ISSN:0975-9646

A Secure Architecture for Anonymizer Networks

K.RAVINDRANATH [1], B.V.S.N CHAITANYA [2], K.KRISHNA CHAITANYA [3], G.ANIL REDDY [4], B.HARISH [5]

Department of Information Science and Technology, KLUniversity, Vaddeswaram, Guntur, Andhra Pradesh, India

***Abstract* - Anonymity has received increasing attention in the literature due to the users' awareness of their privacy nowadays. Anonymity provides protection for users to enjoy network services without being traced. While anonymity-related issues have been extensively studied in payment-based systems such as e-cash and peer-to-peer (P2P) systems, little effort has been devoted to wireless mesh networks (WMNs). On the other hand, the network authority requires conditional anonymity such that misbehaving entities in the network remain traceable. Here, we propose security architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users for network authorities in WMNs. The proposed architecture strives to resolve the conflicts between the anonymity and traceability objectives, in addition to guaranteeing fundamental security requirements including authentication, confidentiality, data integrity, and non repudiation.**

Index Terms—Anonymity, Traceability, Pseudonym, Misbehavior, Revocation, Wireless Mesh Network (WMN).

1 INTRODUCTION

Wireless Mesh Network (WMN) is a promising technology and is expected to be widespread due to its low investment feature and the wireless broadband services it supports, attractive to both service providers and users. However, security issues inherent in WMNs or any wireless networks need be considered before the deployment and proliferation of these networks, since it is unappealing to subscribers to obtain services without security and privacy guarantees. Wireless security has been the hot topic in the literature for various network technologies such as cellular networks [4], wireless local area networks (WLAN) [5], wireless sensor networks [6], [7], mobile ad hoc networks (MANETs) [8], [9], and vehicular ad hoc networks (VANETs) [10]. Recently, new proposals on WMN security [11], [12] have emerged. In [11], the authors describe the specifics of WMNs and identify three fundamental network operations that need to be secured. We [12] propose an attack-resilient security architecture (ARSA) for WMNs, addressing countermeasures to a wide range of attacks in WMNs. Due to the fact that security in WMNs is still in its infancy as very little attention has been devoted so far [11], a majority of security issues have not been addressed and are surveyed in [13]. Anonymity and privacy issues have gained considerable research effort in the literature [1], [2], [10], [12] [14] [16], which have focused on investigating anonymity in different context or application scenarios. One requirement for anonymity is to unlink a user's identity to his or her specific activities, such as the anonymity fulfilled in the untraceable e-cash systems [1], [14] and the P2P payment systems [2], [15], where the payments cannot be linked to the identity of a payer by the bank or broker.

2 PRELIMINARIES

2.1 IBC from Bilinear Pairings

ID-based cryptography [3](IBC) allows the public key of an entity to be derived from its public identity information such as name, email address, etc., which avoids the use of certificates for public key verification in the conventional PKI (public key infrastructure) [18]. Boneh and Franklin [19] introduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically, let $G1$ and $G2$ be an additive group and a multiplicative group, respectively, of the same prime order p. Discrete logarithm problem (DLP) is assumed to be hard in both $G1$ and $G2$. Let P denote a random generator of $G1$ and

$e: G1 £ G1 ! G2$ denote a bilinear map constructed by modified Weil or Tate pairing with the following properties:

1) Bilinear: $e(aP; bQ) = e(P;Q)ab$, $8P;Q\ 2\ G1$ and $8a; b\ 2\ Z¤\ p$, where $Z¤\ p$ denotes the multiplicative group of Zp, the integers modulo p. In particular, $Z¤\ p = fx\ j\ 1 · x · p\ ¡\ 1g$ since p is prime.

2) Non-degenerate: $9P;Q\ 2\ G1$ such that $e(P;Q)\ 6= 1$.

3) Computable: there exists an efficient algorithm to compute $e(P;Q)$; $8P;Q\ 2\ G1$.

