2012 2nd International Conference on Computer Design and Engineering (ICCDE 2012)
IPCSIT vol. 49 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V49.23

A Wireless Mesh Network PSK Authentication Protocol Based on Secure Multiparty Computation

Linfeng Wei [1+], Guoxiang Yao [1], Jian Weng [1] and Quanlong Guan[2]

[1] Information Science Technology College, Jinan University, Guangzhou, China

[2] Network and Education Technology Center, Jinan University, Guangzhou, China

Abstract. To solve the existing wireless Mesh network authentication security problem, a novel improved pre-shared key authentication protocol is designed and proposed, based on secure multi-party computation theory. The approach combined uses pre-shared key, key recovery, secret sharing and other methods, and applies the Lagrange polynomial. The security and performance of proposed protocol are analyzed. The pre-shared key of proposed protocol applies secure multiparty computation in the (*t, n*) threshold secret sharing scheme. Improved PSK authentication protocol will divide a master key into n shares, which are associated with the n-Mesh nodes. The master key can be recovered if and only if t or more than t shared key of Mesh nodes are joined together. Analysis indicates that the proposed pre-shared key protocol based on secure multi-party computation and threshold secret sharing is safer and more effective, and can be more applicable.

Keywords: WMN, SMPC, PSK, Authentication Protocol.

1. Introduction

In this part, we will introduction the basic concept of Secure Multi-Party Computation (SMPC), and the Prior Shared Key (PSK) authentication of Wireless Mesh Network. SMPC can be described as multi-party with dependent secret information. Each of the party hopes to compute a certain function or deal with a certain problem by their secret inputs. It is required that all the parties are able to receive correctly input results from other parties. However, each part can only get their own process information and con not take information of the other parties. From the above description, SMPC guarantees the correctness of final computation and the confidentiality of each party. In short, SMPC is a mathematical model which places emphasis on, without Trusted Third Party (TTP), how to compute a function or solve a mathematic problem securely. The PSK in WMN can adopt the mathematical model precisely.

As the common authentication way of wireless LAN，the WMN authentication should be effective when Access Point (AP) is joined in at any time. The PSK-authentication is also a universal authentication way in wireless LAN, in which Key can be prior shared in a pair of point or multi-point, and any point can prove their own identity is legal to others with the PSK. When some AP join in the WMN, the PSK authentication process can be describe as follows:

This AP can get the Beacon or Probe Response frame from its adjacent Mesh Point (MP) to confirm if this MP sets up a RSNA and is connected to some Authentication Server (AS). If there is a MP as described above then go to the next step.

This AP applies the open authentication to join in WMN and connects to the adjacent MP. They both (AP and MP) should consult the encryption options when finish the connection.

They both apply the PTK to generate a temporary key as the two parties equivalence key, and encrypt the communication data according to the coordinated encryption options. At the same time, they encrypt the broadcast or multicast data frame with the GTK which can be generated by the two parties.

[+] Corresponding author. Tel.: + 86-20-85223796; fax: +86-20-85220227.
E-mail address: linfengw@gamil.com.

The above PSK-authentication way can't be expanded to the WMN with multi hop routing. It is not secure to be expanded to more than two points of WMN because the AP can't confirm where the information source comes from. For instance, it cannot prevents the Man-in-the-Middle (MITM) attack. In addition, there are many vulnerabilities of the original PSK-authentication among MPs in WMN, basically as shown in the following three aspects:

The WMN has vulnerability which some MPs take the same PSK to authentication. When some mesh nodes in a wireless Mesh network adopt the same pre-shared PSK, the Mesh network formed by these nodes has low security level. If there is a MP's key is lost then the other MPs with the same PSK will be broken.

It is hard to expansion the whole WMN when the sub-WMNs have the own PSK, because any MP has saved the adjacent MP's key, and if there is a change of the whole WMN, the sun-WMNs should be update many keys respectively.

After some time, the PSK of WMN authentication should be updated to avoid the statistics attack.

