MLTSM: A Crucial Multi-Layer Transmission Secure Mechanism for the Online Inspection System of Power Grid

Qinghan Wang, Jianhong Lyu, Zilong Wang, Fei Zhang, Zeyi Xu, Kemeng Jiang
State Grid Intelligent Technology Co., Ltd., Jinan, China.
wang_qinghan@163.com, lv_jianhong@163.com, 562699455@qq.com, 821661887@qq.com, 714494894@qq.com, 462115513@qq.com

Abstract*—A multi-layer transmission secure mechanism (MLTSM) with application into an online power grid inspection system is described and analyzed. Online Inspection System (OIS) is a heterogeneous system utilized in smart grid inspection, featuring multimedia data flow on different network model layers between UAV, ground controller (GC) and distributive cloud server. However, since sensitive visual and location data are frequently transmitted, which unidentified users can illegally access through any layer, a lightweight and all-around secure mechanism must be applied to the system. In particular, the mechanism is: 1. Application Layer Single-Way Encryption (ALSWE): All essential data, including data flow and storage, are encrypted and restricted for accession; 2. Transmission Layer Distributive Verification (TLDV): The UAV Security Cloud (UAV-SC) provides highly managed and centralized macroscopic authorization and key distribution. Finally, our experiment results show the highly elastic performance of MLTSM.

Keywords*—Unmanned aerial vehicle (UAV) security; online inspection system; cryptography; authorization scheme; smart grid.

I. INTRODUCTION

Online Inspection System (OIS) describes a multi-layer distributed operation and maintenance platform utilized in power grid inspection. This platform is driven by cloud services, including mission distribution and flight data collection, as stated by Liu et al. [1], with web service support [2]. The components of this system include autonomous inspecting UAVs, smart airports, and corresponding cloud services. Fig. 1 illustrates the typical scheme of an OIS.

However, given the pervasive integration of the OIS system within the smart grid, it is intricately intertwined with power equipment and power information platforms, engaging in multifaceted data interactions. [3] The security of the OIS system represents a pivotal aspect of the overall security of the power supply. We conceive and implement a multi-layer transmission secure mechanism to manage and verify online inspection terminals automatically and synthetically.

Due to the intricate network relay topology of the OIS system, multiple application service interfaces are accessible via the Internet. In the distribution of a considerable amount of application data (e.g., inspection images) across numerous devices, a series of multi-level transmission link security protocols must be incorporated into the OIS system to address the limitations of relying on firewalls and isolation devices alone in resisting replay attacks [4][5], man in the middle attack[5], social worker intrusions, and anomaly caused by unauthorized traffic[6].

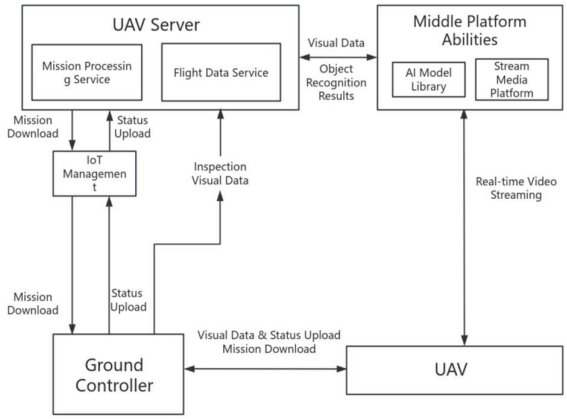

Fig. 1 Scheme of Online Inspection System

Furthermore, the necessity for intelligent protection hubs in the context of smart grid cloud services is a key consideration. In light of this, we put forward the concept of a UAV Security Cloud (UAV-SC). According to Ashish Singh et al. [7], a similar resolution is currently the Internet of Everything (IoE) Secure Cloud, with device biological print working with group encryption for passive defence. The UAV-SC is equipped with highly resilient certificate authentication performance, high-performance network security protocol access, active access traffic detection and classification capabilities, and, more importantly, working as the authorization system.

