

Received February 1, 2022, accepted February 21, 2022, date of publication February 24, 2022, date of current version March 4, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3154012

A Novel Moving Target Defense Scheme With Physical Unclonable Functions-Based Authentication

CHUAN-GANG LIU 

Department of Multimedia and Game Development, Chia Nan University of Pharmacy and Science, Tainan 71710, Taiwan

e-mail: chgliu@mail.cnu.edu.tw

This work was supported in part by the Ministry of Science and Technology of Taiwan under Grant MOST 109-2221-E-041-001.

ABSTRACT Recent studies have discovered possible security issues on Supervisory Control and Data Acquisition systems (SCADA) in the critical architecture and focus on developing protection mechanisms on this system. Moving Target Mobile IPv6 Defense II is one of these schemes, in which the node in SCADA system employs the moving target's mobile IPv6 mechanism to solve the possible security problem the attacker targeting the specific node and launching attacks. However, the node in this novel scheme still should need to send update binding message with its new IP address to other nodes, which still possibly causes IP leakage security problem. Hence, in our study, we propose a moving target defense scheme with Physical Unclonable Functions (PUF) based authentication in SCADA system. In our scheme, PUF based authentication scheme ensures the security of the whole IP updating process. Once the nodes finish authentication process, they can perform IP generation mechanism based on unique parameter resulting from PUF outputs. Hence, our proposed scheme can ensure the unique characteristic of our generated IP address and no packet loss in the duration of IP rotation. Compared with other MTD-based schemes, our performance evaluation also shows that our proposed scheme can achieve good security performance in SCADA systems.


INDEX TERMS Moving target defense, physical unclonable functions, SCADA.

I. INTRODUCTION

Due to the advanced network technology, Internet brings many conveniences to the people's life. Message communication crossing countries just needs about few seconds. Remote control also becomes easy and hence the notion of the Intent of Things is getting popular recently. Users can easily read the messages from remote devices and control their devices through the inter-connected networks. This remote control concept is recently also implemented in national critical architecture. In the past, the national critical architectures were usually isolated from the Internet in order to ensure no attacks from the Internet to damage the national security. These national critical architectures include electricity distribution, petroleum refining, etc. They are really critical for nation's security and economy. If one of these architectures are compromised or controlled by the malicious users, the nation economy and security must face the serious and huge

damages immediately. For example, if electricity distribution is comprised and out of control, it may cause the nation cannot operate normally, which affects people's daily life and leads that many factories cannot work normally and the government operation goes down for a long while. These damages must induce large economy losses. Hence, isolating the critical architecture seems very reasonable and safe for the national security and people's livelihood. However, as the nation keeps developing and the amount of the population increases, critical architecture must expand its scope and range to fulfill the needs of the nation economy and people's life. Hence, remote control in a large critical architecture becomes necessary and the security issues of this architecture also become important to ensure that the critical architecture is safely controlled.

In national critical architectures, SCADA system plays important role controlling the whole control operations of this critical architecture and it is also widely used in controlling industrial systems. SCADA system is composed of two main components, Human Machine Interface (HMI) and Programmable Logic Controller (PLC). HMI can send signaling

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

message to PLC to execute its direct command. Hence, HMI is a user interface with which the users can control SCADA and collect the messages from sensors. However, this system has several security issues [1] if the communication model in this system is not protected by some robust security schemes. For example, the attackers can launch injection, Denial of Service attacks, replay attacks and related cyberattacks, which can cause that the SCADA system performs abnormally. They even can control the SCADA system in critical architecture to execute malicious functions and collect some sensitive information from the sensors through sending commands to the PLC. Hence, protecting the SCADA systems from penetrating is urgently crucial.

According to the previous studies [2], before the attacker launches cyberattacks targeting the remote host or server, he/she should track the target. Hence, Moving Target Defense (MTD) scheme catches much attention. The opinion of MTD is to move important network resources or host resource to another one in a specified time interval. If a host or a server is important for someone or some organization, it is necessary to avoid target discovery by attackers in order to protect the critical equipment from attacking and penetrating. This concept is really useful to avoid possible cyberattacks and has been employed in several network applications. This paper also follows this concept and proposes a more robust moving target scheme in SCADA systems.

In [3], the authors employ the rotation of dynamic IPv6 address of the device to avoid the cyberattacks from remote attackers. IPv6 can provide a significantly larger pool, which can ensure no IP collision while generating IP address. Then, the authors develop improved scheme, MTM6D II [2] employing mobile IP v6 for solving the security issues of their works [3]–[7]. However, this novel scheme still needs the binding update mechanism which helps a target mobile node (MN) inform other MN that it has changed a new temporary IP (e.g. CoA). Usually, the node in critical architecture is fixed and IP update message transferring may leak target IP address. Furthermore, they employ IPsec with IKEv2 to protect communication security, which also cause computation overhead for SCADA system. Hence, in order to solve this possible issue, we propose a moving target scheme with PUF based authentication, which can help the target node generate new IP address based on the feature of PUFs and meanwhile provides authentication between two communication peers. Furthermore, the other node also can change the target node's IP in its IP address table through the IP generation scheme based on PUFs. Hence, no IP information is transferred in public while a given node informs other nodes to update IP address at each time interval.

In a nutshell, our paper has the following contributions.

- 1) In our proposed moving target scheme, each node can execute the IP generation for the target node based on PUFs' outputs without any IP address transferring in public and execute IP rotation by itself.
- 2) In our proposed scheme, the nodes in SCADA systems can asynchronously execute the IP generation

scheme through Informing Moving Target (IMT) message transferring process. Hence, our scheme does not have the problem of time synchronization.

- 3) A light-weight PUFs based authentication algorithm can ensure the security between two communication parts in SCADA system. Furthermore, only after the authentication process, both peers can change target's IP, which can ensure no packet loss during IP rotation.

The rest of this paper is as follows. We describe the background and related works about MTD and PUFs in Section II. Then in Section III, I introduce the communication process in SCADA system and provide the proposed moving target scheme based on PUFs based authentication in SCADA systems. Section IV discusses the features and performance among our proposed scheme and other moving target scheme in SCADA systems. Section V gives some performance evaluations for our scheme and other schemes. Section VI discuss our scheme in more details and explain possible limitations. Finally, we conclude this paper in Section VII.

II. BACKGROUND AND RELATED WORKS

In this section, we discuss some related works about SCADA, moving target defense scheme and the authentication schemes based on PUFs. We firstly talk about SCADA system.

A. SCADA SYSTEM

SCADA system includes two main components, Human Machine Interface (HMI) and Programmable Logic Controller (PLC), and they perform like client-server communication model. HMI acts like a client sending request to the PLC and collecting sensor messages via PLC. HMI also can send signaling message to PLC to execute its direct command. In this communication model, PLC acts like a server listening the client's requests. When it receives the commands from HMI, it executes corresponding commands. Basically, PLC is a control unit which connects to the sensors and actuator physically. PLC can control the operations of the sensor and actuator by following the command from the HMI. Hence, HMI is a user interface with which the users can monitor the national critical architecture and control SCADA system by collecting the messages from sensors.