2. Improved wireless mesh network PSK authentication

According to the previous analysis, there are scalability and security issues in Wireless Mesh Network PSK authentication Protocol. In this paper, we propose an improved Wireless Mesh Network PSK authentication with the theory of secure multipart computation

2.1. The design concept

In the previous part, we analyzed the shortcomings of Wireless Mesh Network PSK authentication protocol application. These shortcomings will greatly reduce the security of Wireless Mesh Network certification, with main problems are to share the same key that have to update for a moment in advance between the mesh nodes. The pre-shared key programs are quite safe under the condition of secure communication channel (information-theoretic model) and a viable third-party certification center or a key distribution center. But in fact, this communication model and viable third-party platform is difficult to be found or difficult to be fully realized. That is why we need to research on it on based on the cryptographic model. Although the communication channel is insecure, the attackers only have probability polynomial computing capability. Also we can keep the security of the wireless mesh network authentication server by using the protection of the spoofing attack and the man-in-the-middle attack[1]. In general, there are two main safety measures to distribute pre-shared key:

Sent pre-shared key through a secure communication channel. In reality it's difficult to find such a secure channel. The implementation of the secure channel including tunnel technology in the wireless network will need a lot of additional computing and storage.

In the process of distributing pre-shared key, it is doped with random variables or used one-way trapdoor functions encryption. The receiver and the sender should have a relevant calculation to confirm the authenticity of the key. As a result, even if the middlemen intercepted the key (such as encountered the man-in-the-middle attack), they cannot forge and tamper the key on the next turn of distribution.

The solution taken in this paper is the secret sharing technology in secure multiparty computation. The specific scheme is to take (*t, n*) threshold secret sharing. Improved PSK authentication protocol can divide pre-shared key information into n keys which assigned to *n* associated mesh nodes. That is to say, a master key is shared by *n* associated mesh nodes. If and only if *t* or more than t mesh nodes combine to recover master key. As the Figure 1 shown below:

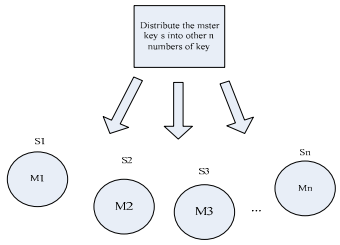

Fig. 1: The figure of the distribution of master key

2.2. Parameter setting of authentication protocol

Authentication protocol's specific parameters and symbols convention as shown in the Table 1 below:

Table. 1: The table of authentication protocol's specific parameters and symbols

Parameters and symbols	The explanation of parameters and symbols
M_i	The number *i* of mesh nodes
MAC_i	Choose each mesh nodes' MAC address as it ID to be mesh node's master key in the process of authentication process.
PKG	Represent a public-key generation system with two creation of space G_1 and G_2
Z_p^*	The remaining set of modulo *p* and *p* is a large prime number
Q	The large prime of number *q*-1, $q \in Z_p^*$
$(G_1, +)$	The additive cyclic group of oder *q*, it's generator is *p*
$(G_2, \cdot)$	Multiplicative cyclic group of order *q*
E	$e: G_1 \times G_1 \rightarrow G_2$, e is the bilinear mapping of G_1 and G_2
$h_1(x)$	One-way hash function of *x*, and Z^*_p
$h_2(x)$	One-way hash function of *x*, and Z^*_p
$h(x,y)$	One-way function of two variables *x, y*, and Z^*_p
$h_g(x)$	One-way trapdoor function of x, and the trapdoor is *g*
S_{pkg}	A private key that PKG randomly chosen
P_{pkg}	$P_{pkg} = S_{pkg} * p$, the corresponding public key of the S_{pkg}
P_i	The public key of node M_i, $P_i=h_1(MAC_i)$, (i=1, 2, … , n)
S_i	The private key of node M_i, $S_i= S_{pkg} *P_i$, (i=1, 2, … , n)
P_d	The master key distribution node that randomly choose from n numbers of nodes, and the $P_d=h_1(MAC_d)$ is the public key of this node.
S_d	The private key of the master distribution node, $S_d=S_{pkg}*P_d$

2.3. The design of authentication protocol

(1) The process of distributing master key

First, n mesh nodes share the master key named Km. It needs the cooperation of any t (or more than t) mesh nodes to restore the master key by using the threshold sharing algorithm. At the beginning, we should select a node or a Mesh routing node as the master key distributor. We assume that the agreement is based on the semi-honest model which means that n nodes behavior is semi-honest rather than malicious, and each mesh node only has the computing power of polynomial time. Specific distribution process are the following steps:

Step 1: We randomly choose *n*+1 random numbers Km_0, Km_1, …, Km_n from Z^*_p. Except for number Km_0, the rest random numbers are randomly keeping secret, and Km_i is saved as secret share to a node M_i, which is used to restore the main key later. And calculate *n* numbers of $KM_i=h(Km_0, Km_i)$ (where i = 1,2, ..., n).

