ICIC Express Letters
Part B: Applications
Volume **7**, Number **6**, June **2016**

ICIC International ©2016 ISSN 2185-2766
pp. 1329–1334

CLUSTER BASED HYBRID KEY MANAGEMENT SCHEME FOR AD HOC NETWORKS

Jing Zhang[1,2], Li Xu[3], Rongmei Tang[1] and Shunmiao Zhang[1]

[1]School of Information Science and Engineering
[2]Fujian Provincial Key Laboratory of Big Data Mining and Applications
Fujian University of Technology
No. 3, Xueyuan Road, University Town, Minhou, Fuzhou 350118, P. R. China
jing165455@126.com

[3]School of Mathematics and Computer Science
Fujian Normal University
Fuzhou University Town, Minhou, Fuzhou 350118, P. R. China

Received November 2015; accepted February 2016

Abstract. *Secure communication is part of the most important aspects for ad hoc networks. One cluster based Hybrid Key Management Scheme is proposed in this paper for ad hoc networks. The clusters are constructed by the R-hop connected dominating sets based Partition Algorithm, which is only with the knowledge of local connectivity information. Furthermore, Hybrid Key Management Scheme can be seen as an integration of both the asymmetric key and symmetric key cryptography. The asymmetric one is based on the elliptic curve cryptosystem, which is an asymmetric one. However, inter cluster key management is based on symmetric key encryption. Experimental results show this scheme is reliable and it is able to achieve higher success of landing ratio than other comparable algorithms.*

Keywords: Ad hoc network, Key management, Clustering, Secret sharing, Elliptic curve

1. **Introduction.** Wireless ad hoc networks are a typical distributed network. Since the cost to set up an ad hoc network is low, it is a very attractive option for wide applications in different areas. However, ad hoc networks are subject to various kinds of attacks. Wireless communication links can be eavesdropped on without noticeable effort and communication protocols on all layers are vulnerable to specific attacks. Furthermore, in a wireless ad hoc network, there exists no fixed infrastructure such as switching centers or base stations. Nodes that are within the communication range of each other can communicate directly whereas. The node that is far apart has to rely on an intermediary node to relay messages. Traditional key management scheme is not suitable for wireless ad hoc networks because of their limited energy and processing capability. Therefore, it is essential to find a safe, efficient key management scheme for such resources limited and security requirements.

Several more advanced key management schemes have been proposed in order to improve the security level and the efficiency of wireless ad hoc networks [7, 10]. There are many key establishment protocols in the literature based on symmetric key cryptography for wireless ad hoc networks [1]. Such type of encryption is well-suited for resources limited nodes. However, it is affected by high communication overhead and requires large memory space to store shared pairwise keys.

More recently, asymmetric key based approaches have been proposed for wireless ad hoc networks [2, 4, 5, 9, 10]. These approaches make use of public key cryptography (PKC) such as elliptic curve cryptography. PKC is more expensive than symmetric key encryption with respect to computational costs. However, a central issue concerning the design of any service in ad hoc networks is not to rely on any centralized entities, because such entities would obviously be easy to attack, and their reach ability would not be guaranteed at all times for all participants of the network. Therefore, it is not feasible to implement a centralized, trusted entity for managing public keys of the participants as performed in local area networks.

In 1979, the concept of secret sharing was put forward by Shamir [11] and Blakley [3] independently. Huang [8] developed a (t, n) threshold secret sharing scheme which is based on the cylinder model, including procedures of master-key reconfiguration and sub-key updating. Guo and Chang [6] proposed a novel secret sharing scheme with general access structures that are based on the key-lock-pair mechanism. In this paper, we introduce a secure and efficient key management in ad hoc networks. The new scheme is a hybrid approach that can be seen as an integration of both the asymmetric key and symmetric key cryptography.

The rest of this paper is organized as follows. Problem statement and preliminaries are given in Section 2. Section 3 presents the key management protocol. Section 4 gives an analysis of what proposed, and Section 5 summarizes the results.

