Kuiwu YANG, Yuanbo GUO

Information Engineering University, Zhengzhou 450004, China

An Anti-Clone Attack Key Management Scheme for DTMSN

Abstract. *This paper proposes a novel anti-clone attack key management scheme for DTMSN based on Physical Unclonable Function (PUF). In this scheme, sensor nodes have PUF units in their microprocessors. According to DTMSN security requirements, we design two types of keys in our scheme and take advantages of the physical characteristics of PUF unit to prevent nodes from cloning. Analysis and simulation indicate that the scheme is not only efficient and resource-saving, but also can resist clone attack and many other network attacks.*

Streszczenie. *W artykule opisano sieć typu DTMSN – delay tolerant mobile service network. Celem było opracowanie systemu uniemożliwiającego klonowanie. (**Schemat zarządzania siecią DTMSN uniemożliwiający atak klonowania**)*

Keywords: Delay Tolerant Mobile Sensor Network, Physical Unclonable Function, Key Management.
Słowa kluczowe: sieć DTMSN, atak klonowania

1. Introduction

DTMSN [1] has received a lot of attention in recent years. Although similar to the traditional Wireless Senor Network (WSN) in hardware components, DTMSN has many other characteristics, such as opportunistic transmission, node mobility, intermittent connectivity, etc. Therefore, DTMSN is susceptible to be attacked by adversary because the sensor nodes are always deployed in challenge environment and cannot monitor each other. As an effective measure to protect network from attacks, key management plays an important role in DTMSN security, but it is still a challenging work since the limited resource of sensor nodes and unpredictable links states.

Due to the resource constraints of sensor nodes, symmetric key algorithms should be more suitable for WSNs[2-5]. Single network-wide key is the simplest key pre-distribution scheme, in which all sensor nodes are preloaded a single key before deployment. But its main drawback is that the compromise of a single node can cause the compromise of the entire network through the shared key. To avoid this risk, Eschenhauer et.al[6] first proposed a random key pre-distribution scheme relies on probability and random graph theory, which let each sensor node randomly pick a set of keys from a key pool before deployment such that two sensor nodes share a key with a certain probability after deployment. However, when enough nodes are compromised, the network becomes unsafe also. Despite the further improvements were suggested by Du et.al[7], key pre-distribution for sensor networks still faces above problem.

Though symmetric cryptography is efficient in resources utilization, the key management is complicated and difficult. Recently, Identity-Based Cryptography (IBC) is being seen as a promising solution for securing delay tolerant network (DTN). Literature [8-11] proposed some authentication and key management schemes based on IBC. However, the IBC-based key management schemes have to fulfill the calculation of bilinear map, which is too complex to resource limited sensor nodes in DTMSN. In addition, the private keys and certificates will be lost if nodes are compromised.

From the above analysis we can see that, although there have been many key management schemes proposed in recent years, but none of them can resist clone attack. That is to say, if one node is compromised and re-cloned by adversary, then the existing key management schemes cannot recognize the cloned malicious node which is very harmful to the whole network. In order to resist clone attack, we propose a novel key management scheme based on Physical Unclonable Function (PUF). PUF are innovative circuit primitives that extract secrets from physical characteristics of integrated circuits (ICs). In our key management scheme, we implement the mutual authentication between nodes by exploiting the physical characteristics of chips with PUF, thus to prevent nodes from cloning. Unlike the protocols [12-14] that need a database with large number of Challenge-Response Pairs (CRPs) of PUF, our scheme is no database supporting and more suitable for resource-restrained DTMSN.

The rest of this paper is organized as follows. Section 2 introduces the PUF. Section 3 describes the network model of DTMSN and assumptions. In Section 4, our PKM scheme is given. In Section 5, analysis and simulation of PKM scheme are shown. Finally, conclusions are presented in Section 6.

