ISSN 2616-5775 Vol. 4, Issue 1: 7-14, DOI: 10.25236/AJCIS.2021.040102

Secure identity authentication scheme based on PUF for IoUT

Jie Zhou[1]

[1]*Department of Information Engineering ,Shanghai Maritime University,China*

ABSTRACT. *The existing identity authentication schemes based on the devices of Internet of Underwater Things (IouT) are all executed at the network layer and higher layers, which require high computing costs and are not suitable for devices with limited computing resources. By applying PUF to key binding, a physical layer-based identity authentication scheme is proposed. The authentication process is realized by the joint typicality coding and decoding technology based on the packing lemma and the covering lemma. The Achievability and Converse propositions prove the feasibility of the scheme, and the confidential capacity domain is delimited from the perspective of information theory. The false authentication analysis theoretically limits the probability of successful deception by the adversary, and reduces it to the lowest limit.*

KEYWORDS: *physically uncloneable function, authentication, false acceptance, encoding, mutual information*

1. Introduction

The Internet of Things technology has been widely used in intelligent transportation today, smart medical and other fields. As an extension of the sensor network underwater, the Internet of Things has a wide range of applications in the marine and military fields [1-2]. With people's attention to marine resources, the security of IouT has also attracted more and more attention. When we facing attacks, not only network security issues need to be considered, but also the security of node equipment connected to the network.

The current research on underwater Internet of Things focuses on the energy consumption of sensor nodes. The literature [3] applied the asymmetric key algorithm to the underwater Internet of Things, and proposed a pair-based non-interactive identity authentication protocol. Combined with the comparison and analysis of the SOK algorithm and the ECMOQV algorithm, it is concluded that the protocol can effectively reduce energy consumption, but it lacks Sufficient simulation data to support the correctness of the program. Literature [4] realized a low computational complexity authentication scheme, using Vandermonde matrix to replace matrix multiplication with matrix addition to reduce energy consumption. Literature [5] proposed a ticket-based authentication protocol, which reduces the amount of communication required in the authentication process to a certain extent and shortens the length of data transmission, but the article lacks corresponding simulation and security analysis. Literature [6] proposed a new cooperative message authentication protocol based on a group of trusted nodes. Using the strong spatial dependence and time invariance of the distribution of underwater acoustic channel characteristics, the base station node uses the trusted node to determine that the received message is from a legitimate source. The node is still a rival. Literature [7] proposed a physical layer-based authentication scheme to detect spoofing attacks in underwater sensor networks. On this basis, it further proposed an authentication scheme using deep reinforcement learning to improve the accuracy of spoofing detection. Literature [8] proposes an a-spoof algorithm based on a shared key mechanism and a hash algorithm for attacks caused by nodes exchanging location and identity information.

The authentication scheme proposed in this paper is a physical layer-based scheme that can reduce the computational burden of higher-level protocols. Physical Unclonable Functions (PUF) [9-10], as the main technology of physical authentication, mainly uses a challenge-response pair(CRP) to achieve basic authentication. PUF has the characteristics of unclonability, unpredictability, and anti-tampering [11-12], which is a safe, flexible and reliable solution. This article explores the identity authentication

ISSN 2616-5775 Vol. 4, Issue 1: 7-14, DOI: 10.25236/AJCIS.2021.040102

of the IouT from the perspective of information theory, and proposes an authentication scheme based on the physical layer.

Most of the above work is an authentication protocol established at a higher level under the concept of computational confidentiality. In the authentication scheme based on the physical layer, the space and time characteristics of the channel are used to detect adversary spoofing attacks. However, the realization of identity authentication between underwater sensor network nodes at the physical layer and the use of information theory to analyze and define the confidential capacity domain and security are still in the initial stage of research.

