Practical Escrow-free Identity-based Mutual Authentication and Key Management without Pairings

Project PN-II-PT-PCCA-2013-4-1651

Phase I: Study and Analysis

December 7, 2014

Contents

Part I
Summary of Phase I

The first phase of the project, *Study and Analysis*, is dedicated to the study and analysis of the authentication and key management techniques in technologies such as VoIP and SONs (as well as other technologies related to these). Our study shows the limitations of authentication and key management in these technologies.

The studies developed in this phase of the project are included into two research reports:

1. S. Iftene, F.L. Ţiplea: *Authentication and Key Management in VoIP and SONs*, Research Report, Project PN-II-PT-PCCA-2013-4-1651, "Alexandru Ioan Cuza" of Iasi, 2014

2. F.L. Ţiplea, S. Iftene, A.M. Nica: *Identity-based Cryptography*, Research Report, Project PN-II-PT-PCCA-2013-4-1651, "Alexandru Ioan Cuza" of Iasi, 2014

The first research report (RR01), *Authentication and Key Management in VoIP and SONs*, focuses on the authentication and key management problems in VoIP and SONs, highlighting the most relevant features and limitations of them. The second research report (RR02), *Identity-based Cryptography*, aims at discussing one of the most promising key management technologies which has real chances to be a substitute of the Public-Key Infrastructure (PKI) technology. Moreover, RR02 also discusses attribute-based encryption, where access structures defined by Boolean circuits are central.

We consider that the two research reports mentioned above cover very well the objectives of the Phase I of the project, highlighting the most important aspects needed for the second phase.

Part II
Scientifical and Technical Description

Mutual Authentication and Key Management are crucial components of all the security techniques incorporated in the nowadays communication technologies, such as IPsec, SSL&TLS, Voice over IP (VoIP), and Self-organizing Networks (SONs). The existing techniques are mainly based on public key infrastructures (PKI) which have many practical shortcomings highlighted by many researchers and practitioners, that make them impractical for large systems or highly dynamic systems or systems with limited computational power (such as mobile ad-hoc or sensor networks). This is because:

1. Each node in a network (system) is assumed to have a public key signed by a Certifying Authority (CA). This requirement is considerable costly for the node;

2. Almost each PKI based protocol assumes that each node knows the certificate of the destination before it sends the message. Caching certificates rises problems with trust and storage, and this adds large overhead on local storage in large systems or systems with limited computational power;

3. In highly dynamic systems, with nodes constantly joining and leaving the network, certificates can quickly become invalidated and therefore the management process become complex.

All these show that the PKI solution to key management is not very adequate, and better solutions are needed to:

1. Simplify public key distribution and management;

2. Simplify access control;

3. Secure messages and strength the (mutual) authentication in a more lightweight and clean way compared to certificate-based approaches.

The next sections will discuss in more details the authentication and key management mechanisms in these technologies.

1 VoIP and SONs: Authentication and Key Management

1.1 VoIP

Voice over IP (VoIP), which is a generic term given to any technology that enables voice communication over the Internet such as Skype or voice aware IM software, is growing dramatically worldwide.

Standardised VoIP is a combination of four standards:

1. Session Initiation Protocol (SIP) [RFC3261];
2. Session Description Protocol (SDP) [RFC2327];
3. Real-time Transport Protocol (RTP) [RFC3550];
4. The Secure Real-time Transport Protocol (SRTP) [RFC3711].

SIP is a text based protocol with similar formatting to HTTP capable of operating on TCP or UDP and handles all the signaling requirements of a VoIP session. The role of SIP is to establish streaming connection between hosts using two primary messages exchanges: INVITE consisting of a four way handshake (INVITE, RINGING, OK, and ACK) and REGISTER consisting of (REGISTER, Unauthorized, and OK). SIP has also been chosen by the Third-Generation Partnership Project (3GPP) as the protocol for the multimedia applications in 3G mobile networks.

SDP is a descriptive language used to describe the attributes of a media session being established or reconfigured. SDP messages are attached to the INVITE and OK messages during a SIP call establishment. The message is made up of a number of key value pairs called attributes. These attributes include what codecs are available and the IP addresses and port numbers of stream endpoints.