2. Problem Statement and Preliminaries.

Sensor nodes are randomly distributed in the network field and have the same transmission range. The link between any pair of nodes is bidirectional. One network is modeled as a connected bidirectional graph $G = (V, E)$, where V and E represent the node set and the link set in G, respectively. $\forall u, v \in V$, there exists an edge (u, v) in G if and only if u is in v's transmission range in the network, v is also in u's transmission range, and there is no obstacle preventing radio wave transmission between u and v.

Definition 2.1. *(Node neighborhoods)* [12] *Consider a node u. The set of nodes covered by u is represented by $N(u)$, $N(u) = \{v \mid (v, u) \in E\}$ is called the open neighbor set of u. $N[u] = N(u) \cup \{u\}$ is called the closed neighbor set of u.*

Nodes using exchange of hello messages can find its 1-hop neighbour nodes and ascertain its degree. $N_2(u)$ denotes the set of nodes which are at most at 2-hop from u. The 2-hop neighbours of u are represented as $N_2(u) - N(u)$.

Definition 2.2. *(Maximal Independent Set (MIS))* [12] *A Maximal Independent Set of a graph $G = (V, E)$ is a subset $V' \subseteq V(G)$ such that every pair of vertices in V' is not adjacent, and no independent vertex can be added into V'.*

Definition 2.3. *(Connected Dominating Set (CDS))* [12] *A Dominating Set of a graph $G = (V, E)$ is a set of nodes $V' \subseteq V(G)$ such that for every $(u, v) \in E(G)$, $u \in V'$ or $v \in V'$. A Connected Dominating Set of a graph $G = (V, E)$ is a DS of G such that the subgraph of G induced by the nodes in this set is connected.*

In many cases, an MIS construction algorithm is used to find a DS. The nodes in CDS are called the dominators and otherwise the dominatees. The size of CDS is equal to the number of the dominators.

3. Hybrid Key Management Scheme for Ad Hoc Network.

This section introduces the Hybrid Key Management Scheme (HKMS) for ad hoc network. There are 3 phases for HKMS.

Phase 1: R-hop connected dominating sets based Partition Algorithm (RPA).
Phase 2: Intra Clusters key management.
Phase 3: Inter Clusters key management.

3.1. **R-hop connected dominating sets based Partition Algorithm (RPA).** In this section, we introduce an algorithm for finding R-hop connected domatic partitions (R-CDP). There are three steps: (1) construct an R-hop Maximum Independent Set (R-MIS) of a graph $G = (V, E)$; (2) decompose the network into R-hop cluster partition; (3) connect all cluster-heads so that the subgraph induced by cluster-heads is connected.

(1) The first step: R-hop Maximum Independent Sets (R-MIS).

In this step, an algorithm for constructing R-MIS of a graph $G = (V, E)$ will be introduced. We suppose that each node v has a unique ID $id(v)$. In order to establish R-hop knowledge of the neighborhood in the first phase, each node v should periodically broadcast its neighborhood with HELLO messages, which includes its $id(v)$, such that each node knows its neighborhoods. After R rounds neighborhood information exchanging, every node knows its R-hop neighborhoods.

Later, initially each node is colored *white*. Then, we choose a maximum reliability value node and color it *black*, and color its $N_r(max\_id)$ into *grey*. Repeat this process until no white nodes any more. After the first step, all nodes in the R-MIS are colored *black*, and the others are colored *grey*.

(2) The second step: Cluster Partitioning.

When the R-hop Maximum Independent Set is built, we have a dominating set I. The nodes in I are chosen as cluster heads. Then we have to establish the cluster partitioning CP_r of G. Each cluster head broadcasts message m_1 which contained its id to its cluster members with the R times of perceived radius, which is the R hops transmission radius. If a node receives m_1 from its cluster head, it decides whether becoming a member of the cluster head. The following two criteria decide the membership of a vertex v. Criterion 1. A vertex $v \in V - I$ is affiliated to a cluster, where all cluster members are dominated by u only, if v is dominated only by u; Criterion 2. If a vertex v is adjacent to multiple vertices of I, then v is affiliated to the closest vertex $u \in I$. Furthermore, the cluster head can decide who can hold the sub-keys. They choose the nodes, which have the higher reliability value.

(3) The third step: R-hop Connected Dominating Sets (R-CDS).