Step 2: We calculate n numbers of $(h_2(MAC_i), K_{M_i})$ (i=1,…,n) and (0, *Km*) to construct an *n*-th Lagrange interpolation polynomial L(x) [2]:

$$L(x) = K_m * \prod_{i=1}^{n} \frac{h_2(MAC_j) - x}{h_2(MAC_j)} + \sum_{i=1}^{n} K_{M_i} \frac{x}{h_2(MAC_i)} \prod_{j=1, j\neq i}^{n} \frac{h_2(MAC_j) - x}{h_2(MAC_j) - h_2(MAC_i)} \bmod q$$

Step 3: The element x_i is randomly chosen from Z^*_P. The master key should handle with two-variable one-way function after generating a bilinear mapping. We should calculate out the trap door keys of one-way trapdoor function, $g_i = (g_i', g_i'') = h(e(P_i, P_{pkg})^{X_i})$ (i = 1, 2, ..., n).c

Step 4: Calculate $r_i = hg_i''(Km_i)$ from one-way trapdoor function and encrypt $C_i = Eg_i'(Km_i \,||\, r_i)$. Nodes M_i's private key is $s_i = x_i P_{pkg} - r_i S_d$ and the random sequences are $R_i = r_i P_d$. Then we send the sequence ($C_i \,||\, s_i \,||\, R_i$) to the node M_i.

Step 5: Select n-t+1 the smallest integer d_j from the 1-h_2(MAC$_i$) to (q-1)-h_2(MAC$_i$) (i =1,2, ..., n). Calculate the results of function $L(d_j)$ (j = 1,2, ..., n-t+1) from step 2. Then broadcast n-t+1 results of $L(d_j)$.

(2) The reconstruction process of the master key

The pre-shared master key Km can be restored by choose any t node from n mesh nodes. We choose the t nodes $\{M_i \mid i=1,2,\ldots,t\}$. The reconstruction process are the following steps:

Step 1: We choose t nodes M_1, M_2, ..., M_t. Mt, which construct the sequence ($C_1 \| s_1 \| R_1$, $C_2 \| s_2 \| R_2$, … , $C_t \| s_t \| R_t$)the master key distributor have to send. We calculate trap door keys $g_i = (g_i', g_i'') = h(e(P_i, s_i) \cdot e(S_i, R_i))$ (i = 1,2, ..., t) of the one-way trapdoor function respectively. s_i is the distributor's private key and S_i is private key provided by PKG system in this calculation formula. Usually, s_i share a different master key every time and S_i is assigned in the initial of Mesh network.

Step 2: Calculate the trapdoor g_i'(i=1,2,…,t)respectively by using the t nodes M_1, M_2, ..., M_t .Then we can decrypt the sequence $(Km_i \| r_i)$ $(Dg_i'(C_i) = (Km_i \| r_i))$ by using g_i' and C_i which are received respectively, we can also verify the formula $r_i = hg_i''(Km_i)$.If it is equal, it can prove that the distributor sent ($C_i \| s_i \| R_i$) sequence are corresponding to M_i nodes. If it is not equal, the distributor will send error information and it report errors to the distributor and request a re-send.

Step 3: We use two-variable one-way function to respectively calculate $KM_i=h(Km_0,Km_i)$ (i=1 , 2 , … , t) with t nodes M_1, M_2, ..., M_t chosen before. It send KM_i to the designated master key computing nodes for calculating, in which Km_0 information is public. The computing nodes can be the mesh nodes are not selected by or the mesh router nodes connected to wired device. The computing nodes are considered as a secure authentication server or certified Mesh nodes.

Step 4: The master key information computing nodes receive Km_i (i=1 , 2 , … , t) provided by t nodes M_1, M_2, ..., M_t. It can construct t values (h_2(MAC$_i$), KM_i) by using t nodes' MAC$_i$, and select n-t+1 numbers the smallest integer d_j from 1-h_2(MAC$_i$) to (q-1)-h_2(MAC$_i$)(i=1,2 , … , n). Then d_j can construct the function (d_j ,$L(d_j)$).