2. Methodology

2.1 Basic definition and system model

Define uppercase letters such as X and Y to indicate variables, lowercase letters such as x^n and y^n to indicate specific implementations, superscripts to indicate a sequence of continuous variables, and subscripts to indicate the specific location of each variable, such as $X^n = X_1 \cdots X_i \cdots X_n$. The probability distribution of a discrete random variable X is P_X , $X^n \sim \prod_{i=1}^n P_X(x_i)$ which shows that $\prod_{i=1}^n P_X(x_i)$ is a probability function of X^n, and $X_1, X_2 \cdots$ is a series of independent and identically distributed sequences satisfying $X_i \sim P_X(x_i)$. $T_\varepsilon^n(X)$ Represents the typical sequence set of random variable X, H(X) represents the entropy of random variable X, and I(X;Y) represents the mutual

information of random variable X and Y.

As shown in Figure 1 below, the measurement values of stimulus C^n , response X^n, response Y^n , and information acquired by the adversary Z^n are all limited sets, given by $\mathrm{P}_C \mathrm{P}_{X|C} \mathrm{P}_{YZ|XC}$.

Registration process: When an incentive sequence C^n is given to the device, a corresponding response sequence X^n is generated, a key K is randomly selected, and the encoder obtains auxiliary information M according to the response sequence X^n and key K, namely

$$\begin{aligned} X^n &= \mathrm{PUF}(C^n); \\ M &= \mathrm{f}(X^n, K) \end{aligned} \tag{1}$$

Authentication process: The same incentive sequence C^n is input to the device in the authentication phase, and the corresponding response measurement value Y^n is generated. The decoder obtains the measurement value $\hat{K}$ of the key according to the auxiliary information M and the response measurement value Y^n , namely

$$\begin{aligned} Y^n &= \mathrm{PUF}(C^n); \\ \hat{K} &= \mathrm{g}(M, Y^n) \end{aligned} \tag{2}$$

Compare whether K and $\hat{K}$ are equal, if they are equal, the authentication is successful, otherwise the authentication fails.

ISSN 2616-5775 Vol. 4, Issue 1: 7-14, DOI: 10.25236/AJCIS.2021.040102

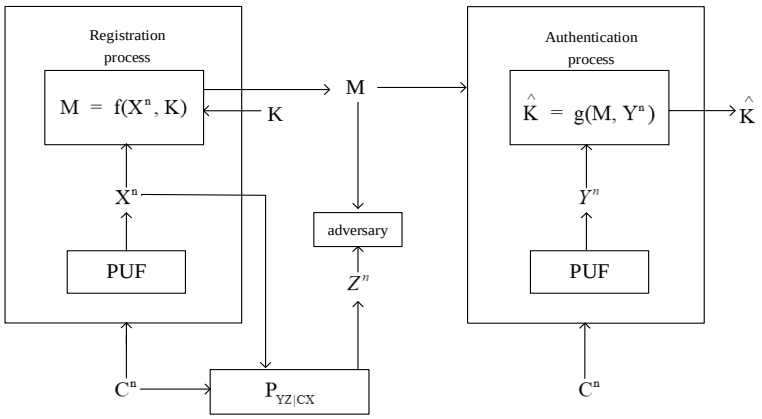

Figure. 1 Identity authentication process

2.2 Achievable leakage and capacity regions

Definition.1 A key-storage-leakage tuple $(R_K, R_M, \Delta) \in R_+^4$ is called reachable, if for any $\delta_n > 0$ and sufficiently large n, there are encoders and decoders such that

$$\begin{aligned} &\mathrm{P}(\hat{\mathrm{K}}_{\mathrm{Z}} \neq \mathrm{K}) \leq \delta_{\mathrm{n}} \\ &\frac{1}{n}\mathrm{H}(K) \geq R_K - \delta_n \\ &\frac{1}{n}\log|M| \leq R_M + \delta_n \\ &\frac{1}{n}\mathrm{I}(X^n; MZ^n) \leq \Delta + \delta_n \end{aligned} \tag{3}$$

The key-storage-disclosure feasible region is the set of all reachable tuples.

