Lightweight Security Authentication Mechanism towards UAV Networks

Teng Li*, Jianfeng Ma*, Pengbin Feng*, Yue Meng*, Xindi Ma*, Jiawei Zhang*, Chenyang Gao† and Di Lu†
*School of Cyber Engineering, Xidian University, Shaanxi, China
†School of Computer Science, Xidian University, Shaanxi, China
Email: litengxidian@gmail.com

***Abstract*—The drones in the UAV networks can communicate with each other through wireless link. Due to the limited computing resources and complicated external environment of drones, UAV networks are subjected to various attacks such as forgery attack, man-in-the-middle attack and reply attack. Identity authentication is extremely urgent to be established before the drones start to communicate with each other and ensuring a legal drone in the network is the priority of UAV network security. However, traditional authentication mechanism based on username/ password or dynamic key has low secure level. RSA certification needs long session key which can not meet the lightweight requirement in the UAV networks. In this paper, we propose a lightweight identity authentication method based on ECC (Elliptic Curve Cryptography). We design three main steps: ECC certification initiate, identity authentication and key consistency verification. The first two steps can guarantee the two-way identity authentication and the third step verify the consistency of session key. Compared with traditional authentication method in UAV networks, our approach has shorter key and lower computing workload. Considering the security, our approach solves the problem of key inconsistence caused by calculation faults or packets transmission drops which can guarantee the UAV identity authentication secure. We apply our approach in the UAV networks and evaluate the runtime and anti-attack performance. The results show that the proposed method can be effectively used in drones identity authentication.**

***Keywords*—UAV networks; Identity authentication; ECC**

I. Introduction

The UAV network consists of a team of drones that can communicate with each other. Compared to a single flight system, the whole team of drones can meet the operational needs of different missions. Each drone in the network can perform different tasks and deploy different network topologies to meet different task requirements. The drone team can expand task execution coverage area. The drones often carry secret data or tasks which even related to national security. When UAV topologies changes, new drones may join in the team and there must be identity authentication before the communication to prevent the malicious nodes or attackers. If malicious or adversaries hack in the UAV team, they may influence the task execution or eavesdrop the secret data through communication which can pose great threat to national security.

There are lots of research working on the authentication. The proposed method [1] improves system performance and increases the efficiency of the transmitted message without affecting security. Stenography or data watermarking technique is used to reduce overheads and increase message confidentiality. Recently, Guo et al. [2] proposed a secure and efficient mutual authentication and key agreement protocol withsmart cards for wireless communications. They claimed that their scheme could withstand variousknown types of attacks: user anonymity, withstanding theinsider attack, the replay attacks, the offline dictionary attacks. Watro [3] proposed a user authentication protocol based on the RSA algorithm of difficult-to-handle mathematical problem and the Diffie-Hellman key exchange algorithm of calculating the encryption key, but the protocol is very easy to suffer the impact of sensor nodes. Therefore, this protocol is vulnerable to users who pretend to be sensors. However, Das [4] and Tseng [5] pointed out that Watro's user authentication method is vulnerable to theft-authentication, replay and forgery attacks. Therefore to prevent these attacks, Das proposed a two-factor user authentication method. Tseng et al. further pointed out that Wong's method is easy to leak passwords and prevents users from freely changing passwords. Therefore, Tseng et al. proposed an enhanced user authentication method to handle various attacks and reduce password leakage vulnerabilities. Khan et al. [6] and Chen et al. [7] found that Das' two-factor approach requires additional security measures.

The current proposed method need to cost huge system computing resources and this can lead a lower UAV network communication quality and efficiency. Such problem can cause serious results during the emergency tasks. Thus the proposed UAV identity authentication approach should meet the following requirements: 1. Lightweight of the computing. The limited computing resource can not allow the drone to do big data analysis or huge information process. The approach should make use of the specific hardware in drone and realize the goal. 2. Identity authentication security. The approach must guarantee the security of the following communication which need to make sure the consistence of the session key negotiation.

In light of the above problems, we propose a UAV network identity authentication scheme based on elliptic curve ECC algorithm. We use the ECC digital certificate as the identity proof of the legal drone. Drones identity Signature verification is performed by using the elliptic curve-based ECDSA signature algorithm with less computation and resource consumption. Then the our approach uses the ECDH exchange

978-1-7281-2629-6/19/$31.00 ©2019 IEEE
DOI 10.1109/NaNA.2019.00072

algorithm to generate the session key used in the UAV communication. The key consistency check is performed in the following to solve the session key inconsistence problem.