Step 5: According to the (h_2 (MAC$_i$), KM_i) (i=1 , 2 , … , t) and (d_j ,$L(d_j)$) (j=1,2 , … , n-t+1), we reconstruct the n-th Lagrange polynomial L(x)[2] by using Lagrange interpolation.

$$L(x)=\sum_{i=1}^{n-t+1} L(d_i)\left[\prod_{j=1}^{t}\frac{h_2(MAC_j)-x}{h_2(MAC_j)-d_i}\prod_{j=1,j\neq i}^{n-t+1}\frac{d_j-x}{d_j-d_i}\right]+\sum_{i=1}^{t} K_{M_i}\left[\prod_{j=1}^{n-t+1}\frac{d_j-x}{d_j-h_2(MAC_i)}\prod_{j=1,j\neq i}^{t}\frac{h_2(MAC_j)-x}{h_2(MAC_j)-h_2(MAC_i)}\right]$$

If x=0, we can calculate the master key information (L(0)= Km). And n values can be constructed n-1th Lagrange polynomial, so we need n+1 values.

(3) The explanation of shared master key information

Shared master key can be used as PSK of a small mesh network to prove the identity of its own network when other networks or other access device. This network's PSK as a shared master key can divide into multiple key share to remain in multiple mesh nodes. This share of the key can be used for multiple master key shared processes without updating regularly. Compared to traditional PSK authentication, this one enhanced security and reduced calculation updating on performance. Shared master key information also can be the authentication scheme for nodes joining into this small mesh network.

3. Performance Analysis

3.1. Correctness analysis of information distribution and reconstruction of the master key

To ensure that the master key is uniform before the information distribution and after the reconstruction, the same as to make sure that the secret sharing scheme used in the improved authentication protocol is correct, we have to use the same trapdoor pair g_i used in Step 3 of the master key distribution process $g_i = (g_i', g_i'') = h(e(P_i, P_{pkg}))^{X_i}$ as the one used in Step 1 of the master key reconstruction process $g_i = (g_i', g_i'') = h(e(P_i, S_i) \cdot e(S_i, R_i))$. So it is necessary to prove the establishment of the following equation $e(P_i, P_{pkg}) = e(P_i, S_i) \cdot e(S_i, R_i)$.

The certification steps are:

Condition ① $s_i = x_i P_{pkg} - r_i S_d$, $R_i = r_i P_d$ （From Step 4 of the master key distribution.）

Condition ② P_{pkg} , S_i, P_i , S_d, $P_d \in G_1$, S_{pkg} , x_i , $r_i \in Z_p^*$ （Precondition）

Condition ③ $h_1\{0,1\}^* \rightarrow G_1$, $h_2\{0,1\}^* \rightarrow Z_p^*$ （Precondition）

Condition ④ $e: G_1 \times G_1 \rightarrow G_2$

By Condition ②, Condition ③ and the definition and character of Bilinear Map, we can get:

$e(S_i , r_i P_d) = e(S_i , P_d) = e(S_i , P_d)^{X_i} = e(P_i , r_i S_d)$;

Then use Condition ①:

$e(P_i, s_i) \cdot e(S_i, R_i) = e(P_i , x_i P_{pkg} - r_i S_d) \cdot e(S_i , r_i P_d) = e(P_i , x_i P_{pkg} - r_i S_d) \cdot e(P_i , r_i S_d) = e(P_i , x_i P_{pkg}) = e(P_i, P_{pkg})^{x_i}$;

Finally it is proved.

So the equation $e(P_i, P_{pkg})^{x_i} = e(P_i, s_i) \cdot e(S_i, R_i)$ has been established what ensure the correctness of the secret sharing scheme mathematically. Other operations in the main key distribution process correspond to those in the main key reconstruction process. n+1 mathematical numbers can be used to construct the highest times for n of Lagrange polynomials by Lagrange interpolation. This proof is based on mathematical theory, which refers to literature[4]. In summary, the correctness of the whole main key sharing scheme is proved mathematically, which can ensure the correctness of the improved authentication protocol.

3.2. Security Analysis

(1) In the information distribution and reconstruction process of the main key, only one mesh node Mi that is selected can get the main key information from the master key distributor. And other selected mesh nodes cannot obtain the main key share.

