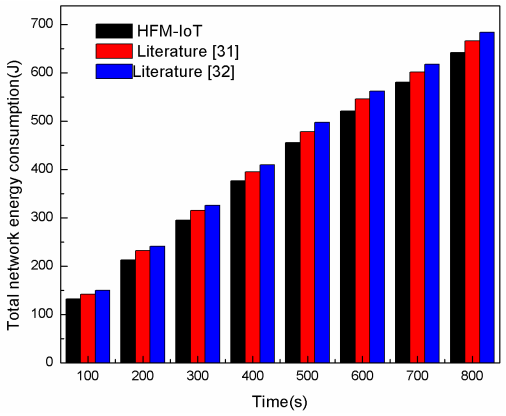

FIGURE 4. Run time and total energy consumption diagram.

the Internet of Things consumes less total network energy consumption than the protocols proposed in [31] and [32]. Because HFM-IoT reduces the computational load between Node and RSA, and reduces the number of message interaction rounds of the protocol, the computational energy consumption required for authentication is less. The running result of Figure 4 is a visual graph generated from the data results of Table 1. From Figure 4, it can be seen directly that the energy consumption of HFM-IoT is lower than the protocols in [31] and [32].

The results in Table 2 show the comparison between the HFM-IoT authentication protocol and the authentication protocols proposed in [31] and [32] on the total network energy consumption under different conditions of the number of roaming nodes. It can be seen from the results in Table 2 that even if the number of roaming nodes in the Internet of Things gradually increases, the energy consumed by the HFM-IoT authentication protocol is still less than the authentication protocol proposed in [31] and [32]. Although as the number of roaming nodes increases, the energy consumption for node communication and computing will continue to increase, however, compared with some traditional authentication protocols, the HFM-IoT authentication protocol pays less energy for protocol calculation and interactive authentication, which

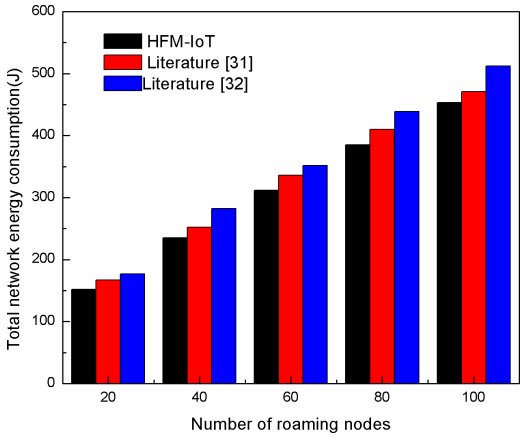

FIGURE 5. Correlation diagram between the number of roaming nodes and total network energy consumption.

TABLE 2. Total network energy consumption under different number of roaming nodes.

Number of roaming nodes	Total network energy consumption(J)		
	HFM-IoT	Literature [31]	Literature[32]
20	152	167	177
40	235	252	282
60	312	336	352
80	385	410	439
100	453	471	512

is conducive to saving network energy. Figure 5 is a visual graph generated from the data results in Table 3. From the figure, it can be intuitively shown that the total network energy consumption increases with the increasing number of roaming nodes, and the total energy cons umed by the HFM-IoT authentication protocol is less than the authentication protocols proposed in [31] and [32].

TABLE 3. Total authentication delay for different roaming nodes.

Number of roaming nodes	Total delay of nodes roaming authentication(s)		
	HFM-IoT	Literature [31]	Literature[32]
20	3.7	4.1	3.9
40	6.5	7.9	6.9
60	10.3	11.5	10.8
80	13.9	14.8	14.3
100	17.2	18.1	17.6

Table 3 shows the comparison of the total delay cost of the HFM-IoT authentication protocol with the protocols proposed in [31] and [32] for security authentication under different conditions of the number of roaming nodes. It can be seen from Table 3 that with the increase in the number of roaming nodes, the more time it takes for the network to authenticate the roaming nodes. As can be seen from

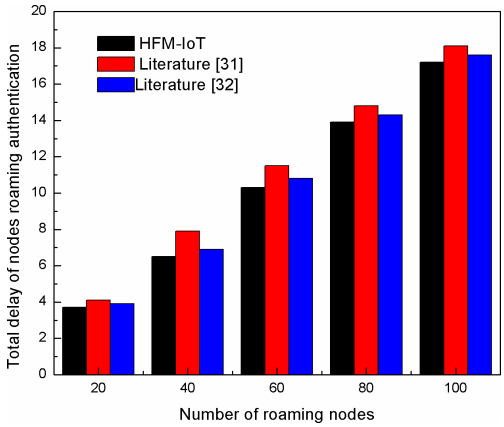

FIGURE 6. Association diagram of different roaming nodes and total authentication delay.

