IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 09-12
www.iosrjournals.org

Pairwise Independent Network Using Key Generation Algorithm

K.Kalaivani[1], K.Renugadevi[2], .Nithya[3]

[1-2] UG Students, Department of Computer Science and Engineering, Surya Group of Institutions, Vikiravandi, India.
3. Associate Professor, Department of Computer Science and Engineering, Surya Group of Institutions, Vikiravandi, India

Abstract: *We consider two secret key generation problems under a pairwise independent network model, and propose low complexity key generation schemes in a framework that connects our problems to network flow problems in graphs. Our schemes have two components: 1) local key generation and 2) global key propagation. In the local key generation, we use point-to-point source coding with side information to establish pairwise keys, from which we construct a graph with the capacity of each edge being the key rate of the corresponding point-to-point local key. In the global key propagation, depending on the particular problem, secret keys are delivered to users in the network using various network flow algorithms.. This approach has a low complexity and has a better performance than the existing approach. For the general case of generating more than two keys, we show that the sum rate of the proposed scheme is larger than an upper bound characterized in this paper divided by a constant.*

Keywords : *Capacity, multicommodity ,pairwise keys .*

I. Introduction

Establishing symmetric key to be shared by a pair of users in secure communications is a challenging task. L. Lai was supported in part by the Division of Computing and Communication Foundations through the National Science Foundation (NSF) CAREER Award under Grant CCF-1318980 and in part by the Division of Computer and Network Systems through NSF under Grant CNS- 1321223. The basic idea of this approach is to use the technique of source coding with side information. Roughly speaking, Alice can divide all possible sequences it observes into bins and reveal the bin number to Bob via the public discussion. By combining its own observations and the bin number sent by Alice, Bob will be able to recover the sequence observed by Alice with a high probability. It can be shown that the bin index tells little information about the index of the sequence within the bin. Hence, both Alice and Bob can use the index within the bin as the generated key. As the result, one can adopt existing practical Slepian-Wolf codes to construct practical schemes for the key generation in this point-to-point symmetric key generation setup. However, unlike the point-to-point scenario, very few practical schemes for network distributed source coding exist. By focusing on a special source model named pairwise independent network (PIN) model,1 Nitinawarat *et al.* [16] Proposed an interesting scheme that converts the group key generation problem into a combination of 1) local pair- wise key generation; and 2) global key propagation. With this approach, one can then again take advantage of the existing practical Slepian-Wolf codes in the first step.

However,in the general case, there are some challenges in the second step of the approach. In particular, finding the best global key propagation pattern in the second step is equivalent to the Steiner tree packing problem in a multigraph, which is NP-complete. In this paper, we extend the work in along two lines with the goal of designing schemes that achieve better key rates while avoiding the complexity issues associated with the Steiner tree packing problem or other combinational optimization problems. The proposed schemes are combinations of point-to-point key generation problem, for which practical coding schemes exist, and low complexity linear programming (LP) problems. They outperform the existing schemes and are optimal in certain scenarios. Our approach draws connections between key generation problems and various problems in graph theory, which allow us to utilize rich tools and literature in graph theory. In the first line, we consider the generation of a *single group* key under the PIN model. The enabling element of our scheme is a close connection between the group key generation and the multicast over graph problem. In the proposed approach, we first construct a graph for the PIN model. In the graph constructed, the set of nodes is the same as *M*, and the link capacity between nodes *i* and *j* is the same as the rate of the mutual information between the source observations at these two nodes. We then construct a network code that achieves the largest multicast throughput from node 1 to the set of users in *A* for the graph constructed. Node 1 then randomly generates a key and multicasts this key to other users in *a* using network coding. At each hop, the information will be encrypted and decrypted using local key established during the graph construction phase. Furthermore, finding the largest achievable rate under the proposed approach is essentially a linear programming (LP) problem, which can be solved efficiently. We also note that network coding has been used for the key generation problem in for a different model. This is motivated by the fact that there are typically multiple pairs of nodes communicating with each other in communication networks.