B. MOVING TARGET DEFENSE

Previously, the concept about moving target defense is used to protect some targets against remote attacks, for example, moving server's location in cloud applications [8]–[10], moving virtual machine [11] and moving IP address [12]. By moving target in use frequently, the attacker cannot track its target in time and hence cannot initiate remote attacks for the targets. Because it is an easy concept and efficient way to prevent possible attacks from intruding the target, many MTD applications in recent years are proposed in the security field. The important one of famous MTD based applications is to ensure the security of cloud based

service while end users use the cloud service to cope with their personal and public works. For cloud-based service applications, the administrator should locate different cloud resource for the users once he discover that the attackers intend to track the target cloud resource in use and launch some attacks on it. Hence, the authors in [9] design a protection scheme against remote attack, Distributed Denial-of-Service attack (DDoS), through moving the server's location. In their scheme, the user accesses one of the several server agents and the central controller locates another server to the user once the attack is detected. MOTAG proposed in [13] employs the authentication server to authenticate the user's legitimacy and locate cloud resource access to the cloud user. Filter ring in their scheme is responsible for detecting the abnormal access events. Once the filter ring detects the attack event, the protection scheme is initiated accordingly. Hence, through the central control, the security of cloud service can be achieved. Furthermore, this moving target scheme applying the authentication mechanism should be much securer. Our moving target scheme also follows this good design concept and exploits the PUFs based authentication in transferring Moving target's IP address message. Virtual machine (VM) live migration is also a famous cloud-based moving target method and some migration schemes are developed [14]. TALENT [15] is developed to migrate from the current cloud resource to the different platform for critical architecture. This scheme firstly detects the attack and then migrates from current cloud resource to the new one. From the above description, we discover that many cloud based moving target schemes are based on central detection method. Hence, the central server protects the cloud users' access once it detects the attacks invading the systems. Hence, it is somewhat dangerous if the attack has already invaded into the network. For critical architectures, if the attacks occur and cause the damage to the operation of these critical architectures, the nation should immediately face the dangerous and huge damage to the people's life and national economy. Based on the above observation, to develop attack prevention is rather better than to design the attack detection. In this paper, in order to build a robust and securer network environment for critical architecture, our moving target scheme is developed in prevention perspective.

Another application of moving target defense scheme, Software-Defined Networking (SDN) based application, employs the moving target concept to solve the problem of policy conflict in the process of transforming cloud platform [16]. This is a novel concept for SDN. It also needs central controller to detect the policy conflicts and then improve it. An example, OpenFlow [12] Random Host Mutation (OF-RHM), selects the unused network address and then assigns it to a given user. In this technique, it needs SDN approach to control the range allocation and mutation coordination. This technique also requests the central management and new equipment to support this IP translation. Hence, SDN based moving target scheme should need more equipment cost.

Recently, a prevention based moving target defense method, MT6D [3], is proposed. Main idea of their scheme is to change target's IPv6 address in communication process without affecting session connection. Because IPv6 addressing provides wide range of IP addresses, their scheme can frequently generate dynamic IPv6 address and address collision almost rarely occurs. In MT6D, in order to generate IP address, it creates specified parameter set, called as dynamic interface ID identifier (IID) to generate dynamic and unique IPv6 address. This parameter set is comprised of three parameters.

- (1) A identifier value for a host (seed ID)
- (2) A secret key for the both sides
- (3) A variable that is negotiated by two sides, (e.g. time)

This scheme is really novel for the moving target defense scheme. MT6D provides a secure way to change the host's IP address in a secure manner. But the authors in [2] find out the possible issues of MT6D, including time synchronization, the lack of key management and packet loss in the duration of IP rotation. Hence, the author in [2] proposed an improved version of MT6D, called MTM6D II. This scheme also utilizes the advantage of large IPv6 address range and employs mobile IPv6 scheme to update the mobile node's IP address. With IP address binding mechanism, all nodes in SCADA systems can change their IP address asynchronously. Hence, they claim their scheme has the following advantages.

- MTM6D II is loss-less because their scheme can create multiple temporal IP addresses, which can ensure no packet loss during IP rotation.
- The scheme employs IPsec with IKEv2 to ensure the security of communication process during IP rotation.
- The node in the scheme can update IPv6 address with the other node without connecting to HA.
- The node can directly connect to the other node and no permanent IP is exposed during the communication process.

Fig. 1 illustrates the brief introduction to the MTM6D II communication between two MNs.

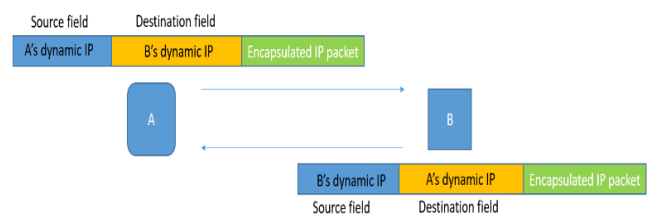


FIGURE 1. The MTM6D II communication between MNs, A and B.

In this communication, Node A hides its permanent IP address and communicates Node B with dynamic IP. Node B also responds message to Node A in a similar manner. Hence, the attacker cannot tell which one node involved in this communication. From investigation on this MTM6D scheme, we find the possible issue in MTM6D II. In MTM6D II, the target node still needs to send binding update to inform the other node that the IP address of this target node is changed.

Hence, the target node should prepare the message containing the new IP address and then send it to the corresponding nodes, which is usually a risk exposing IP to the attackers. Hence, in our scheme, we combine the authentication with moving target defense scheme, which can provide communication security and achieve IP rotation without sending new IP address to the other corresponding node. Next, we introduce the key techniques used in our scheme, authentication based on PUFs.

C. THE AUTHENTICATION BASED ON PUF

The authentication in Internet is essential for ensuring legitimacy of the network resources accessing. Hence, many authentication algorithms were proposed in the past. In the trends of Internet of Thing, the light weight authentication is much preferred and two-factor authentication algorithms are popular for the Internet of Things (IoT) environment [17]–[21]. Among them, password and smart card based authentication algorithms are developed widely. Each authentication algorithm mainly enhances or improves the previous one. The authentication in [17] is very different to other algorithms. It focuses on the node capturing attack for IoT applications and discovers a novel way to achieve the security of the authentication process in IoT. Instead of designing the whole new authentication scheme, the authors in [17] design the authentication information exchange algorithm between Gateway Node(GWN) and the sensors to avoid the secret information leakage from the sensors. Many recent authentication algorithms also employs the personal biometrics [22] (physical or behavioral human characteristics) as authentication factors, including of fingerprints, voice, typing cadence, facial patterns, etc. Recently, physically unclonable functions [23], [24] catch much attention because of its unique computation characteristic. The authors in [25] make use of this to be the second authentication factor because this function can be regarded as cryptographic primitive. Basically, a PUF is circuit which is able to provide the random physical variations for the manufacturing integrated circuits, which can generate a chip-unique signature. Because the result of PUFs is strongly relative to the physical element's characteristic, which means it is very difficult to predict and clone. Hence, authentication scheme makes use of PUFs to generate a one-way output in the authentication process. Furthermore, easy to conduct the output of PUFs also makes it popular for authenticating IoT devices [25]–[27]. Some of them make use of PUFs output to respond to a challenge [25], [28], also called challenge-response pair. Through this authentication method, the user can easily verify the legitimacy of the device. Here we introduce the challenge-response operation of PUF-based authentication scheme. A PUF's response to a challenge can be represented as $R = \text{PUF}(C)$, where R is the response of a PUF and C is the challenge. If the user wants to access a given network resource, the server issues a challenge to the user and the user should respond correct response to the server. The authors in [29] proposed