II. CRYPTOGRAPHY WORKING ON MULTIPLE LAYERS

A. Overview

The security vulnerabilities inherent to the communication as mentioned above architecture can be broadly classified into the following categories:

(1) Application layer. Images are stored and transmitted in clear text in UAV, GC, and Cloud, which can easily lead

to the leakage of images of power equipment, and the site of equipment is vulnerable to the positioning attack of social workers. The protocol stack between UAV and GC is rich and covers multiple levels of the network model, which is, therefore, essential to ensure consistent protection. At the same time, the key should be stored correctly in the chip to prevent man-in-the-middle attacks and key theft.

(2) Service layer. Replay requests or distributed attacks initiated by controlling GCs and UAVs can disrupt cloud services, compromise business information, or paralyze power information systems.

(3) Transmission layer. By illegally accessing the GC/UAV, it is possible to release replay requests or distributed attacks, which can easily lead to the disruption of the GC/UAV itself, cloud services and even the collapse of the power information system. The GC is deployed in an outdoor setting, making it susceptible to unauthorized access via the network. Keys must be stored appropriately, and the system must maintain uniform control over certificates. Furthermore, requests initiated by the terminal side should be accompanied by certificates, which can effectively filter invalid security connection requests and prevent distributed access attacks.

(4) Physical layer. The GC is deployed in an outdoor area, which is vulnerable to the intrusion of unauthorized personnel connecting to the network.

This chapter presents a secure and reliable encrypted communication system and methodology for power inspection UAVs developed based on the communication characteristics mentioned earlier in the hierarchy and architecture. This system enables the secure and encrypted communication and data protection of UAVs, GCs, and the cloud while satisfying the requirements of cryptography compliance and network protection, as shown in Table 1.

TABLE 1. POTENTIAL THREATS OF OIS AND SECURE MECHANISMS

No.	Layer	Threat	Secure Mechanisms
1	Application	direct access to clear text	Application Layer Single-Way Encryption (ALSWE)
2	Service	distributive attack, replay requests	Transmission Layer Distributive Verification (TLDV)
3	Transmission	replay, man-in-the-middle, unauthorized traffic	
4	Physical	social worker intrusion	Physical enhancements + ALSWE + TLDV

B. Transmission Layer Distributive Verification (TLDV) Between UAV and GC

Basics

In transmission layer protection, the two communicating terminals utilize the public keys embedded within the certificates of both parties and the random numbers exchanged in the preceding two-way authentication to execute the key negotiation algorithm. This generates a symmetric key for the current session, establishes a trusted connection, and encrypts the contents of the subsequent sessions of both parties with this key.

Security Mechanism

Both terminals engaged in communication verify their access through the corresponding cloud service. Once both terminals have verified their access, they engage in a signature verification process based on their respective built-in security chips, thereby enabling the encrypted transmission of information. Once the random number signatures of both the UAV and GC terminals are validated, both parties have completed the identity authentication process and are now able to proceed with key negotiation, as following steps.

Step 1. The UAV calls upon the algorithm chip to generate a random number for the terminal. It is transmitted to the ground controller (GC) along with the certificate held by the UAV.

Step 2. The GC then verifies the legitimacy of the UAV certificate and checks that the certificate is included in the access list via the cloud.

Step 3. The GC utilizes the asymmetric private key stored within the chip to sign the UAV random number digitally. Subsequently, the GC requests the chip to generate the random number and transmits the resulting signing data, the certificate held by its own party, and its random number to the UAV.

Step 4. Under the procedure above 2, the UAV then performs a verification process. To verify the legitimacy of the GC's signature on the UAV random number, the UAV utilizes the public key transmitted by the GC. This key can be employed to authenticate the signature, which will be corroborated by the asymmetric private key stored within the security chip. This process will ultimately result in the generation of a digital signature, which will be transmitted back to the GC for verification.

Step 5. The two devices utilize the public keys embedded within the certificates of both parties and the random numbers previously exchanged between them in two-way authentication to execute a key negotiation algorithm, thereby generating a symmetric key for this session and establishing a trusted connection. Both parties use the hash algorithm to verify the plain text in data transmission. Once the session has concluded, the key is irrevocably destroyed. The full algorithm is illustrated in Algorithm 1.

