A Novel Approach on Certificateless Encryption Schemes

R. Rajesh
Research Scholar
School of Information & Technology
Madurai Kamaraj University

S. Gavaskar, PhD
Assistant Professor
Bharathiar University
School of Computer Science

A. Sumithra, PhD
Associate Professor
VSB Engineering College
Technical Campus-Cbm

ABSTRACT
Security remains as a big challenge as there are many advancements as well as applications being proposed in the areas wireless adhoc networks and cloud computing. The modern field of cryptography is divided into two main areas based on the basic encryption mechanism as symmetric key cryptography and Public-key cryptography. Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. But in Public-Key method, two different but mathematically related keys are used—a public key and a private key. So comparatively the second method is more popular. Among various techniques in this method Identity-Based encryption scheme, certificateless encryption as well as certificateless signcryption scheme are gaining popular now-a-days. One of the major advantages of any identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. Certificateless encryption is a form of public-key encryption that is designed to eliminate the disadvantages of both traditional PKI-based public-key encryption scheme and identity-based encryption. The securitygoals associated with signcryption are stronger than those provided by authenticated encryption, where data authenticity suffices and non-repudiation is not required. In this article we present a review on various certificateless encryption schemes proposed for wireless adhoc networks as well as cloud computing. Finally we propose an idea of how to extend identity-based encryption scheme for multi-recipient via randomness-reuse and a hybrid mechanism for providing certificateless encryption. We are also trying to achieve secured certificateless signcryption scheme.

Keywords
Cryptography, symmetric, cipher text, encryption, decryption, certificate, security and adhoc networks.

1. INTRODUCTION
The world is now within the hands of networks. Even very much confidential data not exempting defence system information are communicated through internet. This paved the way for design of secured and efficient encryption schemes. The mathematical study of design and analysis of cryptographic algorithms is called as provable security which analyses the underlying quality of any encryption scheme [1-4]. A secret-key, or private-key, or symmetric encryption (SKE) scheme, consists of an algorithm that produces k number of keys. There is also an algorithm for encryption, which takes a message m and a key k and returns a ciphertext c. Finally it has a decryption algorithm which undoes encryption by taking the ciphertext c and the same key k and returning the message m.

An example of this scheme is one-time pad algorithm where encryption returns $c=m \oplus k$ and decryption recovers m by computing $m = c \oplus k$. Here $\oplus$ denotes the bitwise exclusive or operand: for a and b two bits, we define $a \oplus b = 0$ if a = b and 1 otherwise. Shannon [5] has also given a security proof for this scheme.

In this paper we are discussing about the key management and presented a literature review on certificateless cryptography related with networks as well as cloud computing. Especially public-key management in MANETS is having a rich literature [6-11]. Most of these schemes are based on certificate-based cryptography which needs certificate-based public-key distribution. This is not well suited when the network size increases and so comes the ID-based cryptography [12-14]. It is gaining popularity by eliminating the need for public-key and certificate. Here the nodes share a network master-key using threshold cryptography and issues ID-based private keys [15-19].

2. CERTIFICATELESS CRYPTOGRAPHY
In 2003, Al-Riyami and Paterson [20] proposed a new system known as certificateless cryptography. The basic idea of certificateless cryptography is to combine the merits of both the public key cryptography and ID-based cryptography thereby removing the drawbacks existing in these two systems. In this system, there is a trusted authority called the Key Generation Centre (KGC) which is responsible for generating a partial secret key for the users, when provided the users' identity. Every user is required to generate his/her own partial secret key.Based on these two pieces of information (partial secret keys), the user can generate the public key that needs to be published. Although this system incorporates a public key, this public key does not need to be certified as this public key has been 'implicitly' certified by the partial secret key issued by the KGC. Hence, to verify the authenticity of the public key, the KGC's public key needs to be involved. There is no key escrow problem in this model as the KGC does not know the user's secret key. The KGC can only know the partial secret key but not the complete secret key as some part of the secret key is generated by the user himself/herself.

2.1 Key Management
Key management is defined as a set of techniques and procedures that support the establishment and maintenance of keying relationships between authorized parties [4][5]. A keying relationship is the process by which network nodes share keying material that is used by cryptographic mechanisms. The keying material can include public/private key pairs, secret keys, initialization parameters, and non-

secret parameters that are supporting key management in various instances from compromised nodes and update keys from non-compromised ones. Key management for MANETs must deal with dynamic topology that is self-organized and decentralized [21-22]. It must also satisfy some requirements, such as:

- No single point of failure
- Compromise-tolerant; that is, the compromise of a certain number of nodes does not affect the security between non-compromised nodes
- Ability to revoke keys of com-promised nodes and update keys of non-compromised ones efficiently and securely
- Storage, computation, and communication efficiency.

