Key Pre-distribution Using Nonlinear Codes on Z_4 for Mobile Ad Hoc Networks

Morteza Rahimi
Tehran University, Iran
rahimimmorteza@gmail.com

ABSTRACT: In this paper a new method for key distribution using non-linear codes in mobile ad hoc networks, is presented. This method, in addition to meeting CFF criteria, the same code word length, number of more nodes, more tolerance malicious nodes, less computational complexity and memory size, can also reduce the processing power. The main idea of this method, the use of non-linear codes that produced using cyclic codes on Z_4 for key predistribution in mobile ad hoc networks. In proposed scheme, the resulting codeword for each node, a string of binary presence or absence of the key can specify the location of that, Furthermore that the location of "1", the number specified key is available. These codes in the same conditions (length and size) with a linear codes have a minimum distance.

Keywords: Key Predistribution, Mobile ad hoc Network, MDS Codes, Nonlinear Codes on Z_4 ring, CFF Criteria

Received: 1 December 2014, Revised 28 December 2014, Accepted 3 January 2015

1. Introduction

Mobile ad hoc networks have a features such as no need pre-existing infrastructure, node specific and possible to change the nature of having any condition that is compatible to many applications. These same features plus others such as multi hop communication between nodes, Limitations in memory, computational power and bandwidth, the network challenges face is deep. In this networks for secure communication between nodes require a set of key and security is depends preservation of this key. Meet security services such as: integrity, confidentiality, availability, non repudiation requires a key management scheme with establishing and distribution key in network to provides the required security. For creating key management, symmetric and asymmetric methods that use, between the masymmetrical needs high energy and computational power thus is not suitable for above networks. In fact, key management, the main core network security and key predistribution phase, is the most important part of it.

2. Key Predistribution Method

The DKS method that we present here, combined key distribution methods without TTP that proposed. In the DKS phase, each node randomly picks keys from the universal set (which is publicly known) to form its key ring using a certain procedure to ensure that the exclusion property is satisfied. At the end of this phase, the key chains of all the nodes satisfy the following exclution property with a high probability.

2.1 Key Exclution Property

Any subset of nodes can find from their key chains atleast one common key not covered by a collution of, atmost, a certain number of nodes outside the subset. This method first introduced by Chan [1], but Wu& Wei [5]found that the precondition was falsefy deduced. They claim that the probabilistic methods or Chan method cannot satisfy CFF property in practice.

2.2 Definition of CFF is as follows [2]

Let P be an N-set of points { p_1 , p_2 .... p_N } and B be a set of subsets (called blocks) of P (i.e. $X \subseteq P$, $\forall$ $X \in B$). Also let N and T denote $|P|$ and $|B|$ respectively. Then the set system (P, B) is called a $(w, r; d) - CFF\ (N, T)$ (cover-free family) if, for any w blocks X_1 , X_2 ..... $X_W \in B$, and any other r blocks Y_1 , Y_2 …….$Y_w \in B$, we have .,

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

Where d is a positive integer.

Although CFF is a widely adopted benchmark for formulating the security property of key pre-distribution schemes, the well known constructions (by coding theory or design theory) are centralized. Suppose we want to constructa $(w, r; d) - CFF$ assuming the capacity of each node's key ring is $k \times B$. The detail of the DKS construction is as follows:

Step 1: Select $B\ K \leq K$ *s.t.* d divides k. (k and d could be hard-coded.)

Step 2: Form the universal key set P with size $N = Kur$

Where $du = k$. (P and k are publicly known.9)

Step 3: Divide P into k partitions P_1, P_2,.. .....P_K each of size ur.

Step 4: Each node individually pick keys for his key ring to form $B = \{p_1, p_2, \ldots, p_k\}$ with each pi randomly selected from the partition P_i, $1 \leq i \leq k$. (Each p_i will follow a uniform distribution over all elemen sin P_i.) Finally, this method yields $a\ (w, r; d) - CFF$ (N, T) withthe following guarantee:

Theorem 1: The probability that this system is not $(w, r; d) - CFF\ (N, T)$ is at most $e - t$ if the following condition on T (the number of users) is satisfied:

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

Its note that this formulae by the $k - d < X$ condition, is true and not applicable for all.

