

# Tree based Conference Key Establishment Cost Analysis and Minimization in Heterogeneous Networks

Zhan Liu and Mi Lu

Department of Electrical and Computer Engineering

Texas A & M University

College Station, Texas 77840, U.S.A.

{liuzhan, mlu}@ee.tamu.edu

Tel: 979 845 9578

Fax: 979 845 2630

**Key word:** Conference Key, Heterogeneous Networks

## Abstract

*A shared secret, conference key, must be established among members to securely communicate among them. The Diffie-Hellman is often used for the conference key establishment. In a heterogeneous network, the participants have different resources. Therefore, different burden should be placed on different participants. However, most protocols did not address this problem. Wade Trappe et. al. addressed this problem considering the computational power minimization for Perrig protocol. In this paper, we will consider minimization of the cost with considering the transmission since transmission consumes most of the energy. A cost analysis and a minimum cost protocol with or without constraints are presented.*

## 1 Introduction

Many conference key establishment protocols have been proposed [1]. Only Wade Trappe et al. [4] considered the heterogenous property of network. However, they only discussed the computational cost. In this paper, we will discuss the transmission cost since transmission consumes most of the power [5]. In a heterogeneous network, participants have very different properties. Some have very limited

computation capability. Some are battery-powered device, therefore power consumption is crucial for those devices. In this paper, we will consider a heterogeneous network and analysis the cost of establishing a conference key among the participants.

### Notation used

---

$M_i$ :	A participant
$N$ :	Total number of participants
$T(N)$ :	Times of pairing

---

## 2 Perrig Protocol

To discuss the protocol, we rewrite the Perrig protocol [1] as following:

### Round 1:

$$Z_{1,1} = g^{r_1 r_2}, Z_{1,2} = g^{r_3 r_4}, \dots, Z_{1,2d-1} = g^{r_{N-1} r_N}$$

### Round 2:

$$Z_{2,1} = g^{Z_{1,1} Z_{1,2}}, Z_{2,2} = g^{Z_{1,3} Z_{1,4}}, \dots, Z_{2,2d-2} = g^{Z_{1,2d-1-1} Z_{1,2d-1}}$$

### Round d:

$$Z_{d,1} = g^{Z_{d-1,1} Z_{d-1,2}}$$

The  $Z_{d,1}$  is the conference key.

Perrig protocol is a tree based protocol. The tree is a balanced tree.

### 3 Cost Analysis

#### 3.1 Pairing

**Definition 1** For a set  $S_N = \{u_1, u_2, \dots, u_N\}$ , where  $N \geq 2$ , we randomly choose 2 elements, i.e.  $\forall i, j \in \{0, 1, 2, \dots, N\}$ ,  $\{u_i, u_j\} \rightarrow \{u_k^1\}$ , we call this a pairing.

After one pairing, there are only  $N-1$  elements, we rewrite the new set as  $S_{N-1} = \{u_1^1, u_2^1, \dots, u_{N-1}^1\}$ , where  $u_k^1$  is the combined elements and other element does not change but are given new symbols.

**Lemma 1** For  $N$  elements set  $S_N = \{u_1, u_2, \dots, u_N\}$ ,  $N \geq 2$ ,  $N-1$  times are needed to pairing  $N$  elements into one elements set  $S_1 = \{u_1^{N-1}\}$ . i.e.  $T(N) = N-1$ .

Proof: This claim is obvious for  $N=2$ . i.e.  $T(2) = 2-1=1$ .

Suppose this claim is true for  $N=m$ , i.e.  $m-1$  times are needed to pairing the  $m$  participants. Now for  $N=m+1$ , therefore, we can first pairing any  $m$  participants, which takes  $m-1$  times. Without lost generality, we pair the first  $m$  participants, then we pair the last participant into the group, which take one more time. Therefore,  $m-1+1=m$  times are needed. Therefore,  $T(N) \leq N-1$

Now, suppose we can find a way to pairing  $m$  participants with  $T(m) < m-1$ , then for  $m=2$ , we have  $T(2) < 1$ , which is impossible. Therefore  $T(N) = N-1$ .

**Lemma 2** For  $N$  elements set  $S_N = \{u_1, u_2, \dots, u_N\}$ ,  $N \geq 2$ , no matter how we pairing the elements,  $N-1$  times are needed to pairing  $N$  elements into one elements set  $S_1 = \{u_1^{N-1}\}$ . i.e.  $T(N) = N-1$ .