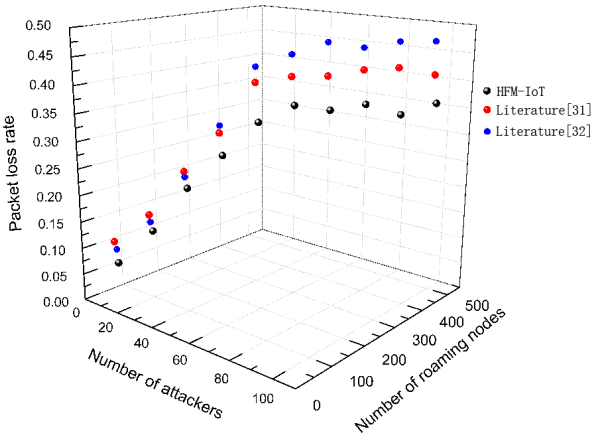

FIGURE 7. Packet loss rate under different attackers.

TABLE 4. Packet loss rate data for different attackers.

Number of attackers	Number of roaming nodes	Packet loss rate		
		HFM-IoT	Literature [31]	Literature [32]
10	50	0.07	0.12	0.09
20	100	0.13	0.17	0.16
30	150	0.21	0.25	0.24
40	200	0.27	0.32	0.34
50	250	0.33	0.41	0.43
60	300	0.36	0.42	0.45
70	350	0.35	0.42	0.46
80	400	0.36	0.43	0.45
90	450	0.34	0.41	0.46
100	500	0.36	0.42	0.47

Table 3, the total delay cost of the HFM-IoT authentication protocol is smaller. This is because the HFM-IoT protocol has fewer interaction rounds on node identity authentication, reduces the communication delay, and is more in line with the low authentication delay requirements of IoT devices on roaming services. Figure 6 is a visual display of the data table in Table 3. It can be seen from the figure that the total delay cost of the HFM-IoT authentication protocol is smaller.

In order to verify the effectiveness of the protocol in attack resistance, this article adds a certain number of nodes to the network simulation. The number of nodes changes in the interval [50,500], and different numbers of attacker nodes are added for simulation experiments. In the simulation experiment, the attacker node continuously and maliciously registers the RSA, and implements a denial of service attack to paralyze the RSA, so that normal nodes will lose packets when they communicate with the RSA. This group of experiments verifies the effectiveness of the protocol in attack resistance through the packet loss rate of the network. Figure 7 shows the packet loss rate of the HFM-IoT protocol and the literature [31] and literature [32] protocols when the Internet of Things is subjected to different numbers of attacker nodes. It can be seen from Figure 7 that with the increase in the number of attacker nodes, the number of attacks on the network increases, and the packet loss rates of the three protocols have gradually increased. The packet loss rate of the HFM-IoT protocol is smaller than the protocols in [31] and [32], which shows that the HFM-IoT protocol shows a better effect on attack resistance.

When an attacker uses a malicious access method to attack the network, in order to prevent malicious intrusion, the security verification protocol needs to spend more energy to verify the validity of the visitor's identity. In order to verify the energy loss efficiency of the protocol in the face of attacks, this article also uses a certain number of attack nodes in this set of experiments, and detects the extra energy loss of the protocol. Figure 8 shows the additional energy loss of RSA in the network under the condition of increasing the number of attacker nodes. Table 5 is the experimental data recorded by this group of experiments. It can be seen from Figure 8 that as the number of attacker nodes increases, RSA in the Internet of Things consumes more energy. Because of frequent attacks by attackers, it takes RSA to verify the validity of node identity more and more energy. From the comparison of different protocols, the additional energy consumed by RSA under HFM-IoT protocol to deal with attackers is less than that in [31] and [32], therefore, it can be seen that HFM-IoT protocol can better retain system energy and reduce energy loss when facing attackers.