To prove with the reduction to absurdity: If other selected mesh nodes can obtain the main key share, we would deduce the opposite conclusion

The proof: Other mesh nodes could obtain the main key share Km_i only by intercepting the following two cipher-text sequences: C_i and R_i, from the sequence $C_i \| s_i \| R_i$ sending to node M_i. But it is computationally infeasible to get Km_i from the equation $C_i = E_{g_i''}(Km_i \| r_i)$ due to the difficulty to break the symmetric key encryption algorithm. On the other hand, to obtain Km_i by breaking the one-way trapdoor function through $R_i = r_i P_d = r_i = h_{g_i''}(Km_i) P_d$ without trapdoor g_i'' is very difficult to be calculated in polynomial time. It shows that the assumption does not hold. And other selected mesh nodes cannot obtain the main key share Km_i. Only node M_i can get the main key share Km_i by doing unsigncryption on the signed cipher-text sequence $C_i \| s_i \| R_i$.

(2) The master key share that is not updated regularly will not affect the security of the authentication protocol, which particularly can resist statistical attacks that traditional PSK may suffer by updating from time to time.

The proof: The main key Km would not use every node's main key share when it is reconstructed, but compute each node's main key share what has been processed by two-variable one-way function $h(x,y)$. From the two-variable one-way function property[5], it is infeasible to compute y (or x) by knowing x (or y) and $h(x, y)$. And for one x and two different y (y_1 and y_2), it is also infeasible to compute $h(x,y_1) = h(x, y_2)$. So is y. In the reconstruction, a mesh node provides its main key share to compute . Then it sends the shielded key share to the specified to calculate the main key information. Though is open, by the two-variable one-way function, anyone who knows , Km_0 and $h(x, y)$ is computationally infeasible to get the main key share . The main key share of each mesh node can be used multiple times, which can prove that the main key share that does not update will not threaten the security of the authentication protocol.

The security of the traditional pre-shared key mode is enhanced by the use of en: PBKDF2 key derivation function. However, the attacker may crack the pre-shared key from the statistical analysis of a typical weak passphrase. Generally, using 8 Diceware words or 22 random letters and regularly updating pre-shared key can be relatively safe. The improved authentication scheme ensures safety in the situation that the pre-shared key is not updated. It can be explain from the following two sides:

In theory, the storage structure that the main key secret sharing of the authentication protocol used will satisfy the requirements in the security and reconstruction of the statistical secret sharing scheme. Only through the statistical main key share is not it feasible to get the main key information in the probabilities.

In reality, the attacker generally meet the information theory model (a secure channel and the attacker have unlimited computing power). That the storage structure that the main key secret sharing of the authentication protocol used will satisfy the requirements in the security and reconstruction of the statistical secret sharing scheme is enough. The threshold secret sharing scheme this authentication protocol uses has perfect security to passive static (t ,n) threshold attackers in the information theory model. Specific proof refers to the literature[2] which is also proved that perfect sharing system security is greater than the statistical sharing scheme mathematically.

The sharing scheme of the master key of the authentication protocol meets the (t, n) threshold secret sharing scheme. Reconstruction under the master key to the recovery process, any t of the mesh nodes is difficult to obtain primary key information. Even if the master key information distribution process has been made public n-t +1 pairs of values (d_j - L (d_j) (where j = 1,2, ..., n-t+1). To break the secret sharing scheme by less than the n +1 pairs of values is equivalent to break the door Shamir threshold scheme. In mathematics, it will be a large integer factorization complex problem, which is computationally infeasible. T (or more) participating nodes through their t pairs of values (h_2(MAC$_i$), KM_i) (where i = 1,2, ..., t), and public n - t +1 pairs of values (d_j - L(d_j) (where j = 1,2, ..., n - t + 1) can be very easy to construct lagrange polynomials of n-th order L(x), in order to obtain the master key information. So the sharing scheme of the master key of the authentication protocol in line with the (t, n) threshold secret sharing scheme of the two conditions, those are met (t, n) threshold secret sharing scheme.

(3) If the pre-shared main key information distributor's private key leak, it will not leak previous pre-shared main key Km. It means that this authentication protocol is with forward secrecy.

The proof: From (1), we know that only one selected mesh node M_i can get the main key Km_i from the main key information distributer, and other selected mesh nodes can't. Even though the distributer's private key leak, every mesh node's main key share Km_i is still safe. The main key information distributer use one-way trapdoor function $r_i = hg''_i(Km_i)$ to sign each main key share Km_i. The attacker can not obtain Km_i without trapdoor g''_i through computing. So leaking the distributer's private key S_d does not leak previous pre-shared main key K_m. This authentication protocol is with forward secrecy.