In R-CDS, each cluster head administrates a '*routing table*' T, which includes the path towards to the other nodes in the R-MIS. In the beginning, each cluster head broadcasts message toward those nodes R hops away, which includes its id and the path it has traveled. After each cluster head exchanges each other's routing table, a path can be found to connect all cluster heads. Note that there are some gateway nodes and dominating

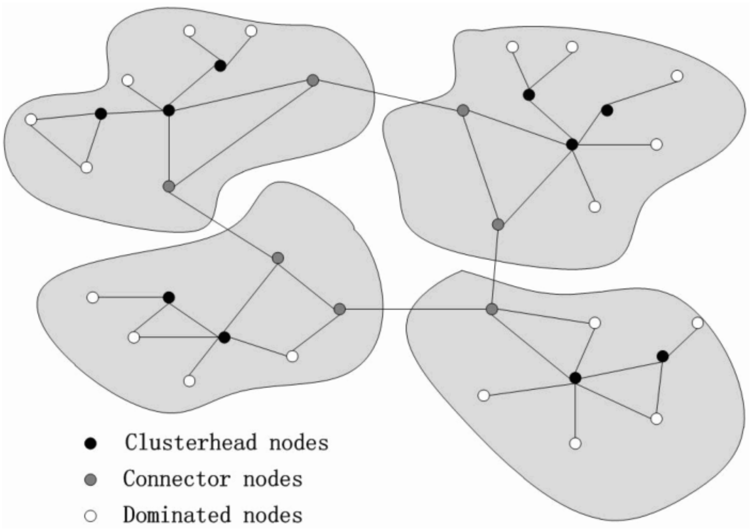

Figure 1. An example of CDS-based clusters

nodes in R-MIS on the path. The other nodes in the graph are dominatees. An example for CDS is illustrated in Figure 1.

3.2. **Intra clusters key management.** In a wireless ad hoc network environment, more communications will bring longer time and lower success rate to the generation of new shares, and more difficult to the key management. This paper uses a new secret share generation protocol in each cluster. At first, each cluster-head chooses a secret elliptic curve $E_q(a, b)$, which is

$$y^2 = x^3 + ax + b, \quad q > 3 \tag{1}$$

where $a, b \in GF(q)$, and $4a^3 - 27b^2 \neq 0$. G is a basic point, whose order is a big prime number n, where $n \geq 160$ bit.

The cluster-head chooses n parameters from an elliptic curve $E_q(a, b)$, denoted as k_i, $i \in \{1, 2, \ldots, n\}$, which are the secret sub-key. Those keys are forwarded to the cluster-members CM_i safely. The cluster-head calculates $G' = k_iG$, and publicly parameters $(E, G, n, H(x), G')$.

Step 1: Key distribution.

1. The cluster-head chooses one point Q from an elliptic curve $E_q(a, b)$ randomly, and one $t - 1$ polynomial $f(x)$, where t for the threshold:

$$f(x) = a_0 + \sum_{i=1}^{t-1} a_i x^i (\text{mod } n) \tag{2}$$

2. The cluster-head chooses n different parameters $x_1, x_2, \ldots, x_n$, calculates $f(x_i) = y_i$, $A_l = a_lG(mod\ n)$, $1 \leq l \leq t - 1$ and $D_i = (x_i, f(x_i)) - k_iQ$, and then publishes A_i and D_i.

3. The cluster-head calculates and publishes $F_i = H(K_iQ)$, which is used for verifying the key for each cluster.

Step 2: Master key refractory based on polynomial interpolation method.

1. Each cluster member receives l, $l > t$ secret sub-keys for master key refractory.

2. There is an equation set

$$\begin{bmatrix} 1 & x_{i_1} & x_{i_1}^2 & \ldots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \ldots & x_{i_2}^{t-1} \\ 1 & x_{i_3} & x_{i_3}^2 & \ldots & x_{i_3}^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_l} & x_{i_l}^2 & \ldots & x_{i_1}^{t-1} \end{bmatrix} \begin{bmatrix} s \\ a_1 \\ a_2 \\ \vdots \\ a_{l-1} \end{bmatrix} = \begin{bmatrix} y_{i_1} \\ y_{i_2} \\ y_{i_3} \\ \vdots \\ y_{i_l} \end{bmatrix}$$

where $y_{i_j} = f\left(x_{i_j}\right)$, $1 \leq j \leq l$.