2. Physical Unclonable Function

A PUF is a function that maps challenges to responses and that is embodied in a physical object. It is easy to evaluate and hard to characterize[15].We denote the responses of a true PUF to challenges C and C' by R and R', and denote the response of a fake PUF to the same challenge C by X , $R, R', X \in \Re^n$ and $C \neq C'$ .The pair (C, R) is a CRP. Here we can look R, R', X as random variables. Let $\delta, \varepsilon \geq 0$ and $d(a,b)$ denotes the Hamming distance of variables a and b . Then the PUF satisfies the following probability formulas:

(1) $$Prob(d(X,R)) \leq \delta) \leq \varepsilon$$

(2) $$Prob(d(R,R')) \leq \delta) \leq \varepsilon$$

The above formulas (1) and (2) imply that if we input the same challenge to different PUFs, then the responses are high probability far apart. Similarly, if we put different challenges into the same PUF, then the responses are high probability far apart too. In fact, we can look the ideal PUF as a function P with an input C and an output R , so we can get $R = P(C)$.

Generally, the structure of PUF is simple and can be easily embedded into chips with very low extra cost.

3. DTMSN Model

The Fig.1 shows the network model of our DTMSN. In the area *A*, the Sink node is the manager of the network. There are two types of *sensor nodes* in DTMSN: Ferries and Endpoints. Ferries have more memory space and energy than Endpoints, and can assist Endpoints to forward sensing messages to Sink. Only a few Ferries in the network, but the number of Endpoints are large.

In our model, Endpoints only communicate with Ferries and Sink, and they can forward sensing messages through

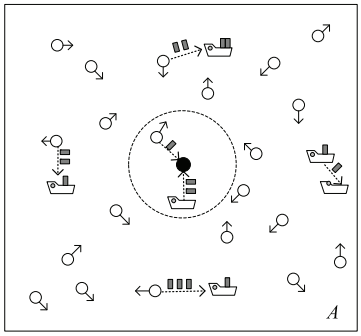

Fig.1. Model of DTMSN in our key management scheme

Ferries to Sink if they cannot establish links with Sink. Every node has a unique identity, and all the nodes are mobile except Sink. The movements of sensor nodes are based on some mobility model (e.g. Random Way-point Model, RWP[16]). Nodes have to verify the legitimacy of the others before communication in order to avoid potential attacks. In addition we have the following assumptions:

- In our key management scheme, we propose to equip the microprocessors of all nodes with PUFs which are inseparably linked to the microprocessors, and any operations attempt to remove the PUFs from the chips will lead to the destruction of the PUF.
- The Sink, acting as a controller, is assumed security and no resource-constrained. And the ferries have no energy and memory restriction. But the Endpoints are resource-limited.

4. PKM Scheme

4.1 Overview

The design of this scheme is motivated by the observation that deferent types of messages exchanged between sensor nodes have deferent security requirements, and that a single keying mechanism is not suitable for meeting these deferent security requirements. We design two types of keys for each sensor node in our scheme like LEAP[17]. We now introduce each of them.

- Global Key: This key is shared by all nodes in the network. It mainly used for Sink to encrypt broadcasting messages to every sensor nodes.
- Challenge Key: Every pair of nodes that can communicate with each other share a challenge key. Not only the challenge key can be used as the challenge to the PUFs of nodes during the process of mutual authentication, but also is used to encrypt messages between nodes. Thus, Ferries, the forwarding nodes, cannot get the plain messages that are generated by Endpoints and sent to the Sink.

Table 1 shows the notations that will be appeared in the rest of discuss.

Table.1. Notations

GK	: The global key;
CK_{ij}^{l}	: The callenge key between node *i* and *j* after updated *i* times;
$\|$	: Concatenation operator;
$\rightarrow$	: Unicast;
$\Rightarrow$	: Broadcast;
$\oplus$	: XOR operator;
$H(s)$	: Hash operation on message s ;
$P_i(C)$	: The response of node i's PUF to challenge C ;
$MAC(k,s)$	: Message authentication code of message s with key k .

