International Journal of Multimedia and Ubiquitous Engineering
Vol.9, No.9 (2014), pp.231-240
http://dx.doi.org/10.14257/ijmue.2014.9.9.24

Security Data Auditing based on Multifunction Digital Watermark for Multimedia File in Cloud Storage

Yongjun Ren[1,2], Jian Shen[1,2], Jin Wang[1,2],JiangXu[1,2] and Liming Fang[3]

[1]Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing 210044, China
[2] School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China.
[3] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210044, China.
renyj100@126.com; wangjin@nuist.edu.cn

Abstract

Cloud computing is a promising computing model that enables convenient and on-demand network access to a shared pool of configurable computing resources. In cloud computing, data owners host their data on cloud servers and data consumers can access the data from cloud servers. This new paradigm of data storage service also introduces new security challenges, because data owners and data servers have different identities and different business interests. Therefore, an independent auditing service is required to make sure that the data is correctly hosted in the Cloud. However, the existing solutions are not specific to the multimedia data. Moreover copyright protection is not provided.

In this paper, we define specially a provable data possession model for multimedia file, and present a framework based on digital watermarking for multimedia data storages audit service, in which we analyze the security features of audit service for multimedia data outsourcing and the corresponding properties of digital watermarking. Moreover as an example, we present a provable data possession scheme based on double function self-embedded digital watermark, which integrate image content audit service and copyright protection.

Keywords: *data storage auditing; provable data possession; watermark*

1. Introduction

Cloud Computing has been envisioned as the next generation architecture of IT Enterprise, which is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. For example, Amazon Elastic Compute Cloud (Amazon EC2) provides cloud computation and Amazon Simple Storage Service (Amazon S3) provides cloud storage.

Storing the data in cloud environment becomes natural and also essential. But, security becomes one of the major concerns for all entities in cloud services. Firstly, data owners would worry their data could be misused or accessed by unauthorized users. Secondly, the data owners would worry their data could be lost in the Cloud. This is because data loss could happen in any infrastructure. Moreover, the cloud service

ISSN: 1975-0080 IJMUE

providers (CSP) may be dishonest and they may discard the data which has not been accessed or rarely accessed to save the storage space or keep fewer replicas than promised. As a result, data owners need to be convinced that their data are correctly stored in the Cloud. It is desirable to have data storage auditing （DSA） service to assure data are correctly stored in the Cloud.

Though many data storage auditing schemes are presented, these solutions are not specific to the multimedia data. The existing data storage auditing methods can be classified into three categories: Message Authentication Code methods, RSA-based homomorphic methods and BLS signature based homomorphic methods [1], in which all data as binary bit stream are calculated using message authentication code or digital signature and attached to the protected information with the transmission. Unfortunately the disadvantage of traditional DSA schemes lies in(1) Need to transport the additional data, increasing the amount of data communication; (2) Encrypted messy code easy to attract the attention of the attacker; (3) unable to locate tamper with the location and thus cannot judge bad-mouth’s attempt. In addition, more important is that users in cloud storage service can get multimedia data and illegally propagate them, which is a big problem of the influencing the development of the cloud computing. But the existing DSA schemes do not provide copyright protection. It is well believed that supporting copyright protection can be of vital importance to the practical application of multimedia data storage outsourcing services.

In this paper, we at first define specially a provable data possession (PDP) model for multimedia file, and present a framework based on digital watermarking for multimedia data storage audit service, in which we provide the security features of audit service for multimedia data outsourcing and the corresponding properties of digital watermarking. As an example, we introduce an efficient watermarking-based audit service for image outsourced storages. Our audit system use self-embedding watermarking to provide image content audit and support authenticity and integrity for image content in cloud storage. In addition the audit system supports the copyright protection of image by using self-embedded technology. That is, we integrate image content audit service and copyright protection through a double function self-embedded watermarking scheme, which greatly reduced the consumption of resources and is very suitable for multimedia data in cloud environment.

2. Related Work

Cloud computing is a promising computing model that enables on-demand network access to a shared pool of configurable computing resources. The first offered cloud service is cloud storage: data owners let cloud service providers host their data on cloud servers and data consumers can access the data from the cloud servers. Because data owners and data servers have different business interests, this new paradigm of data storage service also introduces new security challenges. Therefore, independent auditing service is required to make sure that the data is correctly hosted in the Cloud. Recently, much of growing interest has been pursued in the context of stored data audit.