PUF-based mutual authentication for IoT environment. P. Gope and B. Sikdar [25] think the environmental noise interference may make PUF output (the response to a challenge) incorrect. Hence, they proposed a two-factor authentication scheme with the use of PUFs and reverse fuzzy extractor (FE). They therefore claim their scheme can perform well in a noisy environment. In order to prevent the illegitimate users from accessing SCADA system, we consider the authentication is also needed for the security of this system and ensuring only legitimate users able to transfer updating IP change message in our proposed MTD-based scheme. However, different to other researches, in our scheme, PUFs support not only for the authentication but also for moving target scheme. Because we focus the authentication algorithm design and moving target process design in SCADA systems, hence, noisy interference effect have not been taken into account in this paper. Our scheme still can provide a secure and robust moving target scheme in SCADA systems for national critical architectures.

III. THE PROPOSED MOVING TARGET DEFENSE SCHEME

In this Section, we introduce our novel moving target scheme with PUFs based authentication. First, we illustrate our SCADA systems in Fig. 2. There are one HMI and two PLCs in this system and four sensors are connected to PLCs. In Fig. 2, HMI sends the commands to PLCs to control PLC and collect sensor information.

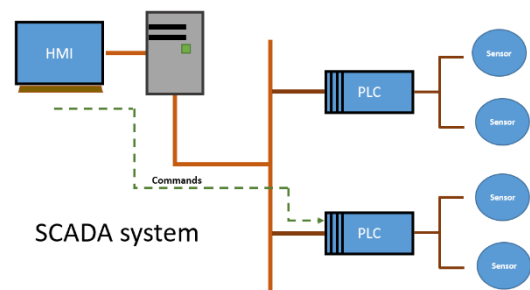


FIGURE 2. The HMI-PLC communication in a SCADA system.

Here, we introduce the communication process in SCADA system. While HMI intends to read the sensed information from the sensors connected to PLCs, HMI sends the command message, whose source IP address and destination IP address are HMI and PLC's dynamic IP addresses, respectively, to corresponding PLC. The permanent IP addresses of both sides are encapsulated in this MTD packet just like the design in [3]. In order to avoid that the attacker tracks dynamic IP addresses of HMI or PLC, both sides should execute our proposed moving target scheme.

Our scheme is comprised of two parts, one is authentication scheme and the other one is moving target scheme. Basically, two sides involved in our moving target process should execute authentication scheme firstly to validate

the legitimate access. Then the node (e.g. HMI or PLC) execute moving target scheme to generate and change dynamic IP addresses. So our scheme is also called as moving target scheme with PUF based authentication (MT-PUFAuth). Fig. 3 and 4 show our Flowchart of our MT-PUFAuth scheme. If a node (e.g. HMI) in SCADA scheme intends to execute MT-PUFAuth scheme, it should send Informing Moving Target (IMT) message to the corresponding node (e.g. PLC). In order to explain operations of both sides clearly, we define two kinds of the nodes for both sides. The first one is the active node which actively initiates moving target scheme and sends IMT message to other nodes. The second one is passive node which receives the IMT message. Basically, the proposed scheme can be executed between the active node and multiple passive nodes, but with only one passive node at each time. Then our scheme commences a challenge-response pair authentication and then the active and passive nodes execute IP generation scheme to change active node's dynamic IP address. Passive node records this active node's dynamic IP address in its IP address tables. The response in authentication process, the output of PUFs, is also later on exploited in the dynamic IP generation scheme. Now, we describe the procedure of both nodes performing our scheme as shown in Fig. 3 and 4.

- For active node: If active node intends to change its dynamic IP address, it firstly sends IMT message to the corresponding passive node. Then active node waits for the response. If the active node cannot receive the IMT acknowledgement from the passive node in a specific time interval, we regard these events as the failure events. In such case, the active node retries to send IMT message again until the retry times reach a threshold (e.g. 3). Then it selects another router to send this IMT message just like the way in [2]. Basically, in our threat model, our critical architecture performs under the wired network and the adversary cannot destroy the network physically. Hence, this failure event usually occurs due to the temporary network error. After the authentication process, active node launches moving target defense scheme. Later on, it removes its old address and uses the new dynamic IP address.
- For passive node: When passive node receives IMT message, it verifies this message and responds authentication message to the corresponding active node if received IMT message is valid. After verification of IMT message, passive node computes the active node's dynamic IP address by launching MTD scheme and stores it in its IP address table for a corresponding active node.

Then we introduce the details of the authentication and moving target schemes. Before introducing two parts in our proposed scheme, we introduce our threat model and explain our setup phase which sets up all necessary authentication information and computation factors in dynamic IP address generation process.

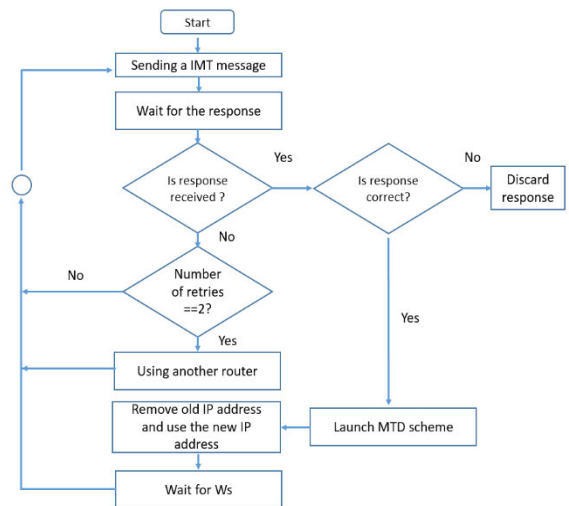


FIGURE 3. The work flowchart of active node in our proposed scheme.

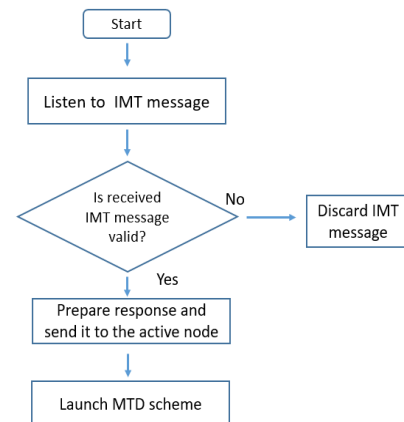


FIGURE 4. The work flowchart of passive nodes in our proposed scheme.

A. THREAT MODEL

In this Section, we describe the threat model in our SCADA system. We list the following attack capacities in our threat model.