Theorem.2 The key-storage-leakage domain R is given by the following tuple $(R_K, R_M, \Delta, E_{FA}) \in R_+^4$ and satisfies:

$$\begin{aligned} &R_K \leq \mathrm{I}(U;Y|W) - \mathrm{I}(U;Z|W) \\ &R_M \geq \mathrm{I}(U;X|W,Z) \\ &\Delta \geq \mathrm{I}(X;U) + \mathrm{I}(X;Z) \end{aligned} \tag{4}$$

Proof: Proof of achievability:

For a given joint distribution $\mathrm{P}_{W|X}\mathrm{P}_{U|W}$, use the following coding scheme:

(1) Codebook generation: randomly and independently generate a sequence $w^n(q)$ for $q \in [1: 2^{n(\mathrm{I}(X;W)+\delta_n)}]$, obey the distribution $\prod_{i=1}^n \mathrm{P}_W(w_i)$, then randomly and independently divide all sequences into $2^{n(\mathrm{I}(X;W)-\mathrm{I}(Y;W)+2\delta_n)}$ clusters $\mathrm{B}(m_1)$ for $m_1 \in [1: 2^{n(\mathrm{I}(X;W)-\mathrm{I}(Y;W)+2\delta_n)}]$ For each q, randomly and conditionally independently generate $2^{n(\mathrm{I}(X;U|W)+\delta_n)}$ sequences $u^n(q,r), r \in [1: 2^{n(\mathrm{I}(X;U|W)+\delta_n)}]$, obey the distribution $\prod_{i=1}^n \mathrm{P}_{U|W}(u_i|w_i)$, and randomly and independently divide these sequences into $2^{n(\mathrm{I}(X;U|W)-\mathrm{I}(Y;U|W)+3\delta_n)}$ clusters $\mathrm{B}(m_2)$ for $m_2 \in [1: 2^{n(\mathrm{I}(X;U|W)-\mathrm{I}(Y;U|W)+3\delta_n)}]$, At this time, each cluster contains $2^{n(\mathrm{I}(U;Y|W)-2\delta_n)}$ sequence u_n, and these sequences are randomly and independently divided into $2^{n(\mathrm{I}(U;Y|W)-\mathrm{I}(U;Z|W)-\delta_n)}$ clusters $\mathrm{B}(j,l)$ for $j \in [1: 2^{n(\mathrm{I}(U;Y|W)-\mathrm{I}(U;Z|W)-\delta_n)}]$, $l \in [1: 2^{n(\mathrm{I}(U;Z|W)-\delta_n)}]$ in each cluster, so there is $r = (m_2, j, l)$.

(2) Registration process: Given an excitation sequence C^n, PUF is equivalent to a one-way hash function. According to C^n, we have the response sequence $X^n = \mathrm{h}_a(C^n)$, for each response

ISSN 2616-5775 Vol. 4, Issue 1: 7-14, DOI: 10.25236/AJCIS.2021.040102

sequence X^n, the encoder search sequence w^n which satisfied $(w^n, X^n) \in T_\varepsilon^{(n)}$. Since the number of generated sequences w^n exceeds $2^{n(I(X;W))}$, according to the coverage quote Theory can find such a sequence w^n, if there is more than one sequence, randomly select one from it, and send its corresponding cluster index m_1 to the decoder. The encoder continues to search for the sequence u^n which satisfies $(u^n, X^n, w^n) \in T_\varepsilon^{(n)}$. Since more than $2^{n(I(X;U|W))}$ sequence is generated, a sequence u^n that meets the requirements can be found according to the covering lemma. If there is more than one, one is randomly selected from them, and its corresponding cluster index m_2 is sent to the decoder. Now randomly select one from the uniformly distributed set $k = \{1, 2, \cdots 2^{n(I(U;Y|W)-I(U;Z|W)-\delta_n)}\}$ as the key *K*, and send $j \oplus K$ to the decoder, where $\oplus$ is the modular $2^{n(I(U;Y|W)-I(U;Z|W)-\delta_n)}$ operation.

(3) Decoding process: After giving the same excitation sequence C^n, the decoder gets a response sequence $Y^n = h_b(C^n)$. After receiving the index $(m_1, m_2, j \oplus K)$, the decoder searches for a unique sequence $w^n \in B(m_1)$ to meet the requirements $(w^n, Y^n) \in T_\varepsilon^{(n)}$. Since there are less than $2^{nI(Y;W)}$ sequence w^n in the sequence $B(m_1)$, according to the packing lemma, it can find sequence w^n that meets the requirements. Then the decoder searches for the unique sequence $u^n \in B(m_2)$ to meet the requirements $(u^n, w^n, Y^n) \in T_\varepsilon^{(n)}$, for it has less than $2^{n(I(Y;U|W))}$ sequence u^n in $B(m_2)$. According to the packing lemma, a sequence u^n that meets the requirements can be found. Therefore, the estimated value $\hat{K}$ of the key *K* is obtained, $\hat{K} = \hat{j} \oplus (j \oplus K)$, where $\hat{j}$ is the index of the subcluster where the sequence u^n is located.