When more malicious nodes attack the network, it will increase the workload of the security protocol for authentication. Because the operating speed of the security protocol is limited under certain hardware conditions, when the security protocol needs to process more malicious attack events, it will consume more computing time and have more delay when performing roaming authentication. In order to verify the roaming authentication delay of the protocol in this paper when it is maliciously attacked, in this set of experiments, the protocol is verified by gradually increasing the number of malicious attack nodes and recording the roaming authentication delay of the protocol. Figure 9 shows the additional

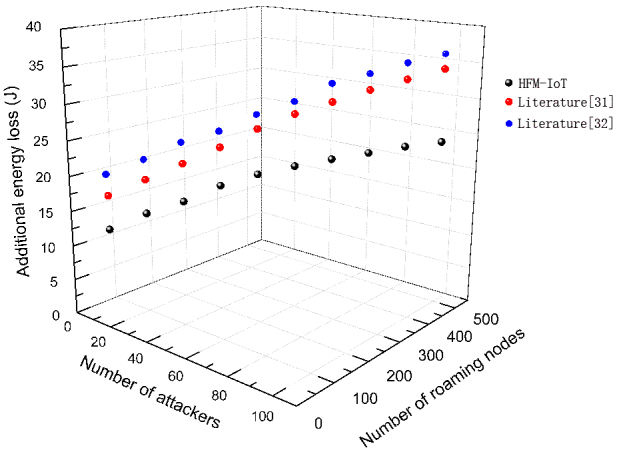

FIGURE 8. Additional energy loss of RSA under different attackers.

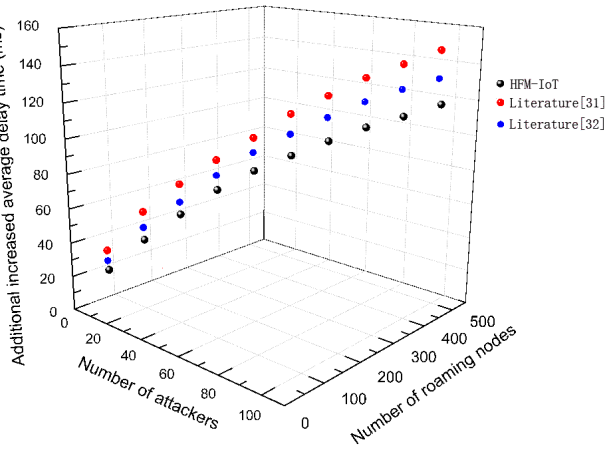

FIGURE 9. The additional average delay time for the network to perform roaming authentication.

TABLE 5. Additional energy loss table for RSA under different attackers.

Number of attackers	Number of roaming nodes	Additional energy loss (J)		
		HFM-IoT	Literature [31]	Literature [32]
10	50	12.3	16.7	18.6
20	100	14.5	18.9	20.7
30	150	16.1	21.1	23.1
40	200	18.3	23.3	24.6
50	250	19.8	25.8	26.9
60	300	20.9	27.8	28.7
70	350	21.8	29.4	31.2
80	400	22.6	31	32.5
90	450	23.4	32.4	34
100	500	24	33.8	35.2

TABLE 6. Data sheet of additional increased average latency.

Number of attackers	Number of roaming nodes	Additional increased average delay time (ms)		
		HFM-IoT	Literature [31]	Literature [32]
10	50	23.7	31.5	28.2
20	100	41.5	53.8	47.6
30	150	56.1	69.4	62.1
40	200	70.3	83	77.3
50	250	81.1	95.2	90.2
60	300	89.6	108.3	100.3
70	350	97.6	118.2	109.5
80	400	105.3	127.9	118.1
90	450	111.2	135.2	124.8
100	500	117.9	142.7	130.6

average delay time of the network during roaming authentication under the condition that the number of malicious nodes changes. Table 6 shows the data of this group of experiments. From the simulation results in Figure 9, it can be seen that with the increase of the number of malicious nodes, the average delay time added by the network during roaming authentication continues to rise. This is because the increase in the number of malicious nodes leads to a higher frequency of attacks on the network, and the computational burden of the authentication protocol is greater. Therefore, under the condition that the computing power of the server is constant, as the number of malicious nodes increases, the average delay time added by the network during roaming authentication continues to rise. From the comparison results in the figure, it can be seen that in this group of experiments, the average delay time of the protocol in this paper is lower than that in [31] and [32].