RTP on the other hand is a UDP based streaming protocol capable of using arbitrary profiles and parameters. It handles buffering, jitter correction and is reliant upon SIP to know which profile and codecs to use and which ports to utilise for the media stream.

SRTP is a later extension to RTP which provides cryptographic support for privacy and integrity (using Advanced Encryption Standard (AES) in Counter Mode (CM)).

Although SRTP has been intended as a security extension of RTP, VoIP still lacks some basic security features with respect to authentication and key management:

1. the default authentication method used in SIP is HTTP Digest authentication (see Figure 1) which is vulnerable to many forms of attacks (see RFC2617);

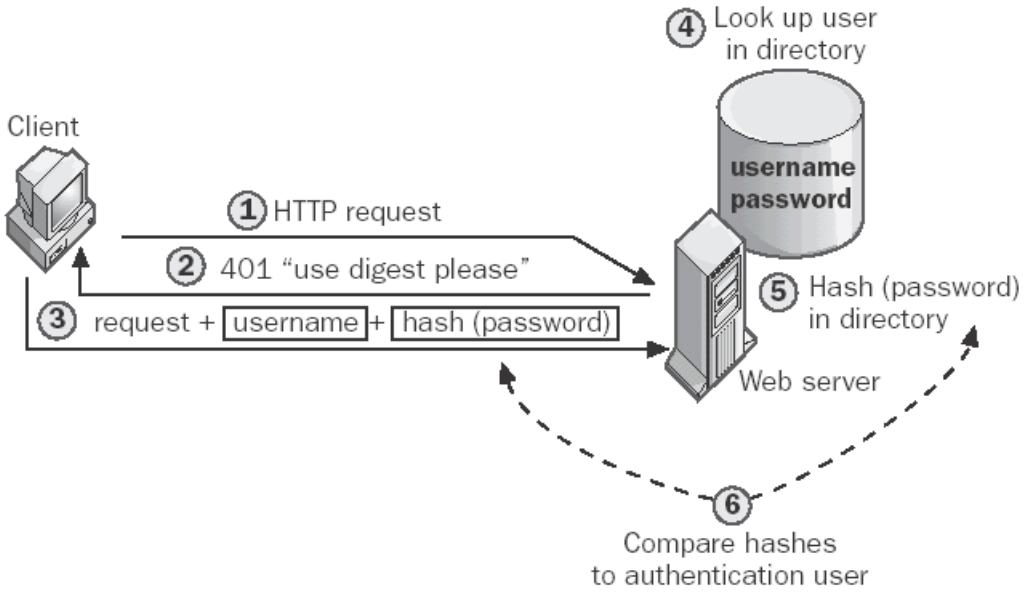

Figure 1: HTTP Digest authentication (from Microsoft®Encyclopedia of Security)

2. SIP allows encryption using S/MIME, but S/MIME is dependent upon a Certifying Authority (CA) and accompanying Public Key Infrastructure (PKI), and therefore limited by the adoption of such a system. Moreover, S/MIME is likely to be too heavy for resource constrained handsets;

3. SRTP provides cryptographic and integrity checks to the media stream through the use of the Advanced Encryption Standard (AES) in Counter Mode (CM). However, the master key that is required by SRTP has no means of being established between two previously unknown parties.

A recent comprehensive survey on SIP authentication and key agreement is given in [16]. According to this, the existing schemes classified in:

1. Password Authenticated Key Exchange (PAKE) based schemes - most of these schemes combine Diffie-Hellman protocol with a certain preshared password technique in order to avoid the Man-In-The-Middle (MITM) attacks. We only mention [31];

2. Hash and symmetric encryption based schemes - based on several elaborated keyed hash functions/hash chains or block cryptosystems (and preshared information). We only mention [2], [11], and [29];

3. Public Key Cryprography (PKC) based schemes - which assume the existence of a Public Key Infrastructure (PKI). We only mention [28] and [17];

4. Identity (ID) based schemes - which combine certain ID based signatures (used for authentication) with certain ID based key agreement protocols. We mention [23], [13], and [22]. The main problem of these schemes is the key escrow. Certificate-less cryptography based solutions (as [30] and [21]) for SIP authentication and key agreement avoid this problem (the private key of an user is derived from a partial private key provided by KGC (PKG) and some secret information known only to the user - in this way, KGC (PKG) does not have access to the user's private key) but in this case the public key of an user is no longer computable only from the user's identity.