- The adversary can eavesdrop the message between the active and passive nodes through various network tools. And hence the adversary can use network analysis tool to read the message and try to crack the messages.
- The adversary can impersonate the user to send the messages to the node in SCADA system or send control commands to the PLCs.
- In order to ensure the security of SCADA system, the network in SCADA system is usually wired and the adversary cannot destroy physically the network wire because it can be easily aware of the malicious behavior by the administrator.
- The adversary can easily clone the message sent from the active node to passive one. Hence, it can launch the replay attack.

The adversary can initiate the various attacks based on above capacities. Basically, SCADA system is vulnerable to these attack behaviors without any security defense schemes. Table 1 lists the used parameters in our work.

TABLE 1. The symbols used in this paper.

Symbol	Definition
UID	One-time identity
SK	The shared session key
PUFs	Physically Unclonable functions
C	The Challenge
R	Resulting output of PUF(C)
K_n	The random nonce
$h(\cdot)$	The hash function

Next, we explain the setup Phase as follows.

B. SETUP PHASE

Basically, HMIs and PLCs may be active or passive node alternately depending on who initiating this moving target event. Hence, all nodes should execute necessary setup operations in Setup Phase. These operations in Setup Phase should be carried out in a secure channel before our scheme beginning. The goal of these operations is to setup authentication information and a challenge set for active nodes and their corresponding passive nodes in SCADA systems. The operations of this phase is similar to the setup phase proposed in [25]. But different to [25], in our scheme, one active node may communicate with multiple passive nodes because a HMI may control and signal multiple PLCs in SCADA systems. Hence, an active node should prepare multiple challenge sets for multiple corresponding passive nodes. Now, we describe the setup process. The whole process is also shown in Fig. 5. In the beginning of this phase, the active node should setup its identity, challenge set, the results of PUF(C) and the random nonce, and then it sends these parameters to the corresponding passive node. Here, the identity of the active node is generated by hashing K_n and R where K_n is a random nonce and R is the resulting output of PUF(C). Then both nodes store (UID, C, R, K_n) in their database. By using this information, the passive node can distinguish which active node sends the IMT message and find out the corresponding challenge-response pair in the database. After setting up all necessary information, active node can start our MT-PUFAuth scheme to change its dynamic IP address. In order to explain the operations clearly in this Phase, we just explain setup process between one active and one passive node.

C. AUTHENTICATION AND KEY AGREEMENT PHASE

In this section, we describe the authentication process prior to that an active node changes its dynamic IP address. This process can also be called as IMT message process. In this process, there are two communication rounds between active and passive node.

The first round is that the active node intending to change its IP address will inform its corresponding passive node

and the other one round is that the corresponding passive node receiving this IMT message responds to the active node. The whole process is shown in Fig. 6. Basically, our scheme ensure mutual authenticates between both nodes involved in this process, which can achieve security insurance of our proposed scheme while transferring IMT message between the active and passive nodes. Next, we explain the first communication round, IMT message sending.

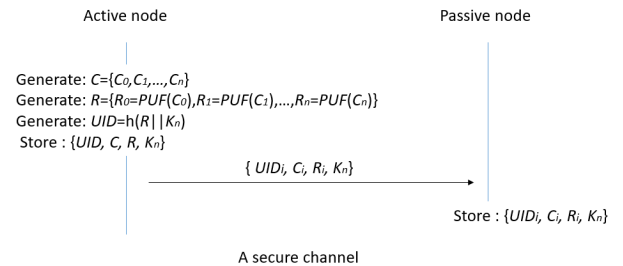


FIGURE 5. The setup phase.

The first round: In this round, the active node intends to change its dynamic IP address at a specified time interval. In order to inform other passive nodes to update this active node's dynamic IP address, the active node should send an IMT message firstly. Hence, this active node executes the following steps:

- i. The active node makes use of one time identity UID_i and selects the corresponding challenge C_i in set C for this passive node. Then it sends $S_1:\{UID_i, C_i\}$ to the passive node.
- ii. After sending IMT message, the active node waits for the response form the passive node and prepares to execute the moving target scheme to change its dynamic IP address.

The second round (Moving Target Informing Acknowledgement): In this round, the passive node should respond the challenge to the active node. Hence, the active and passive nodes execute the following steps

- i. The passive node receives the message S_1 and extracts UID_i and C_i from received message. Then the passive node employs (UID_i, C_i) to search the message item (UID_i, C_i, R_i, K_n) in the database. If it cannot find the matching data item for UID , it deletes this informing message.
- ii. If the passive node can find out the matching data item (UID_i, C_i, R_i, K_n) in passive node's database, it generates a nonce N_s and computes a mask $N_s^*=N_s \oplus K_n$. Then it computes $V_1 = h(UID_i||K_n||N_s)$ and sends the message $S_2:\{N_s^*, V_1\}$ to the active node. The passive node can also compute the shared session key $SK = h(K_n||N_s)$.
- iii. After the active node receives IMT acknowledgement, S_2 , it computes the $N_s = N_s^* \oplus K_n$ and then it can obtain $V_1^* = h(UID_i||K_n||N_s)$. It checks if V_1^* is equal to received V_1 . If it holds, the

active node confirms that the corresponding passive node has received the moving target informing message correctly. Then, the active node can compute the shared session key $SK = h(K_n || N_s)$ with computed N_s and the stored K_n . Next, in order to update authentication information, active node computes new (UID_i, C_i, R_i, K_n) as $(UID_{new}, C_{new}, R_{new}, K_{n_{new}})$. It also employs N_s to encrypt R_{new} and computes $V_2 = h(UID_i || R_{new} || N_s || R_i)$. Finally, active node sends S_3 to the passive node.

After above two rounds, the active and passive nodes can compute the shared key by $SK = h(K_n || N_s)$.

The third round: The active node sends S_3 to the passive node in order to update the authentication information for the future authentication.

- i. The passive node receives S_3 and calculates $R_{new} = R_{new} \oplus N_s$. The passive node can compute $V_2^* = h(UID_i || R_{new} || N_s || R_i)$ and verifies received V_2 . Thereafter, passive node also can obtain UID_{new} , C_{new} , R_{new} , $K_{n_{new}}$ for the future authentication.

Above steps describe the normal procedure of our authentication scheme in SCADA system.

After this IMT message process, the active and passive nodes execute moving target scheme to change the active node's dynamic IP address. In the following subsection, we introduce the process of moving target scheme implemented in active and passive nodes.

D. MOVING TARGET SCHEME EXECUTION PHASE

In this paper, we explain the advantage of moving target defense scheme for SCADA system in critical architecture. And we also design our moving target scheme with the aid of the authentication scheme, named MT-PUFAuth. In our scheme, the active node sends IMT message to the passive node through an authentication scheme and then the active and passive nodes prepare to execute the dynamic IP address rotation process.