The existing data storage auditing methods can be classified into three categories: Message Authentication Code (MAC)-based methods, RSA-based Homomorphic methods and BLS-based Homomorphic methods. The message authentication code (MAC) is a kind of hash function which has been used for checking the data integrity for a long time. In the cooperative Internet backup scheme proposed by Lillibridge *et al.* [2], the Reed-Solomon erasure-correcting codes [3] are applied to generate redundancy blocks. After that, the MAC is calculated for each encrypted data block. Then, the system peers perform spot-checks of data blocks using MACs. They protocol in which an error-correcting code is applied to a file and blocks are then MACed. Whenever a verifier (the Owner or the Auditor) needs to check data integrity, he retrieves a random set of blocks from the Server and re-computes the MAC of each block for comparison. Based on the pre-computed MACs stored on the verifier, the protocols proposed by Lillibridge *et al.* and Naor *et al.* can detect any data loss or corruption with high probability. However, in these two protocols, the Server was required to send the original data to the Auditor, which would leak data to the Auditor. Furthermore, World Wide Web they also required the Auditor to store all the MACs. Therefore, both Lillibridge's and Naor's protocols are not suitable for the Third Party Auditing.

In CCS'07, Ateniese *et al.* [4] defined the provable data possession model and proposed the first publicly verifiable PDP scheme. Their scheme used RSA-based homomorphic authenticators and sampled a number of data blocks rather than the whole data file to audit the outsourced data, which can reduce the communication complexity significantly. However, in their scheme, a linear combination of sampled blocks is exposed to the third party auditor (TPA) at each auditing, which may leak the data information to the TPA. At the meantime, Juels and Kaliski [5] described a similar but stronger model: proof of retrievability (POR), which enables auditing of not only the integrity but also the retrievability of remote data files by employing spot-checking and error correcting codes. Nevertheless, their proposed scheme allows for only a bounded number of auditing services and does not support public verification.

Shacham and Waters [6] presented a publicly verifiable POR scheme and gave a comprehensive proof of security under the POR model [5]. Similar to [6],their scheme utilized homomorphic authenticators built from BLS signatures [7]. Subsequently, Erway [8], Zeng *et al.* [9], Wang *et al.* [10] proposed some similar constructions for publicly verifiable remote data integrity check, which adopted the BLS based homomorphic authenticators. With the same reason as [6], these protocols do not support data privacy. In [11], Wang *et al.* extended their scheme to be privacy preserving. The idea is to mask the linear combination of sampled blocks in the server's response with some random value. With the similar masking technique, Zhu *et al.* [12] introduced another privacy-preserving public auditing scheme. Later, Hao *et al.* [13] and Yang *et al.* [14] proposed two privacy-preserving public auditing schemes without applying the masking technique. Yuan *et al.* [15] gave a POR scheme with public verifiability and constant communication cost.

3. Watermarking Based Security Data Auditing in Cloud Storage

The digital revolution, the explosion of communication networks, and the increasingly growing passion of the general public for new information technologies lead to exponential growth of multimedia document traffic (image, text, audio, video, *etc.*). This phenomenon is now so important that insuring protection and control of the exchanged data has become a major issue. Indeed, from their digital nature, multi-media documents can be duplicated, modified, transformed, and diffused very easily. In this context, it is important to develop systems for copyright protection, protection against duplication, and authentication of content. Watermarking seems to be the alternative solution for reinforcing the security of multimedia documents.

The aim of watermarking is to include subliminal information (*i.e.*, imperceptible) in a multimedia document to ensure a security service or simply a labeling application. It would be then possible to recover the embedded message at any time, even if the document was altered by one or more nondestructive attacks, whether malicious or not. Until now, the majority of publications in the field of watermarking mainly address the copyright of still images. Other security services, such as image content authentication, are also still important. Image authentication is important in many domains: military target images, images for evidence in court, digital notaries' documents, and pharmaceutical research and quality control images. All these images have to be protected in order to avoid false judgments. In the security community, an integrity service is unambiguously defined as one, which insures that the sent and received data are identical. This binary definition can also be applicable to image, however it is too strict and not well adapted to this type of digital document. Indeed, in real life situations, images will be transformed. Their pixel values will therefore be modified but not the actual semantic meaning of the image.