3. LITERATURE REVIEW

Shaheena Khatoon et al [23], proposed a certificate less key management for MANET using threshold cryptography. They have presented a distributed key mechanism, where certificate less public key cryptography and threshold cryptography are combined and employed. They have proved that their method is a secured scheme for MANET as well as it eliminates the need for certificate-based public key distribution and the key escrow problem.

Certificateless Efficient Group Key Management Scheme in Mobile Adhoc Networks [24], was proposed by Sanjeev Kumar et al. They have implemented identity based cryptography for secure multicast group communication.the method reduces storage space by avoiding the usage of PKI. They have hided the public key which is visible only to the trusted nodes and thereby increasing security from crackers as well as making the encryption and decryption faster. They divided the network into groups and the leaders of the groups can have secured communication with the group key.

Preeti et al [25], in their article proposed a key management with pairing and certificate less cryptography in MANETs. They have incorporated the idea of Shamir's secret sharing scheme in their method. The master secret keys are shared some are all the nodes in the MANET. They have proposed an improved secure tripartite au-thenticated key agreement protocol . they have enhance d the key strength with some simulation mechanism. They have also presented an idea of adopting certificateless public key encryp-tion (CL-PKE) schemes over mobile ad hoc network (MA-NET).

Fagen Li et al [26], has proposed a scheme titled key management using certificateless public key cryptography in ad hoc networks. They have presented a distributed key management approach by using the recently developed concepts of certificateless public key cryptography and threshold secret sharing schemes.They have assured that their method does not have the built-in key escrow feature of ID-PKC. In their method the KGC computes a partial private key from the user's identity and a master key. The user then combines the partial private key with some secret information to generate the actual private key.

Sattam S. Al-Riyami et al [20], has presented a certificateless public key cryptography which is a model for the use of public key cryptography that is intermediate between traditional PKI and ID-PKC. They have proved that their encryption scheme is secure in a new and appropriate model, given the hardness of an underlying computational problem. They have showed how their concept can be realized by specifying a certificateless public key encryption (CL-PKE) scheme that is based on bilinear maps.

Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks was proposed by Yanchao Zhang et al [27]. In their method in order to satisfy the demand for private keys during network operation, they have employed the secret-sharing technique to distribute a system master-key among a preselected set of nodes, called D-PKGs, which offer a collaborative private-key-generation service. As well as in addition to it they have also identified the pinpoint attacks against D-PKGs. For this they have also proposed anonymizing D-PKGs as the countermeasure. They have determined optimal secret sharing parameters to achieve the maximum security.

Bhavesh Rahulkar et al [28] has proposed a scheme called " A Two Layer Encryption Approach to Secure Data Sharing in Cloud Computing" in which they have given double encryption for securely outsourcing the data in cloud. They have made use of RSA algorithm of asymmetric key approach to resolve the key escrow problem and data revealing problem. Their method has certificate for the user and two layer encryption where one is done by the cloud and the other by the user thereby increasing the security.

Securing Mobile Ad Hoc Networks with Certificateless Public Keys has been presented by the authors Yanchao Zhang et al [17]. They have discussed about key management in their article as well as presented an ID-based key management scheme which is a combination of ID and threshold cryptography. In addition they have also provided guidelines about how to choose the secret sharing parameters that are used with the cryptography so as to improve security and robustness.

4. CONCLUSION

In this paper a detailed survey has been done on the encryption schemes especially on those which are based on the certificateless public keys. The wide application of networks has forced the people communicating through it in all the ways for exchanging any kind of information including more confidential messages. This gives rise to the need for security as well as avoiding complexity. So based on this survey it is concluded that there is always a need for efficient and secured way of communication which made us to focus on finding an innovative method of communication which eliminates the existing problems to an extent.

5. REFERENCES

[1] K. Kurosawa. Multi-Recipient, 2002, " Public-Key Encryption with Shortened Ciphertext", Springer-Verlag, LNCS 2274:48–63.

[2] H. Krawczyk, 1994, "Secret Sharing Made Short", Springer-Verlag, LNCS 773 : 136–146.

[3] A. Khalili, J. Katz, and W. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," 2003, IEEE Workshop on Security and Assurance in Ad Hoc Networks, pp. 342–346.