2.2 Blind Signature

Blind signature is first introduced by Chaum [17]. In general, a blind signature scheme allows a receiver to obtain a signature on a message such that both the message and the resulting signature remain unknown to the signer. We refer the readers to [20] for a formal definition of a blind signature scheme, which should bear the properties of verifiability, unlinkability, and unforgeability according to [17]. Brands [21] developed the first restrictive blind signature scheme, where the restrictiveness property is incorporated into the blind signature scheme such that the message being signed must contain encoded information.

As the name suggests, this property restricts the user in the blind signature scheme to embed some account related secret information into what is being signed by the bank (otherwise the signing will be unsuccessful), such that this secret can be recovered by the bank to identify a user if and only if he double spends. The restrictiveness property is essentially the guarantee for traceability in the restrictive blind signature systems. Partial blind signature schemes [22], [23] allow the resulting signature to convey publicly visible information on common agreements

between the signer and the signee. This is useful when certain information in the signature needs to be reviewed by a third party. One example is the common agreements, the visibility of which enables the intermediate parties who examine the signature, to first check the compliance of the signee to the items specified in the agreements, before proceeding to the verification of the signature and other operations.

3 SYSTEM MODEL

3.1 Definitions

Anonymity (Untraceability): The anonymity of a legitimate client refers to the untraceability of the client's network access activities. The client is said to be anonymous if the TA or the gateway, or even the collusion of the two cannot link the client's network access activities to his real identity. *Traceability*: A legitimate client is said to be traceable if the TA is able to link the client's network access activities to the client's real identity *if and only if* the client misbehaves, i.e., one or both of the following occurs: ticket-reuse and multiple-deposit.

Ticket-reuse: one type of misbehavior of a legitimate client that refers to the client's use of a depleted ticket (*val*=0).

Multiple-deposit: one type of misbehavior of a legitimate client that refers to the client's disclosure of his valid ticket and associated secrets to unauthorized entities or clients with misbehavior history, so that these coalescing clients can gain network access from different gateways simultaneously.

Collusion: the colluding of malicious TA and gateway to trace a legitimate client's network access activities in the TA's domain (i.e., to compromise the client's anonymity).

Framing: a type of attack mounted by a malicious TA in order to revoke a legitimate client's network access privilege. In this attack, the TA can generate a false account number and associate it with the client's identity. The TA can then create valid tickets based on the false account number and commit fraud (i.e., misbehave). By doing so, the TA is able to falsely accuse the client to have misbehaved and to revoke his access right.

3.2 Network Architecture

Consider the network topology of a typical WMN depicted in Fig. 1. The wireless mesh backbone consists of mesh routers and gateways interconnected by ordinary wireless links (shown as dotted curves). Mesh routers and gateways serve as the access points of the WMN and the last resorts to the Internet, respectively. The hospital, campus, enterprise and residential buildings are instances of individual WMN domains subscribing to the Internet services from upstream service providers, shown as the Internet cloud in Fig. 1. Each WMN domain, or trust domain (to be used interchangeably) is managed by a domain administrator that serves as a trusted authority (TA), e.g., the central server of a campus WMN.