(4) Analysis of the probability of error: According to the encoding and decoding process $P(\hat{K} \neq K) = P(\hat{j} = j)$, let $P(\varepsilon) = P(\hat{j} = j)$, the decoder report an error if and only when at least one of the following situations occurs:

$$\varepsilon_1 = \{(u^n, w^n, Y^n) \notin T_\varepsilon^{(n)}\}$$

$$\varepsilon_2 = \{u^n \in B(m_2) \text{ for } \tilde{u}^n \neq u^n, (\tilde{u}^n, w^n, Y^n) \in T_\varepsilon^{(n)}\}$$

The upper bound of the average error probability is $P(\varepsilon) \leq P(\varepsilon_1) + P(\varepsilon_2)$, Now delimit each term of the probability of error, by the law of large numbers, $P(\varepsilon_1)$ with $n \to \infty$ tends to zero.

$$P(\varepsilon_2) = P\{\tilde{u} \in B(m_2) \text{ for some } \tilde{u}^n \neq u^n, (\tilde{u}^n, w^n, Y^n) \in T_\varepsilon^{(n)}\}$$

$$= P\{\tilde{u}^n \in B(m_2) \text{ for } \tilde{u}^n \neq u^n, (\tilde{u}^n, w^n, Y^n) \in T_\varepsilon^{(n)} \mid (w^n, Y^n) \notin T_\varepsilon^{(n)}\} P((w^n, Y^n) \notin T_\varepsilon^{(n)})$$
$$+ P\{\tilde{u}^n \in B(m_2) \text{ for } \tilde{u}^n \neq u^n, (\tilde{u}^n, w^n, Y^n) \in T_\varepsilon^{(n)} \mid (\tilde{w}^n, Y^n) \in T_\varepsilon^{(n)}, \tilde{w} \neq w^n\} P((\tilde{w}^n, Y^n) \in T_\varepsilon^{(n)}, \tilde{w} \neq w^n\}$$

$$\overset{(a)}{=} P\{\tilde{u}^n \in B(m_2) \text{ for } \tilde{u}^n \neq u^n, (\tilde{u}^n, w^n, Y^n) \in T_\varepsilon^{(n)} \mid (\tilde{w}^n, Y^n) \in T_\varepsilon^{(n)}, \tilde{w}^n \neq w^n\} P((\tilde{w}^n, Y^n) \in T_\varepsilon^{(n)}, \tilde{w}^n \neq w^n\}$$

$$\overset{(b)}{\leq} \delta_n$$

(a) Obtained by the law of large numbers, (b) Obtained by the packing lemma.

(5) Key rate: the key *K* is generated by the set $k = \{1, 2, \cdots 2^{n(I(U;Y|W)-I(U;Z|W)-\delta_n)}\}$, then H(*K*) $= n(I(U;Y|W) - I(U;Z|W) - \delta_n) \geq n(R_K - \delta_n)$.

(6) Storage rate: obtained according to the encoding and decoding process $M = (m_1, m_2, j \oplus K)$

$$\log|M| = n(I(X;W) - I(Y;W) + 2\delta_n) + n(I(X;U|W) - I(Y;U|W) + 3\delta_n) + n(I(U;Y|W) - I(U;Z|W) - \delta_n)$$

$$\overset{(a)}{=} n(H(W|Y) - H(W|X) + H(U|W,Z) - H(U|W,X) + 4\delta_n)$$

ISSN 2616-5775 Vol. 4, Issue 1: 7-14, DOI: 10.25236/AJCIS.2021.040102

$$= n(\mathrm{I}(W;X,Y) + \mathrm{I}(U;X \mid W,Z) + 4\delta_n)$$
$$\overset{(b)}{=} \mathrm{n}(\mathrm{I}(U;X \mid W,Z) + \delta_n)$$

(a) (b) from Markov Chain *U*-*X*-(*Y*,*Z*).

