Identification Model of Power Network Information Based on Multi-dimensional Identity Authentication Technology

Nan Hu, Pan Hu, Jun Qi and Yu Xia

State Grid Liaoning Elect Power Supply Co Ltd, Informat & Commun Co, Shenyang, Liaoning 110006, China

38343464@qq.com

Keywords: Multi-dimensional identity; Grid identity information; IMSAKA algorithm

Abstract: A new improved access algorithm that is based on IMSAKA is proposed in this paper where IMSAKA authentication algorithm is briefly introduced first. IMSAKA algorithm is achieved by a long-term shared key and a serial number (SQN), which can ensure two-way authentication between user and network, and perform well in terms of integrity and confidentiality. Moreover, through serial number, users can fight against replay attacks so that attackers do not reuse authentication information RAND and AUTN to deceive network.

1 Introduction

With construction and development of electric power communication network in State Grid Corporation, communication business is no longer limited to voice and data services, and new demands have been placed on multimedia services. Therefore, it provides various multimedia services such as corporate directory, video conferencing, and linked calling, unlimited devices such as mobile phones and fixed phones or access media such as GSM, GPRS, PSTN, and WIMAX. Nowadays, State Grid Corporation of China has identified IMS as mainstream technology for next generation grid management switching network [1-2].

2 An Authentication Algorithm Combining Key-less Encryption Technology and ECC

2.1 Security Vulnerabilities in IMASAKA Mechanism

MSAKA mechanism has some shortcomings at security level.

(1) If attacker sends REGISTER request containing user's identity to obfuscate network and prevent legal users from performing authentication, which will increase time generating authentication vector AV, legitimate users will fail to operate when they want to authenticate. In other words, legitimate users will be subject to denial of service attack.

(2) IMSAKA does not guarantee user's identity protection. Moreover, if message is sent when security key has not been negotiated, eavesdroppers will capture such sensitive information and affect services such as user calls [3]. For example, that DOS attack consumes network resources and SPIT attack will occur, which threatens user's information security.

(3) Attacker can extract information about UE by analyzing traffic during session initialization. For example, attacker can obtain user’s information, the most frequently requested service and the user’s location from it. In addition, if Zb interface is not implemented, in theory, any attacker located in internal network can monitor message exchange.

2.2 Specific Process of Improved Algorithm

In order to address security loopholes in IMSAKA authentication mechanism, a new type of improved authentication algorithm that can be applied to electric power IMS network is proposed in this paper. Algorithm proposed in this paper is mainly composed of two modules. One is identity protection module, which aims to protect user privacy. The other is authentication key agreement module, which has better performance in terms of two-way authentication, authorization,

DOI: 10.25236/icme.2019.061

confidentiality and integrity.

2.2.1 Identity Protection Module

This module where key-less encryption technology is used and one-time identity mechanism is proposed protects user identity IMPI and IMPU transmitted between UE P- CSCF. What’s more, UE is able to generate one-time random identity for each newly established session, which obscures user's true identity in response to eavesdroppers [4]. Besides it, based on nature of exchange in cryptography, both communicating parties can exchange data without sharing keys, and share information in the solution. In addition, any infrastructure is not needed to be modified.

In order to generate one-time random identity, IMPI, IMPU and random key of users are entered into exchange encryption function, where a meaningless string is output as user's one-time identity. Since user will use different random key for each newly established session, each established session will generate one-time identity.

During blurring user identity module, UE generates random prime number *p*. UE and P- CSCF randomly select two random numbers *a* and *b* where $a,b \in [1, p-2]$. Moreover, the greatest common divisor *gcd(a,p-1)=1,gcd(b,p-1)=1.* Additionally, UE and P- CSCF calculate inverse of $(a-1)\bmod(p-1)$ and $(b-1)\bmod(p-1)$.

