2013년 8월 전자공학회 논문지 제 50 권 제 8 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 8, August 2013 http://dx.doi.org/10.5573/ieek.2013.50. 8.103

논문 2013-50-8-13

익명성을 보장하는 클러스터 기반 이동 애드혹 네트워크에서의 클러스터 갱신 프로토콜

(Cluster Reconfiguration Protocol in Anonymous Cluster-Based MANETs)

박 요 한*, 박 영 호**

(YoHan Park and YoungHo Park©)

요 약

이동 애드혹 네트워크는 역동적인 구조를 가지는 단독적 네트워크로서 기반 시설을 필요로 하지 않는다. 애드혹 네트워크에서 사용자의 안전성을 제공하기 위해서는 기본적이면서도 다양한 보안 서비스가 제공되어야 한다. 특히 모바일 상업 시장을 고려할 때, 사용자의 프라이버시 보호는 중요하게 고려 되여야 할 보안 요구사항이다. 최근 클러스터 기반 이동 애드혹 네트워크 환경에서 익명성을 보장하는 보안 시스템이 연구되고 있다. 본 논문에서는 익명성을 보장하는 클러스터 기반 이동 애드혹 네트워크에서 네트워크의 안정성을 향상시키기 위한 클러스터 갱신 프로토콜을 제안한다. 제안하는 방식을 통해서 개선된 익명성을 보장하는 이동 애드혹 네트워크는 특정 클러스터 헤더의 비정상적인 상태에서도 네트워크 구조를 회복할 수 있다.

Abstract

Mobile ad hoc networks (MANETs) are infrastructure-less and stand-alone wireless networks with dynamic topologies. To support user's safety in MANETs, fundamental and various security services should be supported. Especially in mobile commercial market, one of the major concerns regarding security is user privacy. Recently, researches about security system to protect user privacy in cluster-based MANETs have been introduced. This paper propose a cluster reconfiguration protocol under anonymous cluster-based MANETs to enhance the network stability. The improved anonymous cluster-based MANETs can recover the network structure against abnormal states of clutserheads.

Keywords: cluster reconfiguration, improved cluster-based mobile ad hoc networks, ID-based cryptography, threshold scheme, pseudonym

Ⅰ. Introduction

Mobile ad hoc networks (MANETs) are considered as future technologies for generating instant communication networks for commercial and military applications. Properties of MANETs are infrastructure-less, autonomous, and stand-alone wireless networks with dynamic topologies. Also, MANETs are deployable quickly with self-organizing and self-maintaining capabilities. Because of the advantages of these features, MANETs refer to networks created for a special purpose. Recently, MANETs have been extended to cluster-based architectures to enhance the efficiency and security of

* 정회원, 싱가폴 국립대학교 컴퓨팅학부
(National Universtity of Singapore)
** 정회원, 경북대학교 산업전자공학과
(Kyungpook National University)
© Corresponding Author(E-mail: parkyh@knu.ac.kr)
※ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(NRF-2012R1A1A4A01002603)
접수일자: 2013년4월5일, 수정완료일: 2013년7월23일

MANETs[1-2].

However, MANETs are subject to various types of attacks because of the wireless and infrastructure-less environment. Moreover, it is difficult to apply conventional security mechanisms such as certificate-based cryptography (CBC) directly, because user's private keys and public keys are issued by a certification authority (CA). Even though it is feasible to support on-line public key infrastructure (PKI) services on MANETs, this limits their application areas when the dynamic property and the poor connectivity are considered. As an alternative to CBC, ID-based cryptography (IBC)[3] has been gaining interest. In IBC, a trusted private key generator (PKG) issues a pair of private key and public key corresponding to each user's identity before users join the networks.

Recently, Boneh and Franklin[4] suggested distributed PKGs (D-PKGs) using a threshold scheme to spread the role of the PKG. To apply D-PKGs to MANETs, the cluster-based structure have been researched. In cluster-based MANETs, the security issues are focused on the design of security systems which contain network architecture, privacy of users, key management, cluster configuration, and so on. The privacy problem in particular has received considerable attention with the growing importance of avoiding commercial and criminal abuse of personal information. This issue is very much a study in progress in VANETs and mesh networks where the trusted entity helps managing networks operations [5~6]. Also, these are cluster-based MANETs which consider user's privacy[7~8]. Especially, [7] proposed a novel security system with pseudonyms, called anonymous cluster-based MANETs. However, it does not mention about dynamic topologies considering emergency situations which are caused by malfunctions of nodes. This feature could put users in danger of privacy and security.