(7) Information leakage rate:

$$\mathrm{I}(X^n;M,Z^n)$$
$$= \mathrm{I}(X^n;m_1,m_2,j \oplus K,Z^n)$$
$$\le \mathrm{I}(X^n;q,m_2,j \oplus K,Z^n)$$
$$= \mathrm{H}(X^n) - \mathrm{H}(X^n \mid q,m_2,j \oplus K,Z^n)$$
$$= \mathrm{H}(X^n) - \mathrm{H}(X^n,q,m_2,j \oplus K,Z^n) + \mathrm{H}(q,m_2,j \oplus K) + \mathrm{H}(Z^n \mid q,m_2,j \oplus K)$$
$$= -\mathrm{H}(Z^n \mid X^n) - \mathrm{H}(q,m_2,j \oplus K \mid X^n,Z^n) + \mathrm{H}(q,m_2,j \oplus K) + \mathrm{H}(Z^n \mid q,m_2,j \oplus K)$$
$$\overset{(a)}{\le} -\mathrm{H}(Z^n \mid X^n) - \mathrm{H}(K) + \mathrm{H}(q,m_2,j \oplus K) + \mathrm{H}(Z^n \mid q,m_2,j \oplus K)$$
$$\overset{(b)}{\le} -\mathrm{H}(Z^n \mid X^n) - \mathrm{H}(K) + \mathrm{H}(q) + \mathrm{H}(m_2) + \mathrm{H}(j \oplus K) + \mathrm{H}(Z^n \mid W^n)$$
$$\le n[-\mathrm{H}(Z \mid X) - \mathrm{I}(U;Y \mid W) + \mathrm{I}(U;Z \mid W) + \mathrm{I}(X;W) + \mathrm{I}(X;U \mid W) - \mathrm{I}(Y;U \mid W) + \mathrm{I}(U;Y \mid W) - \mathrm{I}(U;Z \mid W) + \mathrm{H}(Z \mid W) + \delta_n']$$
$$\overset{(c)}{=} n[\mathrm{I}(X;U) + \mathrm{I}(X;Z) + \delta_n']$$

(a) is obtained by the conditional reduction of entropy, and K is independently and random generated, (b) is generated by w^n is the function of q, (c) is obtained by the Markov chain (Y, Z)-X-U-W.

Proof of the converse:

(1) Key rate: $n(R_k - \delta_n) \le \mathrm{H}(K)$

$$= \mathrm{H}(K \mid MZ^n) + \mathrm{I}(K;MZ^n)$$
$$\overset{(a)}{\le} \mathrm{H}(K \mid MZ^n) - \mathrm{H}(K \mid Y^nM) + n\delta_n + n\varepsilon$$
$$= \sum_{i=1}^{n} \mathrm{I}(K;Y_i \mid M,Y_{i+1}^n) - \mathrm{I}(K;Z_i \mid M,Z_{i+1}^n) + n(\delta_n + \varepsilon)$$
$$\overset{(b)}{=} \sum_{i=1}^{n} \mathrm{I}(K;Y_i \mid M,Y_{i+1}^n,Z^{i-1}) - \mathrm{I}(K;Z_i \mid M,Y_{i+1}^n,Z^{i-1}) + n(\delta_n + \varepsilon)$$

Let $U_i = (M,K,Y_{i+1}^n,Z^{i-1})$ $W_i = (M,Y_{i+1}^n,Z^{i-1})$

$$= \sum_{i=1}^{n} \mathrm{I}(U_i;Y_i \mid W_i) - \mathrm{I}(U_i;Z_i \mid W_i)$$

(a) is obtained from Fano's inequality and condition $\frac{1}{n}\mathrm{I}(K;MZ^n) \le \varepsilon$, (b) is obtained from the *Csisza'r* summation formula.

