On the Algorithms Related to Threshold Cryptography Based Network Protocols

Qi Duan and Mohit Virendra

(Corresponding author: Qi Duan)

Department of Computer Science and Engineering
State University of New York at Buffalo, Buffalo, NY 14260, USA
(Email: qduan@uncc.edu)

(Received Sep. 23, 2010; revised and accepted Jan. 11, 2011)

Abstract

In this paper we analyzed the algorithms related to threshold cryptography based protocols in networks security. We showed the hardness of threshold minimum cut problem, revealed its relationship with two other problems. Two approximation algorithms for threshold minimum cut were presented. We also show the hardness of determining the probability of threshold access to service nodes in a node-based stochastic graph, and propose a heuristic algorithm for the optimal service node assigning problem. To the best of our knowledge, this is the first work to address these algorithmic problems for threshold cryptography based protocols in network security and reliability.

Keywords: Algorithm design, minimum cut, security protocol, threshold cryptography

1 Introduction

Threshold cryptography and threshold related protocols have wide applications in network security. They can be used in many protocols for different types of networks.

Dharma Agarwal et al. [6] proposed a distributed key management and authentication scheme for networks with mobile ad hoc wireless nodes, that entirely relies on identity-based cryptography and threshold secret sharing. In [18], threshold cryptography is employed to distribute Certificate Authority functionality over specially selected nodes based on the security and physical characteristics of the nodes. The selected nodes that collectively provide the PKI functionality are called Mobile Certificate Authorities (MOCA)s. Di Crescenzo et al. [3, 4] proposed a suite of threshold cryptography based key generation and signature protocols. S. Sarkar et al. [16] proposed a new RSA-threshold cryptography-based scheme for MANETs (Mobile Ad hoc Networks) using verifiable secret sharing(VSS) scheme. The main challenge of threshold cryptography based protocols is that there are some topological requirements to ensure that the protocols can be correctly executed, for example, it may be required that a client node must be connected to at least a certain amount of service nodes, or a node must have at least a certain amount of neighbors. These requirements pose new problems in network security, for example, how to assign and distribute service nodes in a network to make sure every client can execute the threshold cryptography based protocols, how to balance the load among different service nodes, how to recover quickly from node failure, etc. From the adversary's point of view, it needs to find an optimal way to thwart the execution of the protocol, or crack some crucial information by compromising a number of nodes.

In this paper we discuss the algorithmic aspects of the threshold cryptography based protocols in a network. Note that the purpose of our work is not to design a specific threshold based security protocol. Here we mainly investigate algorithms related to general threshold based security protocols. For the attacks against the threshold based protocols, we mainly discuss blocking attacks. We show the intractability of the minimum threshold node cut problem, and propose some algorithms for them. We also investigate the hardness and algorithms of service node assigning in threshold based protocols. Our main contribution includes:

- We show that the minimum threshold node cut problem doesnot have polynomial time approximation scheme, and the relationship between this problem and other NP-hard problems.
- We devise two approximation algorithms for the threshold minimum cut problem, and proved their ratios.
- We investigate the hardness and algorithms of the optimal service assigning problems. We show that determining the probability of threshold access to

service nodes in a node-based stochastic graph is #P-hard, and propose a heuristic algorithm for the optimal service node assigning problem.

To the best of our knowledge, our work is the first to address the threshold minimum cut problem and the optimal service node assigning problem. These two problems also have important applications in some areas other than network security, for example, in emergency responding, when a certain number of network nodes are compromised or a certain number of water resources of a water flow system is contaminated, how to block a threshold number of harmful flow with minimum cost? This is similar to the threshold minimum cut problem. The optimal service node assigning problem can also be applied to other areas in operational research, for example, how to assign a number of service stations in a region optimally that every mobile device in the region can access at least a certain number of stations at any time. So we believe that it is important to investigate the hardness and algorithms of these problems.

The remaining sections of the paper are organized as follows: Section 2 discusses the hardness and algorithms of the threshold minimum cut problem. Section 3 discusses the hardness and algorithms of the optimal service node assigning problem. Section 4 shows related works. Section 5 concludes the paper.