3.1. System Model

An typical architecture for cloud multimedia storage is usually consists of three different entities: multimedia data owner (MDO), who has multimedia data to be stored in the cloud; cloud service provider (CSP), who provides multimedia data storage service and has enough storage space and computation resources; multimedia data auditor (MDA), who has capabilities to manage or monitor the outsourced multimedia under the delegation of MDO.

In our model the MDO at first pre-processes the multimedia file, embedding watermarking to original multimedia file, transmits the file to the CSP, and may delete its local copy. The CSP stores the file and responds to challenges issued by the MDA. Note that in our model the MDO does not require any local storing for the multimedia file, which is more suitable for multimedia application in the cloud storage environment.

3.2. Framework based on Digital Watermarking for Cloud Storage Auditing

Although the existing schemes aim at providing data storage auditing for different data storage systems, the problem of supporting copyright protection has not been addressed. But in the real environment, because of the multimedia file without copyright protection, it will hinder the large-scale use. In order to solve the problem, we define the secure features of the DSA schemes, and propose a framework based on digital watermarking of multimedia data for cloud auditing, which seamless integrate DSA and copyright protecting.

Data is usually based on the content of the digital information, thus the auditing of multimedia data can be transformed into the auditing of multimedia content. We can use watermarking technology to support the auditing of the multimedia data. Meanwhile, we can also use the watermark for the copyright protection of multimedia data. In the following we define the security requirement for multimedia data auditing in cloud storage and give the countermeasures based on watermarking. Thus a framework of auditing multimedia based on watermarking is formed.

In constructing DSA scheme in multimedia data for the following are basic requirements to be followed.

- **Unforgeability**: to ensure that there exists no dishonest cloud server that can pass the audit from MDA without indeed storing users' data intact; the property is can be obtained from a robust watermarking algorithm.
- **Unbounded use of queries**: to ensure that the MDA draws unlimited number of queries in the auditing protocol for multimedia data verification; because the MDA can detect the embedded watermarking without unlimited number, the property is can get from watermarking algorithm.
- **Copyright protection**: to ensure that the user of multimedia data has been authorized; the property is can get from a fragile or semi-fragile watermarking algorithm.

- **Recoverability**: checking correct possession of data is not enough and hence the scheme has to add some technique for data resilience; the property is can get from multimedia data recovery processing of watermarking algorithm, such as the recovery of self-embedding watermarking.
- **Dynamic operation support**: to allow the MDO block-level or file-level (if possible) operations on the data files while maintaining the same level of data correctness assurance; we can dynamically adjust multimedia and embedded watermarking to support the property.
- **Public auditability**: to allow anyone, not the MDO who originally stored the file on cloud servers, to verify the correctness of multimedia data on demand; In our multimedia data auditing for cloud storage, any users or auditor can verify the embedded watermarking, so it can be obtained.
- **Private auditability**: in some scenario, MDO who originally stored the file on cloud servers, need to designate someone to verify the correctness of multimedia data on demand.

From the above discussed, we achieve a multimedia data auditing for cloud storage framework, which can provide multimedia data security audit and copyright protection. In the next section we take image auditing of cloud storage as example to show it.

4. Self-Embedding Watermark-Based Data Auditing for Cloud Storage

The picture is a very common multimedia file. Especially mobile devices such as smart phones are getting smaller, faster, and more feature-rich. Fast proliferation of mobile cameras creates more needs in determining the security of the images since mobile devices are consumers and producers of images.

According to the frame above mentioned, we adapt a self-watermarking to construct our PDP scheme for cloud image auditing, which can simultaneously support authenticity and integrity for image content and copyright protecting in cloud storage auditing.

4.1. Watermark Generation and Embedding

Let the original image (Q) is $N\times N$. In cloud image owners make the following calculation to generate watermark for image auditing.

①.The original Q is divided into $n\times n$ sub-block without overlap. Each sub-block is recorded as OB_k, k is the serial number the sub-block, and $k=1,2,\ldots,(N/n)^2$.

②.The least significant m bits of each pixel of OB_k are set into zero. And the new sub-block is recorded as $OB_k{}'$. The process can be marked as the equality.

$$OB_k{}' = BitSet(OB_k, j, 0) \quad (1)$$

$j=1,2,\ldots,m$, $BitSet(.)$ *is setting function.*

③.Computing singular value decomposition (SVD) of $OB_k{}'$.The generated singular value is recorded as δ_k^i, i is the serial number of singular value, and $i=1,2,\ldots,n$.