(2) Storage rate: $n(R_M + \delta_n)$

$$\ge \log|M|$$
$$\ge \mathrm{H}(M)$$
$$\ge \mathrm{H}(M \mid K)$$

ISSN 2616-5775 Vol. 4, Issue 1: 7-14, DOI: 10.25236/AJCIS.2021.040102

$$\geq \mathrm{H}(M \mid K) + \mathrm{H}(K) - \mathrm{H}(X^n, K)$$

$$\overset{(a)}{\geq} \mathrm{H}(M \mid K) + \mathrm{H}(K) - \mathrm{H}(M)$$

$$= \mathrm{H}(X^n \mid M) - \mathrm{H}(X^n \mid K, M)$$

$$= \mathrm{I}(X^n; K \mid M)$$

$$= \mathrm{H}(K \mid M) - \mathrm{H}(K \mid M, X^n)$$

$$\overset{(b)}{=} \mathrm{H}(K \mid M, Z^n) - \mathrm{H}(K \mid M, X^n, Z^n)$$

$$= \mathrm{H}(K \mid M, Z^n) - \mathrm{H}(K \mid M, Y^n) + \mathrm{H}(K \mid M, Y^n) - \mathrm{H}(K \mid M, X^n, Z^n)$$

$$= \sum_{i=1}^{n} \mathrm{I}(K; Y_i \mid M, Y_{i+1}^n) - \mathrm{I}(K; Z_i \mid M, Z^{i-1}) + \mathrm{I}(K; X_i, Z_i \mid M, Z^{i-1}) - \mathrm{I}(K; Y_i \mid M, Y_{i+1}^n)$$

$$\overset{(c)}{=} \sum_{i=1}^{n} \mathrm{I}(K; Y_i \mid M, Y_{i+1}^n, Z^{i-1}) - \mathrm{I}(K; Z_i \mid M, Z^{i-1}, Y_{i+1}^n) + \mathrm{I}(K; X_i, Z_i \mid \mathrm{M}, Y_{i+1}^n, Z^{i-1}) - \mathrm{I}(K; Y_i \mid M, Y_{i+1}^n, Z^{i-1})$$

$$= \sum_{i=1}^{n} \mathrm{I}(K; X_i, Z_i \mid M, Y_{i+1}^n, Z^{i-1}) - \mathrm{I}(K; Z^i \mid M, Z^{i-1}, Y_{i+1}^n)$$

Let $W_i = (M, Y_{i+1}^n, Z^{i-1})$ $U_i = (M, K, Y_{i+1}^n, Z^{i-1})$

$$= \sum_{i=1}^{n} \mathrm{I}(U_i; X_i \mid W_i, Z_i)$$

(a) is obtained by (X^n, K) is the function of M, (b) is obtained by Markov chain $(K, M) - X^n - (Y^n, Z^n)$, (c) is obtained by the *Csisza'r* summation formula.

(3) Information leakage rate:

$$n(\Delta + \delta_n) \geq \mathrm{I}(X^n; MZ^n)$$

$$= \mathrm{I}(X^n; M) + \mathrm{I}(X^n; Z^n \mid M)$$

$$= \mathrm{H}(X^n) - \mathrm{H}(X^n \mid M, Y^n, K) - \mathrm{I}(X^n; Y^n, K \mid M) + \mathrm{I}(X^n; Z^n \mid M)$$

$$= \mathrm{H}(X^n) - \mathrm{H}(X^n \mid M, Y^n, K) - \mathrm{I}(X^n; Y^n \mid M) - \mathrm{I}(X^n; K \mid Y^n, M) + \mathrm{I}(X^n; Z^n \mid M)$$

$$= \mathrm{H}(X^n) - \mathrm{H}(X^n \mid M, Y^n, K) - \mathrm{I}(X^n; Y^n \mid M) - \mathrm{H}(K \mid Y^n, M) + \mathrm{H}(K \mid X^n, Y^n, M) + \mathrm{I}(X^n; Z^n \mid M)$$

$$\overset{(a)}{\geq} \mathrm{H}(X^n) - \mathrm{H}(X^n \mid M, Y^n, K) - \mathrm{I}(X^n; Y^n \mid M) + \mathrm{I}(X^n; Z^n \mid M) - n\varepsilon$$