Proof: Randomly choose  $2m_1$  participants, where  $m_1 \leq \lfloor N \rfloor$ , and randomly pairing them, i.e.

$\forall i, j \in \{0, 1, 2, \dots, N\}$ ,  $\{u_i, u_j\} \rightarrow \{u_k^1\}$ . There are  $m_1$  times pairing. The set becomes

$S_{N-m_1} = \{u_1^1, u_2^1, \dots, u_{N-m_1}^1\}$ , which has  $N-m_1$  elements.

Randomly choose  $2m_2$  participants, where  $m_2 \leq \lfloor (N-m_1)/2 \rfloor$ , and randomly pairing them, i.e.

$\forall i, j \in \{0, 1, 2, \dots, N-m_1\}$ ,  $\{u_i^1, u_j^1\} \rightarrow \{u_k^2\}$ . There are  $m_2$  times pairing. The set becomes

$S_{N-m_1-m_2} = \{u_1^2, u_2^2, \dots, u_{N-m_1-m_2}^2\}$ , which has  $N-m_1-m_2$  elements.

In general, if

$$S_{N-\sum_{i=1}^l m_i} = \{u_1^l, u_2^l, \dots, u_{N-\sum_{i=1}^l m_i}^l\}$$

Then randomly choose  $2m_{l+1}$  participants, and pairing them randomly, i.e.

$$\forall i, j \in \{0, 1, 2, \dots, N-\sum_{i=1}^l m_i\}, \{u_i^l, u_j^l\} \rightarrow \{u_k^{l+1}\}.$$

There are  $m_{l+1}$  times pairing. The set becomes

$$S_{N-\sum_{i=1}^{l+1} m_i} = \{u_{1+1}^{l+1}, u_2^{l+1}, \dots, u_{N-\sum_{i=1}^{l+1} m_i}^{l+1}\},$$

which has  $N-\sum_{i=1}^{l+1} m_i$  elements.

Finally, we will have

$$S_{N-\sum_{i=1}^n m_i} = S_1 = \{u_1^n\}, \text{ i.e. } \sum_{i=1}^n m_i = N-1.$$

**Definition 2** For a Diffie-Hellman key exchange, one member in group  $A$  sends a message  $g^{k_a}$  to another group  $B$  and one member in group  $B$  sends a message  $g^{k_b}$  to group  $A$  is called a message exchange.

**Theorem 1** For a tree based Diffie-Hellman conference key establishment, no matter how we form the tree, the number of message exchange is always  $N-1$  times.

Proof: For a tree based Diffie-Hellman conference key establishment, each key exchange is the same as pairing. Therefore, from lemma, we know the time is always  $N-1$ .

### 4 Cost Analysis

Up to now, Wade et al [4]. considered the cost problem in heterogenous network. Because the heterogenous property, we suppose each participant has different cost for a DH key exchange. The cost could be energy or any other things.

It is quite obvious that the total cost for a conference key establishment is a function of the total message exchange  $M$ , the cost  $c_i (i=1, 2, \dots, N)$  of each participate for each round of message exchange and the times  $T_i (i=1, 2, \dots, N)$  each participant conducts a DH key exchange. Therefore,

$$C = f(M, c_1, c_2, \dots, c_N, T_1, T_2, \dots, T_N)$$

In [4], a Huffman coding tree is proposed to minimize the cost of tree base DH protocols. However, the approach can only be applied for computational cost, not for transmission cost. Here we would like to propose a cost analysis for transmission.

When considering transmission, Huffman coding tree can't be used. We need a new approach. Not

like computation, in which each round, all the participants in that round should calculate the key, only one participant in one group and one participant in another group need to broadcast the message.

No matter how we construct a binary tree, the total message exchange is always  $N - 1$ . Therefore,

$$C = f(c_1, c_2, \dots, c_N, T_1, T_2, \dots, T_N) = \sum_{i=1}^n c_i T_i$$

So rearrange a binary tree will not increase the total message exchange. We can arrange a binary in any way, which will make the least cost participant have more chance to transmit. Therefore the protocol should like the following. Without loss the generality, suppose  $c_1 \leq c_2 \leq \dots, \leq c_N$ .

## 4.1 Minimum Cost

The protocol

1  $M_2$  send  $g^{r^2}$ ,  $M_1$  send  $g^{r^1}$

2  $M_3$  broadcast  $g^{r^3}$ ,  $M_1$  send  $g^{K_1}$

...

i  $M_{i+1}$  broadcast  $g^{r^{i+1}}$ ,  $M_1$  send  $g^{K_{i-1}}$

...