The security and performance of all mentioned schemes are discussed and compared in [16] - the conclusion is that the ID based schemes are the best from the security viewpoint, but also that their performance is inversely proportional to the security features, mainly due to the fact that the computational cost for a pairing computation is still expensive compared to a single or double exponentiation in a finite field. Thus, finding efficient ID based schemes which are not based on bilinear pairings is a very important task and we hope that schemes based on quadratic residues may be appropriate from the performance viewpoint.

1.2 SONs

Self-organizing Networks (SON) such as Wireless Mobile Ad-hoc Networks (MANET), Wireless Sensor Networks (WSN) (including Wireless Body Sensor Networks (WBSN)), Wireless Mesh Networks (WMN), and Vehicular Ad-hoc Networks (VANET) have attracted a lot of attention from both the research and industry communities, due their tremendous applications in military, disaster relief and emergency or healthcare environments.

There is a great need for authentication and key management in Self-organizing Networks. Several factors as (high) dynamic topology, lack of management nodes, or resource-constrained nodes make this task very challenging.

According to [27], the existing schemes may be classified in:

1. Symmetric key schemes;
2. Asymmetric key schemes (which include ID-based schemes);
3. Hybrid schemes.

Although symmetric schemes require significantly less processing than asymmetric ones, they are not scalable, demanding that a certain keying material must be shared either by a secure pre-established channel or before network formation. Therefore, the classical symmetric schemes are difficult to apply in such networks. On the other hand, traditional public key solutions require a trusted entity to issue certificates and ensure that public keys belong to an identity. However, establishing a trusted entity in a Self-organizing Network is a challenge due to their decentralized organization and lack of trust model. In hybrid schemes, symmetric cryptography is combined with the asymmetric one in order to take advantage of each category. For example, in Zone-Based Key Management Scheme, the nodes are partitioned in zones and symmetric key management is used intra or inside a zone and asymmetric key management is used for inter-zone security.

ID based schemes are surveyed in [26, 33]. The main advantages of ID based solutions are the simpler key management process and the reduced memory storage cost compared to traditional public key methods (because the nodes must maintain only the PKG parameters, not the public key of all other nodes). The major problem with ID based schemes is that the private key of all users must be known by the PKG. In conventional networks this is not an issue, but in Self-organizing Networks in which the PKG must be distributed or emulated by an arbitrary entity, this might be a major issue. It also may require a safe channel to exchange private keys with each node (or these keys need to be pre-distributed/pre-installed, as in sensors case). Also, ID-based schemes lack anonymity and privacy preservation, as public keys are directly derived from the identity of the nodes (which may lead to clandestine tracking).

Interestingly, the characteristics of these networks may naturally eliminate the key escrow problem (inherited from ID based blocks). More exactly, due to (high) dynamic topology, which implies that specialized nodes (as routers, certification authorities (CA), public key generators (PKG), key generation centers (KGC))

do not exist, the role of PKG must be distributed, i.e., the nodes themselves will participate in private key generation of a node. *Threshold* ID-based schemes combine (dealer-free) secret sharing with certain ID-based schemes - in this case, the master key of PKG is shared among the existing nodes and it is never explicitly reconstructed - thus, the private key of an user cannot be found by unauthorized groups. We mention the schemes from [15], [12], [19]. All these schemes use Shamir's secret sharing scheme. It will be interesting to develop ID based schemes using Asmuth-Bloom secret sharing scheme (which is based on the Chinese Remainder Theorem). It is worth mentioning that there already exist approaches based on the Chinese Remainder Theorem (see, for example, [24]) but they are not ID based. Also, threshold ID based schemes with non-threshold access structures for multiple/distributed PKGs may be considered - a compartmented scheme has been recently proposed in [4]; we may focus on hierarchical access structures.