This paper proposes cluster reconfiguration protocol about broken clusters for some malfunctions of clusterheads. We consider and provide the privacy of users within broken clusters by reconfiguring an each cluster. Therefore, users in improved anonymous cluster-based MANETs can be supported privacy protection against cluster-broken situations. And improved anonymous cluster-based MANETs can be applied to fluctuating situations.

The rest of the paper is organized as follows. In Section Ⅱ, we survey the related works. Next we introduce an improved anonymous cluster-based MANETs in Section Ⅲ. Then we propose a cluster reconfiguration protocol in Section Ⅳ. Finally, we analyze the correctness of our proposal in Section Ⅴ and conclude our findings in Section Ⅵ.

Ⅱ. Preliminaries

In this section, we present the cryptographic system and notations used as building blocks.

1. ID-Based Cryptosystem

Recently IBC has its rapid development taken place due to the application of the pairing technique outlined below.

Let p,q be the large primes and E/F_p indicate an elliptic curve $y^2 = x^3 + ax + b$ over the finite field F_p. We denote by G_1 a q-order subgroup of the multiplicative group of the finite field $F_{p^2}^*$. The discrete logarithm problem (DLP) is required to be hard in both G_1 and G_2. For us, a pairing a map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ with the following properties:

- *Bilinear*:

  $\forall P,Q,R,S \in G_1$,

  $\hat{e}(P+Q,R+S) = \hat{e}(P,R)\hat{e}(P,S)\hat{e}(Q,R)\hat{e}(Q,S)$.

  Consequently, for $\forall a,b \in Z_q^*$, we have

  $\hat{e}(aP,bQ) = \hat{e}(aP,Q)^b = \hat{e}(P,bQ)^a = \hat{e}(P,Q)^{ab}$

  etc.

- *Non-degenerate*: If P is a generator of G_1, then $\hat{e}(P,P) \in F_{q^2}^*$ is a generator of G_2.
- *Computable*: There is an efficient algorithm to compute $\hat{e}(P,Q)$ for all $P,Q \in G_1$.

Note that $\hat{e}$ is also *symmetric*, i. e., $\hat{e}(P,Q) = \hat{e}(Q,P)$, for all $P,Q \in G_1$, which follows immediately from the bilinearity and the fact that G_1 is a cyclic group. Modified Weil[4] and Tate[9] pairing are examples of such bilinear maps for which the *bilinear diffie-hellman problem (BDHP)* is believed to be hard.

2. Threshold Scheme

Secret sharing schemes were independently introduced by the Blakley[10] and the Shamir[11] in 1979. They introduced a way to split a secret K into n shares. And only t or more than t shares among n can reconstruct a secret K. It is called (t,n)-secret sharing, denoted as (t,n)-SS.

Shamir's (t,n)-SS. Shamir's (t,n)-SS is based on polynomial interpolation. The scheme consists of two algorithms:

1) **Secret Sharing Generation** : A trusted party T distributes shares of a secret K to n users as follow:

- T chooses a prime $p > \max(K,n)$, and defines $a_0 = K$.
- T picks a polynomial $f(x)$ of degree $(t-1)$ randomly: $f(x) = a_0 + a_1 x + \cdots a_{t-1} x^{t-1}$, in which the secret $K = a_0 = f(0)$ and all coefficients $(a_0,\ldots,a_{t-1})$ are in a finite field $F_p = GF(p)$ with p elements.
- T computes $K_i = f(s_i) \pmod p$ for i=1,...,n. and securely transfer the shares K_i to each user.