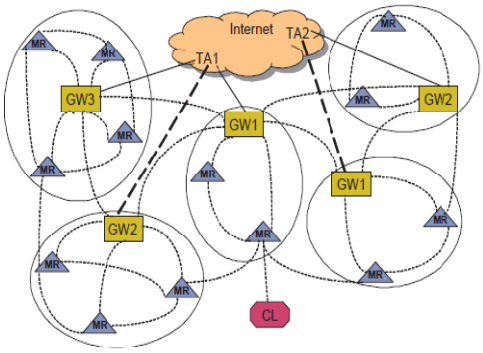

Fig. 1: Network Topology of A Typical WMN

3.3 Mobile banking:

A mobile banking application is, first of all, a mobile application. To conceptualize a mobile application, additional informational added values have to be targeted, using mobile added values [24]. In other words, it is far from sufficiency to just porting an existing Internet application on a mobile device. Mobile applications have to be specifically made-to-measure on the one hand side to the needs and expectations of the mobile user, and on the other hand side to the specific restrictions of mobile communication techniques and mobile devices. In order to derive a set of requirements to mobile banking applications we pursue two steps: Firstly we identify general characteristics of the mobile use which are relevant. Secondly we closely watch the user and his context when wanting to use mobile banking. The use of mobile applications underlies several specific restrictions. We consider five characteristics of the mobile use to be particularly relevant as they greatly influence the design of mobile banking applications and the suitability of certain technical solutions. A mobile application is used via a mobile device. For these devices (currently either a mobile phone or a PDA), special limitations are valid [25]. For the mobile banking context, above all, these are the limited input and display capabilities. The connection is provided by a mobile network operator (MNO). This is especially important if applications need to access certain parts of the infrastructure which are under control of the MNO (e.g. the SIM card). In the case of negotiations, these have to be pursued with all MNO on the designated market. The use of mobile data transmission is expensive. In the case of circuit-switched data transmission (e.g. GSMCSD or HSCSD) this extends to the connection time, in the case of packet-switched data transmission (e.g. GPRS) this extends to the transferred data volume.

4 EXPERIMENTAL RESULTS

This section deals with the experimental performance evaluation of our system through **simulation**. In order to test our model, the sun java wireless tool kit is used. We developed the code using J2ME version of java. In this paper we tried to develop the traceability and anonymity features for a wireless mesh network considering mobile

banking as an example. The sample screen shots are as follows:

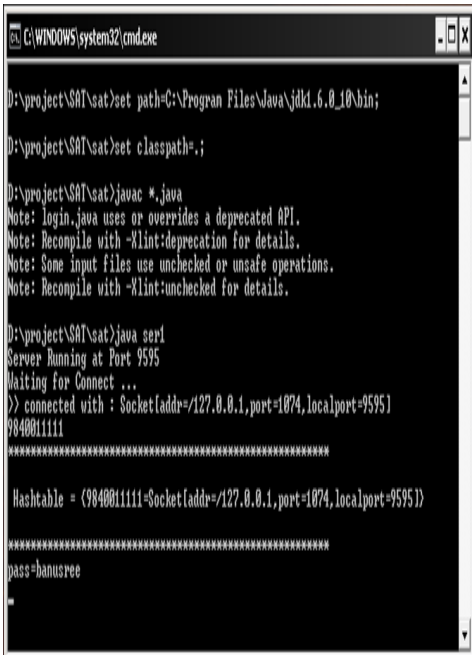

Fig 2: the server running and connected to a mobile device

Fig 3: performing secure transaction

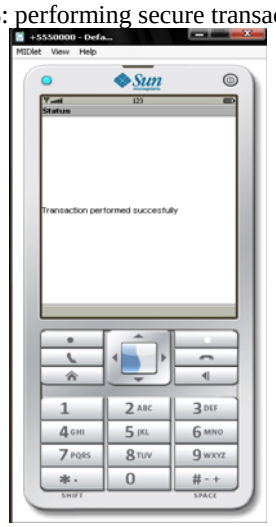

Fig 4: Transaction performed successfully

5 CONCLUSION

In this paper, we propose a security architecture, SAT, mainly consisting of the ticket-based protocols which can be considered as application-layer protocols that resolve the conflicting security requirements of unconditional anonymity for honest users, and traceability of misbehaving users. By utilizing the tickets, self-generated pseudonyms, and the hierarchical identity-based cryptography, the proposed architecture is demonstrated to achieve desired security objectives and efficiency. We tried to simulate the architecture using sun java wireless toolkit for mobile banking.

Acknowledgment

This work was supported by our Head of the Department and faculty who guided for the completion of this work. The author's would like to thank everyone who supported us with this work.