2 Identity-based Cryptography

A new approach to key management was recently developed with the emerging field of Identity-based Cryptography (IBC). IBC was proposed in 1984 by Shamir [25] who formulated its basic principles but he was unable to provide a solution to it, except for an identity-based signature (IBS) scheme. In 2000, Sakai, Ohgishi and Kasahara [SaOK2000] have proposed an identity-based key agreement (IBKM) scheme, and one year later, Cocks [10] and Boneh and Franklin [8] have proposed the first identity-based encryption (IBE) schemes. Cocks' solution is based on quadratic residues. It encrypts a message bit by bit and requires $2 \log n$ bits of cipher-text per bit of plain-text. The scheme is quite fast but its main disadvantage is the ciphertext expansion. The Boneh and Franklin's solution is based on bilinear maps. Moreover, Boneh and Franklin also proposed a formal security model for IBE, and proved that their scheme is secure under the Bilinear Diffie-Hellman (BDH) assumption.

An IBE consists of four probabilistic polynomial-time (PPT) algorithms: Set-Up, Key-Gen, Encrypt, and Decrypt. The first one takes as input a security parameter and outputs the system public parameters together with a master key. The Key-Gen algorithm takes as input an identity ID together with the public parameters and the master key and outputs a private key associated to ID. The Encrypt algorithm, starting with a message m, an identity ID and the public parameters, encrypts m into some cypherthext c (the encryption key is ID or some binary string derived from ID). The last algorithm decrypts c into m by using

the private key associated to ID. A standard scenario on using IBE is as follows. Whenever Alice wants to send a message m to Bob, she encrypts m by using Bob's identity ID(B). In order to decrypt the message received from Alice, Bob asks the Private-Key Generator PKG to deliver him the private key associated to ID(B).

It is interesting to compare how the three key management systems (symmetric, public, and identity-based key management systems) meet the six requirements formulated by *Voltage Security* (`http://www.voltage.com/`).

As the identity-based key management (IBKM) is viewed as the future of key management systems and our project focuses on it, we will describe below the main shortcomings of the identity-based key management existing techniques:

1. The Key Escrow Problem all identity-based cryptographic schemes have an inherent weakness, the key escrow property. In IBC, the PKG issues private keys to all users using its master secret key. As a result, the PKG can decrypt or sign any messages. In terms of encryption, this property might be useful in some situations where user's privacy can possibly be limited, for example, due to the involvement in the crime, the user's message should be opened by a court order. However, in terms of signature, this key escrow property is not desirable at all since the non-repudiation property is one of the essential requirements of digital signature schemes. Some significant steps were performed along alleviating this problem [1, 5, 18, 32]. But, the solutions are still further from being good enough and so, the main question of whether it is possible or not to construct an efficient IBC scheme that does suffer from the key escrow problem still remains;

2. The Identity Disclosure Problem closely related to the key escrow problem is the identity disclosure problem. Due to the intrinsic nature of identity-based cryptography, the identity of agents (users, nodes in a network) risks a potential disclosure to all others. In some systems this is not desirable at all. Not too much is known about this problem [20], and a deep insight into the problem is necessary;

3. The Revocation Problem in public key cryptography, the revocation of the public key is a big problem in the sense that the users who want to encrypt messages or to verify signatures should first check whether the concerning public keys have been revoked or not. To solve this problem, a PKI should maintain a Certificate Revocation List (CRL) whose management may be one of the factors that slows down the deployment of PKI. In identity-based encryption schemes, this problem no longer exists as any identities can

be served as public keys. However, another kind of revocation problem occurs in identity-based cryptography. Suppose that Bob wants others to use his email address to encrypt messages. But, suppose that the private key associated with Bob's email address has been compromised, so he cannot use his email address as a public key any more. Does he have to obtain a new email address? A solution would be to concatenate the e-mail address together with some information about the current date or time. Anyway, this is a particular solution and a more general approach is needed;

4. Efficiency Problem Identity-based cryptographic schemes proposed so far in the literature can be categorized into three classes: schemes based on quadratic residues, schemes based on bilinear pairings, and schemes based on lattices. A few information about them follow:

   (a) The first class mainly refers to the IBE scheme proposed by Cocks [10] and some of its variations [9, 14, 6]. The original Cocks' scheme is not very efficient because each bit of plaintext is encrypted by 2log(n) bits of cyphertext (n is the public parameter). Boneh, Gentry, and Hamburg [9] obtained a scheme which improves the space efficiency, but the encryption and decryption efficiencies are worse. Jhanwar and Barua focused later [14] on improving the Boneh-Gentry-Hamburg's variant with respect to encryption and decryption. Revising the Cocks' scheme, Ateniese and Gasti proposed a new variant which also provides anonymity and has good efficiency in comparison with the Boneh-Franklin scheme.

   (b) The schemes based on bilinear pairings seem to be the most efficient for the time being. Recently, techniques for speeding up the bilinear pairing computation have been developed (see [7] for a good survey). However, the computational cost for the pairing computation is still expensive compared to a single or double exponentiation in a finite field;

   (c) In the lattice based approach (see [3]), the IBE schemes are usually based on a technique called Pre-Image Sampling, and the security is based on the Learning with Errors problem. The main advantages of these schemes consist of the fact that they do not require multi-precision arithmetic and no quantum algorithms for solving lattice problems are known. However, the key size and cyphertext size are far too large compared to the schemes in the first two classes.

3 Conclusions

The results obtained during the first phase consist of two research reports, covering the authentication and key management in VoIP and SONs, as well as identity-based cryptography together with its problems (such as key-escrow and construction of ABE schemes for general Boolean circuits). These completely cover the proposed outputs of Phase I. We thus consider that the objectives of the Phase I of the project have been completely reached, preparing the way for the second phase.

References

[1] In Jean-Jacques Levy, ErnstW. Mayr, and JohnC. Mitchell, editors, *Exploring New Frontiers of Theoretical Informatics*, volume 155 of *IFIP International Federation for Information Processing*. 2004.

[2] *Telecommunication Systems*, 36(4), 2007.

[3] In Henri Gilbert, editor, *Advances in Cryptology EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*. 2010.

[4] An ID-based signcryption scheme with compartmented secret sharing for unsigncryption. *Information Processing Letters*, 115(2):128 –133, 2015.

[5] S. S. Al-Riyami, J. Malone-Lee, and N. P. Smart. Escrow-free encryption supporting cryptographic workflow. *Int. J. Inf. Secur.*, 5(4):217–229, September 2006.

[6] Giuseppe Ateniese and Paolo Gasti. Universally anonymous ibe based on the quadratic residuosity assumption. In *Proceedings of the The Cryptographers' Track at the RSA Conference 2009 on Topics in Cryptology*, CT-RSA '09, pages 32–47, Berlin, Heidelberg, 2009. Springer-Verlag.

[7] Lynn B. *On the implementation of Pairing Based Cryptosystems*. PhD thesis, Stanford University, 2007.

[8] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, pages 213–229, London, UK, UK, Aug. 2001. Springer-Verlag.

[9] Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient identity based encryptionwithout pairings. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '07, pages 647–657, Washington, DC, USA, 2007. IEEE Computer Society.

[10] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, pages 360–363, London, UK, UK, Dec. 2001. Springer-Verlag.

[11] Italo Dacosta and Patrick Traynor. Proxychain: Developing a Robust and Efficient Authentication Infrastructure for Carrier-scale VoIP Networks. In *Proceedings of the 2010 USENIX Conference on USENIX Annual Technical Conference*, pages 10–10, 2010.

[12] Hongmei Deng, A. Mukherjee, and 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 2004)*, volume 1, pages 107–111 Vol.1, 2004.

[13] Kyusuk Han, Chan Yeob Yeunand, and Kwangjo Kim. Design of Secure VoIP using ID-Based Cryptosystem. In *Proceedings of the 2008 Symposium on Cryptography and Information Security (SCIS 2008)*, pages 22–25, 2008.

[14] Mahabir Prasad Jhanwar and Rana Barua. A variant of boneh-gentry-hamburg's pairing-free identity based encryption scheme. In *Inscrypt*, pages 314–331, 2008.