2 Threshold Minimum Cut Problem

There are several possible types of attacks against the threshold cryptography based protocols. An adversary may compromise some nodes or intercept threshold number of transmitted messages to obtain the some secret information. An adversary may also use wormhole attacks to attract as many traffic flows as possible to pass through it. Here we consider the blocking attacks. The goal of the adversary is to block some nodes, such that a client node cannot connect to a threshold number of service nodes. If the adversary can achieve this, the protocol cannot be executed normally. Suppose there is an associated cost to block a node, the objective of the adversary is to find a set of nodes that blocking them will cause the client node cannot connect to more than a given number of service nodes, and the total cost of the selected nodes is minimized.

We can formalize the problem as the following optimization problem.

Given a graph $G = (V, E)$ and k service nodes $S_1, S_2, \ldots, S_k$, ($S_i \in V$ for $1 \leq i \leq k$), a client node A, and a threshold integer l, and every node v in G has an associated cost c, how to find a minimum cost node cut such that at least l out of the k service nodes will be disconnected from A?

The decision version of the problem is:

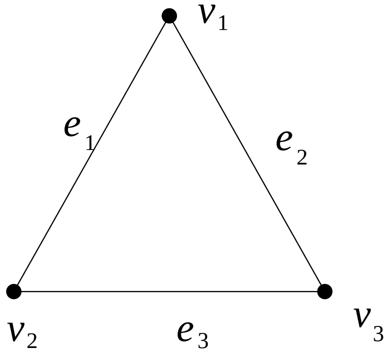

Figure 1: The graph G_1

Given a graph $G = (V, E)$ and k service nodes $S_1, S_2, \ldots, S_k$, ($S_i \in V$ for $1 \leq i \leq k$), a client node A, and a threshold integer l, and another integer B, and every node v in G has an associated cost c, how to find a node cut such that at least l out of the k service nodes will be disconnected from A and the total cost of the cut is no more than B?

We name this problem as threshold minimum node cut problem. The threshold minimum edge cut problem can also be similarly defined.

2.1 Hardness of the threshold minimum node cut problem

We can show that the problem is NP-complete.

Theorem 1. *The threshold minimum node cut problem is NP-complete.*

Proof. We can reduce clique to the problem. Given an instance of clique with a graph $G_1 = (V_1, E_1)$ ($|V_1| = n$) and number k_1, we can construct a new graph G. For every edge e_i of G_1, we have a service node S_i in G. For every node v_i in G_1, we also have a node A_i in G. For every edge e_i in G_1, if its two incident nodes are v_i and v_j in G_1, then we connect node S_i to A_i and A_j in G. Finally, all nodes $A_i (1 \leq i \leq n)$ in G are connected to a client node A. For example, Figure 2 is the constructed G for graph G_1 as in Figure 1. We set k to be $|V_1|$, $l = k_1(k_1 - 1)/2$, and $B = k_1$. Set the weight of nodes A_i ($1 \leq i \leq n$) to be 1, and the weight of other nodes in G to be infinity. Now it is easy to see if G_1 has a clique with size k_1, then in G, we can choose to cut the nodes in $\{A_1, \ldots, A_n\}$ correspond to the nodes in the clique of G_1. Now the cut has total cost k_1, and it can block $l = k_1(k_1 - 1)/2$ service nodes. On the other hand, if a cut with total cost no more than k_1 can block $l = k_1(k_1 - 1)/2$ service nodes, then the cut must correspond to a clique in G_1. This means threshold minimum node cut problem is NP-complete. □

Next we show that even for degree 3 graphs, the problem is NP-complete.

Corollary 1. *The problem is NP-complete even for degree 3 graphs.*

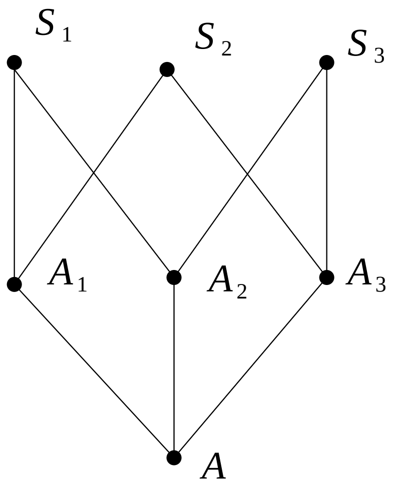

Figure 2: The constructed graph G

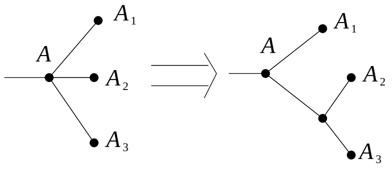

Figure 3: The conversion for G

Proof. In the construction of G in the above proof, for all nodes that have degree more than 3, we can convert it as in Figure 3. In the construction, all newly added nodes have an infinity cost. It is easy to see the transformed graph now has degree at most 3, and the minimum node cut in the new graph is equivalent to the minimum node cut in the original graph. This means the problem is NP-complete even for degree 3 graphs. □

Note that the above hardness result cannot be applied to threshold minimum edge cut. The hardness of threshold minimum edge cut is an open problem.