4.2 Establishing of Keys

Suppose there are n Endpoints and m Ferries in a DTMSN $(m << n)$, and the identity of sensor node k (Ferry or Endpoint) is ID_k , here k is integer. The Sink node identity is SID . Before the network is deployed, the Sink generates a series of parameters for each sensor node as following:

1) Establishing of the initial challenge key: First, Sink node randomly generates a shared initial challenge key $CK_{ij}^{0} \in \Re^n$ for any Endpoint i and Ferry j , and gets the responses $P_i(CK_{ij}^{0})$ and $P_j(CK_{ij}^{0})$ from their respective PUFs. Second, Sink selects a one way hash function H (e.g. MD5), and computes the $H(P_j(CK_{ij}^{0}))$ and $H(P_i(CK_{ij}^{0}))$ for i and j . Last, Sink loads H , 3-tuples $< ID_i, CK_{ij}^{0}, H(P_i(CK_{ij}^{0})) >$ into Ferry j , and loads H and $< ID_j, CK_{ij}^{0}, H(P_j(CK_{ij}^{0})) >$ into Endpoint i . Similar to the above process, Sink also generates shared initial challenge keys for sensor node and itself.

2) Establishing of the global key: The global key, GK ,is a key shared by all the nodes in the network, and it is necessary when the Sink distributes a confidential message. In our scheme, Sink generates and pre-loads GK into every node before the network deployed, which is the simplest way to establish a global key.

4.3 Node Mutual Authentication of DTMSN

In DTMSN, nodes should verify the legitimacy of each other in each communication. In the following content, we propose a node mutual authentication scheme by an example of the first communication between node i and j .

1) Connection requirement: In neighbor discovering process, node always broadcast Hello message which contains node's identity and a random number, and the random number is changed in every broadcasting. For example, node *i* broadcasts its Hello message as follow:

$$i \Rightarrow *: ID_i, nonce_i$$

2) Connection response: Receiving the Hello message, node *j* should return a response if it wants to communicate with *i* . And the response steps are as follow:

Step1: Node j searches the 3-tuple $< ID_i, CK_{ij}^{0}, H(P_i(CK_{ij}^{0})) >$ in its memory and gets the responses $P_j(CK_{ij}^{0})$ and $P_j(CK_{ij}^{1})$ from its own PUF according to the challenges CK_{ij}^{0} and CK_{ij}^{1} , here $CK_{ij}^{k+1} = H(CK_{ij}^{k})$, $k \geq 0$. And then, node j calculates the $H(P_j(CK_{ij}^{1}))$.

Step2: Node j forwards the following message to node i , then erases $P_j(CK_{ij}^{0})$, $P_j(CK_{ij}^{1})$,and $H(P_j(CK_{ij}^{1}))$ from its memory to prevent leaking.

$$j \rightarrow i: ID_j, P_j(CK_{ij}^{0}) \oplus CK_{ij}^{0}, H(P_j(CK_{ij}^{1})) \oplus CK_{ij}^{0}, MAC(CK_{ij}^{0}, P_j(CK_{ij}^{0}) \oplus CK_{ij}^{0} \| H(P_j(CK_{ij}^{1})) \oplus CK_{ij}^{0} \| nonce_i)$$

The MAC (e.g. HMAC) operation is used to guarantee the message integrity.

3) Mutual authentication: Receiving the response message from node j , node i verifies the legitimacy of node *j* firstly as the following steps.

Step1: Node i verifies the integrity of the response message by $nonce_i$ and CK_{ij}^{0} which is extracted from 3-tuple $< ID_j, CK_{ij}^{0}, H(P_j(CK_{ij}^{0})) >$. If the validation is wrong, the message is distorted and node i gives up the connection.