3.3. Improved certification plan for computation feasibility analysis

The distribution process of main key information involves the below 4 step.

Step 1 : Calculates n times $h(Km_0, Km_i)$

Step 2: Calculates n times h_2(MAC$_i$) and construct a n times Lagrange interpolation polynomial $L(x)$

Step 3: Calculated n pairs one-way trapdoor function pair $g_i = (g'_i, g''_i) = h(e(P_i, P_{pkg})^{x_i})$,

Step 4 : Calculate the n times one-way trapdoor function $hg''_i(Km_i)$.

Where h (x, y) is a one-way function of the bivariate, the $h_2(x)$ is a one-way hash function. Both are polynomial-time problems, which can be solved in polynomial time. If the function is selected properly can control the computational complexity O(n); e is a bilinear map on the cyclic group G_1 of order q and cyclic group G_2 of q Multiplication, xi is an element of Z^*_P . By the bilinear mapping theory to know: for any P , $Q \in G_1$, existence of the effective algorithm of computing e (P, Q). On the above cyclic group G_1 and G_2, You can define as many Cryptography difficult issues. Such as computing the Diffie-Hellman (CDH), Decision-making the Diffie-Hellman (DDH) problem, Therefore, computationally feasible of $e(P_i, P_{pkg})$; For one-way trapdoor function $h_k(x)$ to seeding x in no key "k" is NP problem. In case if there are k, seeking x is a polynomial time, n For the Lagrange interpolation polynomial, the literature [6] [7] [8] described the definition, existence and uniqueness. Improved n times Lagrange Polynomial to new Lagrange Polynomial, Each basic polynomial computational complexity reduced from O(n^2) to O(n), key recovery processed same as the Here is not to enumerate old. In summary, improved authentication scheme is computationally feasible.

3.4. Comparison of the authentication protocol using the master key scheme to share information with other scheme

Compare this article's Main key information sharing program with a block codes based on the system (t, n) threshold secret sharing scheme from Chien[9] et al and a secret sharing scheme based on Shamir A from Yang[10] et al. It mainly depends on the public the amount of information as inspection, because the size of the public information is an important parameter of a scheme performance. It affects the complexity of storage, communications and computing[11]. If m master keys are secretly shared, the quantity of public information they need is portrayed[12] with a complexity of O(n), shown in Table 2.

Table. 2: Comparison table of each scheme's complexity

Scheme name	**The required amount of public information**	
	$m < t$	$m \geqslant t$
Chien et al. scheme	O(n+m-t+1)	O(n+m-t+1)
Yang et al. scheme	O(n+1)	O(n+m-t+1)
This authentication protocol sharing scheme	O(n+m-t+1)	O(n+m-t+1)

The above Table 2 shows that when $m < t$ the program has less complexity dimension than the one of Yang, et al.. In other cases, when the complexity is O (n+m-t+1), the programs of Chien et al. and Yang et al. both reconstruct and recover the master key by solving an n+m-t order equations. In this paper, we realize it by constructing a n+m-t order Lagrange polynomial. Reference [10] proved that the Lagrange polynomial method is easier than solving equations under the same order. This means, the computational complexity of the proposed authentication protocol sharing scheme is actually less than the that of Chien et al. and Yang et al.

The proposed master key information sharing program has been compared with that proposed by Shamir A [13] , Huang RJ [14], and Wang YM et al [15]. The specific results are shown in Table 3.

Table. 3: Comparison table of each scheme's strengths and weaknesses

Variety Scheme	Whether secure channel is required	Whether the the master key is allowed to be reused	Whether it has forward-security	Whether the quota needs to be manipulated before distributed
Shamir A et al	Require	Cannot be reused	Does not have	No description
Hwang RJ et al	Don't require	Reusable	Have	Need to be handled through consultation
Wang YM et al	Require	Reusable	Does not have	Need to encrypted
This scheme	Don't require	Reusable	Have	Need to deal with

It can be seen from the above comparison in Table 3 That the master key sharing scheme used in our authentication protocol does not require additional communication securing channel. In addition, the master key share can be distributed in a timely manner without requiring to be manipulated before distributed, and has a forward security [16]. The program has better performance in terms of using the MAC address of each mesh node as the node identity authentication, and not requiring updating master key share regularly than the early scheme proposed by Shamir A.