2) **Secret Reconstruction** : Any group of size t or more than t can reconstruct the polynomial $f(x)$ as

$$f(x) = \Sigma_{i \in A} \lambda_i(x) K_i \pmod q,$$

where $A = \{1,\ldots,t\} \subseteq \{1,\ldots,n\}$, $\lambda_i(x) = \Pi_{j \in A \setminus i} \frac{s_j - x}{s_j - s_i}$ is called a Lagrange coefficient. The secret is recovered by $f(0) = K$.

For more information on this scheme, readers can refer to the original paper[11].

3. Notations

Table 1 lists some important notations whose concrete meanings will be further explained.

표 1. 기호들
Table 1. Notations.

G_1, G_2	cyclic groups of order q
$\hat{e}$	pairing s. t. $\hat{e}: G_1 \times G_1 \rightarrow G_2$
P	generator of G_1
CH_j / ID_A	network ID of clusterhead j and common node A
PS_A	pseudonym of ID_A
S_j / Q_j	private/public key pair of clustehead j
S_A / Q_A	private/public key pair of common node A
S_{PS_A} / Q_{PS_A}	private/public key pair of pseudonym PS_A
U	maximum update phase index
K_m	cluster key at m-th update phase
$g_m(x)$	polynomial for cluster key K_m
$f_m^{CH_j}(x)$	polynomial of CH_j
(t,n)	secret sharing parameters for $g_m(x)$
(t_1,n_1)	secret sharing parameters for $f_m^{CH_j}(x)$
S_G	group secret key
H_0	mapping $(0,1)^* \rightarrow Z_p^*$
H_1	mapping $(0,1)^* \rightarrow G_1$
H_2	mapping $Z_p^* \rightarrow (0,1)^*$
H_3	mapping $G_1 \rightarrow Z_p^*$

Ⅲ. Improved Anonymous Cluster-Based MANETs

In this section, we review the anonymous cluster-

based MANETs[7]. The anonymous cluster-based MANETs are constructed on three steps, system setup, cluster setup, and pseudonym generation. In this paper, we review the basic network architecture and the generation process of private/public key pairs. And we supplement the generation process of secret sharings for CHs using the respective polynomial to enhance network stability.

1. Network Architecture

The anonymous cluster-based MANETs are composed of several clusters. Each cluster has a clusterhead (CH) and common nodes. Figure 1 illustrates the network architecture for cluster setup and pseudonym generation.

CHs firstly share their secret sharings and reconstruct a same cluster key K_m. Then using a cluster key K_m, each CH generates it's polynomial, called respective polynomial. Finally, they generate pseudonyms for common nodes using their respective polynomials. Common nodes receive private/public key pairs of pseudonyms and can establish secure channel with other common nodes or a their CH using these pseudonym key pairs.

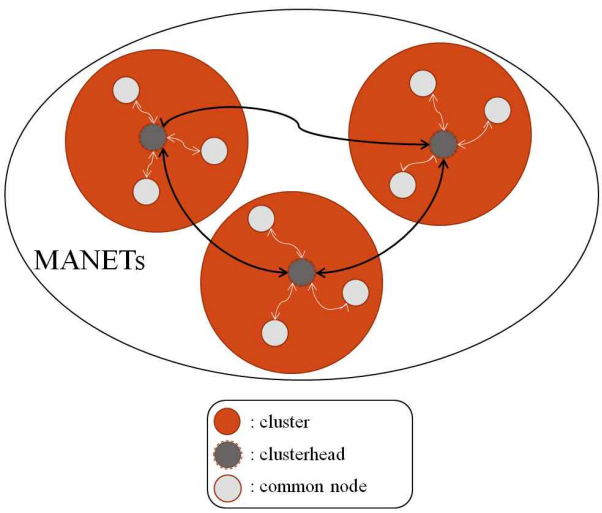

그림 1. 익명성을 제공하는 클러스터 기반 이동 애드혹 네트워크의 기본 구조

Fig. 1. The Basic Architecture of Anonymous Cluster-Based MANETs.