When a network is attacked by a malicious node, the security protocol takes more time to complete the authentication of all roaming nodes. In order to verify the efficiency of the protocol of this paper in the authentication of roaming nodes, in this group of experiments, set the number of malicious attack nodes to a fixed number of 50, and make the number of

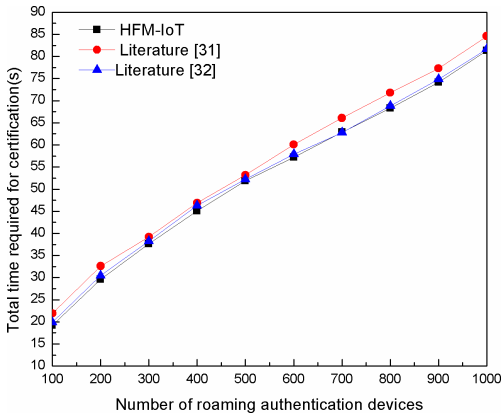

FIGURE 10. Total time spent on roaming device authentication.

roaming nodes gradually increase, and record the total time of authentication in the experiment. Figure 10 shows the total time it takes for the network to complete the authentication of a roaming device in the case of a denial-of-service attack by 50 malicious nodes. Table 7 is a table of experimental

TABLE 7. Total timeline for roaming device authentication under attack conditions.

Number of roaming authentication devices	Total time required for certification (s)		
	HFM-IoT	Literature [31]	Literature [32]
100	19.2	21.9	19.9
200	29.6	32.6	30.5
300	37.6	39.2	38.2
400	45.1	46.9	46.3
500	51.9	53.2	52.2
600	57.2	60.1	57.9
700	62.9	66.1	62.8
800	68.3	71.8	68.8
900	74.2	77.3	74.9
1000	81.3	84.6	81.7

data results. As can be seen from the data in Table 7 and the visual graph in Figure 10, in the case of a network attack, as the number of roaming devices that need to be authenticated increases, the total time spent by the network protocol for identity authentication is greater. Among them, the time cost of the protocol in this paper is smaller than that in [31] and [32], therefore, under the same conditions of network attacks, it can be seen that the authentication efficiency of this protocol of this paper is higher.

VI. CONCLUSION

Aiming at the problem of roaming authentication security of IoT mobile devices in heterogeneous environment, this paper proposes an IoT roaming authentication protocol based on heterogeneous fusion mechanism. The protocol protects heterogeneous networks and other IoT nodes by enhancing security authentication for roaming devices and preventing counterfeit malicious nodes from joining the network. In the paper, an IoT node roaming authentication model is proposed to simulate the network environment. The roaming authentication protocol of the heterogeneous fusion mechanism is used to authenticate the roaming device. It can be seen from the experimental simulation results that the proposed protocol has lower energy consumption and delay, and exhibits better performance in terms of packet loss rate and additional energy consumption when attacked by malicious nodes.

REFERENCES

[1] B. Ndibanje, H.-J. Lee, and S.-G. Lee, "Security analysis and improvements of authentication and access control in the Internet of Things," *Sensors*, vol. 14, no. 8, pp. 14786–14805, Aug. 2014.

[2] B. R. Ray, M. U. Chowdhury, and J. H. Abawajy, "Secure object tracking protocol for the Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 544–553, Aug. 2016.

[3] J.-L. Bayo-Monton, A. Martinez-Millana, W. Han, C. Fernandez-Llatas, Y. Sun, and V. Traver, "Wearable sensors integrated with Internet of Things for advancing eHealth care," *Sensors*, vol. 18, no. 6, p. 1851, Jun. 2018.