In this paper, the nodes use the PUFs output to compute dynamic IP address. Our IP generation scheme follows the rule of the IP generation scheme in MT6D. In MT6D, the active node computes the dynamic IP address with the dynamic interface identifier comprised of three parts: an individual host identifier, a secret key and a given variable. In their work, a given variable should be agreed by two communication parts and timestamp is their suggested variable. Hence their scheme must face a serious performance issue, tight time synchronization. If without this, their scheme may cause packet loss during IP rotation process. In our scheme, we also design three parameters as $\{UID, K_n, R\}$ where R is $PUF(C)$. According to the dynamic addressing scheme, the obscured IID is constructed based on the following equation.

$$IID = h[UID_{Di} || K_n || R]_{0..63} \quad (1)$$

Then, the IPv6 address is generated by concatenating the host's subnet with IID. In SCADA system. The active

and passive nodes can compute active node's dynamic IP address by itself because they have the same parameter set $\{UID, K_n, R\}$ after authentication process.

E. IMPROVEMENTS OVER MT6D

Through our design, our scheme can solve the problems in MT6D and explain them as follows.

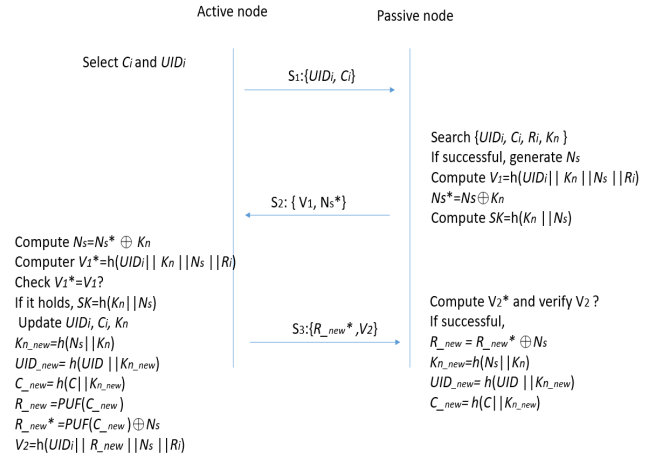


FIGURE 6. The authentication phase.

- i. Our authentication process can ensure the security of sending IMT message because it can achieve the mutual authentication between active and passive nodes. Furthermore, our scheme changes key parameters, UID and C , each time the active node informing the passive node to change target active node's IP address. Hence, our authentication process can prevent the illegal access from the adversary. Compared to other moving target schemes, our paper proposes a securer moving target defense scheme in critical architecture environment.
- ii. Our moving target defense scheme does not adopt time variable, which also means that our scheme does not have to consider tight time synchronization. Instead, we make use of the PUFs in the IP address generation process, which also can ensure the unique characteristic of dynamic IP address. Hence, active and passive nodes can execute IP address computation, respectively, after IMT message process.
- iii. In our scheme, both parts (active and passive nodes) generate dynamic IP address without the need of sending message containing IP address in public to other node. Hence, our scheme can avoid the risk of the exposure of dynamic IP address during sending IMT message.
- iv. Our scheme can achieve the key agreement and the key can be used to encrypt the original packet, which forms a tunnel sending encapsulated packet to the destination for the following communication. Hence, our

authentication and key agreement scheme can ensure the security of the communication in SCADA systems.

- v. Our scheme owns a robust moving target informing and confirmation scheme between active and passive nodes, which can ensure no packet loss during the IP rotation process among passive and active nodes.

Based on above discussion, we can find that our scheme is a more robust and securer moving target defense scheme in critical architecture.

IV. SECURITY ANALYSIS FOR AUTHENTICATION

In this section, we provide security evaluation to show that our authentication scheme can make the moving target defense scheme secure.

In our proposed scheme, the both parts (active and passive node) set up all necessary authentication information in Setup Phase and hence they can communicate with each other in a securer manner. We now explain that the authentication process in our proposed MT-PUFAuth scheme can fulfill the security requirement to resist possible attacks.

A. MUTUAL AUTHENTICATION

Different to other moving target scheme, our scheme employs the PUF-based authentication to ensure the security of the IMT message process. In our scheme, the active node should initiate the IMT message process to inform the passive node that the active node intends to change its IP address. Hence, our active node should firstly send IMT message (S_1) to the passive node. The passive should make use of authentication information described in Section 3 to verify this informing message. S_1 message contains UID and C . Only legitimate passive node can find the data item in its database because the attacker cannot guess the result of $PUF(C)$ even if he/she can get the challenge C . Hence, the passive node can easily authenticate the active node via the check of the correctness of M_1 . After confirmation of the authentication information, the passive node acts like the active node to change target's IP address with PUF and meanwhile changes UID , C for the next moving target task. So, the passive node also prepares V_1 and N_s^* and send them to the active node. V_1 contains three parameters (UID , K_n , N_s) and these parameters are only known by both parts. Hence, the active node can use K_n to recover the N_s and checks if received V_1 is correct. Based on this rigorous authentication process, we believe that the both parts can execute the dynamic IP address change scheme securely in our proposed MT-PUFAuth scheme.

B. DEVICE ANONYMITY

In our scheme, once the active node completes IMT message transferring, it generates a new (UID , C) and so does the passive node. Because the attacker cannot know the secret nonce K_n , the attacker cannot obtain the next UID of one active node. So, our scheme is not only useful to ensure the security of the device privacy but also efficient for resisting eavesdropper attack.

C. CLONING ATTACK PROTECTION

The active and passive nodes in our scheme make use of the output of PUF, which is one way function and difficult to predict and clone, to be one of three parameters generating dynamic IP address. In the past, the attacker usually tries to clone authentication message through investigate the behavior of the device. It is not workable in our scheme because our scheme makes use of PUFs which is strongly relative to physical elements. Hence, even if the attacker can get S_1 and extract the challenge C from S_1 , the attacker still cannot get $PUF(C)$ and furthermore C is replaced with the new one each time the IMT message being sent. Hence, we can protect the important authentication process and the parameter used in generating dynamic IP address against the cloning attacks.

D. REPLAY ATTACK RESISTANCE

In our proposed scheme, the active node changes its UID and C each time it sending IMT message. Hence, the messages S_1 and S_2 change each time the active node initiates the IMT message process, which leads the adversary cannot reuse the UID and C to reproduce S_1 and S_2 . Through this renewing scheme, we can prevent replay attack which usually easily happens in an authentication process.

E. IMPERSONATION ATTACK RESISTANCE

MT-PUFAuth scheme can easily resist impersonation attacks. In our proposed scheme, if the adversary attempts to impersonate a legitimate device to control or influence the SCADA systems in critical architecture, he/she firstly must obtain challenge and device identity (UID) for a specified active node. However, as we described before, UID and challenge C are changed each time IMT message process ends. Furthermore, in order to know the next dynamic IP address, the adversary should predict or guess the output of $PUF(C)$ which is very difficult. Hence, the adversary has no chance to impersonate the legitimate user to control the SCADA system in critical architecture.

V. PERFORMANCE EVALUATION

This section describes the performance analysis of moving target defense scheme including security improving, performance analysis and emulation results.