Step2: Utilizing CK_{ij}^{0} , node i calculates $H(P_j'(CK_{ij}^{0})) = H((P_j(CK_{ij}^{0}) \oplus CK_{ij}^{0})' \oplus CK_{ij}^{0})$, in which

$(P_j(CK_{ij}^0) \oplus CK_{ij}^0)'$ is the second parts of the received response message. Then node i compares $H(P_j'(CK_{ij}^0))$ with $H(P_j(CK_{ij}^0))$ in its 3-tuple. If they are equal, then node j is legitimate. Next, node i extracts $H(P_j(CK_{ij}^1))$ from the response message and stores it.

Step3: Node i computes $CK_{ij}^1 = H(CK_{ij}^0)$, and gets the responses $P_i(CK_{ij}^0)$ and $P_i(CK_{ij}^1)$ from its PUF. Then node i calculates $H(P_i(CK_{ij}^1))$ and transmits the following authentication message to node j. Last, it deletes $P_i(CK_{ij}^0)$, $P_i(CK_{ij}^1)$, $H(P_i(CK_{ij}^1))$ from its memory.

$$i \to j : ID_i, P_i(CK_{ij}^0) \oplus CK_{ij}^0, H(P_i(CK_{ij}^1)) \oplus CK_{ij}^0, MAC(CK_{ij}^0, P_i(CK_{ij}^0) \oplus CK_{ij}^0 \| H(P_i(CK_{ij}^1)) \oplus CK_{ij}^0 \| nonce_i)$$

Step4: Receiving above message from node i, Node j can authenticate the legitimacy of node i by performing the same operations as node i in step1 and step2.

4) Parameters updating: For security consideration, nodes have to authenticate each other in each communication no matter whether they have authenticated or not. Therefore, the authentication parameters must be updated for the next verification, which can also prevent replay attack. The updating process is simple, after the kth authentication, the challenge key CK_{ij}^{k-1} is renewed by CK_{ij}^k, and $H(P_i(CK_{ij}^{k-1}))$, $H(P_j(CK_{ij}^{k-1}))$ should be replaced by $H(P_i(CK_{ij}^k))$ and $H(P_j(CK_{ij}^k))$.

4.4 Updating of Keys

1) Updating of challenge keys: The update method of challenge keys is shown in the above authentication scheme. After each successful authentication and communication, the challenge key CK_{ij}^{k-1} should be renewed by $CK_{ij}^k = H(CK_{ij}^{k-1})$.

2) Updating of global keys: In our key management scheme, the global key should be updated regularly, especially when the network is under dangerous circumstance for example some sensor nodes are compromised. Taking advantage of the mobility of DTMSN, we carry a simple scheme to distribute the new global keys GK_{new}. On the one hand, Sink can distribute the new global key to the sensor nodes that have links with it through encrypting GK_{new} by their shared challenge keys. On the other hand, the ferries that have received GK_{new} can forward GK_{new} to the no-received sensor nodes through encrypting it by their challenge keys too.

5. Analysis

5.1 Security Analysis

The security of PKM scheme is based on the PUF which is un-separated from the chip of node and any operations to destroy the chip will lead to the damage of PUF. Therefore, PKM can resist the main following attacks:

1) Clone attack: In DTMSN, nodes are susceptible to be captured and compromised by adversary. Hence, adversary can easily carry out the clone attack which is difficult to resist by existing key management scheme. However, our key management scheme can prevent DTMSN from this attack efficiently because the PUF cannot be cloned even nodes are compromised. Anti-clone attack is the most significant advantage of our key management scheme.

2) Masquerade attack: In our scheme, all nodes are authenticated to each other before communication. Therefore the disguised nodes cannot be accepted by the legitimate nodes.

3) Compromising attack: In our key management scheme, sensor nodes have not common challenge keys. Hence, even one sensor node is compromised and damaged, the adversary can only get the global key and eavesdrop the broadcasting information. Once the global key is updated, the adversary cannot do any more negative impact on the network. The compromising attack can be effectively alleviated.