2. Generation of Pseudonym Key Pairs

CHs generate pseudonym private/public key pairs for nodes which are in their cluster. Before pseudonym generation, CHs have a same cluster key K_m by reconstructing polynomial $g_m(x)$. Then each CH generates a respective polynomial $f_m^{CH_j}(x)$. These respective polynomials have same secret, that is, $f_m^{CH_j}(0) = K_m$. A CH generates common nodes' pseudonyms which are within a cluster using common nodes' identities. For example, the pseudonym of ID_A within the cluster CH_j is $PS_A = f_m^{CH_j}(id_A)$. And the public and private key pair is $Q_{PS_A} = PS_A K_m P$ and $S_{PS_A} = PS_A$.

CHs generate pseudonyms and record identities and corresponding pseudonyms at pseudonym lookup table (PLT), then forward pseudonym key pairs to corresponding nodes using a secure channel established by initial private/public key pairs. For more information on anonymous cluster-based MANETs, readers can refers to the original paper[7].

3. Generation of Secret Sharings for CHs

A CH which generates it's respective polynomial computes secret sharings for other CHs. These secret sharings are used to reconfigure clusters against cluster-broken situations. The secret sharings for other CHs are made by their identity. For example, a secret sharing of the clusterhead k is $f_m^{CH_j}(ch_k)$. In this way, the CH_j generates and distributes secret sharings to other CHs.

Ⅳ. Cluster Reconfiguration Protocol

The structure of the networks and the clusters is easy to be changed because of the characteristic of wireless and dynamic environment. Therefore, the system should consider the changing of network structure and reconfigure the cluster depending on the network structure. The joining and eviction of a

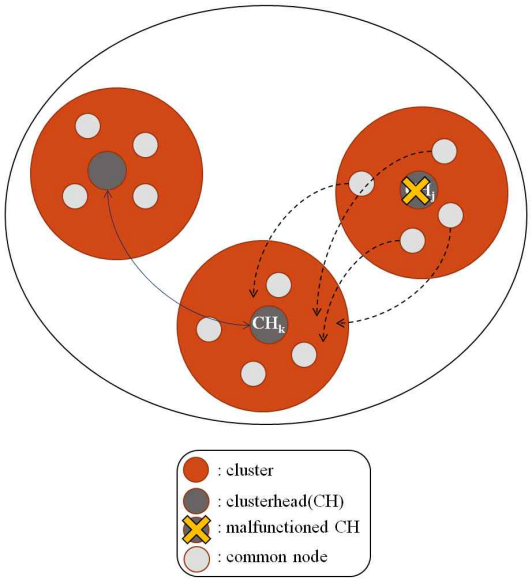

그림 2. 클러스터 재구성 시나리오
Fig. 2. Cluster Reconfiguration Scenario.

CH/node in [7] is very efficient because of the property of the secret sharing scheme. However, they did not consider the change of networks due to the unpredictable elimination of a CH. In this section, we propose a cluster reconfiguration protocol to enhance network stability against abnormal actions of CHs. Figure 2 illustrates the process of cluster reconfiguration.

If a CH is broken (the yellowed 'X' mark) due to some malfunctions or attacks, the remaining nodes in the broken cluster are in need of help to continue communicating. In this case, other CHs who have received secret sharings generated by a broken cluster can check the validity of the remaining nodes by collaborating their secret sharings. Cluster reconfiguration protocol is performed as follows;

① Malfunction of a CH_j

If a CH_j is broken at the m-th update phase, remaining t_r common nodes in the broken cluster move to the nearest cluster, CH_k, and request security services.

② Validity check for moved t_r common nodes

To check the validity of those remaining t_r nodes, CH_k who has already received a secret sharing $f_m^{CH_j}(CH_k)$ from CH_j asks remaining t_r nodes for initial identities and pseudonyms. With the help of other $(t_1 - t_r - 1)$ CHs who have received a secret sharing from CH_j, CH_k can reconstruct $f_m^{CH_j}(x)$ and verify the validity of the remaining nodes by computing $f_m^{CH_j}(0) = K_m$.

③ Security services for moved t_r common nodes

The CH_k provides security services to t_r nodes, and all CHs change the update phase into $(m+1)$ by pooling each secret sharing $g_{m+1}(CH_j)$

V. Correctness

The security analysis were already introduced in [7]. Thus in this section, we presents the correctness of cluster reconfiguration.