$$= \sum_{i=1}^{n} \mathrm{H}(X_i) - \mathrm{H}(X_i \mid Y_i, M, K) - \mathrm{I}(X_i; Y_i \mid M) + \mathrm{I}(X_i; Z_i \mid M) - n\varepsilon$$

$$= \sum_{i=1}^{n} \mathrm{H}(X_i) - \mathrm{H}(X_i \mid Y_i, M, K) - \mathrm{H}(X_i \mid M) + \mathrm{H}(X_i \mid M) - \mathrm{H}(X_i \mid M, Z_i) - n\varepsilon$$

$$\geq \mathrm{I}(X_i; Z_i) + \mathrm{H}(X_i \mid Y_i, M) - \mathrm{H}(X_i \mid Y_i, M, K) - n\varepsilon$$

$$\overset{(b)}{=} \sum_{i=1}^{n} \mathrm{I}(X_i; Z_i) + \mathrm{H}(X_i \mid Y_i, M) - \mathrm{H}(X_i \mid Y_i, M, K, Y_{i+1}^n, Z^{i-1}) - n\varepsilon$$

Let $U_i = (M, K, Y_{i+1}^n, Z^{i-1})$

ISSN 2616-5775 Vol. 4, Issue 1: 7-14, DOI: 10.25236/AJCIS.2021.040102

$$= \sum_{i=1}^{n} \mathrm{I}(X_i; Z_i) + \mathrm{I}(X_i; U_i \mid Y_i, M) - n\varepsilon$$

$$\overset{(c)}{=} \sum_{i=1}^{n} \mathrm{I}(X_i; Z_i) + \mathrm{I}(X_i; U_i) - n\varepsilon$$

(a) is obtained from Fano's inequality, (b) is obtained from Markov chain $(X_i, M, K, Y_i^n) - X^{i-1} - (Z^{i-1}, Y_{i+1}^n)$, (c) is obtained from Markov chain $U_i - X_i - (M, Y_i)$.

3. Error authentication analysis

In the scheme proposed in this paper, the adversary simulates a correct response value to impersonate a legitimate user based on the existing information, which leads to false authentication. The adversary selects a sequence to imitate the response value of PUF according to M. Z^n, M can obtain the estimated value of the key $\hat{K}_z$ according to Y_z^n, the maximum false acceptance rate (mFAR, False Acceptance Rate) is defined as $\mathrm{mFAR} = \mathrm{P}\{\hat{K}_z = K\}$.

Definition.3 If for all $\delta > 0$ and sufficiently large n, there is an encoder and decoder such that $\frac{1}{n}\log\frac{1}{mFAR} \geq E_{FA} + \delta_n$,the error acceptance index is considered reachable.

Theorem.4 In the PUF-based identity authentication scheme, the error acceptance exponent index $\mathrm{E_{FA}}$ satisfies $\mathrm{E_{FA}} \leq \mathrm{I}(U;Y \mid W) - \mathrm{I}(U;Z \mid W)$.

Proof: The adversary obtains the estimated value $\hat{K}_z$ of the key according to the side information Z^n and the auxiliary information M, so as to satisfy $\hat{K}_z = K$ as much as possible. According to the coding scheme, only one $\hat{j}$ equal to j needs to be found, so only the sequence u^n needs to be considered, so

$$mFAR = \sum_{|M|} \frac{\mathrm{P}(M = m_1, m_2).2^{n(\mathrm{I}(X;U,W)+\delta_n)}}{|j|}.2^{-n(\mathrm{I}(X:U,W)+\delta_n)}$$

$$\leq \sum_{|M|} \left(\frac{\mathrm{P}(M = m_1, m_2).2^{n(\mathrm{I}(X;U,W)+\delta_n)}}{|j|} + 1\right).2^{-n(\mathrm{I}(X:U,W)+\delta_n)}$$

$$= \sum_{|M|} \frac{\mathrm{P}(M = m_1, m_2).2^{n(\mathrm{I}(X;U,W)+\delta_n)}}{|j|}.2^{-n(\mathrm{I}(X:U,W)+\delta_n)} + \sum_{|M|} 2^{-n(\mathrm{I}(X;U,W)+\delta_n)}$$