4) Replay attack: Because of the openness of radio, attacker can capture radio signal and carry out replay attack very easily. This attack can usually consume much energy of victim node. In our scheme, nodes use different keys in their communication each time. Therefore, replay attack can be effectively inhibited in our scheme.

5) Eavesdropping: An eavesdropping attack is that the adversary sniffers the channel of two nodes in hopes of learning something useful. A passive listener will fail in any tracking attempts since the response of PUF is protected by the challege key with XOR operation.

5.2 Performance Analysis

As the Sink and Ferries are all energy-rich and have strong computing ability and enough storage space, here we are just concerned with the cost of Endpoint in our key management scheme. At the same time, since all the keys are preloaded before network is deployed, the main cost is focus on the authentication process.

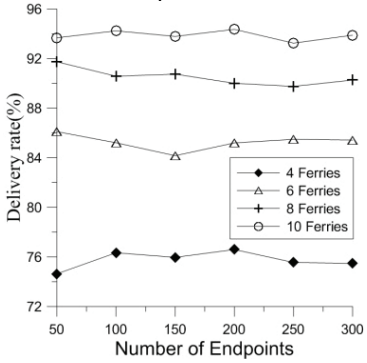

Fig.2. Average delivery rate with changing of Ferries

1) Storage requirement: In our scheme, the storage requirement of each Endpoint is just $m+1$ 3-tuples; here m is the number of Ferries. Base on the RWP movement model and its default values of parameters in Table 2, we simulate the network by Netlogo4.0. From Fig.2 we can see that, with the change of network size, the delivery rate is stable. And the Endpoints only need to store nine 3-tuples when the delivery rate more than 90%.

Table.2. Parameters of RWP

Parameter	Value	Parameter	Value
Network size	$200 \times 200 m^2$	Sink position	(100,100)
Speed of sensor	0~5 m/s	Pause time	0~20 s
Message	0.1/ s	Radius of ratio	3 m
Queue size of	80	Run time	20000 s
Living period of	No limit	Times of	100

2) Computational cost: Table 3 shows the cost of computation in anonymous authentication scheme4 and our authentication process. We can see that each Endpoint only need to complete 3 hash and 2 MAC operations in our scheme, which is more efficient than anonymous scheme. We implement the hash function of MD5 with 128bit digest in chip CC2430 at 4MHz in only about 5.6ms. As to PUF

operation, we can omit it because the PUF operation is carried out by hardware and one operation only takes tens of milliseconds[12].

Table.3. Cost of computation in authentication

Authentication scheme	Endpoint Operations				
	Pairing	PUF	MAC	Multiplica-tion	Hash
Our scheme	0	2	2	0	3
Anonymous scheme	1	0	2	2	1

3) Communication cost: Assuming the response of PUF and digest of function H are all 128bit, and the output of MAC is 160 bits. Thus, in our scheme, the min-length of verification messages of Endpoint is not more than 544bit which is the same with the anonymous authentication scheme and less than many other authentication schemes, e.g. RSA. Hence, PMK transmission cost is low and acceptable for DTMSN.

6. Conclusion

There are two main contributions of this paper. First, we introduce the PUF into the DTMSN, and design a lightweight key management scheme for it. Second, we resolve the problem of cloning attack in sensor network by using PUF which can be implemented at very low cost. Therefore, the PUF is a promising method to realize the key management in resource-limited devices and delay tolerant networks.

Acknowledgments: This work is supported by National Natural Science Foundation of China (60821001, 61070204,); Fundamental Research Funds for the Central Universities (BUPT2010PTB0503); National S&T Major Program (2010ZX03003-003-01); Excellent Youth Foundation of He'nan Scientific Committee (104100510025).

REFERENCES

[1] Y.Wang, F. Lin, and H.Wu, "Efficient data transmission in delay fault tolerant mobile sensor networks (DFT-MSN)", IEEE International Conference on Network Protocols (ICNP-05), Boston, MA, November, 2005.pp.6-9.