A. SECURITY IMPROVING

In this subsection, we introduce security improvement, no IP address leakage, in our proposed moving target defense scheme. Previous study [2] proposed MTM6D II to improve the security drawbacks of MT6D. In their scheme, they claim the active node can securely perform moving target defense scheme in SCADA system. However, in their scheme, the active node still must send the update message containing new IP address to inform other nodes that it has changed IP address. Although their scheme employs IPsec with IKEv2 to ensure the security of their updating message, the computation overhead and complexity is worthy to consider.

Furthermore, transferring IP address message in public still faces many risks from various network attacks. Especially in such a network with rapidly-developed computation technique, we can imagine that network will have high computation capacity in very near future. In our scheme, any information containing IP address is not allowed to expose in public. We only send the one-time alias identity, the challenge and authentication information in public. Hence, the adversary cannot get the target's IP address from fetching the message transferring between both parts. Our scheme can provide a securer moving target scheme than before and perform well in practice.

B. PERFORMANCE ANALYSIS

In this subsection, we discuss the performance of our moving target scheme in terms of following four performance topics.

1) THE FEASIBLE MOVING TARGET DEFENSE SCHEME

In our scheme, the dynamic IP address generation is developed by referring to the generation of dynamic IP address scheme in the study [3]. As we described before, our scheme makes use of UID , K_n , and PUF output to construct the dynamic interface Identifier. Then this identifier is used to create dynamic IP address. Hence, our design is feasible to create dynamic IP address. After the active node changing IP address, the active node can communicate with the passive node with new dynamic IP.

2) TIME ASYNCHRONOUS

In order to achieve the goal which active and passive nodes can change IP addresses information together, the central control is a possible way to coordinate all nodes' address information. However, it needs additional cost to deploy a central server to control or coordinate all IP information among the nodes. MT6D provides a good method to compute dynamic IP address in a distributed manner. However, it makes use of time parameter to generate dynamic IP address, which means their scheme needs tight time synchronization. It is usually hard to achieve time synchronization and it easily lead to the packet loss during IP rotation. In our scheme, we replace the time parameter with PUF output and PUF owns the one way function and unique characteristic like time variable. Furthermore it is hard to clone and predict for the adversary. Hence, in our scheme, active and passive nodes can generate dynamic IP address by themselves once the authentication process completes. From this observation, our scheme can flexibly execute moving target defense function, which can save the central control cost and can easily extend existing network to large-scale network architecture.

3) NO PACKET LOSS

The proposed a moving target defense scheme with PUBs based authentication process also can ensure no packet loss during IP rotation. In our scheme, the active node should inform passive node to change IP address. The passive node should confirm the correctness of IMT message before

changing the corresponding active node's IP address in its IP address table. While the active node and passive nodes confirm IMT message, they change the active node's IP address with dynamic IP generation scheme and the passive node stores this new IP into its IP address table for this active node.

4) LIGHT WEIGHT PRIVACY SECURITY SCHEME

MTM6D II exploits mobile IPv6 network technique, in which a node owns two IP address, one is permanent and the other is temporary. The active and passive nodes should communicate with each other with their temporary IP addresses. The active nodes should update dynamic IP address and the passive node also updates this in passive node's binding table. In order to ensure the security of update messages, in MTM6D II, IPsec with IKEv2 is employed for authentication, encryption, etc. These mechanisms can provide security protection for SCADA system but with much higher computation cost. In our system, we design a light weight authentication with PUF based information, which can provide a secure authentication and shared key agreement. Further, this PUF-based information also can be unique information generating dynamic IP address.

C. EMULATION RESULTS

Here, we validate the performance of our scheme. Our network structure is shown in Fig. 6. There are six types of the devices in this network and we explain their jobs here.

- PC: The users remotely control this SCADA system through the PC connecting to HMI server or client. Then the users can remotely read and control corresponding sensors.
- HMI_Client: this is a human-machine interface in SCADA system. The insider in SCADA system can control this system, including reading and signaling, through this interface.
- PLC: This device is Programming Logic Controller which can communicate with SCC through Modbus/TCP protocol and contacts with sensor via RS485.
- SCC: Supervisory computer control system receives commands from the users and transfers them to corresponding PLC.
- HMI_Server: This server provides a Web interface with which the users can query the sensed information and control SCADA system.

The users can query and control sensors through HMI_Server or HMI_Client which transfer the commands to SCC with Modbus/TCP protocol. SCC then transfers these commands to corresponding PLCs which also command corresponding sensors.

In the next two subsections, we consider the comparison among MT6D, MTM6D II and our proposed scheme. Basically, the opinion of MT-PUFath is more similar to MT6D because both make the active and passive nodes compute dynamic IP addresses by itself. However, MTM6D and

MTM6D II are proposed based on the same way applying mobile IPv6 in SCADA system in order to solve time synchronization issue. Later two schemes should send binding update message containing IP address information to inform passive nodes that the active node has change IP address. Hence, it possibly has IP address leakage issue. Hence, the working operation opinion of MT-PUFAth is totally differently from MTM6D II but it can achieve the same security performance without IP leakage issue. Hence, in order to show MT-PUFAth can solve the drawback of MT6D, the packet loss problem due to time synchronization, the first simulation compares packet loss rate between MT-PUFAth and MT6D. The second subsection compares MT-PUFAth with MTM6D II in terms of five aspects. This can show MT-PUFAth less complex than MTM6D II with the same packet loss rate and our proposed scheme does not have possible IP leakage issue.

1) PACKET LOSS

As mentioned in [2], MTM6D has handoff delay because the packet cannot be sent during handoff period. MTM6D II can solve this problem through the use of multiple CoAs (i.e. old CoA and new CoA are allowed to coexist during handoff period).

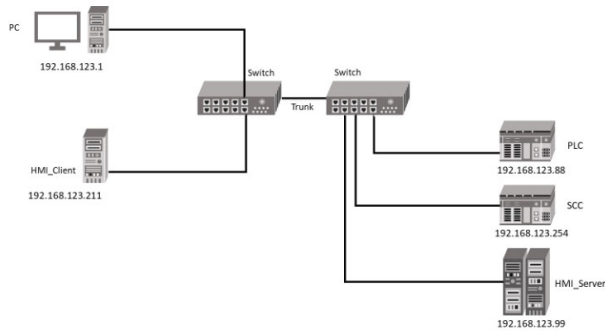


FIGURE 7. The network structure in our simulations.

Hence, the packet with old CoA is received validly during this handoff period until its CoA is replaced with new CoA. In MT6D, each node maintains three addresses for previous, current and next interval, in order to eliminate any packet loss due to the tight time synchronization during handoff period, which still may have packet loss due to serious time synchronization problem. In our scheme, we generate dynamic IP address with PUF(C) instead of timestamp. Furthermore, our scheme, MT-PUFAth, also allow old and new dynamic IP addresses can coexist during handoff period, which also can ensure no packet loss over this period. Fig. 7 shows the network structure in our simulations. In this simulation, we set shuffling interval as 5 and 10 seconds. Further, we also set query frequency, which means HMI client sends query request to PLC, as 600 and 300 times/s. From observing Table 2, we find that our scheme has no packet losses during IP rotation and MT6D has some packet losses under different

scenarios. Basically, MTM6D II also contains no packet loss because it is also irrelative to time synchronization. However, MTM6D II has high overhead and possible security issue (i.e. IP exposing). Then we compare the overhead between our scheme and MTM6DII.