Process of exchanging messages is as follows. UE initiates session to P- CSCF. First, UE randomly selects the number *a* as private key, and calculates ID^{a}modp[5-6]. Moreover, "SIP REGISTER" message with ciphertext IDamodp as one-time identification is sent to P- CSCF through public channel. When P- CSCF receives it, P- CSCF also randomly generates number *b* and calculates $(ID^a)^b \bmod p$. Besides it, "401 Unauthorized Response" with $(ID^a)^b \bmod p$ is sent to UE through public channel, then UE increases double-encrypted ciphertext $(ID^a)^b \bmod p$ to a power of a^{-1}. According to $(ID^a)^b \bmod p = (ID^{a*(-a)})^b = ID^b \bmod p$, UE sends new REGISTER message to P- CSCF, and P- CSCF extracts user's actual ID for identity verification. What’s more, in case of successful verification, agent responds with "200 OK" message. Since input of encryption function is different, new random key is not needed, and generated ciphertext is also the same. In addition, ID represents user's IMPI and IMPU.

UE sends IDamodp to P- CSCF.

CSCF sends $(\mathrm{ID}^{a})^{b}\mathrm{modp}$ to UE.□

UE sends IDbmodp to P- CSCF.

2.2.2 Authentication and Key Agreement Module

The first step is designed to address need for mutual authentication between UE and HSS to manage there after user is authorized. The second step is to establish confidentiality and integrity keys to achieve IPSec associations so that SIP messages transmitted between UE and P- CSCF can be protected. In addition, this module must ensure that it is not replayed when performing authentication[7-8]. Since Elliptic Curve Cryptography technology meets all needs of this module, ECC technology is used in this module.

The first step: Mutual authentication of UE and HSS. First, meaning of parameters in HSS execution steps is described. *p* is generated prime number, elliptic curve equation on FP is $E_p(a,b): y^2 = x^3 + ax + b(\bmod p)$, $a,b \in F_p$, $4a^3 + 27b^2 \neq 0(\bmod p)$, and B refers to base point on elliptic curve. Besides it, $S \in z_p^*$, which is stored in UICC of HSS and UE, h (*) refers to secure hash function, and shared message sent by HSS is $\{E_p(a,b), B, h(\cdot)\}$.

When UE is registered to IMS network, it uses HSS to perform following steps.

(1) UE selects a random private key $x \in z_p^*$ and calculates its public key V = x * B. Then, REGISTER request containing public key (V) is sent to HSS.

(2) Upon receiving the request, HSS randomly generates private key $c \in z_p^*$ whose public key and session key AICK = c * V are calculated according to W = c * B. HSS authentication token is calculated through $Auth_{Hss} = h\left(w \| s * AICK\right)$, and UE authentication token is calculated through $Auth_{UE}' = h\left(V \| s * AICK\right)$. Then, HSS sends its authentication token to terminal UE with its public key (W).

(3) After UE receives the message, UE calculates session key AICK = c * W locally and calculates HSS authentication token $Auth_{Hss}'$. Then, UE verifies whether $Auth_{Hss} = Auth_{Hss}'$ is established. If it is established, HSS identity will be authenticated. Next, UE calculates its authentication token and sends it to HSS.

(4) HSS compares received token with the token that has been calculated. If they are equal, UE will be authenticated.

Figure 1 below is access flow chart of improved algorithm.

