Comments on “Distributed Symmetric Key Management for Mobile Ad hoc Networks” from INFOCOM 2004

J. Wu and R. Wei

Department of Computer Science
Lakehead University
Thunder Bay, Ontario P7B 5E1, Canada
jwu1@lakeheadu.ca
wei@ccc.cs.lakeheadu.ca

Abstract. In IEEE INFOCOM 2004, Chan proposed a distributed key management scheme for mobile ad hoc networks, and deduced the condition under which the key sets distributed to the network nodes can form a cover-free family (CFF), which is the precondition that the scheme can work. In this paper, we indicate that the condition is falsely deduced. Furthermore, we discuss whether CFF is capable for key distributions in ad hoc networks.

1 Introduction

In [1] Chan introduced a Distributed Key Pre-distribution Scheme (DKPS) for ad hoc networks. One key idea of the DKPS is that each node individually picks a set of keys from a large publicly-known key space following some procedure so that at the end, the key patterns of all the nodes satisfy the following exclusion property with a high probability: any subset of nodes can find from their key sets at least one common key not covered by a collusion of at most a certain number of nodes outside the subset. In the next section, we analyze this scheme and prove that [1] falsely deduced the condition under which the scheme can yield the desired key patterns, then we further discuss whether any similar scheme that produces the desired key patterns is practical.

2 Analysis of Chan's Scheme

Chan's scheme is based on cover-free family (CFF) [2]. It requires that the sets of keys held by the network nodes form a $(w, r; d) - CFF(N, T)$ cover-free family, i.e., any w nodes share at least d keys that are not held by any other r nodes. The keys are selected from a pool of size N, and at most T nodes are supported. A $(w, r; d) - CFF(N, T)$ is formally defined as follows:

Definition 1. *Let $\mathcal{X}$ be a set of points, $\mathcal{F}$ be a set of subsets (called blocks) of $\mathcal{X}$. Let $N = |\mathcal{X}|, T = |\mathcal{F}|$. The set system $(\mathcal{X}, \mathcal{F})$ is called a $(w, r; d) - CFF(N, T)$*

if for any w blocks $B_1, \cdots, B_w \in \mathcal{F}$ and any other r blocks $A_1, \cdots, A_r \in \mathcal{F}$, we have

$$\left| \left(\bigcap_{i=1}^{w} B_i \right) \setminus \left(\bigcup_{i=1}^{r} A_i \right) \right| \geq d$$

where d is a positive integer.

In [1], a probabilistic method called Distributed Key Selection (KDS) is used to construct the $(w, r; d) - CFF(N, T)$. Its procedure is as follows:

1. Select k such that d divides k.
2. Form the universal key set P with size $N = k^2 r/d$.
3. Divide P into k partitions $P_1, P_2, \cdots, P_k$ each of size kr/d.
4. Each node individually pick keys for his key ring to form $B = \{p_1, p_2, \cdots, p_k\}$ with each p_i randomly selected from the partition P_i, $1 \leq i \leq k$. (Each p_i will follow a uniform distribution over all elements in P_i.)

Note that k is actually the number of keys that a node has to store. In its Theorem 1, [1] deduced that the above scheme yields a $(w, r; d) - CFF(N, T)$ with at least a probability $1 - e^{-t}$, if

$$T \leq e^{\frac{2k\left(2 - \frac{d}{k} - e^{-\frac{d}{k}\left(\frac{d}{kr}\right)^{w-1}}\right)^2 - t}{w+r-1}}. \tag{1}$$

The deduction sketch is as follows:

For a fixed block B_1, select $w-1$ other blocks B_i, $2 \leq i \leq w$ and r other blocks C_j, $1 \leq j \leq r$. For any $p_i \in B_1$, define

$$q = P_r\{p_i \notin \cap_{i=2}^{w} B_i \setminus \cup_{j=1}^{r} C_j\}.$$

Let $X_i = \delta[p_i \notin \cap_{i=2}^{w} B_i \setminus \cup_{j=1}^{r} C_j]$ where $\delta[\ ]$ is the delta function, then

$$P_r\{X_i = 1\} = q, P_r\{X_i = 0\} = 1 - q.$$

Let $X = \sum_{i=1}^{k} X_i$, and apply Chernoff bound to estimate the upper bound of

$$P_r\{| \cap_{i=1}^{w} B_i \setminus \cup_{j=1}^{r} C_j | < d\} = P_r[X > k - d].$$

But the application of Chernoff bound in this proof is problematic. Let$\overline{X}$ be the expectation of X. Chernoff bound is applied to estimate the upper bound of $P_r[X > c]$ when $c > \overline{X}$, or the upper bound of $P_r[X < c]$ when $c < \overline{X}$. The above deduction implicitly assumes the precondition that $k - d > \overline{X}$. However, we have the opposite result:

Theorem 1. *For the set system constructed from the KDS, $k - d < \overline{X}$*

Proof. By definition, we have $d \le k$ and $w \ge 2$.