4. Summary and next works

As the mobile communications been developed to 4G era, securely anytime anywhere access to the Internet has become new requirements for mobile communications. This article proposed a new Wireless Mesh Networks PSK authentication scheme, and described the authentication protocol parameter settings of the master key shared system and the distribution and reconstruction of the master key information . In addition, we also described the implementation of the authentication scheme. The security of network access node authentication has been improved through the designed security authentication protocol. Finally, we analyze the improved certification scheme, in terms of the program's correctness, security and certification performance. Finally, the advantage of the improved scheme is provided. The analysis on secure authentication protocol and the proposal of suggested scheme will certainly accelerate the development and application of the Mesh Network. We have improved the efficiency of certification and certification of authorization mechanisms, fatherly improved the mesh network routing protocol, added in the function of

multi-gateway, and ensured the speed is higher under multi-gateway. This can be used as research topic of the next phase of the study.

5. Acknowledgments

This work is supported by the State Natural Sciences Foundation Monumental Projects of China under Grant No. 61133014, the CEEUSRO project of Guangdong province, China under Grant No. 2011B090400469, the scientific and technological plan project of Guangdong province, China under Grant No. 2008A010100001 and the key project of transformation of scientific and technological achievements of college of Guangdong province, China Grant No. cgzhzd0807.

6. References

[1] Yao G X, Wei L F, Guan Q L. Research and design of the Intranet authentication management framework based on intrusion tolerance. Asia-Pacific Conference on Information Processing 2009, pp. 487-488 .

[2] Kurosawa, K. General Error Decodable Secret Sharing Scheme and Its Application. Information Theory, IEEE Transactions on.2011, 57(09):6304-6309 .

[3] D. Boneh and M. Franklin. Identity Based Encryption from the Weil Pairing, CRYPTO'01, LNCS 2139 (2001), pp. 213-229 .

[4] N. Kohlmtiller, G.Ntiruberger, and F. Zeilfelder. Construction of cubic 3D spline surfaces by Lagrange interpolation at selected points. In Curve and Surface Fitting, Saint-Malo 2002, pages 245-254, 2003 .

[5] Liaojun Pang; Huixian Li; Ye Yao; Yumin Wang; A Verifiable (t, n) Multiple Secret Sharing Scheme and Its Analyses.Electronic Commerce and Security, 2008 International Symposium on.2008, Page(s): 22-26 .

[6] Jean-Paul Berrut, Lloyd N. Trefethen(2004). Barycentric Lagrange Interpolation. SIAM Review，46(3)：501-517 .

[7] E. Meijering. A chronology of interpolation: From ancient astronomy to modern signal and image processing,. Proceedings of the IEEE：323 .

[8] Julius Orion Smith III. Lagrange_Interpolation. Center for Computer Research in Music and Acoustics (CCRMA), Stanford University .

[9] H Y Chien, J K Jan，Y M Tseng. A practical (t,n) multi-secret sharing scheme[J]. IEICE Transactions on Fundamentals，2000，E83-A (12)：2762-2765 .

[10] Yang C C, Chang T Y，Hwang M S. A (t,n) multi-secret sharing scheme[J]. Applied Mathematics and Computation，2004，151(2)：483-490 .

[11] Giovanni Di Crescenzo. Sharing one secret VS. sharing many secrets：Tight Bounds on the average improvement ratio[J]. Theoretical Computer Science，2003，295(13)：123-140 .

[12] Yehuda Lindell. General Composition and Universal Composability in Secure Multiparty Computation. Journal of Cryptology, 2009, 22(03), pp: 395-428 .

[13] Shamir A. How to share a secret .Communications of the ACM, 1979, 22 (11) :612-613 .

[14] Hwang R J, Lai C H, Su F F . An Efficient Signcryption Scheme with Forward Secrecy Based on Elliptic Curve[J] .Applied Mathematics and Computation, 2005, 167 (1) :870-881 .

[15] Pang L J, Wang Y M. (t, n) threshold secret sharing scheme based on RSA cryptosystem .Journal of Communications, 2005, 26 (6) :70-73 .

[16] Jen-Ho Yang; Chin-Chen Chang; Chih-Hung Wang; An Efficient V-Fairness (t, n) Threshold Secret Sharing Scheme.Genetic and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on,2011 , Page(s): 180-183 .