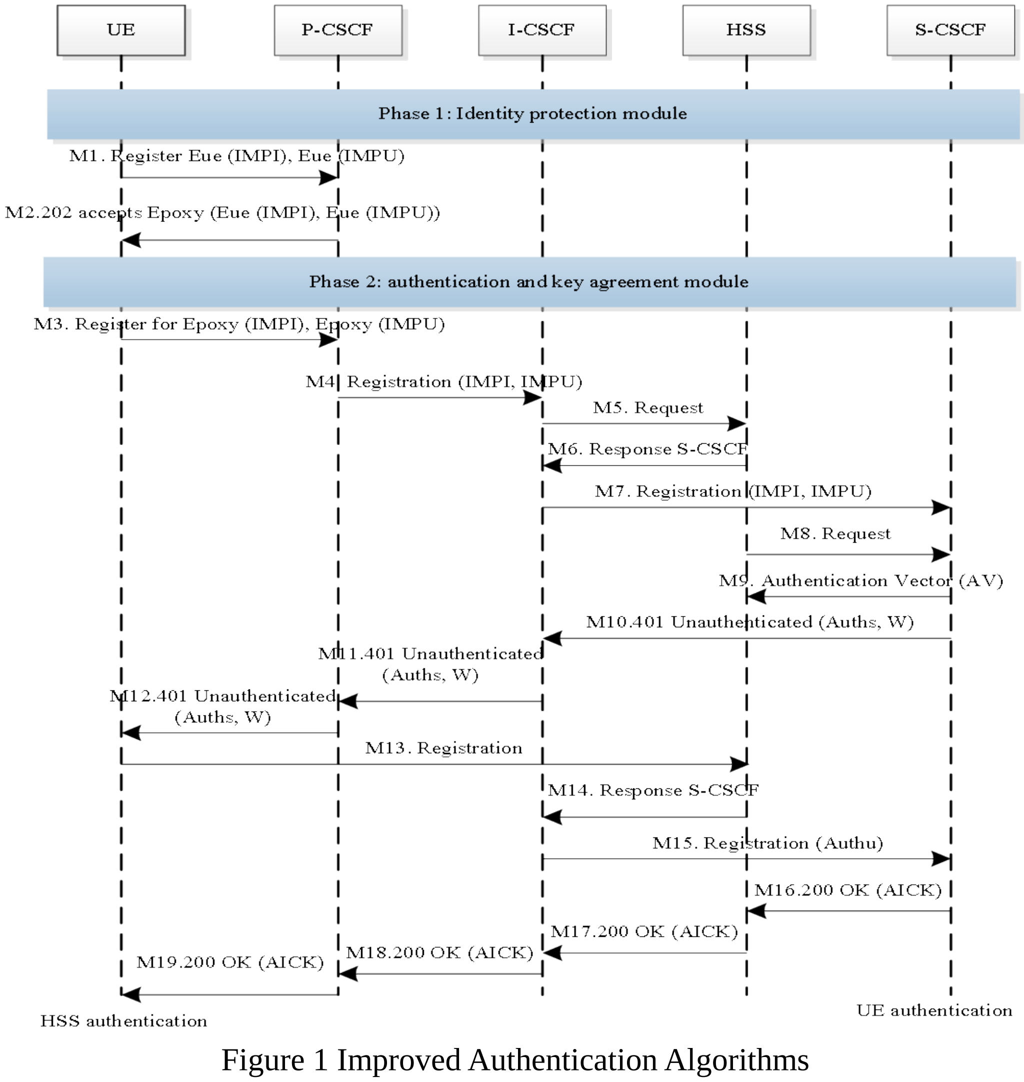
UE
P-CSCF
I-CSCF
HSS
S-CSCF
Phase 1: Identity protection module
M1. Register Eue (IMPI), Eue (IMPU)
M2.202 accepts Epoxy (Eue (IMPI), Eue (IMPU))
Phase 2: authentication and key agreement module
M3. Register for Epoxy (IMPI), Epoxy (IMPU)
M4. Registration (IMPI, IMPU)
M5. Request
M6. Response S-CSCF
M7. Registration (IMPI, IMPU)
M8. Request
M9. Authentication Vector (AV)
M10.401 Unauthenticated (Auths, W)
M11.401 Unauthenticated (Auths, W)
M12.401 Unauthenticated (Auths, W)
M13. Registration
M14. Response S-CSCF
M15. Registration (Authu)
M16.200 OK (AICK)
M17.200 OK (AICK)
M18.200 OK (AICK)
M19.200 OK (AICK)
HSS authentication
UE authentication

Figure 1 Improved Authentication Algorithms

3 Algorithm Simulation and Analysis

Replay attack: It is supposed attacker intercepts the first REGISTER (V) message and replays it to simulate UE. However, since attacker has neither secret key "s" nor private key "x" refreshed for each new session, correct AuthUE cannot be calculated and sent to HSS, identity of UE cannot be faked. If attacker intercepts message 401 Unauthorized and replays it to simulate HSS, but intercepted information has actually expired and belongs to old session, UE-side authentication cannot be achieved.