TABLE 2. Packet loss rate.

Query frequency	shuffling interval	MT-PUFAth	MT6D
600	5	0%	11.22%
600	10	0%	0.62%
300	5	0%	3.31%
300	10	0%	0.33%

2) THE OVERALL PERFORMANCE COMPARISOIN

This subsection compares MT-PUFAth with MTM6D II in terms of five aspects. Firstly, MTM6D II claims it can provide authentication and decryption for SCADA system by using IPSec with IKEv2. MT-PUFAth also can provide these two functions. However, MTM6D II requires end servers must support IPSec with IKEv2 but MT-PUFAth does not need additional support in original SCADA network. Secondly, MTM6D II employs mobile IPv6 to execute IP rotation and hence, active node should send binding update message containing dynamic IP information to inform passive node. MT-PUFAth lets the active and passive node generate active node’s dynamic IP address. Hence, it is more simple and secure than MTM6D II and MTM6D II should require extra signaling overhead ($\frac{408B}{(N \times t)}$ [2]). For transmission overhead, MTM6D II needs at least extra 24B overhead due to the use of IPSec with IKEv2. MT-PUFAth needs 48B overhead as MT6D. However, in summary, MT-PUFAth is much more simple and secure than MTM6D, and furthermore MT-PUFAth can have the same loss rate as MTM6D II. Table 3 shows the comparison between MTM6DII and MT-PUFAth in terms of five aspects.

TABLE 3. The comparison between MTM6DII and MT-PUFAth.

	Authenticat ion and decryption scheme	IP generation scheme	Signaling overhead	Transmissio Overhead	Router support
MTM6D II	IPSec with IKEv6	Mobile IPv6	Mobile IPv6 $\frac{408B}{(N \times t)}$	24B~	○
MT-PUFAth	PUF-based	Node-based	×	48B	×

VI. DISCUSSION AND LIMITATIONS

In this paper, our proposed scheme, MT-PUFAth, employs PUF-based authentication and generates IP addresses with the output of PUF. Because the outputs of PUFs are fundamentally random physical variations, which are supposed to be unclonable [30], MT-PUFAth can resist against several

security threats such as message replay, impersonation and eavesdropping. Basically, a PUF can be classified into two different kinds, strong and weak based ones. The strong PUF can provide larger challenge response space than the weak one. Strong PUF is often used for authentication protocols and the weak one is used for generating cryptographic keys [31], [32]. Hence, our authentication scheme also utilizes strong PUF. So, It seems that PUF-based security protection schemes can perform well and securely. However, PUF-based schemes have some inherent vulnerability and limitations. Firstly, according to the references [33]–[36], a malicious attacker can have the ability modeling PUF just via gaining the access of a subset of Challenge-Response Pairs (CRPs). Hence, the attacker can intercept the CRP message from authentication messages in transit between active and passive nodes. Next, he can model the behavior of PUF via Machine Learning technologies. In order to protect PUF from modeling attack, several protection schemes are developed [37]–[43]. However, some disadvantages, mainly including high computational and hardware overhead or inability to resist some Neural Networks, are discovered thereafter. Recently, a new novel scheme is proposed by the authors in [44]. Their opinion of protecting CRP is to split challenge message into several partitions, which can prevent the whole challenge message from being intercepted by the attacker. Their light-weight PUF-based authentication is composed of three schemes, challenge splitting, scrambling and padding. Although this new PUF-based authentication scheme is novel and effective, it needs multiple helper nodes to complete whole authentication process. Hence, though several solutions have been developed for resist against modeling attack, it is still open issue developing a light weight PUF based authentication with low hardware or computational overhead in the future. Secondly, PUF is sensitive to noise and environment conditions. The authors in [45] tried to address the issues with the reverse fuzzy extractor (FE). Through two functions, FE.Gen and FE.Rec, PUF operation can perform well under noisy environment. Hence, PUF-based authentication can apply such scheme alleviating noise factor. This paper mainly focuses on MTD scheme based of PUF based authentication and hence the issues of PUF based authentication is out of the scope in this paper. However, previous improved PUF-authentication schemes still can help this work perform better. Thirdly, though the large pool of IPv6 can alleviate the risk of IP collision, this risk still may happen possibly. Hence, my previous work also provides a solution [46]. As proposed previously, in the dynamic IP address of the packet, we take the first eight bits of the host ID as the device identifier. The purpose of the device identifier is to avoid IP address collision. Please refer to the reference [46] for more details.

VII. CONCLUSION

In a national critical architecture, SCADA system plays a key role in controlling the operations of this architecture. In such controlling model, the security is becoming important

because the damages on it usually cause the national security damage and large economical lost. Hence, MTD based defense, MT6D, MTM6D II, try to solve the security issues on SCADA system, which can prevent critical architecture from various attacks launched by malicious users through tracking target's IP. However, they also have their some new security problems, e.g. packet loss or IP addresses exposed to public during handover period. This paper proposes a Moving Target Defense scheme based on PUF-based authentication, which can generate dynamic IP addresses securely and prevent the new issues arising from tight time synchronization and IP exposing. In MT-PUFath, PUF-based authentication can provide mutual authentication between active and passive nodes, which can provide a secure communication. Then the active and passive nodes can employ PUF outputs to generate the active node's IPv6 address and change active node's IP address by itself. We also provide extensive security analysis for authentication and performance evaluation for our proposed moving target defense scheme. The results also show our scheme, MT-PUFath, performs much better than other MTD based schemes.

REFERENCES

- [1] W. Gao, T. Morris, B. Reaves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *Proc. eCrime Researchers Summit*, Oct. 2010, pp. 1–9.
- [2] V. Heydari, "Moving target defense for securing SCADA communications," *IEEE Access*, vol. 6, pp. 33329–33343, 2018.
- [3] M. Dunlop, S. Groat, W. Urbanski, R. Marchany, and J. Tront, "MT6D: A moving target IPv6 defense," in *Proc. MILCOM Mil. Commun. Conf.*, Nov. 2011, pp. 1321–1326.
- [4] V. Heydari and S.-M. Yoo, "Securing critical infrastructure by moving target defense," in *Proc. 11th Int. Conf. Cyber Warfare Secur. (ICCSWS)*, Boston, MA, USA, Jan. 2016, pp. 382–390.
- [5] V. Heydari, "IP hopping by mobile IPv6," in *Handbook Cyber-Development, Cyber-Democracy, Cyber-Defense*, E. G. Carayannis, D. F. J. Campbell, and M. P. Efthymiopoulos, Eds. Cham, Switzerland: Springer, 2017, pp. 1–28.
- [6] V. Heydari, S.-M. Yoo, and S.-I. Kim, "Secure VPN using mobile IPv6 based moving target defense," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.
- [7] V. Heydari, "Preventing SSH remote attacks using moving target defense," in *Proc. 13th Int. Conf. CyberWarfare Secur. (ICCSWS)*, Washington, DC, USA, Mar. 2018, pp. 272–280.
- [8] P. Wood, C. Gutierrez, and S. Bagchi, "Denial of service elusion (DoSE): Keeping clients connected for less," in *Proc. IEEE 34th Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2015, pp. 94–103.
- [9] H. Wang, Q. Jia, D. Fleck, W. Powell, F. Li, and A. Stavrou, "A moving target DDoS defense mechanism," *Comput. Commun.*, vol. 46, pp. 10–21, Jun. 2014.
- [10] S. Venkatesan, M. Albanese, K. Amin, S. Jajodia, and M. Wright, "A moving target defense approach to mitigate DDoS attacks against proxy-based architectures," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2016, pp. 198–206.
- [11] B. Danev, R. J. Masti, G. O. Karame, and S. Capkun, "Enabling secure VM-vTPM migration in private clouds," in *Proc. 27th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, 2011, pp. 187–196.
- [12] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, 2012, pp. 127–132.
- [13] Q. Jia, K. Sun, and A. Stavrou, "MOTAG: Moving target defense against internet denial of service attacks," in *Proc. 22nd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2013, pp. 1–9.

