p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

Configuration of network coding in Adhoc network

Ms. K.MOUNIKA REDDY

Mr. K.Raju

Abstract: In this paper, we analyze the impact of network coding (NC) configuration on the performance of ad hoc networks with the consideration of two significant factors, namely, the throughput loss and the decoding loss, which are jointly treated as the overhead of NC. In particular, physical-layer NC and random linear NC are adopted in static and mobile ad hoc networks (MANETs), respectively. Furthermore, we characterize the goodput and delay/goodput tradeoff in static networks, which are also analyzed in MANETs for different mobility models (i.e., the random independent and identically distributed (i.i.d.)mobility model and the random walk model) and transmission schemes (i.e., the two-hop relay scheme and the flooding scheme). Moreover, the optimal configuration of NC, which consists of the data size, generation size, and NC Galois field, is derived to optimize the delay/ goodput tradeoff and goodput. The theoretical results demonstrate that NC does not bring about order gain on delay/goodput tradeoff for each network model and scheme, except for the flooding scheme in a random i.i.d. mobility model. However, the goodput improvement is exhibited for all the proposed schemes in mobile networks. To our best knowledge, this is the first work to investigate the scaling laws of NC performance and configuration with the consideration of coding overhead in ad hoc networks.

EXISTING SYSTEM:

- The capacity of wired networks can be improved by network coding (NC), which can fully utilize the network resources. Due to this advantage, how to employ NC in wireless ad hoc networks has been intensively studied in recent years.
- Important to design the NC in wireless ad hoc networks with interference to achieve the improvement on system performance such as goodput and delay/goodput tradeoff.

- An important work by Liu et al. in introduced the observation that only a constant factor of throughput improvement can be brought about to k-dimensional random static networks. It was indicated in their results that order improvement of throughput scaling laws can be achieved by adopting RLNC in MANETs.

DISADVANTAGES OF EXISTING SYSTEM:

- The probability that the random linear NC was valid for a multicast connection problem on an arbitrary network with independent sources.
- It was indicated in their results that order improvement of throughput scaling laws can be achieved by adopting RLNC in MANETs.

PROPOSED SYSTEM:

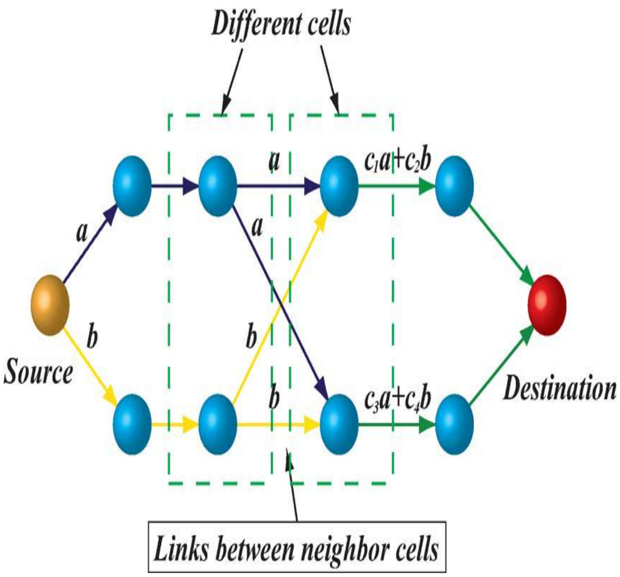
- ❖ We have analyzed the NC configuration in both static and mobile ad hoc networks to optimize the delay/ goodput tradeoff and the goodput with the consideration of the throughput loss and decoding loss of NC.
- ❖ The mobile model, the two-hop relay scheme and the flooding scheme are proposed for both random independent and identically distributed (i.i.d.) mobility model and random walk model with random linear NC.
- ❖ The throughput loss and decoding loss of NC, which are treated as the overhead of NC, are also considered. The decoding loss is caused by decoding failure of RLNC. Since the NC coefficients are randomly selected from Galois field Fq, the destination may not decode the k original packets successfully.

ADVANTAGES OF PROPOSED SYSTEM:

- ✓ The scaling laws of NC overhead, which were not considered in most previous works in wireless ad hoc networks.
- ✓ Theoretical results indicate that the goodput and delay/goodput tradeoff cannot be improved in order sense by employing NC when considering the throughput loss and decoding loss.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

SYSTEM ARCHITECTURE:



1 INTRODUCTION

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data [1]. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers.

However, security concerns become the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud [2]. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud.