We have applied our approaches in a real UAV communication network. The results show that the proposed method can effectively and precisely produce the session key and realize a secure drone identity authentication which can prevent from the cyber attacks from the malicious nodes. In summary, this paper makes the following contributions:

1. We design an ECC algorithm-based identity authentication scheme for UAV network which achieves efficient two-way identity authentication between drone nodes. Our approach has shorter key length and smaller calculation than the current UAV identity authentication method mainly using RSA digital certificates.

2. We implement UAV session key consistency check method solving the problem of inconsistent negotiation key caused by key calculation error or packet loss during message transmission. This can guarantee a higher security in UAV communication.

3. We compare our method with the existing approaches and apply it in a real UAV network and system which tests the efficient and secure performance of the method.

II. Overview and Roadmap

A. Attacker Mode

Modeling the attack types helps us to understand the security threats of the actual UAV network, and can develop corresponding security mechanisms based on this attacker model to improve the security of the UAV communication process. When a drone enters the network, this paper assumes that an attacker can initiate a message interception attack, a fake ID attack, and a replay attack.

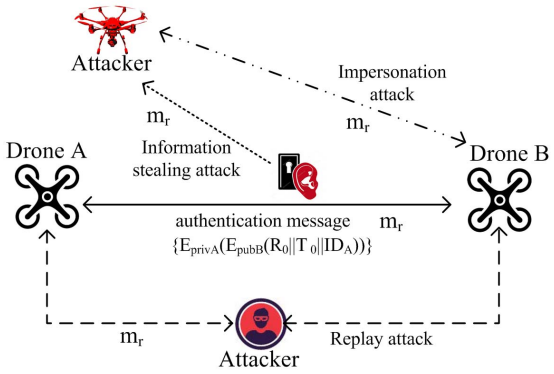

Fig. 1: Attacker Mode

We denote the identify sequence number of drone is ID_i. There are four parameters in this approach: UAV identity authentication public key (Pub_i), UAV identity authentication private key ($Priv_i$), UAV identity authentication symmetric key (K) and UAV identity authentication certification (f_i). We also define the encryption function E and the decryption function D to implement the encryption and decryption operations in the scheme. The transmission message format is denoted in Equation 1.

$$m_r = \{E_{privA}(E_{pubB}(R_0||T_0||ID_A))\} \quad (1)$$

$E_{pubB}(R_0||T_0||ID_A)$ indicates that we use the public key of done B to encrypt the identify number (ID_A), random number (R_0) and timestamp (T_0) of drone A. $E_{privA}(E_{pubB}(R_0||T_0||ID_A))$ indicates signing the encrypted information using the private key of drone A. This paper assumes that the adversary can launch the following attacks:

1. Message interception attack. The attacker can use techniques or tools to capture the authentication message m_r in the network, and analyze the message m_r to obtain valid information such as the ID of drone. Message interception attack can only steal sensitive data from network without tampering.

2. Fake ID attack. In the UAV network, the attacker obtains the identity information ID of the legal drone by intercepting the authentication message m_r transmitted between the UAV nodes, and the attacker F can use this identity to connect to the network. In this way, the attacker pretends to be a legal drone A to access the UAV network and communicate with the UAV nodes in the network, and intercepts the messages transmitted in the network or issues false messages.

3. Replay attack. The attacker can send a message that the destination host has received to achieve the purpose of spoofing the system, and obtain the sender's authentication message m_r, which is mainly used for the identity authentication process and destroys the correctness of the authentication. The attack can be a drone or ground facility, defined as attacker C. C can intercept the message m_r sent by A to the B through the solid line. C masquerades that A forwards m_r to B according to the path indicated by the dotted line, and B misunderstands that C is A, and sends the response message to C. Although the message m_r is encrypted, C can directly masquerade as A to send a message to B without deciphering.

III. Identity Authentication based on ECC Algorithm

The certificate-based authentication scheme is a traditional public key-based multicast authentication scheme. The certificate authentication scheme based on traditional public key algorithms such as RSA usually has high computational, communication, and storage overhead. In contrast, the ECC algorithm and ECDH key exchange are used to authenticate the identity of each node in the network. In theory, the algorithm can get to a higher security level and reduce the cost of identity authentication with a shorter key length, faster calculation speed and smaller storage overhead.