Each pair of nodes needs to establish a key between them so that they can use their respective secret key for encryption and decryption. Under the model studied, there are a set of terminals *M*, among which *T* pairs of terminals want to generate *T* independent keys with the assistance of the remaining users. Clearly, there are tradeoffs among the rates of generating these *T* keys. We are interested in characterizing the key rate region. We propose a simple approach to propagate the keys through the network. In the proposed approach, we first construct a graph for the PIN model, same as the first scenario. The terminals then establish routes between the terminals that need to establish common keys. Using these routes, one of each pair of terminals that are involved in establishing a common key then sends randomly generated keys to the other terminal involved. Along each route, this randomly generated key will be encrypted and decrypted using local key established via local correlated estimates.By deriving an outer bound on the rate region coupled with results from graph theory, we show that the proposed key propagation approach is optimal for simultaneously generating two keys for two pairs of nodes. The multiple key generation problem: we study a novel model of generating multiple keys simultaneously. We propose a simple secure routing approach for generating multiple keys. This secure routing approach effectively connects the simultaneous key establishment problem to a multi- commodity flow problem in a graph. By deriving an outer bound on the rate region coupled with results from graph theory, we show that the proposed key propagation approach is optimal for simultaneously generating two keys for two pairs of nodes. We fully characterize the rate region for this case. We also extend the study to the case of simultaneously generating more than two keys. In this general case, we show that the maximum sum- rate can be characterized by a LP. Furthermore, we show that the proposed approach achieves a sum-rate that is constant factor to that of an upper-bound derived in the paper.

II. Literature Review

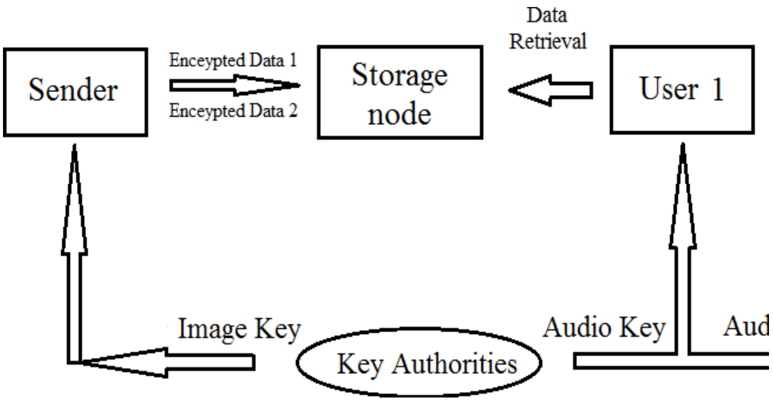
The method used for data collected in sensor network our approach is based on concept of provanance As sensor networks are being increasingly deployed in decision-making infrastructures such as battlefield monitoring systems and SCADA (Supervisory Control and Data Acquisition) systems. To obtain trust scores, we propose a cyclic framework which well reflects the inter-dependency property: the trust score of the data affects the trust score of the network nodes that created and manipulated. As increasing amounts of valuable information are produced and persist digitally, the ability to determine the origin of data becomes important In science, medicine, commerce, and government, data provenance tracking is essential for rights protection, regulatory compliance, management of intelligence and medical data, and authentication of information as it flows through workplace tasks, we show how to provide strong integrity and confidentiality assurances for data provenance information.

III. Materials And Methods

These users are allowed to exchange information with each other using a public channel with infinite capacity. However, any information exchanged using the public channel will also be perfectly received by Eve. Without loss of generality, one can assume that these users take turn in sending public information for *r* round Eve knows the functions used by each user for generating the public information, and knows **F** perfectly. We consider two scenarios: 1) to generate a single group key for a group of users; and 2) to generate multiple independent keys, each for a pair of users.

3.1 Single Group Key Generation

In the first scenario, we consider the generation of h re implies that the users in group *A* generate the same key *K* with a high probability, (3) implies that the generated key is nearly uniformly distributed and (4) implies that Eve learns a limited amount of information about the generated key from the public discussion. We call the largest achievable key rate as the key capacity *C*.