In total,  $M_1$  does  $N - 1$  DH message exchange, and  $M_i$  does one DH message exchange, where  $i = 2, 4, \dots, N$ . Therefore, the total cost for this protocol is

$$C_{total} = (N - 1)c_1 + \sum_{i=2}^N c_i$$

This is the least cost protocol for tree based DH key exchange protocol.

## 4.2 Constraints

There might be a limitation on transmission time for each participant because of the limited resource. We first arrange the participants according to their cost. Without loss of generality, suppose the cost  $C = \{c_1, c_2, \dots, c_N\}$ , where  $c_1 \leq c_2 \leq \dots, \leq c_N$ . Then the participants are in the sequence of  $M_1, M_2, \dots, M_N$ . The corresponding allowed maximum transmission times are  $T = \{T_1, T_2, \dots, T_N\}$ , where  $T_i$  is the maximum transmission time for participant  $M_i$  and  $T_i \geq 1$ .

**Lemma 3** For a group of  $N$  participants  $M_i (i = 1, 2, \dots, N)$  with corresponding allowed maximum transmission time  $T_i (i = 1, 2, \dots, N)$ , if  $T_i \geq 1 (i =$

$1, 2, \dots, N)$  and  $\sum_{i=1}^N T_i \geq 2(N - 1)$ , then it is possible for the group to establish a conference key. Or else, it is not possible for them to establish a key.

*Proof:* Since each participant should transmits at least one time, therefore  $T_i \geq 1 (i = 1, 2, \dots, N)$ . Or else, the conference key can not be established. This means that if any  $T_i < 1 (i = 1, 2, \dots, N)$ , there is not conference key.

For each DH message exchange, there are two transmissions. Since we need  $N - 1$  message exchange, therefore, the total transmission time should be  $2(N - 1)$ . This means that if  $\sum_{i=1}^N T_i < 2(N - 1)$ , there is not conference key.

Now, if  $T_i \geq 1 (i = 1, 2, \dots, N)$  and  $\sum_{i=1}^N T_i \geq 2(N - 1)$ , let us construct a protocol like the following.

Each participant  $M_i$  transmit up to  $T_i$ , then next participant  $M_{i+1}$  will take over until all the participants join the group.

Here is the protocol

1.1  $M_2 \rightarrow M_1 : g^{r^2}$

1.2  $M_1 \rightarrow M_2 : g^{r^1}$

Then  $M_1$  calculates  $K_1 = (g^{r^2})^{r^1}$  and  $M_2$  calculates  $K_1 = (g^{r^1})^{r^2}$

⋮

After  $M_1$  has transmitted  $T_1$  times,  $M_2$  take over  $M_1$ 's role and start to broadcast the message.

$(T_1 + 1)$ .1  $M_{T_1+2} \rightarrow M_1, M_2, \dots, M_{T_1+1} : \text{broadcast } g^{r_{T_1+2}}$

$(T_1 + 1)$ .2  $M_2 \rightarrow M_{T_1+2} : g^{K_{T_1}}$ .

Then  $M_{T_1+2}$  calculates  $K_{T_1+1} = (g^{K_{T_1}})^{r_{T_1+2}}$  and  $M_1, M_2, \dots, M_{T_1+1}$  calculate  $K_{T_1+1} = (g^{r_{T_1+2}})^{K_{T_1}}$ .

⋮

Since  $M_2$  already transmitted one time when he first joined the group, so after he take over  $M_1$ 's role, he has  $T_2 - 1$  times transmission limitation. When it is  $T_1 + T_2 - 1 + 1 = T_1 + T_2$  times transmission,  $M_3$  take over.

$(T_1 + T_2)$ .1  $M_{T_1+T_2+1} \rightarrow M_1, M_2, \dots, M_{T_1+T_2} : \text{broadcast } g^{r_{T_1+T_2+1}}$

$(T_1 + T_2)$ .2  $M_3 \rightarrow M_{T_1+T_2+1} : g^{K_{T_1+T_2-1}}$ .

Then  $M_{T_1+T_2+1}$  calculates  $K_{T_1+T_2} = (g^{K_{T_1+T_2-1}})^{r_{T_1+T_2+1}}$  and  $M_1, M_2, \dots, M_{T_1+T_2}$  calculate  $K_{T_1+T_2} = (g^{r_{T_1+T_2+1}})^{K_{T_1+T_2-1}}$ .