This paper adopts the elliptic curve cryptography to realize the authentication of the UAV identity. Specifically, the lightweight ECC digital certificate is used as the credential of the UAV identity, and the ECDSA signature algorithm and the verification signature algorithm are used to identify the UAV identity and verify the signature. We also use the ECDH key

exchange algorithm to negotiate the session key used in the communication process for the drones.

In order to ensure the security of communication content between drones, lightweight remote authentication technology needs to enable legal drones to exchange authentication information with each other. The machine negotiates the same encryption key and encrypts the communication content and transmits it to the other party. For the high security requirements of the authentication process, the digital certificate is used as the identity certificate of the legal drone; after the two parties exchange the digital certificate, the other party can be confirmed as a legal drone by verifying the signature of the other party's certificate. At the same time, for the communication between the UAVs, the requirements for delay, bandwidth and power consumption are high. The lightweight ECC digital certificate is adopted to reduce the consumption of system resources, and the security of the authentication scheme is guaranteed.

Specifically, the lightweight authentication scheme based on the ECC certificate can be simply divided into three stages: authentication initialization phase, identity authentication phase, and key verification.

A. Certificate Generation and Authentication Initialization

Before authenticating two communicating parties of UAV, it is necessary to initialize the authentication materials and prestore the authentication materials of the UAVs. The UAV needs to pre-store the public key of the CA at the certification center, the ECC digital certificate (including the public key) of the UAV issued by the certification center CA, the private key of the drone, and the ECC digital certificate (including the public key) of the communication drone. And a certificate revocation list issued by the Certification Authority. The structure of ECC certification is shown in Figure.

The difference between an ECC certificate and an RSA certificate is mainly the public key information and the signature algorithm. The public key information in the ECC certificate is generated based on the ECC algorithm, and the certificate is signed by an elliptic curve signature algorithm. The public key information in the RSA certificate is generated based on the RSA algorithm. The ECC certificate-based authentication scheme enables high security with a small key length and is suitable for resource-limited drone networks. During the implementation, we develop pre-existing certificate based on the OpenSSL development software library:

1. The ECC key generation algorithm generates the CA private key, and the ECC private key of both drone A and drone B. The private key information is saved in the local key management area.

2. The approach generates an X.509 CA root certificate in a PEM format using the self-signed certificate function provided by OpenSSL based on the generated CA private key.

3. Generate a certificate request file according to the private keys of the drone A and the drone B.

4. Using the CA to issue the certificate request file of the drones A and B, and generate the ECC digital certificate of the drone A and the drone B.

5. Use the UDP socket to send the certificate to the other drone for pre-storage in order to facilitate the use of the certificate information to authenticate the drone identity.

The ECC key required to achieve the same security level is significantly shorter than the RSA key, so the storage space occupied by the ECC key is smaller and the bandwidth requirement is lower, which reduces the storage overhead of the UAV network. This can enhance usability of the drone system.

B. Identity Authentication

The identity authentication phase mainly relies on the certificate information pre-stored by the UAVs in advance, which is consistent with the implementation principle of the ECC algorithm. The ECC algorithm based on the elliptic curve is used to realize the signature and verification signature of the UAV identity to verify the legality of the UAV identity. At the same time, the ECDH key exchange algorithm based on the ECC algorithm is used to generate the session key required for the following communication, which is shown in Figure 2.

Specifically, when the code is developed, the step of encrypting the random number using the unmanned private key can be implemented based on the OpenSSL signature algorithm. Specifically, the ECDSA signature algorithm is used to sign the authentication message, and the communication link is established by using the UDP socket and the signature information is sent. The receiver uses the ECDSA verification signature algorithm to verify the signature message to confirm the identity of the other party. After the identity of both parties is authenticated, the session key of the subsequent communication is generated by using the ECC algorithm based on the ECC algorithm.

According to the above steps, the two-way identity authentication of both parties can be realized. After both parties have successfully authenticated, the session key required for subsequent communication is generated. Because in the process of key exchange, the negotiated key may cause inconsistency due to problems such as packet loss or calculation errors during message transmission, so the consistency check of the negotiated key is required.

C. Key consistency check

Since the UAV network is an open network system, it is highly susceptible to external environment interference such as severe weather and unstable communication links, resulting in a security defect that cannot be resolved normally due to packet loss of transmission information. Therefore, in the process of key exchange, the key inconsistency may be caused by problems such as packet loss or calculation errors during message transmission. Since the session key plays an important role in the subsequent communication process, it is very meaningful to check the consistency of the session keys generated by the two drones.