2. Key Predistribution Using MDS Codes

The main idea in this scheme, is to use a global Mdscode to generate a node's key chain. For this purpose, a publicly known MDS generator matrix will be available inthe network for every node. Every node that wants to join the network can retrieve this G matrix by asking neighbors for the parameters of the generator matrix (α , n, k and q)and then the node will generate a random vector V within a prime field $GF(q)$. the elements of the generator matrix are $G_{ij} = (i-1)\ (j-1)\ \alpha$ with α as a primitive root for q.

$$G = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \ldots & (\alpha^{n-1})^2 \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ 1 & \alpha^{k-1} & (\alpha^2)^{k-1} & \ldots & (\alpha^{n-1})^{k-1} \end{bmatrix}$$

In this method, with G in hand, node i will generate random vector v_i of length k and calculate it's secret key chain (K_i).

4. The Mathematical Model for Key predistribution Using MDS Codes

The effect of number of users T, universal set size N, and key chain size k to achieve CFF was not studied in DKS. For a k-uniform (w, r; 1) – CFF (N, T), stinson [2] proved the lower bound for N with respect to w, r and T must satisfy.

$$N \geq \binom{w+r+1}{w} \, log\,(T-r-w+2) \qquad (1)$$

and

$$N \geq r\,(wlogT - logr - \; wlogw) \qquad (2)$$

With (w, r, 1) – CFF(N, T) in hand, it is easy to construct (w, r; d) – CFF ((d + 1) N, T) by repeating each element d + 1 times in the block. DKS method can be viewed as (2, r; d) – CFF (N, T).

$$X \geq (d+1) \binom{w+r+1}{w} \, log\,(T-r-w+2) \qquad (3)$$

$$X \geq r\,(d+1)\,(wlog\;T - log\;r - w\;log\;w) \qquad (4)$$

With $X = (d + 1)N$ For (1, r; 1) – CFF (N, T) the key chain size k must satisfy

$$T \leq \binom{N}{t} \Big/ \binom{k-1}{t-1} \quad , t = \left[\frac{k}{r}\right]$$

The above bound, can be scaled for (1, r; d) – CFF (X, T) as

$$T \leq \binom{(d+1)\,N}{t} \Big/ \binom{k-1}{t-1} \quad , t = \left[\frac{k}{r}\right]$$

Suppose we have T, w, r and l, we want to construct (w, r; d) CFF (N, T), the lower bound for k can be formulated :

$$k > \frac{8}{p}\,((w+r)\;log\;T - log\;w! - log\;r!) \;\text{ Where } p = \frac{(l-1)^r}{l^{w+r+1}}$$

with a maximum distance of $d = \frac{pk}{l} + 1$ and $N = k \times 1$ .We can see that any two nodes can find a shared key with any other node in the network. Hence G's rows are linearly independent, a coalition of less than T cannot reveal useful information about node I key chain.

Theorem 2: With key pre-distribution using algebraic codes can we find (2, r; d) – CFF (N, T) with $\frac{d-1}{2}\,e^{-t}$ when r less than d.

Proof: for nodes i, j and v_i ,v_j to satisfy [n, k, d] MD Scode properties, any other node m will have sub keys with distance d from v_i ,v_j . suppose S = $v_i \cap v_j$ and S has at most $n - d$ sub keys that v_i, v_j have. Because ofthe distance property of MDS codes, node m will have atmost $n - 2d$ sub keys similar to S. At least d nodes mustcooperate to make S and any number less than d can not make it. So any value $r < d$ will generate

$$\left| \boldsymbol{v}_i \cap \boldsymbol{v}_j \setminus \bigcup_{s=1}^{r} \boldsymbol{v}_{s\neq\{i,j\}} \right| > d$$

thus, we have a (2, *r*, *d*) – *CFF*. General (*w*, *r*; *d*) – *CFF* (*N*, *T*) can be achived using this approach parameter. Thus:

$$q^k n \geq \binom{w+r+1}{w} \, log\,(T - r - w + 2)$$

And

$$q^k\, n \geq r\,(d + 1)\,(w\, log\, T - log\, r - \ w\, log\, w)$$

Where

$$q^k n > N$$

Theorem 3: In this scheme we can find (*w*, *r*; *d*) – *CFF* (*N*, *T*) with e^{-t} and (*d*–1)/2when $r < d - w$.

To analysis this method that described, for satisfy *CFF*, we simulate to generate the keys as specified before. Two nodes are used, and each node constructs its key chain. Then, we compare the key chain intersections with any set of *r* nodes, and we run this method for different values of *r*. thisgraph is simulated for percentage of *CFF* satisfy with *r* = 3, 4 and 5.

