Certificate Dispersal Problems
Open Problem Session in IWOCA 2007

Koichi Wada
Nagoya Institute of Technology
Gokiso-cho, Syowa-ku, Nagoya 466-8555, JAPAN
wada@nitech.ac.jp

May 9, 2008

We consider a mobile network, where each node u has a private key $pri.u$ and a public key $pub.u$. Users themselves create their public and private keys. In this network, in order for a node u to send a message m to a node v securely, u needs to know $pub.v$ to encrypt the message with it, denoted by $pub.v < m >$. If a node u knows the public key $pub.v$ of another node v in the network, then the node u can issue a certificate from u to v that identifies $pub.v$. A certificate from a node u to a node v is of the following form: $pri.u < u, v, pub.v >$. The certificate is encrypted by using $pri.u$ and it contains three items: (i) the identity of the certificate issuer u, (ii) the identity of the certificate subject v, and (iii) the public key of the certificate subject $pub.v$.

Any node who knows $pub.u$ can use it to decrypt the certificate from u to v for obtaining $pub.v$. When a node u wants to obtain the public key of another node v, u acquires a sequence of certificates $pri.u < u, v_0, pub.v_0 >, pri.v_0 < v_0, v_1, pub.v_1 >, \ldots pri.v_\ell, v_\ell, v, pub.v >$ which are stored in either u or v.

All certificates issued by nodes in a network can be represented by a directed graph, called *a certificate graph*, denoted by $G = (V, E)$. We define a *dispersal* D of a directed graph $G = (V, E)$ as a family of sets of edges indexed by V, where $D = \{D_v \subseteq E | v \in V\}$. We define a request for a certificate graph G as a reachable ordered pair of nodes in G, denoted by (u, v). A set of requests, denoted by R, is called *full* if all reachable pairs of nodes in G are contained in R. We call a dispersal D of a directed graph $G = (V, E)$ *satisfies* a set of requests R, if for any request (u, v) in R, there exists a path from u to v in $D_u \cup D_v$, where D_u and D_v are dispersal of u and v. Let D be a dispersal of G satisfying R. The *cost* of dispersal D, denoted by $c.D$, is the sum of cardinalities of each dispersal in D. A dispersal D of G satisfying R is optimal if and only if for any other dispersal D' satisfies R, $c.D \leq c.D'$.

MINIMUM CERTIFICATE DISPERSAL PROBLEM(MCD) is defined as follows:

INPUT: A directed graph $G = (V, E)$ and a set of requests R

OUTPUT: A dispersal D of G satisfying R with the minimum cost.

It has been shown that MCD is NP-complete, even if the input graph is restricted to a strongly connected one. Also a polynomial-time 2-approximation algorithm can be constructed for strongly connected graphs. Moreover, it can be shown that this algorithm outputs optimal dispersals for complete graphs, trees, rings and Cartesian product of graphs.

In general, MCD is NP-complete for strongly connected graphs. A remaining question is whether MCD remains NP-complete for bidirectional graphs(or undirected graphs) and/or full requests or not.

Can the approximation ratio of MCD algorithms can be improved? That is, can a polynomial-time α-approximation algorithm such that $\alpha < 2$ be constructed for any directed graph?

The 2-approximation algorithm shown in [**?**] becomes optimal one for complete graphs, trees, rings hypercubes(more generally, Cartesian product of graphs). For some useful graph classes, such as chordal graphs or interval graphs, can we construct an optimal MCD algorithm?

References

[1] H. Zheng, S. Omura, K. Wada: A 2-approximation algorithm for minimum certificate dispersal problems, Proceedings of the 16th Australasian Workshop on Combinational Algorithms, 384-394 (2005).