$$\begin{aligned}
k - d - \overline{X} &= k - d - \sum_{i=1}^{k} Exp(X_i) \\
&= k - d - kq \\
&= k - d - kP_r\{p_i \notin \cap_{i=2}^{w} B_i \backslash \cup_{j=1}^{r} C_j\} \\
&= \left(\frac{d}{rk}\right)^{w-1} \left(1 - \frac{d}{rk}\right)^{r} k - d \\
&< \left(\frac{1}{r^{w-1}} \left(\frac{d}{k}\right)^{w-2} e^{-\frac{d}{k}} - 1\right) d \\
&< 0
\end{aligned}$$

Then we have $k - d < \overline{X}$ □

Therefore, the inequation (1) is incorrect, and the viability of the KDS scheme is questionable.

3 Discussion on Key Distribution and CFF

The KDS in [1] is in fact an instance of the following probabilistic construction of k-uniform $(w, r; d) - CFF(N, T)$ presented in [2]:

1. Form k universal key sets P_i, $i \in [1, k]$, where $|P_i| = l$.
2. Each node individually pick keys for his key set $B = \{p_1, p_2, \cdots, p_k\}$ with each p_i randomly selected from P_i, $1 \le i \le k$.

For a $(w, r; d) - CFF(N, T)$ used in key distribution, we require $d \ge 1$. In the following part we consider the simplest case where $d = 1$. With the standard probabilistic method similar in [2], we get the following result about the construction of k-uniform $(w, r; d) - CFF(N, T)$:

Theorem 2. *If*

$$Exp = \frac{T^{w+r}\left(1 - (\frac{1}{l})^{w-1}(1 - \frac{1}{l})^{r}\right)^{k}}{w!r!} < 1, \tag{2}$$

then a $(w, r; 1) - CFF(kl, T)$ exists.

The formula in (2) has the following properties:

1. For given w, r, k and T, Exp is a function of l with one minimum value point where
$$l = l_0 = \frac{w - 1 + r}{w - 1}.$$
2. Exp increases as T or w or r increases, or k decreases.

3. When three of the four parameters (w, r, k and T) are fixed, at the point $l = l_0$, the remained one parameter reaches its minimum (for k) or maximum value (for w, r or T) that does not violate the inequation in (2). For example, for given T, w and k, when $l = l_0$, r can reach its maximum value while the inequation in (2) still holds.

The above result shows that given T, w and k, for a k-uniform $(w, r; 1) - CFF(kl, T)$ to exist, r has to be very limited. The following table gives some examples of the maximum r value given $w = 2$, certain T and k:

T	k	maximum r
500	200	2
500	400	4
1000	200	2
1000	400	3

One main concern for the ad hoc networks such as wireless sensor networks is the robustness of the networks, i.e., when some of the network nodes conspire, or be compromised by the adversary, the keys of the other nodes are still secure [3–7]. From the above analysis, we see that the probabilistic method in Section 3 can not yield CFF practical for key distribution where r has to be reasonably large. At the same time, among all known methods, this probabilistic construction provides the best sufficient conditions to ensure the existence of a CFF. That means based on the currently known methods, we can not construct or prove the existence of CFF that can provide satisfactory performance for ad hoc network key distribution. On the other hand, the research on CFF has not found a minimum block size that is the necessary condition for a CFF to exist, and is forbiddingly large to rule out CFF for key distribution in ad hoc networks. Therefore we can not conclude that *any* CFF is not capable for the ad hoc network key distribution. Further research on the bound of block size of CFF may be necessary to solve the problem.

4 Conclusion

In this paper, we analyzed a key distribution scheme based on CFF. We indicate that the performance of the scheme is falsely deduced. Furthermore, any existing CFF is not capable of key distribution in ad hoc networks where node conspiring or compromising is a main concern, and whether there is CFF that is capable is still an open problem, which relies on further research on the bound of CFF.

References

1. Aldar C-F. Chan, Distributed symmetric key management for mobile ad hoc etworks, IEEE INFOCOM 2004.
2. D.R. Stinson and R. Wei, Generalized cover-free families, Discrete Math., 279(2004), 463-477.

3. H. Chan, A. Perrig and D. Song, Random key predistribution schemes for sensor networks, IEEE Symposium on Research in Security and Privacy, (2003), 197-213.
4. W. Du, J. Deng, Y. S. Han and P. K. Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, Proc. of the 10th ACM conf. on Computer and communications Security, (2003), 42-51.
5. L. Eschenauer and V. D. Gligor, A key-management scheme for distributed sensor networks, Proc. of the 9th ACM conf. on Computer and communications Security, (2002), 41-47.
6. D. Liu and P. Ning, Establishing pairwise keys in distributed sensor networks, Proc. of the 10th ACM conf. on Computer and communications Security, (2003), 52-61.
7. R.Wei and J. Wu, Product construction of key distribution schemes for sensor networks, proceeding of Workshop for Selected Area in Cryptography, 2004