Based on the proof of the NP-completeness of threshold minimum cut, it is easy to see the following problem is NP-complete.

Definition 1. *Given an undirected graph $G = (V, E)$ and a number m, can one find a subgraph with at least m edges, and the number of nodes in the subgraph is minimized?*

Note that this is the inverse problem of the maximum k-subgraph problem (unit weight case). And this inverse k-subgraph problem can be further generalized to the following set minimum cover problem:

Definition 2. *Given a set S of n elements, a collection C of m_1 subsets of S, and positive integer $m \leq m_1$, can one find m subsets from C such that the total number of distinct elements in the union of the m subsets is minimized?*

We can see the set minimum cover problem is the generalization of the inverse k-subgraph problem, so the set minimum cover problem is also NP-complete.

For the max k-subgraph problem, it is known that there exists a $n^{1/3-\epsilon}$ ratio approximation algorithm where ϵ is a small number [9]. It is conjectured that the problem cannot be approximated within n^{δ} for some $0 < \delta < 1$, but currently the best known hardness result is that it has no polynomial time approximation scheme [9, 12].

Next we show the relationship of the approximation between the max k-subgraph problem and its inverse problem.

Theorem 2. *If the inverse k-subgraph problem can be approximated within ratio $1+\epsilon$ ($0 < \epsilon < 1$, that is, there is an algorithm that can return a subgraph with no more than $1+\epsilon$ times number of nodes compared with the optimal solution), then the max k-subgraph problem can be approximated within ratio 16^{ϵ} (that is, there exists an algorithm that can return a subgraph with at least $16^{-\epsilon}$ times number of edges compared with the optimal solution).*

Note that $16^{-\epsilon}$ is very close to 1 if ϵ is very close to 0.

Proof. Suppose we have an algorithm A for the inverse k-subgraph problem that can achieve ratio $1+\epsilon$ ($0 < \epsilon < 1$). For input graph G and integer m, we define $A(G, m)$ to be the output of algorithm A. For an instance of max k-subgraph problem (G and integer k), we can use binary search method to find an integer m_0 such that $A(G, m_0) \leq \lfloor k(1+\epsilon) \rfloor$ and $A(G, m_0+1) > \lfloor k(1+\epsilon) \rfloor$. Then the optimal solution of max k-subgraph (denoted as OPT_k) will be $\leq m_0$. Now consider the output subgraph of applying A on input G and m_0, we denote it as G_{m_0}. Apply the following algorithm on G_{m_0}:

Algorithm 1.
Repeat remove the node with lowest degree in the current graph (choose an arbitrary node in case of tie).
Until the number of nodes in G_{m_0} becomes k.

We denote the resulting graph of the above algorithm to be G_1. Now it is easy to see the number of edges in G_1 (denoted as $e(G_1)$) is

$$\begin{aligned} e(G_1) &\geq (1-\frac{2}{k_1})(1-\frac{2}{k_1-1})\ldots(1-\frac{2}{k+1})m_0 \\ &\geq (1-\frac{2}{k+1})^{k_1-k} m_0 \\ &\geq (1-\frac{2}{k+1})^{\frac{k+1}{2}\cdot\frac{2k\epsilon}{k+1}} m_0 \end{aligned}$$

Where $k_1 = \lfloor k(1+\epsilon) \rfloor$. Without loss of generality, we can assume $k > 3$. Then

$$\begin{aligned} e(G_1) &\geq 4^{\frac{-2k\epsilon}{k+1}} m_0 \\ &= 16^{-\frac{k\epsilon}{k+1}} m_0 \\ &\geq 16^{-\frac{k\epsilon}{k}} m_0 \\ &= 16^{-\epsilon} m_0 \end{aligned}$$

But we have $OPT_k \leq m_0$, and we constructed a subgraph of k nodes with at least $16^{-\epsilon}m_0$ edges, this means we find an algorithm that can approximate the max k-subgraph problem within ratio 16^{ϵ}. □

Corollary 2. *The inverse k-subgraph problem does not have polynomial time approximation scheme.*

Proof. This follows from the above theorem and the result that max k-subgraph problem does not have polynomial time approximation scheme. □

Corollary 3. *Both the threshold minimum node cut problem and the set minimum cover problem do not have polynomial time approximation scheme.*

We conjecture that the threshold minimum cut problem and the set minimum cover problem cannot be approximated with n^{ϵ} for some $\epsilon < 1$. Though the inapproximability result we obtain is rather weak, we believe that to approximate the two problems is hard.