[4] A. Menezes, P. van Oorschot, and S. Vanston, "Handbook of Applied Cryptography", Boca Raton, FL: CRC Press, Oct. 1996.

[5] C. Shannon, 1949, "Communication Theory of Secrecy Systems", Bell System Technical Journal, Vol. 28, No. 2, pp. 656–715.

[6] L. Zhou and Z. J. Haas, 1999,"Securing ad hoc networks," IEEE Network, vol. 13, no. 6, pp. 24–30.

[7] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, 2001,"Providing robust and ubiquitous security support for mobile ad hoc networks," in IEEE ICNP, Riverside, CA, pp. 251–260.

[8] M. Narasimha, G. Tsudik, and J. H. Yi, 2003, "On the utility of distributed cryptography in p2p and manets: the case of membership control," IEEE ICNP, pp. 336–345.

[9] S. Yi and R. Kravets, 2003, "MOCA: Mobile certificate authority for wireless ad hoc networks," 2nd Annual PKI Research Workshop (PKI03), pp. 65–79.

[10] M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, 2004, "A cluster-based security architecture for ad hoc networks," IEEE INFOCOM, pp. 2404–2413.

[11] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, 2004, "URSA: ubiquitous and robust access control for mobile ad hoc networks," IEEE/ACM Trans Networking, vol. 12, no. 6, pp. 1049–1063.

[12] A. Shamir, 1984 "Identity based cryptosystems and signature schemes," CRYPTO'84, Santa Barbara, CA, pp. 47–53.

[13] A. Khalili, J. Katz, and W. Arbaugh, 2003, "Toward secure key distribution in truly ad-hoc networks," in IEEE Workshop on Security and Assurance in Ad Hoc Networks, pp. 342–346.

[14] H. Deng, A. Mukherjee, and D. Agrawal, 2004,"Threshold and identitybased key management and authentication for wireless ad hoc networks," International Conference on Information Technology: Coding and Computing (ITCC'04), pp. 107–111.

[15] N. Saxena, G. Tsudik, and J. H. Yi, 2004, "Identity-based access control for ad hoc groups," Int. Conf. Inform. Security Cryptology (ICISC'04), pp. 107–111.

[16] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang, 2006, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys", IEEE transactions on dependable and secure computing, vol. 3, pp..1-15.

[17] A. Shamir, 1979, "How to share a secret," Comm. ACM, vol. 22, no. 11, pp. 612–613.

[18] Y. Desmedt and Y. Frankel, 1989, "Threshold cryptosystems," in CRYPTO'89, pp. 307–315.

[19] S.S.Al-Riyami K.G.Paterson. 2003, "Certificateless public key cryptography", page 452C473. C.S. Laih (ed.) Advances in Cryptology C Asiacrypt, Lecture Notes in Computer Science, .

[20] Samba Sessay, Zongkai Yang and Jianhua He , 2004"A Survry on Mobile Ad Hoc Wireless Network, " Information Technology Journal 3(2):168-175.

[21] van der Merwe, J., Dawoud, D., and McDonald, 2007 " A survey on peer-to-peer key management for mobile ad hoc networks," ACM Comput. Surv. 39, 1.

[22] Shaheena Khatoon and Balwant Singh Thakur, 2015, " Certificate less key management scheme in manet using threshold cryptography", International Journal of Network Security & Its Applications (IJNSA) Vol.7, pp.55-59.

[23] Sanjeev Kumar Rana and Manpreet Singh, 2011, "Certificateless Efficient Group Key Management Scheme in Mobile Adhoc Networks", International Journal of Computer Science Issues, Vol. 8, pp.343-351.

[24] Preeti Sheoran and Virender Kumar , "Key management with pairing and with certificateless cryptography in manets", International Journal of Advanced Computer Technology (IJACT), Vol. 3., pp.27-35.

[25] Fagen Li, Masaaki Shirase1, and Tsuyoshi Takagi1, 2008, "Key Management Using Certificateless Public Key Cryptography", International Federation for Information Processing, pp.116-126.

[26] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang and Younggoo Kwon, 2005, "AC-PKI: Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks", IEEE, pp. 3515-3519.

[27] Mr. Bhavesh Rahulkar , Mr. Praveen Shende, 2013, " A Two Layer Encryption Approach to Secure Data Sharing in Cloud Computing", International Journal of Advanced Research in Computer Engineering & Technology, Vol 2, pp.3252-3254.