Algorithm 1. Transmission Layer Distributive Verification (TLDV) Between UAV and GC

Input: UAV certification $\mathbf{C_1}$, GC certification $\mathbf{C_2}$, GC private key $\mathbf{Pri_{GC}}$, UAV private key $\mathbf{Pri_{UAV}}$
Output: Symmetric key $\mathbf{K}$

	UAV	GC
1	$\mathbf{M_{UAV}}$ = {rand(), $\mathbf{C_1}$}	$\mathbf{M_{UAV}}$ = receive(UAV)
	//$\mathbf{M_{UAV}}$: verifying message of UAV	
2	send(GC, $\mathbf{M_{UAV}}$)	i_1 = verify($\mathbf{M_{UAV}}$.$\mathbf{C_1}$) && cloud.has($\mathbf{M_{UAV}}$.$\mathbf{C_1}$)
		//query Secure Cloud for UAV cert existence
3	$\mathbf{M_{GC}}$ = receive(GC)	if i_1 then
4	i_2 = verify($\mathbf{S_1}$, $\mathbf{M_{GC}}$.$\mathbf{C_2}$.$\mathbf{Pub_{GC}}$)	$\mathbf{S_1}$ = sign($\mathbf{M_{UAV}}$.rand, $\mathbf{Pri_{GC}}$)
	//verify signature of GC with public key	
5	if i_2 then	$\mathbf{M_{GC}}$ = {rand(), $\mathbf{S_1}$, $\mathbf{C_2}$}
6	$\mathbf{S_2}$ = sign($\mathbf{M_{GC}}$.rand, $\mathbf{Pri_{UAV}}$)	send(UAV, $\mathbf{S_1}$)
7	send(GC, $\mathbf{S_2}$)	else goto end
8	start_negotiation() -> $\mathbf{K}$	i_3 = verify($\mathbf{S_2}$, $\mathbf{M_{UAV}}$.$\mathbf{S_2}$.$\mathbf{Pub_{UAV}}$)
		//verify signature of UAV
9	end if	if i_3 then
10		start_negotiation() -> $\mathbf{K}$
11		end if
12	//End of algorithm, secure data sending start	
	start_crypto_session($\mathbf{K}$)	
13	Sending encrypted message with hash of original data	
14	Receiving message, decrypt and hash	
15	end_crypto_session()	
16	destroy($\mathbf{K}$)	

C. TLDV Between UAV/GC and Cloud Services

As previously outlined in section 2.2, it is similarly imperative that appropriate transport layer mechanisms are in place between the UAV/GC (terminals) and the cloud service to safeguard the cloud service access connection. Furthermore, a security gateway is incorporated at the exit point from the public network. The UAV Security Cloud (UAV-SC) oversees the management of access rules and maintains an endpoint-gateway certificate access list.

Step 1. The terminal requests the chip to generate a random number of terminals and transmits this data, along with its own certificate, to the gateway. The gateway then validates the legitimacy of the terminal's certificate and transmits it to the cloud for further verification. This process involves confirming that the certificate provided by the current terminal is included in the access list.

Step 2. The gateway generates a random number and uses an asymmetric private key to sign the terminal random number. The signing result, the certificate, and the gateway random number are then sent to the terminal, which verifies the result's legality and uses the certificate's public key to verify that the signature is valid. The asymmetric private key stored in the chip should be used to sign the gateway random number and transmit it to the gateway.

Step 3. The gateway utilizes the public key embedded within the terminal's certificate to ascertain the legitimacy of the endpoint's signature on the gateway's random number and to initiate the key negotiation process.

Step 4. Subsequent encrypted communication steps are under the specifications delineated in section 2.2. The key must be destroyed after the process.

The full algorithm is illustrated in Algorithm 2.