2.2 Two Approximation Algorithms

We present two algorithms for the threshold min cover problem. The first is a greedy algorithm, the second one is an LP based algorithm.

The main idea of the greedy algorithm is that one always adds a new server node that will increase the cut by a minimum value.

Algorithm 2. $C = \Phi$

```
    Repeat
    for every $v \in V \backslash C$, compute the minimum cut between A and $C \cup v$, denote this value as $c_v$. Add the v has the minimum $c_v$ into C
    Until $| C |= l$
    Return the cut between nodes in C and A.
```

We can show that the algorithm achieves a ratio of l.

Theorem 3. *The greedy algorithm achieves a ratio of l.*

Proof. Suppose in the optimal solution, service nodes $S_1, S_2, \ldots S_l$ are blocked. We denote $Cut(v)$ to be the value of the minimum cut to separate node v and A. Suppose $h = max(Cut(S_1), \ldots Cut(S_l))$. In every step of the algorithm, the current cut value will increase at most h. Since the optimal solution is at least h, so the returned cut value of the algorithm is at most lh. □

The second algorithm is a linear programming based algorithm.

Algorithm 3. *Solve the following LP:*

$$Maximize \sum_{all\ nodes\ v} X_v w_v$$

Subject to

$$Y_i \leq X_i + Y_j \ \ for\ all\ neighbors\ v_j\ of\ v_i\, \forall v_i$$

$$0 \leq X_i \leq 1\,, 0 \leq Y_i \leq 1\,, for\ all\ node\ v_i$$

$$Y_A = 0$$

$$\sum_{i=1}^{k} Y_{S_i} \geq l$$

After solving the LP, sorting the nodes $S_1, S_2, \ldots S_k$ according to their accumulated cut value (Y_{S_i}) in descending order, and return the minimum cut between $S_1, S_2, \ldots S_l$ and A.

Theorem 4. *The LP based algorithm achieves a ratio of $k - l + 1$.*

Proof. The LP defines a fractional cut between the nodes $S_1, S_2, \ldots S_k$ and A, and the summation of the accumulated cut value of nodes $S_1, S_2, \ldots S_k$ is at least l. If we sort the nodes $S_1, S_2, \ldots S_k$ according to their cut value (Y_{S_i}) in descending order, consider the lth largest value Y_{S_l}, this value will be at least $1/(k - l + 1)$. Between nodes $S_1, S_2, \ldots S_l$ and A, we have a fractional cut with value at least $1/(k - l + 1)$, so the value returned by the algorithm is at most $k - l + 1$ times of the value returned by the LP, which is at most the optimal value. □

3 Service Nodes Assigning in Threshold Cryptography Based Protocols

The central idea of threshold cryptography is to divide a cryptographic action into k participants (usually the participants are servers, in some occasion they can also be clients), in such a way only a number of more than threshold (denoted as l) of participants can execute the protocols correctly. The adversary cannot obtain certain secret information by intercepting less than threshold number of messages. Also the adversary cannot thwart the execution of the protocol by compromising less than $k - l$ participants. This means threshold cryptography can greatly improve the security and reliabiliy of the network protocols.

3.1 Choose Service Nodes in a Static Network

In a static network, how to choose a set of service nodes is an optimization problem. We can give a formal definition of the minimization problem:

Definition 3. *Suppose we have a graph $G = (V, E)$, where $V = V_1 \cup V_2$,$|V_1| = n_1$, $|V_2| = n_2$, $n_1 + n_2 = n$, $V_1 \cap V_2 = \phi$ (here V_1 is the set of client nodes, V_2 is the set of candidate service nodes), and every node $v_i \in V_2$ ($i = 1, 2, \ldots, n_2$) has an associated cost c_i, can one find a subset V_3 of V_2 such that every node $u_i \in V_1$ ($i = 1, 2, \ldots, n_1$) is connected to at least l nodes in V_3 and the total cost of nodes in V_3 is minimized?*

The above problem is equivalent to the set multi-cover problem, and some greedy algorithms or LP based algorithms can be used to solve it [10].