[4] W. Wei, J. Su, H. Song, H. Wang, and X. Fan, "CDMA-based anti-collision algorithm for EPC global C1 Gen2 systems," *Telecommun. Syst.*, vol. 67, no. 1, pp. 63–71, Jan. 2018.

[5] S. Rani, S. H. Ahmed, R. Talwar, J. Malhotra, and H. Song, "IoMT: A reliable cross layer protocol for Internet of multimedia Things," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 832–839, Jun. 2017.

[6] D. He, N. Kumar, and J.-H. Lee, "Secure pseudonym-based near field communication protocol for the consumer Internet of Things," *IEEE Trans. Consum. Electron.*, vol. 61, no. 1, pp. 56–62, Feb. 2015.

[7] C.-S. Park, "A secure and efficient ECQV implicit certificate issuance protocol for the Internet of Things applications," *IEEE Sensors J.*, vol. 17, no. 7, pp. 2215–2223, Apr. 2017.

[8] L. González-Manzano, J. M. D. Fuentes, S. Pastrana, P. Peris-Lopez, and L. Hernández-Encinas, "PAgIoT–Privacy-preserving aggregation protocol for Internet of Things," *J. Netw. Comput. Appl.*, vol. 71, pp. 59–71, Aug. 2016.

[9] T. Qiu, X. Liu, L. Feng, Y. Zhou, and K. Zheng, "An efficient tree-based self-organizing protocol for Internet of Things," *IEEE Access*, vol. 4, pp. 3535–3546, 2016.

[10] Y. Sun, H. Qiang, and J. Xu, "IoT-based online condition monitor and improved adaptive fuzzy control for a medium-low-speed maglev train system," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2019.2938145.

[11] A. Aijaz and A. H. Aghvami, "Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 103–112, Apr. 2015.

[12] M. Kamal and M. Tariq, "Light-weight security and data provenance for multi-hop Internet of Things," *IEEE Access*, vol. 6, pp. 34439–34448, 2018.

[13] J. K. Liu, C.-K. Chu, S. S. M. Chow, X. Huang, M. H. Au, and J. Zhou, "Time-bound anonymous authentication for roaming networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 178–189, Jan. 2015.

[14] C. Xu, X. Huang, M. Ma, and H. Bao, "An anonymous handover authentication scheme based on LTE–A for vehicular networks," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–15, Jul. 2018.

[15] W. W. X. Xia, M. Wozniak, X. Fan, R. Damaševičius, and Y. Li, "Multi-sink distributed power control algorithm for cyber-physical-systems in coal mine tunnels," *Comput. Netw.*, vol. 161, pp. 210–219, Oct. 2019.

[16] M. Safkhani and N. Bagheri, "Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things," *J. Supercomput.*, vol. 73, no. 8, pp. 3579–3585, Aug. 2017.

[17] P. Li, R. C. Wang, and X. Y. Su, "Privacy protection based on key-changed mutual authentication protocol in Internet of Things," *Commun. Comput. Inf. Sci.*, vol. 418, pp. 345–355, 2014.

[18] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," *J. Ambient Intell. Humanized Comput.*, vol. 8, no. 1, pp. 101–116, Feb. 2017.

[19] S. Jang, D. Lim, J. Kang, and I. Joe, "An efficient device authentication protocol without certification authority for Internet of Things," *Wireless Pers. Commun.*, vol. 91, no. 4, pp. 1681–1695, Dec. 2016.

[20] Y. B. Liu and W. J. Ren, "Attribute-based authentication protocol of the Internet of Things," *Adv. Mater. Res.*, vols. 765–767, pp. 1726–1729, Sep. 2013.

[21] T. Markmann, T. C. Schmidt, and M. Wählisch, "Federated end-to-end authentication for the constrained Internet of Things using IBC and ECC," *SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 603–604, Aug. 2015.

[22] Y. Kawamoto, H. Nishiyama, N. Kato, Y. Shimizu, A. Takahara, and T. Jiang, "Effectively collecting data for the location-based authentication in Internet of Things," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1403–1411, Sep. 2017.