[15] A. Khalili, J. Katz, and W.A. Arbaugh. Toward secure key distribution in truly ad-hoc networks. In *Proceedings of the 2003 Symposium on Applications and the Internet*, pages 342–346, 2003.

[16] H.H. Kilinc and T. Yanik. A Survey of SIP Authentication and Key Agreement Schemes. *IEEE Communications Surveys Tutorials*, 16(2):1005–1023, Second Quarter 2014.

[17] L. Kong, V.B. Balasubramaniyan, and M. Ahamad. A lightweight scheme for securely and reliably locating sip users. In *Proceedings of the 1st IEEE Workshop on VoIP Management and Security*, pages 9–17, April 2006.

[18] Yu Long, Zheng Gong, Kefei Chen, and Shengli Liu. Provably secure identity-based threshold key escrow from pairing. *International Journal of Network Security*, 8:227–234, 2009.

[19] Xixiang Lv, Hui Li, and Baocang Wang. Virtual private key generator based escrow-free certificateless public key cryptosystem for mobile ad hoc networks. *Security and Communication Networks*, 6(1).

[20] Marco Casassa Mont and Pete Bramhall. Ibe applied to privacy and identity management trusted. *HP Labs*, 2003, 2003.

[21] Liang Ni, Gongliang Chen, and Jianhua Li. A Pairing-Free Identity-Based Authenticated Key Agreement Mechanism for SIP. In *Proceedings of the 2011 International Conference on Network Computing and Information Security (NCIS),*, volume 1, pages 209–217, 2011.

[22] H. Kupwade Patil and D . Willis. Identity Based Authentication in the Session Initiation Protocol. https://tools.ietf.org/html/draft-kupwade-sip-iba-00, 2008.

[23] J. Ring, K.-K. Raymond Choo, E. Foo, and M. Looi. A New authentication Mechanism and Key Agreement Protocol for SIP Using Identity-based Cryptography. In *Proceedings of AusCERT R&D Stream*, pages 61–72, 2006.

[24] 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 *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB 2009)*, pages 258–262, 2009.

[25] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 47–53, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[26] E. Silva, A. Dos Santos, L.C.P. Albini, and M.N. Lima. Identity-based key management in mobile ad hoc networks: techniques and applications. *IEEE Wireless Communications*, 15(5):46–52, 2008.

[27] E. Silva, A. Dos Santos, L.C.P. Albini, and M.N. Lima. A review on key management schemes in manet. *IEEE Wireless Communications*, 3(4):165–172, 2012.

[28] R. Srinivasan, V. Vaidehi, K. Harish, K. Lakshmi Narasimhan, S. Lokeshwer Babu, and V. Srikanth. Authentication of Signaling in VoIP Applications. In *Proceedings of the 2005 Asia-Pacific Conference on Communications*, pages 530–533, 2005.

[29] Cui Tao, Gao Qiang, and He Baohong. A lightweight authentication scheme for session initiation protocol. In *Proceedings of the International Conference on Communications, Circuits and Systems (ICCCAS 2008)*, pages 502–505, 2008.

[30] Fengjiao Wang and Yuqing Zhang. A New Provably Secure Authentication and Key Agreement Mechanism for SIP Using Certificateless Public-Key Cryptography. In *Proceedings of the 2007 International Conference on Computational Intelligence and Security*, pages 809–814, 2007.

[31] Eun-Jun Yoon and Kee-Young Yoo. A New Authentication Scheme for Session Initiation Protocol. In *Proceeding of the International Conference on Complex, Intelligent and Software Intensive Systems (CISIS '09)*, pages 549–554, March 2009.

[32] Tsz Hon Yuen, Willy Susilo, and Yi Mu. How to construct identity-based signatures without the key escrow problem. *Int. J. Inf. Secur.*, 9(4):297–311, August 2010.

[33] Kuo Zhao, Longhe Huang, Hongtu Li, Fangming Wu, Jianfeng Chu, and Liang Hu. A Survey on Key Management of Identity-based Schemes in Mobile Ad Hoc Networks. *Journal of Communications*, 8(11):768–779, 2013.