④.According to the following formula to compute the norm of singular value for $OB_k{}'$, i.e. $Norm_k$.

$$Norm_k = \sqrt{\sum_{i=1}^{n}(\delta_k^i)^2} \qquad (2)$$

⑤.Extraction the parity of the highest order for $Norm_k$ and produce original robust watermark *W*. If the parity of the highest order for $Norm_k$ is even, $W_k = 0$; otherwise $W_k = 1$, W_k is the *k*-th bit of *W*.

⑥.Embedding W_k to the least significant *m* bits of every pixel for $OB_k{}'$ and getting sub-block $OB_k{}''$ with watermarking. $OB_k{}''$ is restructured and produce an image (Q') including watermark. The self-embedding process can be expressed as:

$$OB_k{}'' = BitGet(OB_k{}', j, W_k) \qquad (3)$$

From the above mentioned we know that the length of *W* is $(N/n)^2$ bits, W_k is embedded to n^2 pixels and every pixel is embedded by m bits. So the total bit number of self-embedded W_k is mn^2 and the embedding capacity of the watermarking is mN^2.Because W_k is embedded into the least significant m bits of every pixel for $OB_k{}'$, which lead to mall change, the invisibility of watermark algorithm is very good. Moreover the watermarking *W* is generated by the characteristics of the original image and has the robustness against the attack, which is called *robust watermarking*.

After the above operation, MDO will be able to upload the image Q' with watermarking to CSP for cloud storage service.

4.2. Copyright Protection of Cloud Image Service from Robust Watermarking

Image auditor MDA download image Q' from cloud service provider. And then it extracts the robust watermarking to identify copyright of the image.

①. Image Q' is divided into $n \times n$ sub-block without overlap. Each sub-block is recorded as AB_k ,*k* is the serial number the sub-block, and $k = 1,2,\ldots,(N/n)^2$.

②.The least significant *m* bits of each pixel in AB_k are set into zero. And the new sub-block is recorded as $AB_k{}'$. The process can be marked as the equality:

$$AB_k{}' = BitSet(AB_k, j, 0) \qquad (4)$$

$j = 1,2,\ldots,m$, $BitSet(.)$ is a setting function.

③.Computing singular value decomposition of $AB_k{}'$.The generated singular value is recorded as $\delta_k^i{}'$, *i* is the serial number of singular value, and $i = 1,2,\ldots,n$.

④.Computing the norm of singular value for $AB_k{}'$,i.e. $Norm_k{}'$.

$$Norm_k{}' = \sqrt{\sum_{i=1}^{n} (\delta_k^i{}')^2} \qquad (5)$$

⑤.Extraction the parity of the highest order for $Norm_k{}'$ and produce robust watermark W'. If the parity of the highest order for $Norm_k{}'$ is even, $W' = 0$; otherwise $W' = 1$.W' is the *k*-th bit of W'.

⑥.Calculating and analyzing the NC identify copyright of W' and W

$$NC = (\sum_{k=1}^{(N/n)^2} (W_k \times W_k')) / (\sqrt{\sum_{k=1}^{(N/n)^2} W_k{}^2} \times \sqrt{\sum_{k=1}^{(N/n)^2} W_k{}'^2}) \qquad (6)$$

Because the extraction of the robust watermarking w' does not original image, the watermark extraction process is blind extraction, in which the property is very suitable for PDP in cloud image storage.

4.3. Integrity and Authenticity Verification of Image Content

Image auditor download image Q' from cloud service provider and implement the following operation to verify the image content.

①. Image Q' is divided into $n \times n$ sub-block without overlap. Each sub-block is recorded as AB_k , k is the serial number the sub-block, and $k = 1,2,...,(N/n)^2$.

②.The least significant m bits of each pixel in AB_k are extracted, i.e.

$$L_k^j(r) = BitGet(AB_k, j) \tag{7}$$

$BitGet(.)$ is extraction potential function. $L_k^j(r)$ is the bit sequence of the minimum j bits for each pixel in the k-th sub-block. $j = 1, 2, \cdots, m$, and $r = 1, 2, \cdots, n^2$.