3.2 Service Nodes with Patterned Mobility

Next we consider the case that the service nodes in wireless networks can have patterned mobility. In many wireless networks, the mobility pattern of the nodes (or routers) can be predicted, that is, they have a certain kind of mobility orbit and the position of a node has a probability distribution over the positions of the orbit. In this case, we can consider the service nodes with patterned mobility as the dynamic nodes in a stochastic graph. Now we first give the definition of node-based stochastic graphs.

Definition 4. *(node-based stochastic graph): A node-based stochastic graph is an undirected graph such that a subset of node in the graph is dynamic, that is, every such node may be located in multiple positions. Formally, suppose we have a graph with n nodes and these nodes form an undirected graph $G = (V, E)$, where*
$V = \{v_{11}, \ldots, v_{1t_1}, \ldots,$
$v_{h1}, \ldots, v_{ht_h}, v_{h+1}, \ldots, v_n\}$,
which means V contains two types of nodes, which are fixed nodes and dynamic nodes, respectively. Nodes $v_{h+1}, \ldots, v_n$ are fixed nodes, nodes $v_{i1}, \ldots, v_{it_i}$, $1 \leq i \leq h$ are possible positions of node v_i, $1 \leq i \leq h$, and there is an associated probability p_{ij} for every v_{ij}, $1 \leq i \leq h$, $1 \leq j \leq t_i$, which means node v_i has probability p_{ij} in position v_{ij} of G. Also in the edge set E, there is no edge between any two nodes in $v_{i1}, \ldots, v_{it_i}$ (This means no edge exists between two possible positions of a dynamic node).

We have the following hardness result for determining the probability of threshold access to service nodes in a node-based stochastic graph.

Prop 5. *Suppose we have a node-based stochastic graph $G = (V, E)$, a set of service nodes K, where $K \subseteq \{v_1, \ldots, v_h\}$, a set of client nodes C, where $C \subseteq \{v_1, \ldots, v_h, v_{h+1}, \ldots v_n\}$, $C \cap K = \emptyset$, and a positive integer value l, the problem to determine the probability that every node in C have direct access to at least l of the service nodes is $\#P$-hard.*

Proof. We can reduce $\#SAT$ to this problem (which we call $\#Access$). Given a $3SAT$ instance, we create a dynamic node for every variable, which has two possible positions in the stochastic graph, and every position has probability 1/2. We also create a new fixed node for every clause, which is connected to the 3 dynamic nodes correspond to the three variables in the clause. Now consider the probability that all fixed nodes have direct access to one of their corresponding dynamic nodes in the clause (here we set the threshold number to be 1), it is easy to see that this probability is exactly the probability that the $3SAT$ instance is satisfied, which means $\#Access$ is $\#P$ hard. Figure 4 shows the $\#Access$ instance we constructed through this procedure for the $\#SAT$ instance:

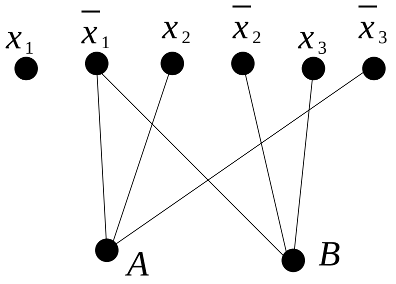

Figure 4: Stochastic graph instance

$$(\overline{x}_1 \vee x_2 \vee \overline{x}_3 \wedge (\overline{x}_1 \vee \overline{x}_2 \vee x_3)$$

□

3.3 Static Service Nodes in Stochastic Graph

If we consider the problem of choosing fixed service nodes in a stochastic graph, we can have a new optimization problem. Before we give the formal definition of the new problem, we define the connection probability of a single node in a node-based stochastic graph.

Definition 5. *Given a positive integer l and a node-based stochastic graph $G = (V, E)$, in which $v_1, \ldots v_h$ are dynamic client nodes, $v_{h+1}, \ldots, v_n$ are fixed candidate service nodes, and $V_1 \subseteq \{v_{h+1}, \ldots, v_n\}$ is the set of service nodes chosen by the network designer, for every client node v_i, $1 \leq i \leq h$, the connection probability is $\sum_j p_{ij}$ in which the summation is over the j such that v_{ij} is connected to at least l nodes in V_1.*

Now we give the formal definition of fixed node assigning in stochastic graphs (minimization version).