3.2 Network-Coding Based Single Group

In this section, we consider the group key generation for a set of users *A*. The proposed scheme has two steps:

1) graph construction via local key generation; 2) key propagation using network coding. Our algorithm is based on a simple observation that the group key generation problem is closely related a multicast over an undirected network problem. This observation allows us to design a network coding based key generation scheme that outperforms the routing-based key generation scheme proposed. In addition, as will be clear in the sequel, finding the largest achievable rate using our scheme is a LP problem, while finding the largest achievable rate using the scheme is a NP- complete problem. We describe our key generation algorithm . In the graph, the capacity of eachedge is *n*. Using our approach, the users in *A* can generate 2*n* bits of keys, hence achieving a key rate of 2

bits per source observation. To achieve this, node 1 randomly generates **Algorithm 1** Network Coding Based Single Group Key Generation In the following, instead of using both *Ki j* and *K j i* to denote the value of the local key between *(i, j)*, we will use *Ki j* to denote both keys with the understanding that there is a small probability that the value of local keys at *(i, j)* are different. Based on the topology of the undirected graph constructed in the step 1, construct a network code [19] that achieves the largest multicast capacity from node 1 to all other users in set *A* using this network.2 Let *nR* be the multicast capacity achieved in this network. Node 1 randomly generates a key *K* from the set {1, · · · , 2*nR*} using a uniform distribution. Node 1 then multicasts this key to other nodes in the Another advantage of our approach is its low complexity. Finding the largest achievable rate using the approach in [16] is equivalent to the Steiner tree packing [22], which is NP-complete. On the other hand, finding the largest achievable rate using our approach is a LP problem, as finding the capacity achieving network coding scheme in [21] is a LP problem, which can be solved efficiently remain the same.

IV. Result And Analysis

We now consider the general case in which we are required to generate *T* > 2 keys, one key for each pair *(t, t* + *T),t* = 1, · · · , *T* . In this general case, we discuss the sum of key rates. We will generalize Algorithm 2 to this general case. We will also provide an upper bound on the sum rate, and show that using the routing-based key propagation approach can achieve a sum rate equal to the developed upper bound divided by a constant factor. The secure routing-based key propagation scheme discussed in Section IV-A can be used in this general scenario. In particular, we again construct a undirected graph *Gn(V, E)* with *V* being the same as *M* and *E* being learn negligible amount of information about the established keys. It is clear that this routing-based approach converts the problem into a multi-commodity flow problem in the graph *Gn(V, E).* Finding the maximum achievable sum of rates *Cr* using this approach is equivalent to finding the maximum sum of the rates of fractional multi-commodity flows,5 which has been extensively studied in graph theory We now develop an upper bound for the sum of key rates for any key generation protocols. The proposed scheme can be easily modified to satisfy additional constraints. One such constraint is that the generated keys should also be kept secret from other user pairs.

V. Conclusion

We have considered two scenarios for key generation under PIN model. In the first scenario, in which one is required to generate a group key, we have proposed a network coding based approach. The approach has a low complexity and has a better performance than the existing approach. In the second scenario, we have considered the problem of simultaneously generating multiple keys. A simple secure routing-based key propagation protocol has been proposed. This approach converts the problem under study to a multi-commodity flow problem in networks. We have shown that the proposed approach is optimal for the case of generating two keys. For the general case of generating more than two keys, we have also shown that the sum rate of the proposed scheme is larger than an upper bound characterized in this paper divided by a constant. Furthermore, finding the largest achievable sum rate using our scheme is a LP problem. The proposed scheme can also be easily modified to take additional constraints into consideration.

References

[1]. L. Lai and S.-W. Ho, "Simultaneously generating multiple keys and multi-commodity flow in networks," in Proc. IEEE Inf. Theory Workshop, Lausanne, Switzerland, Sep. 2012, pp. 627–631.

[2]. U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733–742, May 1993.

[3]. R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[4]. V. Stankovic, A. D. Liveris, Z. Xiong, and C. N. Georghiades, "On code design for the Slepian-Wolf problem and lossless multiterminal networks," IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1495–1507, Apr.

[5]. 2006.

[6]. C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," IEEE Trans. Inf. Theory, vol. 58, no. 2, pp. 639–651, Feb. 2012.

[7]. I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," IEEE Trans. Inf. Theory, vol. 50, no.12, pp. 3047–3061, Dec. 2004.

Authors Biography

K.Renugadevi is a final year student of Computer Science and Engineering at surya group of institutions, Vikkiravandi. Her area of interest includes Data Mining and Information & Knowledge Management.

K.Kalaivani is a final year student of Computer Science and Engineering at surya group of institutions, Vikkiravandi. Her area of interest includes Data Mining and Information & Knowledge Management.