③. Contrasting the extracted robust watermark W' and $L_k^j(r)$. Image auditors verify the consistence between them. If any one bit for every j and r is not consistent, the sub-block content has been altered; otherwise the image Q' is intact.

4.4. Performance Evaluation and Security Analysis

Table 1. Experimental Results of Robustness against Attacks

	Adding noise		Cropping	
	Gaussian noise (mean is 0, variance is 0.001)	Salt and pepper noise (noise density is 0.003)	1/32 Upper Left corner	1/16 Upper Left corner

Barbara	NC=0.962;
	PSNR=29.722
		NC=0.983;
		PSNR=30.2
			NC=0.986;
			PSNR=17.551
				NC=0.962;
				PSNR=15.702

Lena	NC=0.961;
	PSNR=29.775
		NC=0.989;
		PSNR=30.6
			NC=0.981;
			PSNR=21.584
				NC=0.970;
				PSNR=17.275

Elain	NC=0.982;
	PSNR=29.844
		NC=0.994;
		PSNR=30.3
			NC=0.981;
			PSNR=23.483
				NC=0.962;
				PSNR=19.864

Zelda	NC=0.969;
	PSNR=29.610
		NC=0.981;
		PSNR=30.0
			NC=0.981;
			PSNR=14.158
				NC=0.972;
				PSNR=12.135

Our experiment is conducted using C on a system with an Intel Core 2 processor running at 2.4 GHz, 768 MB RAM, and a 7200 RPM Western Digital 250 GB Serial ATA drive with an 8 MB buffer. In experiments, 50 images, e.g., Lena, Baboon, Plane and Boats with size of 512×512, are used to evaluate the performance. The original image is divided into8×8 sub-blocks without overlap. The least significant 2 bits of each pixel are set into zero.

The length of the original robust watermark is 4096bits; the capacity of the embedding watermark in our scheme is 524288bits.The Peak signal to noise rations (PSNR) of between the original images and embedding watermark image is greater than 35dB.According to the literatures in [14-15], the scheme has excellent invisibility. Moreover we not only achieve image data possession audit but copyright protection, which is we can provide the verification of image data ownership. In table 1 we list the experimental results of robustness against attacks.

5. Conclusions

We define specially a PDP model for multimedia file, and present a framework based on digital watermarking for multimedia data storage audit service: Defining the security features of audit service for multimedia data outsourcing and the corresponding properties of digital watermarking. We propose a special provable data possession scheme based on multi-function digital watermark, which integrate image content audit service and copyright protection through a double function self-embedded watermarking scheme. It is worth noting that the presented scheme is very efficient compared with the previous PDP schemes, since only watermarking is required.

Acknowledgements

This paper is a revised and expanded version of a paper entitled [Watermark-based Provable Data Possession for Multimedia File in Cloud Storage] presented at [The 2nd International Conference on Computer, Information and Application, Angeles City, April 24 -26, 2014].

This work is supported by the NSFC (NO.61232016, 61300236, 61300237), Jiangsu Province Natural Science Research Program (NO. BK20130809, BK2012461), the prospective research project on the future Networks from Jiangsu Future Networks Innovation Institute (NO.BY2013095-4-04), the open fund project from Jiangsu Engineering Center of Network Monitoring (NO. KJR1305) and the PAPD fund. Prof. Jin Wang is the corresponding author.

References

[1] K. Yang and X. Jia, “Data storage auditing service in cloud computing: challenges, methods and opportunities”, The journal of World Wide Web, vol. 3, no. 15, **(2012)**, pp. 409-428.

[2] M. Lillibridge, S. Elnikety and A. Birrell, M. Burrows and M. Isard, “A cooperative internet backup scheme’, Proceedings of the Annual Conference on USENIX Annual Technical Conference, (**2003**) June 9-14; Berkeley, CA, USA.

[3] P. F. Oliveira, L. Lima, T. T. V. Vinhoza, J. Barros and M. Mdard, “Coding for trusted storage in untrusted networks”, IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, **(2012)**, pp. 1890–1899.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner Z. Peterson and D. Song, “Provable data possession at untrusted stores”, Proceedings of the 14th ACM Conference on Computer and Communications Security, **(2007)** October 29-November 2, Alexandria, VA, USA.