3. Each secret sub-key is (x_i, y_i), and the participators calculate:

$$\begin{aligned} h(x) = & \ y_1 \frac{(x - x_2)(x - x_3) \ldots (x - x_t)}{(x_1 - x_2)(x_1 - x_3) \ldots (x_1 - x_t)} + y_2 \frac{(x - x_1)(x - x_3) \ldots (x - x_t)}{(x_2 - x_1)(x_2 - x_3) \ldots (x_2 - x_t)} + \ldots \\ & + y_l \frac{(x - x_1)(x - x_2) \ldots (x - x_{t-1})}{(x_t - x_1)(x_t - x_2) \ldots (x_t - x_{t-1})}. \end{aligned} \tag{3}$$

According to the properties of polynomials over a finite field, since $h(x)$ is a variable polynomial of degree $t - 1$, the master key can be recovered conditional on t different points and $h(0) = f(0) = S$ are known.

3.3. **Inter cluster key management.** Inter cluster key management is service offered by one sink node to the cluster heads, which is based on symmetric key encryption, the key in consultation between each cluster head and the sink.

4. **Numerical Example.** In order to measure the performance of key management under clustering environment, the successful landing ratio is adopted as a performance index. The successful landing ratio is the ratio of number of nodes successful landing and total number of nodes applying for adding. Success of landing node is defined as a node, which requests to join into a cluster and becomes a full member success. Such nodes need t secret sub-keys, and calculated master key. Nodes, whose reliability value are greater than the threshold value, have the right to send secret sub-keys. Discuss in three different conditions:

1. HKMS: The cluster-members' credibility is greater than the reliability value threshold;

2. Min ID cluster-head: not all the cluster-members' credibility is greater than the reliability value threshold;

3. No CH: Each node has to send a request to all neighborhood nodes. However, a large number of malicious nodes will not forward the request under this condition.

The number of threshold secret sharing, can be dynamically adjusted according to the requirements. The following analysis is for a successful landing ratio with the increasing of the number of threshold secret sharing. Set the transmission range of each node as $r = 40$ and $r = 50$; the number of threshold secret sharing is increased from 5 to 50. The simulation results are simulated averaged 10 groups of 20 times. It is easy to see that in Figure 2 when the transmission radius is $r = 40$, with the increasing of the number of

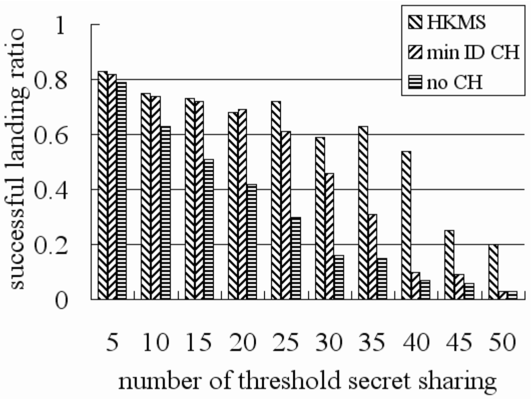

Figure 2. The successful landing ratio of the number of changes required for certification when $r = 40$

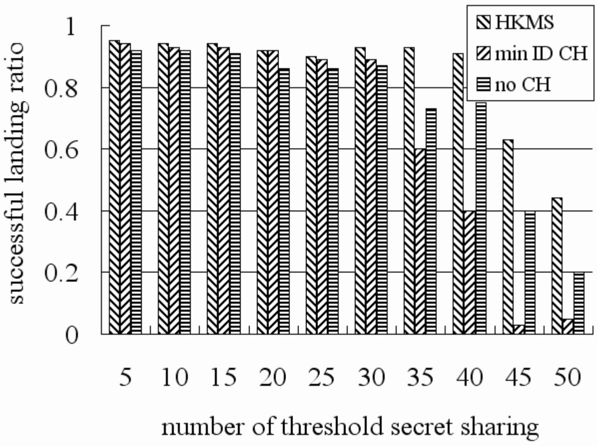

Figure 3. The successful landing ratio of the number of changes required for certification when $r = 50$

threshold secret sharing, the success of landing ratio by HKMS is greater than the other two cases significantly.