⋮

We continue in this way, therefore we have

$$\left(\sum_{j=1}^i T_j - i + 2\right) \cdot \mathbf{1} \quad M_{\sum_{j=1}^i T_j - i + 3} \quad \rightarrow \quad \text{broadcast} \\ M_1, M_2, \dots, M_{\sum_{j=1}^i T_j - i + 2} \quad : \\ g^{\sum_{j=1}^i T_j - i + 3}$$

$$\left(\sum_{j=1}^i T_j - i + 2\right) \cdot \mathbf{2} \quad M_{i+1} \quad \rightarrow \quad M_{\sum_{j=1}^i T_j - i + 3} \quad : \\ g^{K_{\sum_{j=1}^i T_j - i + 1}}$$

Then  $M_{\sum_{j=1}^i T_j - i + 3}$  calculates  $K_{\sum_{j=1}^i T_j - i + 2} = (g^{K_{\sum_{j=1}^i T_j - i + 1}})^{r_{\sum_{j=1}^i T_j - i + 3}}$  and  $M_1, M_2, \dots, M_{\sum_{j=1}^i T_j - i + 2}$  calculate  $K_{\sum_{j=1}^i T_j - i + 2} = (g^{\sum_{j=1}^i T_j - i + 3})^{K_{\sum_{j=1}^i T_j - i + 1}}$ .

When  $M_{i+1}$  takes over and begin to broadcast, we have already broadcasted  $(\sum_{j=1}^i T_j - i + 2)$  times. After  $M_{i+1}$  broadcast  $T'_{i+1} (\leq T_{i+1}) - 1$  times, all the participants are in the group. Therefore,  $M_k (k = 1, 2, \dots, i)$  have transmitted  $T_k (k = 1, 2, \dots, i)$  times,  $M_{i+1}$  has transmitted  $T'_{i+1}$  times.  $M_l (l = i + 2, i + 3, \dots, N)$  have transmitted only one times. So we get a protocol which satisfies the transmission times constraints.

In this way, we also get the minimum cost protocol under the constraints.

$$C_{min} = \sum_{i=1}^N c_i T'_i$$

Where  $T'_i \leq T_i$  is the actual time  $M_i$  transmits ( $i = 1, 2, \dots, N$ ).

A by-product of this protocol is that, subgroup  $sg\{i\} = \{M_1, M_2, \dots, M_i\}$ , where  $i = 2, 3, \dots$ , share a key  $K_{i-1}$ . Therefore, it is possible to establish all kind of subgroup and form hierarchy with the small subgroup on the top. A participant  $M_i$  can decide if the information is going to be shared within subgroup  $sg\{i\}$  or share with  $sg\{j\} (j = i + 1, \dots, N)$

## 5 Conclusion

A tree based DH protocol with minimum cost is achieved. We have analyzed the cost and how to achieve the minimus cost. We have also analyzed the constraints on resource and have given a corresponding protocol.

Our protocol allows all participants except one to send just one unit information, which is the lower boundary of DH algorithm. This protocol is flexible. It allows any participant to send from one unit information to  $N - 1$  unit information. No other protocols can achieve this. It can be assigned as the most unbalance case with one send most of the information and all other just send one unit information. It can also be assigned as most balance case with each participant sends two-unit information and any two participants send just one unit information. And the protocol can be arranged as any case between the most unbalance case and the most balance case. No other protocols have such flexibility. Therefore it is suitable for any kind of heterogeneous network in which devices have very different capability and cost.

## References

- [1] Colin Boyd, et al, "Protocols for Authentication and Key Establishment", *Springer*, 2003
- [2] Klaus Becker, et al, "Communication complexity of group key distribution", *5th ACM conference on Computer and Communications Security*, pp. 1-6, ACM Press, 1998
- [3] Sandro Fafaeli, et al, "A Survey of Key Management for Secure Group Communication", *ACM Computing Surveys*, Vol.35, No.3, Sept. 2003, pp. 309-329
- [4] Wade Trappe, et al, "Establishment of Conference Keys in Heterogeneous Networks", *IEEE Int. Conference on Communications*, pp2201-2205
- [5] J.D. Tygar, et al, "SPINS:Security protocols for sensor networks", *Wireless Networks*, v8, n5, Sept. 2002, pp521-534