Definition 6. *Given a positive value p $(0 < p < 1)$ and a node-based stochastic graph $G = (V, E)$, in which $v_1, \ldots v_h$ are dynamic client nodes, and $v_{h+1}, \ldots, v_n$ are fixed candidate service nodes, can one find a set (denoted by V_1, and $V_1 \subseteq \{v_{h+1}, \ldots, v_n\}$) of service nodes such that every client node has a connection probability at least p and the total cost of nodes in V_1 is minimized?*

Since even the static case of service node assigning problem is NP-hard and cannot be approximated by any ratio less than $c \ln n$ for some constant c, the above problem has at least the same hardness as the static case. For the most simple case when $l = 1$, we propose the following heuristic algorithm. The basic idea is to always choose the candidate service node with the largest "potential" value. When a node with the largest "potential" value is chosen, the "potential" value of other candidate service nodes and the current accumulated connection probability of every client node are updated.

Algorithm 4.

```
1. Set $V_1 := \emptyset$, $V_2 := \{v_1, \dots, v_h\}$, $V_3 := \{v_{h+1}, \dots, v_n\}$, and $\forall v \in V_2$, set $f(v) := 0$
2. Repeat
    2.1 For every $u \in V_3$, set $c(u) := 0$
    2.2 For every neighbor $v_{ij}$ $(1 \leq i \leq h)$ of $u$, if $v_i \in V_2$, set
            $c(u) := c(u) + min(p_{ij}, p - f(v_i))$
    2.3 Choose the $u'$ with the largest $c(u')$
    2.4 For every neighbor $v_{ij}$ $(1 \leq i \leq h)$ of $u'$, set
            $f(v_i) := f(v_i) + min(p_{ij}, p - f(v_i))$
        if $f(v_i) \geq p$, set $V_2 = V_2 \backslash v_i$
    2.5 $V_1 := V_1 \cup u'$, $V_3 := V_3 \backslash u'$
  Until $V_2 = \emptyset$
```

The algorithm runs in time $\mathcal{O}(n^3)$, which means that it can be practically applied.

4 Related Works

Threshold cryptography was first addressed in [7], the application of threshold cryptography in network security was discussed in [1, 3, 4, 6, 8, 13, 16]. In [1], the authors surveyed the threshold cryptography based schemes and the authentication schemes that have been proposed to secure ad hoc networks, and identified the challenges and open research areas associated with each of these approaches. In [3] the authors formalized and presented satisfactory solutions for the general problem of threshold cryptography in Mobile Ad Hoc Networks. A distributed key management and authentication approach by deploying the concepts of identity-based cryptography and threshold secret sharing was proposed in [6]. This work effectively solved the problem of single point of failure in the traditional public key infrastructure (PKI)-supported system without any assumption of prefixed trust relationship between nodes. In [4] the authors investigated and presented a new MANET threshold signature scheme that is secure under significantly improved topology assumptions. A new RSA-threshold cryptography-based scheme for MANETs using verifiable secret sharing (VSS) scheme was proposed in [16] and a new approach to facilitate certificate packet delivery and reduce the overhead caused by threshold cryptography was proposed in [13]. Threshold based cryptography can also be applied in identity-based key escrow [14] and dealer-less key sharing [11].

Greedy algorithm and other related algorithms for set cover was discussed in [2, 17], and approximation algorithms for the partial set cover problem was discussed in [10]. The classical max-flow min-cut problem is well known to be solvable in polynomial time [15, 17]. The minimum multi-terminal cut problem is known to be MAXSNP-hard but have constant approximation algorithms [5]. The max k-subgraph problem (also called the dense k-subgraph problem) has no polynomial time approximation scheme [12], but can be approximated within $n^{\frac{1}{3}-\epsilon}$ where ϵ is a small positive number [9].

However, none of the above works addressed the optimization algorithms we investigate in this work, we believe that our work is the first to address these algorithms related threshold based protocols in network security.

5 Conclusion and Future Research

In this paper we investigate some new problems related to threshold cryptography protocols in network security and reliability. We show the hardness of the threshold minimum cut problem and propose two approximation algorithms. We also show the hardness of the optimal service node assignment problem and present a heuristic algorithm. These problems are important in threshold cryptography protocols and have applications in some other areas.