In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group.

1. We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
2. Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.
3. We provide security analysis to prove the security of our scheme. In addition, we also perform simulations to demonstrate the efficiency of our scheme.

The remainder of the paper proceeds as follows. In section 2, we describe the system model and our design goals. Our proposed scheme is presented in detail in section 3, followed by the security analysis and performance evaluation in section 4 and 5, respectively. Finally, the conclusion is made in section 6.

2 THREAT MODEL, SYSTEM MODEL AND DESIGN GOALS

2.1 Threat Model

As the threat model, in this paper, we propose our scheme based on the Dolev-Yao model [17], in which the adversary can overhear, intercept, and synthesis any message at the communication channels. With the Dolev-Yao model, the only way to protect the information from attacking by the passive eavesdroppers and active saboteurs is to design the effective security protocols. This means there is not any secure communication channels between the communication entities. Therefore, this kind of threaten model can be more effective and practical to demonstrate the communication in the real world.

2.2System Model

As illustrated in figure 1, the system model consists of three different entities: the cloud, a group manager and a large number of group members.

The cloud, maintained by the cloud service providers, provides storage space for hosting data files in a pay-as-you-go manner. However, the cloud is untrusted since the cloud service providers are easily to become untrusted. Therefore, the cloud will try to learn the content of the stored data. Group manager takes charge of system parameters generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other parties. Group members(users)are a set of registered users that will store their own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation.

2.3Design Goals

We describe the main design goals of the proposed scheme including key distribution, data confidentiality, access control and efficiency as follows:

Key Distribution: The requirement of key distribution is that users can securely obtain their private keys from the group manager without any Certificate Authorities. In other existing schemes, this goal is achieved by assuming that the communication channel is secure, however, in our scheme, we can achieve it without this strong assumption.

Access control: First, group members are able to use the cloud resource for data storage and data sharing. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud resource again once they are revoked.

Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. To maintain the availability of data confidentiality for dynamic groups is still an important and challenging issue. Specifically, revoked users are unable to decrypt the stored data file after the revocation.

Efficiency: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the others, which means that the remaining users do not need to update their private keys.

In general, our scheme can achieve secure key distribution, fine access control and secure user revocation. For clearly seeing the advantages of security of our proposed scheme, as illustrated in table 3, we list a table compared with Mona, which is Liuet al.'s scheme, the RBAC scheme, which is Zhou et al.'s scheme and ODBE scheme, which is Delerableeet al.'s scheme. The √in the blank means the scheme can achieve the corresponding goal.

4 CONCLUSION

In this paper, we design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Moreover, our scheme can achieve secure user revocation, the revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

References

[1] M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz,A.Konwinski, G. Lee, D.Patterson, A.Rabkin, I.Stoica, andM.Zaharia. "A View of Cloud Computing,"*Comm. ACM*, vol. 53,no.4, pp.50-58, Apr.2010.

[2] S.Kamara and K.Lauter,"Cryptographic Cloud Storage," *Proc.Int'l Conf. Financial*

Cryptography and Data Security (FC), pp.136-149, Jan. 2010.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K.Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," *Proc.USENIX Conf. File and Storage Technologies*, pp. 29-42, 2003.

[4] E.Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," *Proc. Network and DistributedSystems Security Symp. (NDSS)*, pp. 131-145, 2003.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," *Proc. Network and Distributed Systems SecuritySymp. (NDSS)*, pp. 29-43, 2005.

[6] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," *Proc. ACM Symp. Information, Computer and Comm. Security*, pp. 282-292, 2010.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," *Proc. ACM Conf. Computer and Comm. Security (CCS)*, pp. 89-98, 2006

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," *Proc. ACM Symp. Information, Computer and Comm. Security*, pp. 282-292, 2010.

Author's Profile

Mr. K.Raju received M.Tech degree from Jayamukhi Institute of Technological Science,Narsampet, Warangal affiliated to JNTUH, Hydearabad. He is currently working as Assistant professor, Department of CSE, in Vinuthna Institute of Technology & Science ,Hasanparthy, Warangal, Telangana, India. Hisinterest includes Data Base Management Systems.

Ms. K.MOUNIKA REDDY recived B.Tech Degree from Ganapathy Engineering College Rangashaipet Warangal. Affliated to JNTUH Hyderabad, She Is Currently pursuing M.Tech Degree in Software Engineering Specialization in vinuthna Institute of Technology & Science Hasanparthy ,Warangal, Telangna.India.