Figure 3 shows that when the transmission radius is $r = 50$, also the success of landing ratio by HKMS is greater than the other two cases significantly.

5. Conclusions.

Wireless ad hoc networks have been deployed in a wide variety of applications. Secure communication is part of the most important aspects. This paper introduces a cluster-based architecture for a distributed public key infrastructure that is highly adapted to the characteristics of ad hoc networks. An R-hop connected dominating sets based Partition Algorithm is proposed to construct the R-CDP with the knowledge of local connectivity information only. In order to adapt to the highly dynamic topology and varying link qualities in ad hoc networks, a novel Hybrid Key Management Scheme (HKMS) which is a cluster based is proposed for ad hoc networks. HKMS can be seen as an integration of both the asymmetric key and symmetric key cryptography. The asymmetric one is based on the elliptic curve cryptosystem. Experimental results show this scheme is reliable and it is able to achieve higher success of landing ratio than other comparable algorithms.

For the future research direction, first, we will focus on key management when there are some new nodes joining the network; second, we will further explore key revocation method to manage the emergence of nodes leaving.

Acknowledgment. The authors wish to thank National Natural Science Foundation of China (No. 61072080, No. 61572010, No. U1405255), Fujian Normal University Innovative Research Team (No. IRTL1207), The Education Department of Fujian Province Science and Technology Project (JA15323, 2015H0009) and Natural Science Foundation of Fujian Province of China (No. 2012J01245).

REFERENCES

[1] A. H. Ahmed, M. Ali and O. B. Louis, Authenticated group key agreement protocols for ad hoc wireless networks, *International Journal of Network security*, vol.4, no.1, pp.90-98, 2007.

[2] M. R. Alagheband and M. R. Aref, Dynamic and secure key management model for hierarchical heterogeneous sensor networks, *IET Inf. Secur*, vol.6, no.4, pp.271-280, 2012.

[3] G. R. Blakley, Safeguarding cryptographic keys, *Proc. of AFIPS National Computer Conference*, AFIPS Press, New York, USA, 1979.

[4] K. Chatterjee, A. De and D. Gupta, An improved ID-based key management scheme in wireless sensor network, *Proc. of the 3rd Int. Conf. ICSI*, vol.7332, pp.351-359, 2012.

[5] S. H. Erfani, H. H. S. Javadi and A. M. Rahmani, Analysis of key management schemes in dynamic wireless sensor networks, *ACSIJ Advances in Computer Science: An International Journal*, vol.4, no.13, pp.117-121, 2015.

[6] C. Guo and C. Chang, A construction for secret sharing scheme with general access structure, *Journal of Information Hiding and Multimedia Signal Processing*, vol.4, no.1, pp.1-8, 2013.

[7] F. Gandino, B. Montrucchio and M. Rebaudengo, Key management for static wireless sensor networks with node adding, *IEEE Trans. Industrial Informatics*, vol.10, no.2, pp.1133-1143, 2014.

[8] H. Huang, (t, n) secret sharing scheme based on cylinder model in wireless sensor networks, *Journal of networks*, vol.7, no.7, pp.1009-1016, 2012.

[9] R. K. Kodali, Key management technique for WSNs, *IEEE Region 10 Symposium*, pp.540-545, 2014.

[10] S. H. Seo, J. Won, S. Sultana and E. Bertino, Effective key management in dynamic wireless sensor networks, *IEEE Trans. Information Forensics and Security*, vol.10, no.2, pp.371-383, 2015.

[11] A. Shamir, How to share a secret, *Communications of the ACM*, vol.22, no.11, pp.612-613, 1979.

[12] J. Zhang, L. Xu and H. Lin, A CDS-based network coding scheme in wireless sensor converge-cast networks, *Proc. of IEEE 17th International Conference on Computational Science and Engineering*, pp.1599-1604, 2014.