There are a lot of new problems that can be addressed in future research. The security and reliability of threshold cryptography based protocols are dependent on the topology of the networks. Further research, both theoretically and experimentally, can be done on this relationship. As we have pointed out, the optimal assignment of service nodes is intractable in general, but in some practical situations there may exist good algorithms. For the threshold minimum cut problem, we only get a weak inapproximability result, there is much room for improvement.

References

[1] M. A. Azer, S. M. El-Kassas, and M. S. El-Soudani, "Threshold cryptography and authentication in ad hoc networks survey and challenges," in *Proceedings of the Second International Conference on Systems and Networks Communications*, p. 5, Washington, DC, USA, 2007. IEEE Computer Society.

[2] V. Chvatal, "A greedy heuristic for the set-covering problem," *Mathematical Methods of Operations Research*, vol. 4, pp. 233–235, 1979.

[3] G. D. Crescenzo, G. Arce, and R. Ge, "Threshold cryptography in mobile ad hoc networks," in *SCN 2004*, pp. 91–104, 2004.

[4] G. D. Crescenzo, R. Ge, and G. R. Arce, "Improved topology assumptions for threshold cryptography in mobile ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pp. 53–62, 2005.

[5] E. Dahlhaus, D. S. Johnson, C. H. Papadimitriou, P. D. Seymour, and M. Yannakakis, "The complexity of multiterminal cuts," *SIAM Journal on Computing*, vol. 23, pp. 864–894, 1994.

[6] H. Deng and A. Mukherjee amd D. P. Agrawal, "Threshold and identity-based key management and

authentication for wireless ad hoc networks," in *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC' 04)*, vol. 2, p. 107, 2004.

[7] Y. Desmedt and Y. Frankel, "Threshold cryptosystems," in *Crypt' 89*, vol. LNCS 435, pp. 307–315, 1989.

[8] L. Ertaul and N. Chavan, "Security of ad hoc networks and threshold cryptography," in *2005 International Conference on Wireless Networks, Communications and Mobile Computing*, vol. 1, pp. 69–74, 2005.

[9] U. Feige, G. Kortsarz, and D. Peleg, "The dense k-subgraph problem," *Algorithmica*, vol. 29, p. 2001, 1999.

[10] R. Gandhi, S. Khuller, and A. Srinivasan, "Approximation algorithms for partial covering problems," *Journal of Algorithms*, vol. 53, pp. 55–84, 2004.

[11] M. H. Ibrahim, "Efficient dealer-less threshold sharing of standard rsa," *International Journal of Network Security*, vol. 8, no. 2, pp. 139–150, 2010.

[12] S. Khot, "Ruling out PTAS for graph min-bisection, dense k-subgraph, and bipartite clique," *SIAM Journal on Computing*, vol. 36, no. 4, pp. 1025–1071, 2006.

[13] S. T. Li and X. Wang, "Enhanced security design for threshold cryptography in ad hoc network," in *NEW2AN 2004*, pp. 27–31, 2008.

[14] Y. Long, Z. Gong, K. Chen, and S. Liu, "Provably secure identity-based threshold key escrow from pairing," *International Journal of Network Security*, vol. 8, no. 3, pp. 227–234, 2009.

[15] C. Papadimitriou, *Computational Complexity.* Addison Wesley, 1993.

[16] S. Sarkar, B. Kisku, S. Misra, and M. S. Obaidat, "Chinese remainder theorem-based RSA-threshold cryptography in manet using verifiable secret sharing scheme," in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communication*, pp. 258–262, 2009.

[17] V. V. Vazirani, *Approximation Algorithms.* Springer, 2004.

[18] S. Yi and R. Kravets, "Moca : Mobile certificate authority for wireless ad hoc," in *2nd Annual PKI Research Workshop Program (PKI 03)*, pp. 65–79, 2003.

Qi Duan received his Ph.D in Computer Science and Engineering from State University of New York at Buffalo in 2008. He is currently a postdoc research associate in department of Software and Information Systems, University of North Carolina at Charlotte. His research interests include network security, algorithm design and analysis.

Mohit Virendra received his Ph.D. in Computer Science and Engineering from the State University of New York at Buffalo in 2008. He has been involved with the Design and Development of Networking Protocols in the industry for the last few years. His expertise lies in Computer and Network Security, Storage and Ethernet Networking and Wireless Networks. He is currently affiliated with Brocade Communications Systems, San Jose CA.