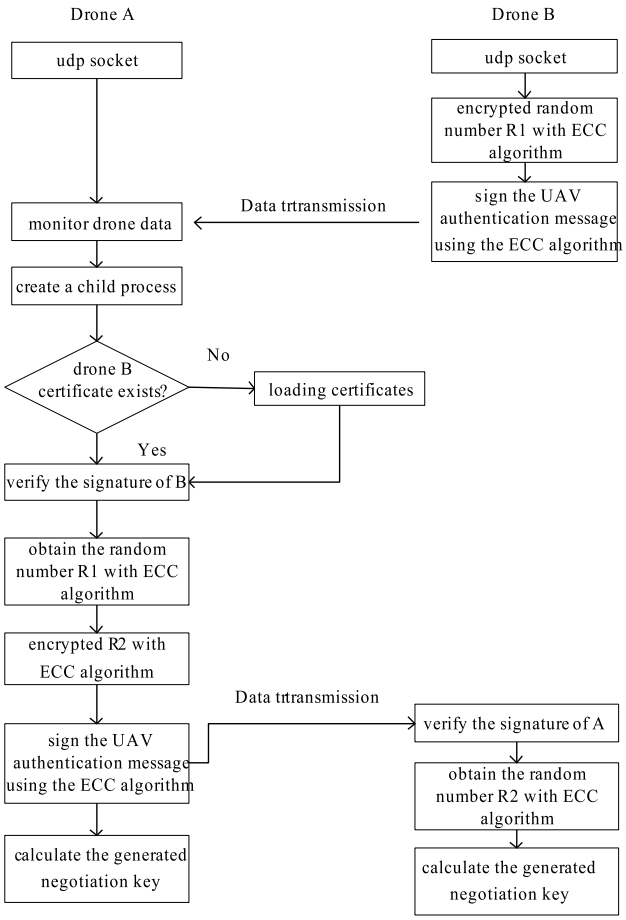

Fig. 2: Basic process of identity authentication

The steps for key consistency checking can be summarized as follows:

a. UAV A uses its SHA-1 to calculate the hash value m of the negotiation key K, and sends m to the drone B;

b. UAV B uses its SHA-1 to calculate the hash value of the negotiation key K' and sends m' to drone A. Compare whether m and m' are equal. If they are equal, the negotiation keys are consistent. If they are not equal, jump to step d;

c. The drone A compares whether the received m' is equal to the calculated m. If it is equal, the key is consistent. If it is not equal, it jumps to step d;

d. When the keys are inconsistent, the session key is regenerated according to the random number in the authentication phase until the session keys of both parties are consistent.

IV. Evaluation

This section completes the deployment of the UAV network based on the actual environment of the UAV network computer system. The real test drone network environment is shown in Figure . These include four drones that communicate with each other via a wireless link. ECC authentication scheme code developed based on OpenSSL development software package. The developed software needs to be ported to the VxWorks 6.9 development board, and the LYS-IMX6Q development board is deployed to the drone to simulate the UAV network topology environment for testing.

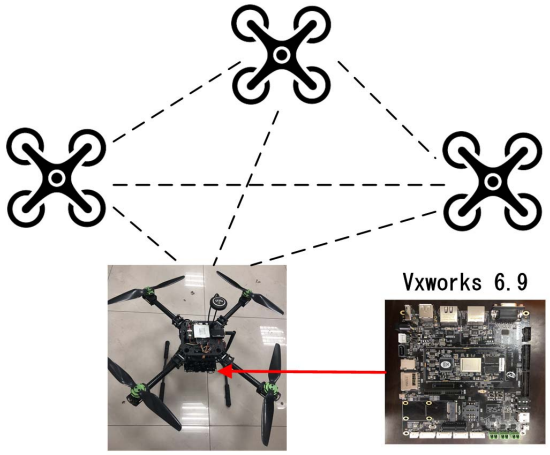

Fig. 3: Experimental UAV network environment

A. Certification scheme functional test

According to the specific requirements of the UAV network authentication function, the functional verification of the designed authentication scheme is carried out. Firstly, the security of the ECC algorithm is theoretically analyzed and compared with the key length required by the RSA algorithm. The analysis results is shown in Table

The experimental results show that when the client sends a forged digital certificate, the server fails to authenticate the client and cannot continue the subsequent operations such as the negotiation key. When the client sends the correct digital certificate, the server can perform the correct authentication and signature operation on the identity of the client. After the identity authentication is passed, a negotiation key is generated based on the transmitted random number, and the unmanned aircraft performs a consistency check on the generated negotiation key. If the two parties agree that the keys are consistent, the output ”Key consistency check passed”; if not, the output is output. ”Key consistency check failure”. The client and server side here can be drones or ground facilities.