5. Proposed Scheme

In a way that key distribution based on MDS codes was presented, Meet criteria for *CFF* need to string keys are too long Therefore, because the length of the string key value by Mr. Stinson has proven, Should be to have:

$$k > \frac{8}{p}\,((w + r)\, log\, T - log\, w! - log\, r!) \text{ Where } p = \frac{(l-1)^r}{l^{w+r+1}} \text{ and } d = \frac{pk}{2} + 1$$

For example, if we want to make system with 100 user and *l* = 7, *w* = 2, *r* = 3. In this case *K* value, i.e the length field will be the key with:

$$p = \frac{(7-1)^3}{7^{2+3-1}} = \frac{6^3}{7^4} \Rightarrow$$

$$k > \frac{8 \times 7^4}{6^3}\,(5log\, 100 - log\, 2 - log\, 6) \Rightarrow$$

$$k > 800$$

Mobile AD HOC networks that perform computation and memory size is very limited making meet such circumstances is very difficult. On the other hand, When the matrix size is large, can be calculated by repeated high avalues, which need large memory conditions that not compatible in mobile ad hoc networks.

We resolve these problems and proposed a method based on it using the ratio of non-linear codes linear codes with the same parameters and higher efficiency Is used for key distribution [4]. In this method first, a cyclic code with length *n*, makes on $Z_4 = \{0, 1, 2, 3\}$.

Then the code obtained by this code, with gray map converts a nonlinear 2*n* length binary code . Gray conversion is defined as follows:

$$\phi : Z_4{}^n \rightarrow Z_2{}^{2n}$$

$$\phi(c) = (\beta(c), \gamma(c) = (\beta(c), \alpha(c) + \beta(c))$$

c	$\alpha(c)$	$(\beta(c)$	$\gamma(c)$
0	0	0	0
1	1	1	1
2	2	2	2
3	3	3	3

Theorem 5

The cyclic code generated by $g\ (X)$, extended by an overall parity check, is a quaternary code C of length 2^m containing 4^{m+1} words. For m odd $m \geq 3$ the corresponding binary code $K = \phi\,(C)$ is the Kerdock code of length 2^{m+1} containing 4^{m+1} words and with minimal distance $d = 2^m - 2^{(m-1)/2}$ [4].

Code obtained in this way, all known linear codes of length and are the same size with distance is minimum Thus, for use in key distribution to more efficiency compare with MDS codes. Other advantages of this method top previous methods in that the generator matrix for the production of each node key chain and must be saved, is very easy is made. Generator matrix that is stored in each node is the following:

$$\begin{pmatrix} -\sum_{0}^{n-k} g_j & g_0 & g_1 & . & . & g_{n-k} & 0 & 0 & 0 & . & . & 0 \\ -\sum_{0}^{n-k} g_j & 0 & g_0 & . & . & . & g_{n-k} & 0 & 0 & 0 & . & 0 \\ . & & & & & & & & & & & . \\ . & & & & & & & & & & & . \\ . & & & & & & & & & & & . \\ -\sum_{0}^{n-k} g_j & 0 & . & . & . & 0 & g_0 & . & . & . & . & g_{n-k} \end{pmatrix}$$

For example, suppose polynomial generator of C (cyclic code on $Z_4 = \{0, 1, 2, 3\}$) has a length 7 as $g\ (x) = x^3 + 2x^2 + x + 1$, thus generator matrix as follow:

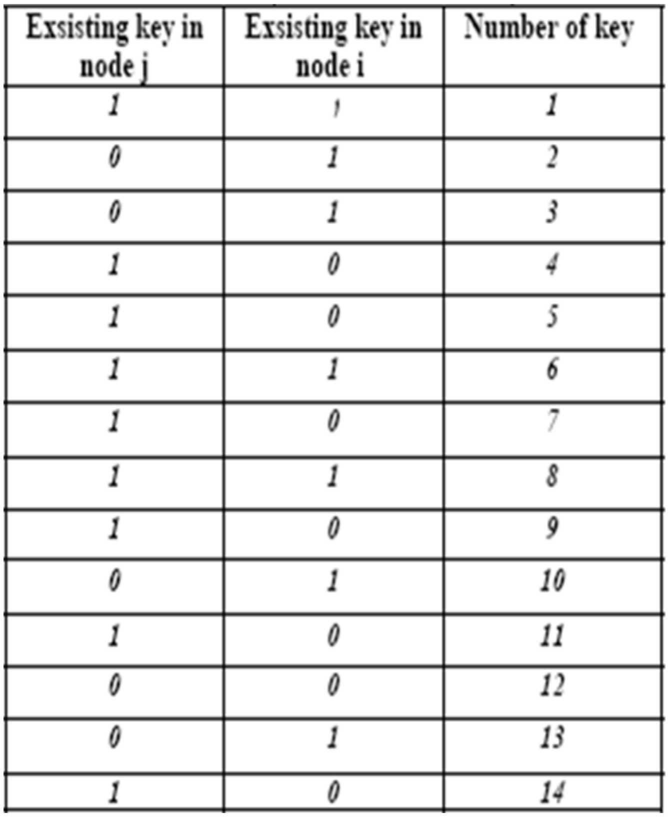
$$G = \begin{bmatrix} 1 & 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 0 & 3 & 1 & 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 3 & 1 & 2 & 1 & 0 \\ 1 & 0 & 0 & 0 & 3 & 1 & 2 & 1 \end{bmatrix}$$

hence, When a node wants to communicate with other nodes is simply a sequence of $\{g_0, g_1, ..., g_{n-k}\}$ numbers with n - k length sends For the other nodes. Each node after received this sequence makes generator matrix in a short time. When a node did the process for generating the key using reliable method such as SSD, sends key chain to other nodes and nodes check it to find common keys. Assuming that the key chain of a node to adjacent node has received the following form is: 0 1 0 0 1 0 1 0 1 0 0 1 1 1 and the keychain for this node is: 1 0 0 1 0 1 1 1 1 1 1 0 0 1. These nodes with compare the position of bits, find common keys.

The table can be concluded that the two nodes in key index 1, 6 and 8 are common. In our scheme as described here, we test the CFF criteria with different malicious node (r = 3, 4, 5, 6) and satisfying CFF improved in our scheme compare with MDS codes method that can be seen in this graph about 15%.

6. Conclusion

Considering the increasing use of mobile ad hoc networks and key distribution problem in this Networks, some methods for this work is provided in practice that efficiency are not significant. in the proposed method for key distribution using nonlinear codes with improved minimum distance code used inthis algorithm, likely met criteria *CFF* has increased. Also, reducing the size calculation method to allow for utilizing this method in this type of mobile networks has increased. Furthermore, the method above to increase tolerance against adversary nodes Compared with the past approach.This paper we simulated $(2, r; d) - CFF\ (N, T)$ with MDS and nonlinear codes and concluded that, our approach have about 15% increases satisfying *CFF* criteria in distribution key between nodes in mobile ad hoc network. In the future work, we will consider use of nonlinear codes on larger space and analysis power consumption in mobile ad hoc networks.



Exsisting key in node j	Exsisting key in node i	Number of key
1	1	1
0	1	2
0	1	3
1	0	4
1	0	5
1	1	6
1	0	7
1	1	8
1	0	9
0	1	10
1	0	11
0	0	12
0	1	13
1	0	14