[23] R. Madhusudhan and R. Shashidhara, "Mobile user authentication protocol with privacy preserving for roaming service in GLOMONET," *Peer-to-Peer Netw. Appl.*, vol. 5, pp. 1–22, Jan. 2019.

[24] S. A. Chaudhry, A. Albeshri, N. Xiong, C. Lee, and T. Shon, "A privacy preserving authentication scheme for roaming in ubiquitous networks," *Cluster Comput*, vol. 20, no. 2, pp. 1223–1236, Jun. 2017.

[25] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, N. Kumar, Y. Park, and S. Tanwar, "Design of an anonymity-preserving group formation based authentication protocol in global mobility networks," *IEEE Access*, vol. 6, pp. 20673–20693, 2018.

[26] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, Nov. 2017.

[27] R. Madhusudhan and Shashidhara, "A secure and lightweight authentication scheme for roaming service in global mobile networks," *J. Inf. Secur. Appl.*, vol. 38, pp. 96–110, Feb. 2018.
[28] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.
[29] J. Xu, K. Xue, Q. Yang, and P. Hong, "PSAP: Pseudonym-based secure authentication protocol for NFC applications," *IEEE Trans. Consum. Electron.*, vol. 64, no. 1, pp. 83–91, Feb. 2018.
[30] L. Wang, Q. Xie, and H. Zhong, "Cooperative Query answer authentication scheme over anonymous sensing data," *IEEE Access*, vol. 5, pp. 3216–3227, 2017.
[31] E.-J. Yoon, K.-Y. Yoo, and K.-S. Ha, "A user friendly authentication scheme with anonymity for wireless communications," *Comput. Elect. Eng.*, vol. 37, no. 3, pp. 356–364, May 2011.
[32] Q. Bao, M. Hou, and K.-K.-R. Choo, "A one-pass identity-based authentication and key agreement protocol for wireless roaming," in *Proc. 6th Int. Conf. Inf. Sci. Technol. (ICIST)*, May 2016, pp. 443–447.

ZHIPING WAN was born in Hubei, China, in 1980. He received the bachelor's degree from the Huanggang Normal College, in 2003, and the master's degree from the Guangdong University of Technology, in 2008. He was a Teacher with the Huali College, Guangdong University of Technology, from 2004 until 2008. Since 2010, he has taught at the School of Information Science, Xinhua College of Sun Yat-sen University–Dongguan, and received the title of an Associate Professor, in 2018. He has been a Visiting Scholar with Sun Yat-sen University. He has published 60 articles and holds two patents and one invention. His research interests include wireless sensor networks, cognitive radio networks, and network security.

ZHIMING XU was born in Guangdong, China, in 1996. He received the bachelor's degree from the Xinhua College of Sun Yat-sen University–Dongguan, in 2019. He is currently a Lab Manager with the School of Information Science, Xinhua College of Sun Yat-sen University–Dongguan. He holds three patents and two inventions. His research interests are embedded system and wireless sensor networks.

SHAOJIANG LIU was born in Guangdong, China, in 1991. He received the bachelor's degree from the Xinhua College of Sun Yat-sen University–Dongguan, in 2014, and the master's degree from the South China University of Technology, in 2019. He is currently a full-time Teacher with the Xinhua College of Sun Yat-sen University–Dongguan. He has published 12 articles and holds two patents and one invention. His research interests are wireless networks and machine learning.

WEICHUAN NI was born in Guangdong, China, in 1990. He received the bachelor's degree from the Xinhua College of Sun Yat-sen University–Dongguan, in 2014. He is currently a Lab Manager with the Equipment and Laboratory Management Department, Xinhua College of Sun Yat-sen University–Dongguan. He has published six articles and holds one patent and one invention. His research interests are machine vision and wireless sensor networks.

SHITONG YE was born in Guangdong, China, in 1981. He received the bachelor's degree from Jiaying University, in 2004, and the master's degree from the Guangdong University of Technology, in 2008. He was a Teacher with the Huali College, Guangdong University of Technology, from 2004 until 2019. Since 2019, he has been an Associate Professor with the Department of Data Science, Huashang College, Guangdong University of Finance and Economics. He has published 15 articles and holds two patents. His research interests include wireless sensor networks, image recognition, and artificial intelligence.