SPIT attack: Only when user's identity is known can SPIT attacks be triggered. In algorithm proposed in this paper, dedicated module based on key-less encryption is used to obfuscate these identities to prevent such attacks.

DoS attack: This attack is based on SQN and its synchronization. However, authentication algorithm proposed in this article does not use SQN. Since it does not require synchronization process, attacker cannot launch such an attack.

Table 1 Comparison of Attack Capabilities Between IMSAKA Algorithm and Optimization Algorithm

Attack type	Improved	proposed improved algorithm
Replay attack	Can cope	Can cope
Man-in-the-middle attack	Can cope	Can cope
SPIT attack	unresponsive	Can cope
DOS attack	unresponsive	Can cope

4 Conclusion

Nowadays, IMSAKA is the most widely used authentication mechanism in IMS networks. However, there are still some vulnerabilities in its security and there is room for improvement in performance. In response to this problem, optimization algorithm proposed in this paper uses key-less exchange encryption technology and Elliptic Curve Cryptography to improve IMSAKA, which not only inherits the advantages of IMSAKA mechanism that can deal with replay attacks and MITM attacks, but also solves DoS and SPIT attacks that IMAAKA cannot solve. In addition, compared with IMSAKA, optimized algorithm has enhanced performance, which reduces calculation cost of CSCF and authentication time. Moreover, optimization algorithm proposed in this paper provides good idea for ensuring secure access of power administrative switching network used by State Grid Corporation.

Acknowledgement

This paper is supported by the project "Research on Key Technologies of trusted identity authentication for core business of power grid", which number is 5222xt180030.

References

[1] Chen Jun. Building a unified identity authentication system based on a distributed SOA architecture [J]. Electronic Technology and Software Engineering, 2019 (10): 168-169.

[2] Hua Jianxiang, Qu Xia. Research on Unified Identity Authentication System Based on LDAP Protocol [J]. Intelligent Computer and Application, 2019, 9 (03): 129-132.

[3] Wang Yao, He Chunzhen, Kang Ying, et al. Application of unified identity authentication in enterprise information system [J]. China Management Informationization, 2019, 22 (01): 193-196.

[4] Su Yatao. Research and Implementation of University's Unified Identity Authentication Platform Based on CAS Framework [J]. Journal of Xi'an University of Arts and Science (Natural Science Edition), 2018, 21 (04): 78-83.

[5] Su J.T., Lin F.H., Zhou X.W., Lv X., Steiner tree based optimal resource caching scheme in fog computing, China Communications, vol. 12, no.8, pp. 161-168, 2015

[6] Dun Xinhui, Zhang Yunqiu, Yang Kaixi. Fine-grained sentiment analysis based on Weibo [J]. Data analysis and knowledge discovery. 2017 (07)

[7] Hongwen Hui, Chengcheng Zhou, Shenggang Xu, Fuhong Lin, A Novel Secure Data

Transmission Scheme in Industrial Internet of Things, China Communications, vol. 17, no. 1, pp. 73-88, 2020.

[8] Fuhong Lin, Yutong Zhou, Xingshuo An, Ilsun You, Kim-Kwang Raymond Choo, Fair Resource Allocation in an Intrusion-Detection System for Edge Computing: Ensuring the Security of Internet of Things Devices, in IEEE Consumer Electronics Magazine, vol. 7, no. 6, pp. 45-50, 2018. doi: 10.1109/MCE.2018.2851723.