Table 1. Key chains of node *i* and *j*

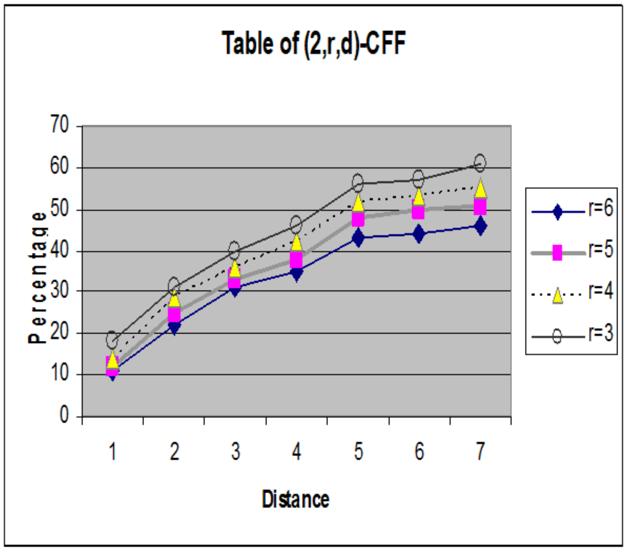


Figure 1. Percentage of (2, r, d) - CFF (N, T) with non linear codes Method

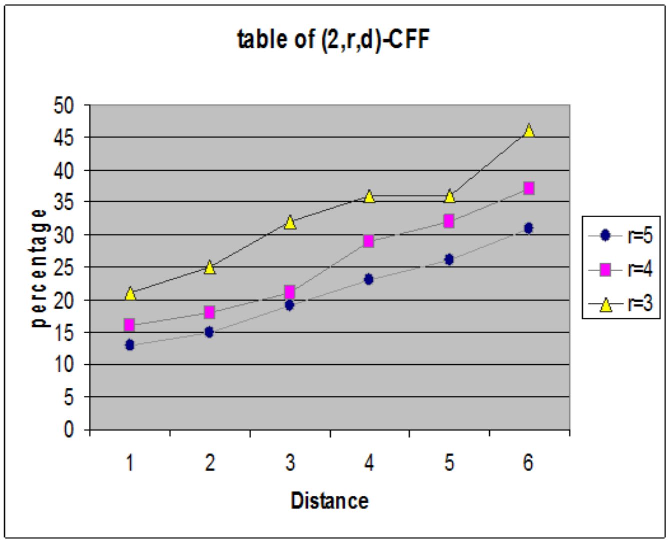


Figure 1. Percentage of (2, r, d) - CFF (N, T) with MDS codes Method

References

[1] Chan, A. C-F. (2004). Distributed Symmetric Key Management for Mobile Ad Hoc Networks, IEEE INFOCOM, 2004.

[2] Stinson, D. D., Wei, R. (2004). Generalized cover-free families, Discrete Math., p. 463-477.

[3] Al-Shurman, M., Yoo, S -M. (2006). Key Pre-Distribution Using MDS Codes in Mobile Ad Hoc Networks, IEEE Information Technology.

[4] Hammons, A. R., Jr. Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., Sol´e, p. (1994). The Z4-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40, 301–319.

[5] Wu, J., Wei, R. (2004). Comments on Distributed Symmetric Key Management for Mobile Ad hoc Networks from INFOCOM.

[6] Stinson, D. R., Wei, R., Zhu, L. (2000). Some New Bounds For Cover-Free Families, Journal of Combinatorial Theory Series A, 90 (1), p. 224-234, April.

[7] MacWilliams, F. J., Sloane, N. J. A. (1998). The Theory of Error-Correcting Codes, North-Holland, Amsterdam.

[8] Erdal Çayirci and Chunming Rong, Security in Wireless Ad Hoc and Sensor Networks, John Wiley & Sons. (2009).

[9] Ola Winberg. (2007). Survey of security solutions for mobile ad hoc networks, IEEE.

[10] Colbourn, C. J., Dukes, P. J., Syrotiuk, V. R. (2007). Generalized Cover-Free Families for Topology-Transparent Channel Assignment, Communications, Computers and Signal Processing, IEEE.

[11] Yang, H., Luo, H. Y., Ye, F., Lu, S W., Zhang, L. (2004). Security in Mobile Ad Hoc Networks: Challenges and Solutions, in IEEE Wireless Communications 11 (1).

[12] Ling, S., Wang, H., Xing, C. (2007). Cover-Free Families and Their Application, Security in Distributed and Networking Systems. World Scientific Press.

[13] Li Xu, J., Chen, X., Wang., (2008). Cover-Free Family based Efficient Group Key Management Strategy in Wireless Sensor Network, J*ournal of Communocations*, 3 (6), 2008

[14] Luo, H., Lu , S. (2004). URSA : Ubiquitous and Robust Access Control for Mobile Ad-Hoc Networks" IEEE/ACM Transactions On Networking, 12 (6), p.1049-1063.

[15] Chan, H., Perrig, A. (2005). PIKE, Peer Intermediaries for Key Establishment in Sensor Networks. *In*: Proceedings of IEEE INFOCOM, p. 524-535, March.

[16] Stinson, R., Wei, L., Zhu. (2000). Some New Bounds For Cover-Free Families, Journal of Combinatorial Theory Series A, vol 90, Issue 1, pp. 224-234, April.

[17] Pedoe, D. (1963). An introduction to Projective Geometry, Oxford.

[18] Shamir, A. How to Share a Secret . Communication of the ACM, 22 (11), p.612.