Algorithm 2. TLDV Between Terminal and Cloud Service

Input: Terminal certification $\mathbf{C_1}$, Cloud certification $\mathbf{C_2}$, Terminal private key $\mathbf{Pri_T}$, Cloud private key $\mathbf{Pri_C}$
Output: Symmetric key $\mathbf{K}$

	Terminal (T)	Cloud (C)
1	$\mathbf{M_T}$ = {rand(), $\mathbf{C_1}$}	$\mathbf{M_T}$ = receive(T)
2	send(C, $\mathbf{M_T}$)	i_1 = local.has($\mathbf{M_T}$.$\mathbf{C_1}$)
3	$\mathbf{M_C}$ = receive(C)	if i_1 then
4	i_2 = verify($\mathbf{C_2}$) && verify($\mathbf{S_1}$, $\mathbf{M_{GC}}$.$\mathbf{C_2}$.$\mathbf{Pub_C}$)	$\mathbf{S_1}$ = sign($\mathbf{M_T}$.rand, $\mathbf{Pri_C}$)
5	if i_2 then	$\mathbf{M_C}$ = {rand(), $\mathbf{S_1}$, $\mathbf{C_2}$}
6	$\mathbf{S_2}$ = sign($\mathbf{M_C}$.rand, $\mathbf{Pri_T}$)	send(T, $\mathbf{S_1}$)
7	send(C, $\mathbf{S_2}$)	end if
8	start_negotiation() -> $\mathbf{K}$	i_3 = verify($\mathbf{C_1}$) && verify($\mathbf{S_2}$, $\mathbf{M_T}$.$\mathbf{S_2}$.$\mathbf{Pub_C}$)
9	end if	if i_3 then
10		start_negotiation() -> $\mathbf{K}$

11	end if

D. Application Layer Single-Way Encryption (ALSWE)

The scenario described in the preceding section of this thesis provides a security framework that safeguards the integrity of each OIS device and the transmission link to the cloud. In this section, the UAV/GC local sensitive power equipment data will be protected by one-way encryption and transmitted to the cloud side for decryption, thereby enabling centralized data control.

Preparation 1. The OIS tells UAV Secure Cloud (UAV-SC) to generate a symmetric key as the terminal root key. The Terminal connects to the OIS to send the ID and certificate, and the OIS transmits the ID and certificate to the UAV-SC, which uses a symmetric cryptographic algorithm to discretize the terminal root key from this ID to obtain the terminal device key. Encrypt the device key using the public key in the endpoint certificate, and sign the device key using an asymmetric private key.

Preparation 2. The UAV-SC sends the encrypted device key, the signature value, and the certificate to the UAV and imports them into the chip. The signature value is verified using the asymmetric public key in the UAV-SC digital certificate. If the verification passes, the device key is decrypted using the asymmetric private key in the first secure chip as the working key.

Step 1. The terminal security chip performs a series of operations to ensure the confidentiality of sensitive information. It first calculates a checksum value for the data and then generates a completely random symmetric key. This key is then used as the working key to encrypt the sensitive information.

Step 2. Once the encryption process is complete, the working key is encrypted with the device key and then combined with the sensitive information cipher text and checksum value to form a combined message, which is then stored.

Step 3. The information is sent back to the Cloud, which passes the stored combination of information and the device's own unique ID to the UAV-SC.

Step 4. When Cloud needs plain text information, UAV-SC discretizes the terminal's root key against the ID to get the terminal's unique device key. The terminal key is used to decrypt the working key, and the working key is used to decrypt the sensitive information.

Step 5. The checksum value of the decrypted sensitive message must be calculated and compared with the checksum value present in the combined message.

The full algorithm is illustrated in Algorithm 3.

Algorithm 3. Application Layer Single-Way Encryption (ALSWE)

Input: Terminal root key **R**, Terminal ID **I**, Terminal certification “cert”, Plain text **P**
Output: Cloud outputs plain text **P**

	Preparation	
1	**R** = key_generate() -> Terminal	
2	Terminal sends {**I**, cert} to UAV-SC	
3	UAV-SC discretize {**R, I**} -> **K**	
4	Sign **K** with cert.**Pub**	
5	Import signed **K** to terminal, terminal verify **K**	
	Terminal (T)	Cloud (C)
1	**E** = {Hash(**P**), encrypt(**W**, **P**)) //E: encrypted text	$\mathbf{M_T}$ = receive(T)
2	$\mathbf{M_T}$ = {**E**, **I**, encrypt(**K**, **W**)}	**W** = decrypt(**K,** $\mathbf{M_T}$)
3	send(C, $\mathbf{M_T}$)	$\mathbf{P_0}$ = decrypt(**W**, **E**)
4		if hash($\mathbf{P_0}$) = hash(**P**) then
5		**P** = $\mathbf{P_0}$
6		end if

Note that the working key can be generated randomly when the terminal is turned on, or each time-sensitive data is entered to ensure its randomness and avoid lowering the security strength by using a fixed key for an extended period. The terminal key only protects the working key, and the UAV-SC controls the validity period.