B. The performance of authentication

Based on the functional test of the authentication scheme, the performance test based on the ECC algorithm authentication scheme is completed, which mainly compares the performance of two popular RSA and ECC algorithms in the network security protocol. The ECDH algorithm calculates the key based on the points on the elliptic curve. When the addition of points on the elliptic curve is multiplied, the original multiplication becomes a power operation, and the form is consistent with the discrete logarithm problem. Although the two forms are identical, they are not equivalent. In fact, the elliptic curve discrete logarithm problem is much

TABLE I: Security comparison between RSA and ECC

Deciphering time/MIPS	RSA key length	ECC key length	RSA/ECC key length ratio
10^4	512	106	5:1
10^8	768	132	6:1
10^{12}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1

more difficult than the large integer factorization (RSA) and DH problems. At the same time, ECDH replaces the modular exponentiation in the DH key exchange algorithm with a point multiplication operation when calculating the shared key, and the calculation amount is much smaller. Therefore, ECDH is faster and more reversible.

In the case of ensuring that a higher security level can be achieved with a smaller key, performance testing of the implemented authentication scheme is required. First, the time overhead required to generate RSA and ECC keys of different lengths was tested. The results is shown in Figure 4.

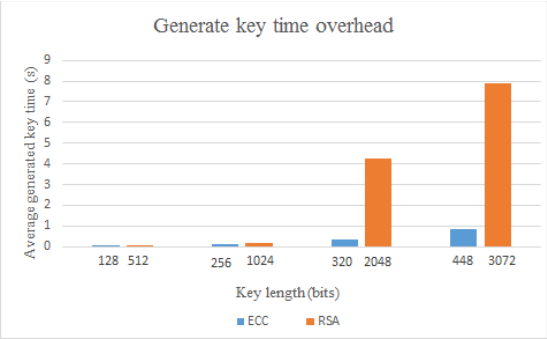

Fig. 4: Time overhead of key generation

The results show that the average generation time for generating ECC keys is shorter than RSA, and this performance advantage is more obvious as the key length increases. Secondly, we compare the time of RSA and ECDSA digital signature and verification signature.

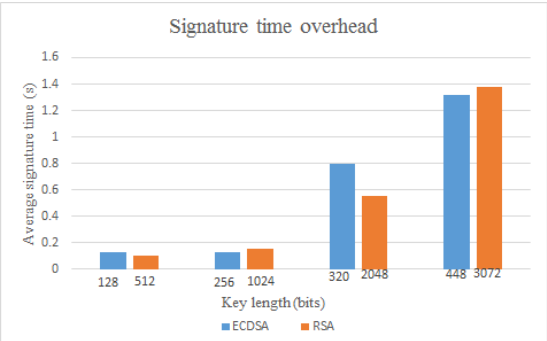

Fig. 5: Time cost of signature

When the key length is small, the performance difference between the two signatures is not very large. When the key length is gradually increased, the signature advantage of ECC gradually appears. RSA verifies signature performance better than ECDSA which is almost negligible, but the time cost of ECDSA verification signature time increases as the key length increases. Finally, the time to generate the session key for the DH and ECDH key exchange algorithms was tested. We test the time required to generate three length keys of 128 bits, 256 bits, and 512 bits.