REFERENCES

[1] S. Brands, "Untraceable off-line cash in wallets with observers," in Proc. CRYPTO'93, 13th Annual Int'l Cryptology Conf. on Advances in Cyptology, pp. 302–318, Aug. 1993.
[2] K. Wei, Y. R. Chen, A. J. Smith, and B. Vo, "Whopay: A scalable and anonymous payment system for peer-to-peer environments," Proc. IEEE Intl. Conf. on Distributed Computing Systems, ICDCS, July 2006.
[3] A. Menezes, P. V. Oorschot, and S. Vanston, Handbook of Applied Cryptography, Boca Raton, CRC Press, 1996.
[4] European Telecommunications Standards Institute (ETSI), "GSM 2.09: Security Aspects.," June 1993.
[5] P. Kyasanur and N. H. Vaidya, "Selfish MAC layer misbehavior in wireless networks," IEEE Trans. Mobile Computing, vol. 4, no. 5, pp. 502–516, Sept. 2005.
[6] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Comm. of the ACM, vol. 47, no. 6, pp. 53–57, 2004.
[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," ACM Trans. Sensor Networks, vol. 2, no. 4, pp. 500–528, Nov. 2006.
[8] W. Lou and Y. Fang, A Survey on Wireless Security in Mobile Ad Hoc Networks: Challenges and Possible Solutions, edited by X. Chen, X. Huang and D.-Z. Du, Kluwer Academic Publishers/Springer, 2004.
[9] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24–30, Dec. 1999.
[10] M. Raya and J-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, vol. 15, no. 1, pp. 39–68, 2007.
[11] N. B. Salem and J-P. Hubaux, "Securing wireless mesh networks," IEEE Wireless Communications, vol. 13, no. 2, Apr. 2006.
[12] Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecture for multihop wireless mesh networks," IEEE J. Select. Areas Communications, vol. 24, no. 10, pp. 1916–1928, Oct. 2006.
[13] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Comput. Netw., vol. 47, no. 4, pp. 445–487, Mar. 2005.
[14] D. Chaum, A. Fiat, and M. Naor, Untraceable electronic cash, in Proc. on Advances in Cryptology (CRYPTO'88), 2002.
[15] D. Figueiredo, J. Shapiro, and D. Towsley, "Incentives to promote availability in peer-to-peer anonymity systems," in Proc. IEEE Int'l Conf. on Network Protocols, ICNP, pp. 110–121, Nov. 2005.
[16] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The secondgeneration onion router," in Proc. The 13th USENIX Security Symposium, pp. 303–320, Aug. 2004.
[17] D. Chaum, Blind signatures for untraceable payments, Advances in Cryptology - Crypto '82, pp. 199-203, Springer-Verlag, 1982.

[18] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 386–399, Oct. 2006.
[19] D. Boneh and M. Franklin, Identity-based encryption from the weil pairings, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.
[20] A. Juels, M. Luby, and R. Ostrovsky, Security of blind digital signatures, Advances in Cryptology - CRYPTO '97, LNCS 1294, pp. 150-164, Springer-Verlag, 1997.
[21] S. Brands, An efficient off-line electronic cash system based on the representation problem, CWI Technical Report CS-R9323, 1993.
[22] M. Abe and T. Okamoto, Provably secure partially blind signatures, Advances in Cryptology - Crypto 2000, LNCS 1880, pp. 271-286, Springer-Verlag, 2000.
[23] S. M. Chow, C. K. Hui, S. M. Yiu, and K. P. Chow, Two improved partially blind signature schemes from bilinear pairings, ACISP 2005, LNCS 3574, pp. 316-328, Springer-Verlag, 2005.
[24] Pousttchi, K.; Turowski, K.; Weizmann, M.: Added Value-based Approach to Analyze Electronic Commerce and Mobile Commerce Business Models. In: Andrade, R.A.E.; Gómez, J.M.; Rautenstrauch, C.; Rios, R.G.: International Conference of Management and Technology in the New Enterprise. La
Habana 2003, pp. 414-423.
[25] Turowski, K.; Pousttchi, K.: Mobile Commerce – Grundlagenund\Techniken.1.Ed.,Heidelbe2003.