- [14] A. Choudhary, M. C. Govil, G. Singh, L. K. Awasthi, E. S. Pilli, and D. Kapil, "A critical survey of live virtual machine migration techniques," *J. Cloud Comput.*, vol. 6, no. 1, pp. 1–41, Nov. 2017.
- [15] H. Okhravi, A. Comella, E. Robinson, and J. Haines, "Creating a cyber moving target for critical infrastructure applications using platform diversity," *Int. J. Crit. Infrastruct. Protection*, vol. 5, no. 1, pp. 30–39, 2012.
- [16] A. Chowdhary, S. Pisharody, and D. Huang, "SDN based scalable MTD solution in cloud network," in *Proc. ACM Workshop Moving Target Defense*, Oct. 2016, pp. 27–36.
- [17] S.-K. Yang, Y.-M. Shiue, Z.-Y. Su, I.-H. Liu, and C.-G. Liu, "An authentication information exchange scheme in WSN for IoT applications," *IEEE Access*, vol. 8, pp. 9728–9738, 2020.
- [18] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K. R. Choo, M. Wazid, and A. K. Das, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment," *J. Netw. Comput. Appl.*, vol. 89, pp. 72–85, Jul. 2017.
- [19] R. Amin, S. H. Islam, M. K. Khan, A. Karati, D. Giri, and S. Kumari, "A two-factor RSA-based robust authentication system for multiserver environments," *Secur. Commun. Netw.*, vol. 2017, pp. 1–15, Aug. 2017.
- [20] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Netw.*, vol. 20, pp. 1–15, Sep. 2014.
- [21] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc Sensor Wireless Netw.*, vol. 10, no. 4, pp. 361–371, Jan. 2010.
- [22] J. Yuan, C. Jiang, and Z. Jiang, "A biometric-based user authentication for wireless sensor networks," *Wuhan Univ. J. Natural Sci.*, vol. 15, no. 3, pp. 272–276, Jun. 2010.
- [23] P. S. Ravikanth, "Physical one-way functions," Ph.D. dissertation, Dept. Archit., Media Arts Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2001.
- [24] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th Annu. Design Autom. Conf.*, Jun. 2007, pp. 9–14.
- [25] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019.
- [26] Y.-P. Kim, S. Yoo, and C. Yoo, "DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2015, pp. 196–197.
- [27] V. Petrov, S. Edelev, M. Komar, and Y. Koucheryavy, "Towards the era of wireless keys: How the IoT can change authentication paradigm," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 51–56.
- [28] K. Frikken, M. Blanton, and M. Atallah, "Robust authentication using physically unclonable functions," in *Proc. ISC*, Pisa, Italy, 2009, pp. 262–277.
- [29] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1327–1340, Oct. 2017.
- [30] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF-based secure communication protocol for IoT," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 3, pp. 1–25, Apr. 2017.
- [31] L. Kusters and F. M. J. Willems, "Secret-key capacity regions for multiple enrollments with an SRAM-PUF," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2276–2287, Sep. 2019.
- [32] H. Yildiz, M. Cenk, and E. Onur, "PLGAKD: A PUF-based lightweight group authentication and key distribution protocol," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5682–5696, Apr. 2021.
- [33] C. Gu, C. H. Chang, W. Liu, S. Yu, Q. Ma, and M. O'Neill, "A modeling attack resistant deception technique for securing PUF based authentication," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, Dec. 2019, pp. 1–6.
- [34] C. Gu, C.-H. Chang, W. Liu, S. Yu, Y. Wang, and M. O'Neill, "A modeling attack resistant deception technique for securing lightweight-PUF-based authentication," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 6, pp. 1183–1196, Jun. 2021.
- [35] M. Khalafalla and C. Gebotys, "PUFs deep attacks: Enhanced modeling attacks using deep learning techniques to break the security of double arbiter PUFs," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2019, pp. 204–209.
- [36] J. Delvaux, "Machine-learning attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF-FSMs," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2043–2058, Aug. 2019.
- [37] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2831–2843, Nov. 2018.
- [38] M. A. Qureshi and A. Munir, "PUF-IPA: A PUF-based identity preserving protocol for Internet of Things authentication," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–7.
- [39] F. Farha, H. Ning, K. Ali, L. Chen, and C. Nugent, "SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5904–5913, Apr. 2021.
- [40] M. Barbareschi, A. D. Benedictis, E. L. Montagna, A. Mazzeo, and N. Mazzocca, "A PUF-based mutual authentication scheme for cloud-edges IoT systems," *Future Gener. Comput. Syst.*, vol. 101, pp. 246–261, Dec. 2019.
- [41] S.-J. Wang, Y.-S. Chen, and K. S.-M. Li, "Adversarial attack against modeling attack on PUFs," in *Proc. 56th Annu. Design Autom. Conf.*, Jun. 2019, pp. 1–6.
- [42] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, 2002, pp. 148–160.
- [43] S. S. Zalivaka, A. A. Ivaniuk, and C.-H. Chang, "Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 1109–1123, Apr. 2018.
- [44] M. Ebrahimabadi, M. Younis, and N. Karimi, "A PUF-based modeling-attack resilient authentication protocol for IoT devices," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3684–3703, Mar. 2022, doi: [10.1109/JIOT.2021.3098496](https://doi.org/10.1109/JIOT.2021.3098496).
- [45] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019.
- [46] J.-S. Li, C.-G. Liu, C.-J. Wu, C.-C. Wu, C.-W. Huang, C.-F. Li, and I.-H. Liu, "Design of industrial control system secure communication using moving target defense with legacy infrastructure," *Sens. Mater.*, vol. 33, no. 10, pp. 3415–3424, Oct. 2021.



CHUAN-GANG LIU received the B.Sc. degree from the Department of Electrical Engineering, Tam Kang University, in 2000, and the M.S. and Ph.D. degrees from the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He is currently an Associate Professor with the Department of Multimedia and Game Development, Chia Nan University of Pharmacy and Science. His research interests include network security, wireless sensor networks, user authentication, the IoT applications, cloud computing, and network performance analysis.

...