[2] A.M.Hegland, E.Winjum, S.F.Mjolsnes, C.Rong, O.Kure, P.Spilling, "A survey of key management in ad hoc networks" , Commun. Surveys& Tuts., Vol.8(3),2006,pp.48-66.

[3] J.C. Lee, V.Leung,K.H.Wong, J.Cao, Henrry C. B. Chan,et.al, "Key management issues in wireless sensor networks: Current proposals and future developments" , IEEE Wireless Commun.,Vol.14(5),2007,pp.76-84.

[4] Yong Wang, Garhan Attebury, and Byrav Ramamurthy, "A survey of security issues in wireless sensor networks" , Commun. Surveys Tuts., Vol. 8, No. 2, pp. 2-23, 2006

[5] H.T.T Nguyen, M. Guizani, J.Minho, E.Huh, "An efficient signal-range-based probabilistic key predistribution scheme in a wireless sensor network", IEEE Transactions on Vehicular Technology, Vol.58(5),2009, pp.2482-2497.

[6] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks," Proc. of the 9th ACM Conference on Computer and Communication Security, Nov. 2002. pp. 41-47.

[7] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks," in Proc. 10th ACM Conf. CCS, Oct. 2003, pp. 77–82.

[8] H.Zhu, X.Lin, R.Lu, X.Shen, D.Xing and Z.Cao "An opportunistic batch bundle authentication scheme for energy constrained DTNs", The 29th IEEE International Conference on Computer Communications (INFOCOM2010), San Diego, CA. March 2010. pp.1-9 .

[9] A. Kate, G. Zaverucha and U. Hengartner, "Anonymity and security in delay tolerant networks",The 3rd International Conference on Security and Privacy in Communications Networks and the Workshops, Secure Communication,September 2007,pp.504-513.

[10] A.Seth,S.Keshav."Practical security for disconnected nodes",Secure Network Protocols, 2005. (NPSec). The 1st IEEE ICNP Workshop on Secure Network Protocols, 2005,pp.31-36.

[11] A.Wan,T.Bin,"A Secure and Highly Efficient Key Management Scheme for MANET", AISS: Advances in Information Sciences and Service Sciences,2011,Vol.3(2), pp.12-22.

[12] G.E.Suh, S.Devadas, "Physical unclonable functions for device authentication and secret key generation", Proc. 44th ACM Annual Design Automation Conference 2007, San Diego, CA , June 2007, pp. 9-14.

[13] H.Ghaith, O.Erdinc, S.Berk, "A tamper-proof and lightweight authentication scheme", Pervasive Mobile Computing, Vol.4(6), 2008, pp. 807-818.

[14] P.Cortese, F.Gemmiti, B.Palazzi, M.Pizzonia, and M.Rimondini. "Efficient and Practical Authentication of PUF-Based RFID Tags in Supply Chains", IEEE International Conference on RFID-Technology and Applications (RFID-TA), Guangzhou, China. June 2010, pp.182-188.

[15] M. van Dijk B. Gassend, D. Clarke, and S. Devadas, "Controlled physical random functions". In Proceedings of the 18th Annual Computer Security Conference, Las Vegas, NV, USA ,Dec 2002,pp.149-160.

[16] D. Johnson and D. Maltz. "Dynamic source routing in ad hoc wireless networks". In: T. Imelinsky and H. Korth, editors, Mobile Computing, Kluwer Academic Publishers, 1996, pp.153-181.

[17] S. Zhu, S. Setia, and S. Jajodia. "LEAP: efficient security mechanisms for large-scale distributed sensor networks". In 10th ACM conference on Computer and communication security (CCS'03), ACM Press, 2003,pp.62-72.

***Authors**: Dr. Kuiwu Yang, Information Engineering University, Zhengzhou,450004,China.E-mail:yangkuiwu@yahoo.com.cn;*
Prof. dr. Yuanbo Guo, Information Engineering University, Zhengzhou,450004,China.E-mail:yuanbo_g@gmail.com