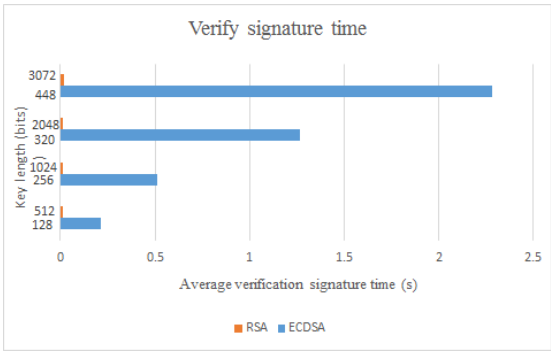

Fig. 6: Time cost of signature verification

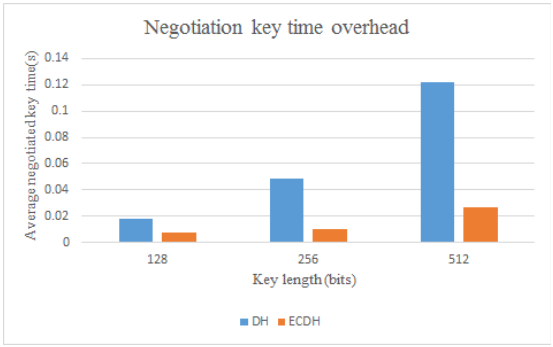

Fig. 7: Time cost of key negotiation

It can be seen from the experimental results that the ECCH key exchange algorithm based on the ECC algorithm takes less time and has better performance than the DH algorithm in generating the same length key. When implementing the same higher security level of authentication (such as 210-bit ECC key can achieve the same security level as the 2048-bit RSA key), the ECC-based authentication scheme performs better than the RSA-based authentication scheme. On devices with smaller computing and storage resources, the computational

cost of key generation can be seen as an important factor in the selection of signature algorithms. Longer keys not only consume a lot of computing resources and bandwidth when computing, but also when stored. It also consumes a lot of storage resources. When implementing the same higher security level of authentication (such as 210-bit ECC key can achieve the same security level as the 2048-bit RSA key), the ECC-based authentication scheme performs better than the RSA-based authentication scheme. On devices with smaller computing and storage resources, the computational cost of key generation can be seen as an important factor in the selection of signature algorithms. Longer keys not only consume a lot of computing resources and bandwidth when computing, but also when stored. It also consumes a lot of storage resources.

It can be seen from the experimental results that the most time-consuming operation is the key generation, and the key generation time of the ECC algorithm is nearly 10 times faster than the RSA algorithm. In terms of signature and verification signature, when the implemented authentication security level is low, the time overhead of RSA and ECDSA signature algorithm is almost the same. As the security strength increases and the key length increases, the ECDSA signature time is shorter than RSA. The RSA algorithm verifies that the signature time is negligible, and the ECDSA verifies the signature time to keep the overhead low. Finally, the performance of the ECDH key exchange algorithm is significantly better than the DH algorithm when performing key negotiation.

V. Conclusion

This paper proposes an identify authentication approach which can be used in UAV networks. The approach is based on ECC algorithm and consists of three steps. The first step generates ECC certification and initiates authentication. Then the identity authentication phase mainly relies on the certificate information pre-stored by the UAVs in advance, which is consistent with the implementation principle of the ECC algorithm. Finally, the approach checks the consistency of the session keys generated by the two drones. We implement UAV session key consistency check method solving the problem of inconsistent negotiation key caused by key calculation error or packet loss during message transmission. This can guarantee a higher security in UAV communication. The experiment shows that our approach can accelerate the speed of authentication in among drones in UAV networks and is scalable and practical for use in real UAV networks.

Acknowledgment

This research was funded by National Natural Science Foundation of Shaanxi Province (2019JM-425, 2019JM-109, 2019ZDLGY12-03, 2019ZDLGY12-04), China Postdoctoral Science Foundation Funded Project(2019M653567, 2018M640962), the Key Program of NSFC-Tongyong Union Foundation(No. U1636209), the Fundamental Research Funds for the Central Universities (JB191507, JB191508), the National Natural Science Foundation of China (No.61602357).

References

[1] M. S. Haque and M. U. Chowdhury, "A new cyber security framework towards secure data communication for unmanned aerial vehicle (uav)," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2017, pp. 113–122.

[2] C. Guo, C.-C. Chang, and S.-C. Chang, "A secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications." *IJ Network Security*, vol. 20, no. 2, pp. 323–331, 2018.

[3] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, P. Kruus, and P. Tiny, "Securing sensor networks with public key technology," in *Proceedings of the 2nd ACM Workshop On Security Of Adhoc and Sensor Networks, SASN2004*, pp. 59–64.

[4] J. Xu, W.-T. Zhu, and D.-G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[5] H.-R. Tseng, R.-H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference*. IEEE, 2007, pp. 986–990.

[6] M. K. Khann and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[7] T.-H. Chen and W.-K. Shih, "A robust mutual authentication protocol for wireless sensor networks," *ETRI journal*, vol. 32, no. 5, pp. 704–712, 2010.