$$= 2^{-n(\mathrm{I}(U;Y|W)-\mathrm{I}(U;Z|W)+\delta_n)} + 2^{-n(\mathrm{I}(U;Y|W)+\mathrm{I}(Y;W)+6\delta_n)}$$

$$\leq 2^{-n[\mathrm{I}(U;Y|W)-\mathrm{I}(U;Z|W)+\delta_n]}$$

So $\frac{1}{n}\log\frac{1}{mFAR} \geq \mathrm{I}(U;Y \mid W) - \mathrm{I}(U;Z \mid W) + \delta_n$

$$\geq E_{FA} + \delta_n$$

4. Conclusion

Aiming at the identity authentication problem of the node equipment of the underwater Internet of Things, this paper proposes a physical layer-based authentication scheme. By applying PUF to the key binding authentication scheme based on fuzzy commitment, the authentication model is established by using multiple codes and random codes.From the perspective of information theory, it verifies that the scheme can achieve successful authentication, and at the same time gives the confidential capacity

ISSN 2616-5775 Vol. 4, Issue 1: 7-14, DOI: 10.25236/AJCIS.2021.040102

domain. Error authentication analysis can prove that the scheme can improve the authentication success rate to a certain extent.

References

[1] Wei Zhiqiang. Research on the security of underwater sensor networks [J]. Chinese Journal of Computers, 2012, 35 (8): 1595-1605.
[2] Zeng Ling, Wang Wei. Research on the Security and Secrecy System of Underwater Sensor Networks [J]. Communication Technology, 2019, 52 (1): 202-206.
[3] David Galindo, Rodrigo Roman, Javier Lopez.A Killer Application for Pairings: Authenticated Key Establishment in Underwater Wireless Sensor Networks [C] //*International Conference on Cryptology and Network Security*, NJ: CANS, 2008: 120-132.
[4] Chi Yuan, Wenping Chen, Yuqing Zhu,Deying Li, Jie Tan. A Low Computational Complexity Authentication Scheme in Underwater Wireless Sensor Network [C] //11th*International Conference on Mobile Ad-hoc and Sensor Networks*, NJ: IEEE, 2010: 116-123.
[5] Chae-Won Yun, Jae-Hoon Lee, Okyeon Yi, Soo-Hyun Park. Ticket-based Authentication Protocol for Underwater Wireless Sensor Network [C] //*Eighth International Conference on Ubiquitous and Future Networks*, NJ: IEEE, 2016: 215-217.
[6] Roee Diamant,Paolo Casari,Stefano Tomasin.Cooperative Authentication in Underwater Acoustic Sensor Networks [J]. *IEEE Transactions on Wireless Communications*, 2019, 18 (2): 954-968.
[7] Liang Xiao, Xiaoyue Wan, Wei Su. Learning-Based PHY-Layer Authentication for Underwater Sensor Networks [J]. *IEEE Communications Letters*, 2019, 23 (1): 60-63.
[8] B.R.Chandavarkar, Akhilraj V.Gadagkar. Mitigating Localization and Neighbour Spoofifing Attacks in Underwater Sensor Networks [C] //*11th International Conference on Computing,Communication and Networking Technologies*, NJ: IEEE, 2020.
[9] Yin Win Xin,Jia Yong Zhe,Gao Yan Song,et al.A Survey of Physical Unclonal Function (PUF) Research [J]. Network Security Technology and Application, 2018 (06): 41-42+54.
[10] Zhang Zi Nan. Research and application of physical unclonable functions [D]. PLA Information Engineering University, 2013.
[11] Zhou Kai. Research on the reliability of physical unclonable functions based on FPGA [D]. Hefei University of Technology, 2019.
[12] RoelMaes.PhysicallyUnclonable Functions [M]. Springer: Berlin, Heidelberg, November 2013:129-130.
[13] Frans M. J. Willems, Tanya Ignatenko. Authentication Based on Secret-Key Generation [C].//*IEEE International Symposium on Information Theory Proceedings*. Cambridge, MA, USA: IEEE, 2012: 1792-1796.