Note the fact that $f_m^{CH_j}(x) = K_m + \sum_{i=0}^{t_1-1} b_i x^i$. And pseudonyms for common nodes within CH_j and secret sharings generated by CH_j for other CHs are made of an identical polynomial. That is, the pseudonym of a common node A within cluster CH_j is $PS_A = f_m^{CH_j}(id_A)$, and the secret sharing of a clusterhead k is $f_m^{CH_j}(ch_k)$. These values have been already distributed by a CH_j before it malfunction. To check the validity of remaining t_r common nodes, the CH_k requests secret sharings for other $(t_1 - t_r - 1)$ CHs which have secret sharings generated by CH_j. And to conclude, CH_k can recover the respective polynomial of CH_j and check the secret K_m because it has at least t_1 secret sharings generated by respective polynomial $f_m^{CH_j}(x)$.

VI. Conclusions

Cluster-based MANETs are being seriously

considered to pioneer new markets; however, there are urgent unresolved security problems. Fundamental aspects of security and the protection of personal privacy are challenging in cluster-based MANETs for the wireless networks have become personal and popular. Furthermore, these cluster-based MANETs should have strong stability against cluster changes and recover the network architecture.

This paper presented a cluster reconfiguration protocol based on the anonymous cluster-based MANETs. The users in a broken cluster can be supported security services from the nearest CH by adopting our cluster reconfiguration protocol. The improved anonymous cluster-based MANETs successfully copes with dynamic environments with stability and efficiency. It could be usefully applied to preserve privacy in dynamic MANETs without a trusted entity, such as military battlefields, emergency areas, mobile marketplaces, and privacy-preserving VANETs.

REFERENCES

[1] R. Dutta and T. Dowling, "Provably secure hybrid key agreement protocols in cluster-based wireless ad hoc networks," Ad Hoc Networks, vol.9, pp.767-787, 2011.
[2] L.-C. Li and R.-S. Liu, "Securing cluster-based ad hoc networks with distributed authorities," IEEE Transactions on Wireless Communications, vol.9, no.10, pp.3072-3081, 2010.
[3] A. Shamir, "Identity-based cryptosystems and signature schemes," CRYPTO 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.
[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," CRYPTO 01, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
[5] C-T. Li, M-S. Hwang, and Y-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," Computer Communications, vol.31, no.12, pp.2803-2814, 2008.
[6] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An Identity-based security system for user privacy in vehicular ad hoc networks," IEEE Transactions on Parallel and Distributed Systems, vol.21, no.9, pp.1227-1239, 2010.
[7] Y. H. Park, Y. H. Park, and S. J. Moon, "Anonymous cluster-based MANETs with threshold signature," International Journal of Distributed Sensor Networks, vol.2013, 2013.
[8] Y. H. Park, Y. H. Park, and S. J. Moon, "Secure ID-based key agreement protocol with anonymity for mobile ad hoc networks," Journal of IEEK, vol.49, no.1, 2012.
[9] P. Barreto, H. Kim, B. Bynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," CRYPTO 02. LNCS 2442, pp.354-369, Springer, Heidelberg, 2002.
[10] G. R. Blakley, "Safeguarding cryptographic keys," AFIPS 79. vol.48, pp.313-317, 1979.
[11] A. Shamir, "How to share a secret," Comm. ACM, vol.22, no.11, pp.612-613, 1979.

저 자 소 개

박 요 한(정회원)

2006년 경북대학교 전자전기 컴퓨터학부 학사
2008년 경북대학교 전자공학과 석사
2013년 경북대학교 전자공학과 박사
2013년 ~현재 싱가폴 국립대학교 컴퓨팅학부 Post Doctor

<주관심분야 : 무선통신, 네트워크 보안, 모바일 컴퓨팅>

박 영 호(정회원)-교신저자

1989년 경북대학교 전자공학과 학사
1991년 경북대학교 전자공학과 석사
1995년 경북대학교 전자공학과 박사
1996년~2008년 상주대학교 전자전기공학부 교수
2003년~2004년 Oregon State Univ. 방문교수
2008년~현재 경북대학교 산업전자공학과 교수

<주관심분야 : 정보보호, 네트워크보안, 모바일 컴퓨팅>