III . IMPLEMENTATION, BENCHMARK, AND ANALYSIS

A. TLDV Performance

By the TLDV scenario, a test system is constructed to evaluate the performance of this cryptographic mechanism. Two sets of UAV and GC systems, each equipped with

specialized ICs for cryptographic algorithms, are deployed and accessed by the cloud service through a security gateway.

The UAV is equipped with a cryptographic chip (Figure 2) and connected to the UAV-SC. During the inspection flight, the UAV continuously transmits video in 1080P H.264 format using TCP and continuously receives and transmits UAV Events using UDP. The test is conducted ten times, and the single authentication time of the TLDV and the average latency of the TCP and UDP packet encryption are recorded (Table 2, Figure 3).

TABLE 2. TLDV LATENCY

Round	Authentication	TCP packets avg.	UDP packets avg.
1	27.45	10.246	1.213
2	44.20	12.791	1.899
3	111.15	8.840	0.946
4	217.32	8.492	1.008
5	45.14	12.261	0.960
6	27.39	11.165	1.202
7	25.17	9.037	6.315
8	28.23	12.767	2.195
9	29.38	11.884	2.441
10	42.24	10.320	2.125

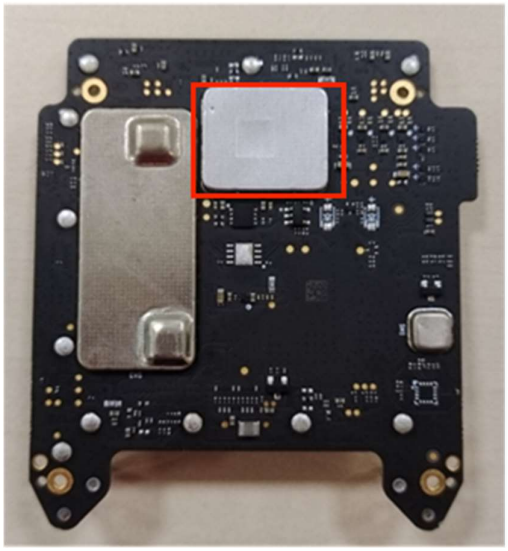

Fig. 2 UAV cryptographic chip (red)

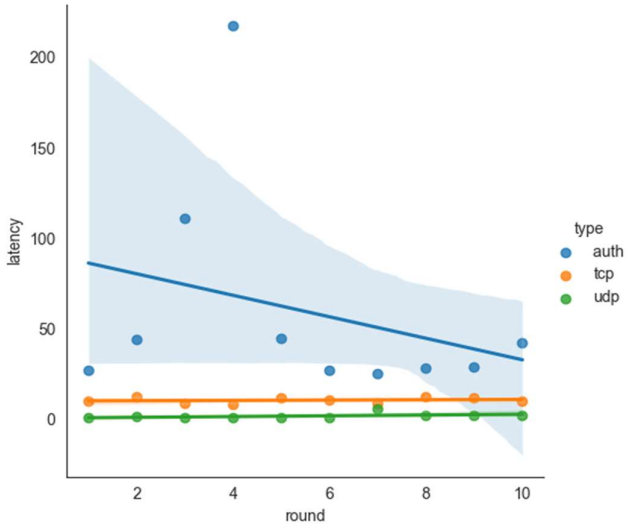

Fig. 3 Latency of TLDV mechanisms

The test data excludes the influence of the network environment, and only the API call logs are analyzed. The test environment analysis reveals that most authentication delays are distributed between 20 and 50ms, while the TCP and UDP encryption delays are between 10 and 1-2ms.

The host's high CPU utilization may cause the deterioration of authentication performance in rounds 3-4 due to the UAV's simultaneous execution of cloud service interactions. The quality of the UAV communication link may affect the UDP encryption performance in round 7, leading to an automatic delay in sending the upper layer event service.