[5] A. Juels, S. Burton and J. Kaliski, “Proofs of retrievability for large files”, Proceedings of the 14th ACM Conference on Computer and Communications Security, **(2007)** October 29-November 2, Alexandria, VA, USA.

[6] H. Shacham and B. Waters, “Compact proofs of retrievability”, Journal of Cryptology, vol. 26, no. 3, **(2013)**, pp. 442–483.

[7] D. Bone, B. Lynn and H. Shacham, “Short signatures from the weil pairing”, Journal of Cryptology, vol. 17, no. 4, **(2004)**, pp. 297–319.

[8] C. Erway, A. Kupcu, C. Papamanthou and R. Tamassia, “Dynamic provable data possession”, Proceedings of the 16th ACM Conference on Computer and Communications Security, **(2009)** November 9-13, Chicago, Illinois, USA.

[9] K. Zeng, “Publicly verifiable remote data integrity”, Proceedings of the International Conference on information and Communications Security, **(2008)** October 20-22, Birmingham, UK.

[10] Q. Wang, C. Wang, J. Li, K. Ren and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing”, IEEE Transactions on Parallel and Distributed Systems ,vol. 5, no. 22 **(2011)**, pp. 847-859.

[11] C. Wang, S. S. Chow, Q. Wang, K. Ren and W. Lou, “Privacy-preserving public auditing for secure cloud storage”, IEEE Transactions on Computers, vol. 2, no. 62, **(2013)**, pp. 362–375.

[12] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu and S. S. Yau, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage", IEEE Transactions on Parallel and Distributed Systems, vol. 12, no. 23, **(2012).**

[13] Z. Hao, S. Zhong and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability", IEEE Transactions on Knowledge and Data Engineering, vol. 9, no. 23, **(2011)**, pp. 1432–1437

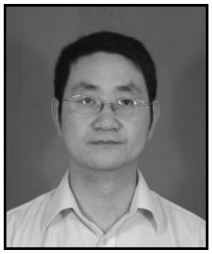
[14] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing", IEEE Transactions on Parallel and Distributed Systems, vol. 9, no. 24, **(2013)**, pp. 1717–1726.

[15] J. Yuan and S. Yu, "Proofs of retrievability with public verifiability and constant communication cost in cloud", Proceedings of the 2013 International Workshop on Security in Cloud Computing, **(2013)** December 2-5, Bristol, United Kingdom, pp. 19–26

[16] Y. tianyu, "A self-embedding image watermarking scheme with dual purpose", ActaPhotonicaSinica, vol. 6, no. 41, **(2012)**, pp. 859-867

[17] A. Niko Aidis and I. Pitas, "Asymptotically optimal detection for additive watermarking in the DCT and DWT domains", IEEE Transactions on image processing, vol. 5, no. 12, **(2003)**, pp. 563-571

Authors



Yongjun Ren, he obtained his Masters in Computer received the M.S. degree in computer science from HoHai University, China, in 2004 and PhD degree in the computer and science Department at Nanjing University of Aeronautics and Astronautics, China, in 2008.Now he is serving as a full time faculty in the computer and software Department at Nanjing University of Information science and Technology. His research interests include network security and privacy and applied cryptography with current focus on security and privacy in cloud computing, lower layer attack and defense mechanisms for wireless networks, and sensor network security.

JianShen, he received the M.E. and Ph.D. degrees in Computer Science from Chosun University, Gwangju, Korea, in 2009 and 2012, respectively. Since late 2012, he has been a Professor in the School of Computer and Software at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include computer networking, security systems, mobile computing and networking, ad hoc networks and systems, and ubiquitous sensor networks.

Jin Wang, he is a professor in the Computer and Software Institute, Nanjing University of Information Science and Technology. He received the B.S. and M.S. degree from Nanjing University of Posts and Telecommunications, China in 2002 and 2005, respectively. He received Ph.D. degree from Kyung Hee University Korea in 2010. His research interests mainly include routing protocol and algorithm design, performance evaluation and optimization for wireless ad hoc and sensor networks. He is a member of the IEEE and ACM.

Jiang Xu, he graduated as the top student in the Nanjing University of Aeronautics and Astronautics where would obtain his PhD in 2013. At the same time, he is serving as a full time faculty in the School of Computer and Software, Nanjing University of Information Science and Technology (NUIST). His research interest includes wireless communication network, wireless sensor networks and Internet of things.