B. ALSWE Performance

For the ALSWE scenario, we still select the OIS and UAV/GC systems from Section 3.1 and analyze their performance. The OIS sends ten routes of 20 waypoints to the GC, and the UAV takes 20-26 photos at each waypoint, with a photo capacity in the range of 4MB-12MB. The logging data includes extracting the log to record the delay in encrypting the photos and counting the delay of photo encryption by the OIS using the UAV-SC. Decryption latency is given in Tables 3,4 and Figures 4,5.

TABLE 3. ALSWE LATENCY (9.5MB < size <= 10.5MB)

Round	UAV-SC distribution	Terminal encrypt avg.	OIS decrypt avg.
1	19.12	152.236	86.880
2	16.95	149.023	90.627
3	17.04	149.595	86.543
4	28.64	138.057	85.610
5	36.30	144.411	86.840
6	19.54	147.781	89.762
7	17.88	137.095	87.052
8	20.75	138.732	89.590
9	28.93	150.003	89.155
10	21.20	149.179	86.741

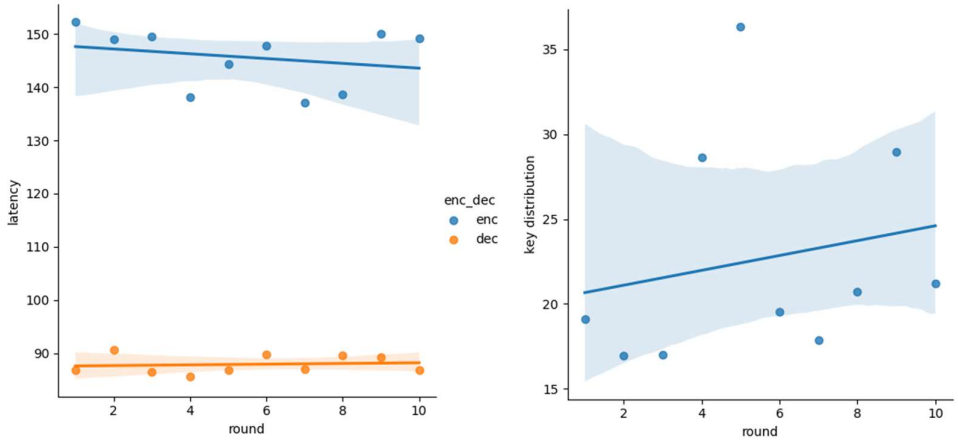

Fig. 3 ALSWE Latency (10MB level, 9.5MB < size <= 10.5MB)

The ALSWE key negotiation cloud latency is more stably distributed in the range of 15-30ms. In contrast, the encryption/decryption latency is distributed between about 140-150ms and 90ms, respectively. No significant performance degradation trend exists with the increase in consecutive execution rounds.

TABLE 4. ALSWE LATENCY (4MB level - 12MB level)

size level (MB)	Number	Terminal encrypt avg.	OIS decrypt avg.
4	38	61.922	87.854
5	152	73.608	87.515
6	290	88.194	88.136
7	189	102.450	88.715
8	440	116.680	87.850
9	418	131.067	89.398
10	329	145.611	88.007
11	199	160.170	89.542
12	85	174.743	88.838

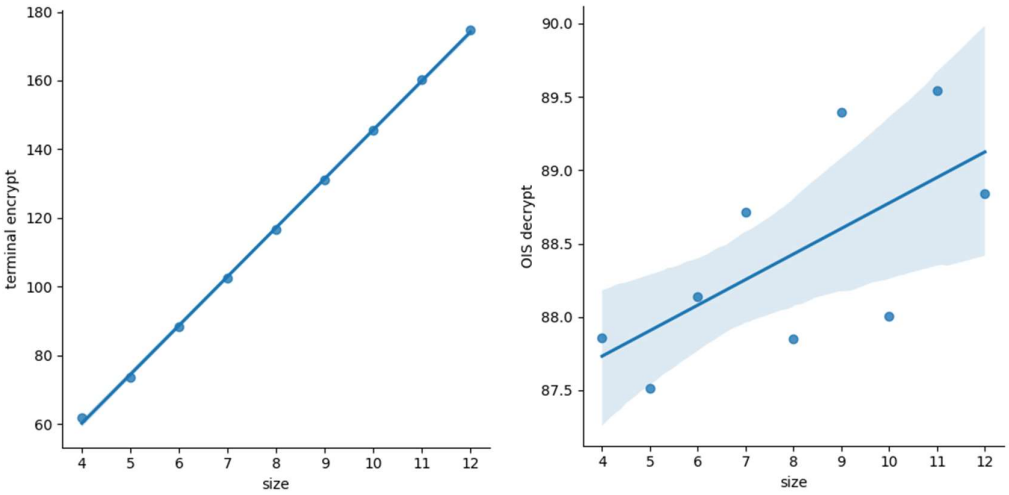

Fig. 4 ALSWE Latency (4MB level - 12MB level)

In this test, it can be found that the terminal encryption delay and the decryption delay on the OIS side deteriorate with the increase of the image size, and the terminal encryption delay is linear. Still, the deterioration of the decryption delay on the OIS side is not significant. This is because we have set up a load-balancing function for the decryption service in the OIS service, and the response latency of the corresponding server interface should be more uniform to protect the user interface operation experience. Overall, the delay of ALSWE in this test can meet the usage requirements.

IV. SUMMARY

The Multi-layer Transmission Secure Mechanism (MLTSM) proposed in this paper provides a comprehensive set of protection measures for the power online inspection system (OIS), fortified at both the transmission layer and application layer services. Additionally, the paper introduces the concept of the UAV Secure Cloud (UAV-SC), which aims to provide centralized intelligent security protection for UAVs and ground control devices. In both the physical and simulated access tests, MLTSM demonstrated superior performance, meeting the actual power inspection business requirements and resisting common attack methods, including man-in-the-middle attacks, distributed attacks, key stealing, and illegal connections.

ACKNOWLEDGEMENT

We thank the Manufacturing High-Quality Development Project of MIIT (No. TC220A04X-2) for funding this work.

REFERENCES

[1] H. Liu, G. Su, M. Hunag, “Design and application of automatic inspection system for smart distribution station based on cloud-edge collaboration,” International Conference on Artificial Intelligence and Intelligent Information Processing (AIIIP 2022): 17-19 June 2022.Qingdao, China.: Society of Photo-Optical Instrumentation Engineers, 2022:1245604-1-1245604-6.

[2] C. Mannebeck, “Online Field Inspection Manager (OFIM)Grid inspection web service.” Chemical engineering transactions: 3rd International conference on environmental odour monitoring and control (NOSE 2012), 23-26 September 2012, Palermo, Italy.: Associazione Italiana Di Ingegneria Chimica, 2012:37-42.

[3] C.N. Priyanka, N. Ramachandran, “Analysis on Secured Cryptography Models with Robust Authentication and Routing Models in Smart Grid,” International Journal of Safety and Security Engineering: An interdisciplinary journal for research and applications,2023,13(1):69-79. DOI:10.18280/ijsse.130108.

[4] C. G. Leela Krishna, R., Murphy, “A Review on Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles”, XPONENTIAL 2018: All Things Unmanned, Denver, Colorado, USA, 30 April - 3 May 2018, volume 1 of 4.: Curran Associates, Inc., 2018:520-531.

[5] T. Li, MA. Jianfeng, P. Feng, “Lightweight Security Authentication Mechanism towards UAV Networks,” 2019 International Conference on Networking and Network Applications: NaNA 2019, Daegu, South Korea, 10-13 October 2019. Institute of Electrical and Electronics Engineers, 2019:379-384.

[6] G. Bae, I. Joe, “UAV Anomaly Detection with Distributed Artificial Intelligence Based on LSTM-AE and AE,” Advanced multimedia and ubiquitous engineering: 14th international conference on future information technology (FutureTech 2019), and 13th international conference on multimedia and ubiquitous engineering (MUE 2019), April 24-26 2019, Xi an, China.:Springer Nature Singapore Pte Ltd., 2020:305-310.

[7] A. Singh, A. Kumar, S. Namasudra, “DNACDS: Cloud IoE big data security and accessing scheme based on DNA cryptography, “. Frontiers of Computer Science,2024,18(1):181801. DOI:10.1007/s11704-022-2193-3.