A Plan and Design to Achieve the State of Unacknowledgement and Obsoleteness in Wireless Mesh Networks

[1]MD. Razia Sultana, [2]B. Rajesh war Singh, [3]M. Srinivas

[1,2,3]Dept of CSE, Swarna Bharathi Institute of Science & Technology, Khammam, India

Abstract

Anonymity is otherwise called as the state of being unacknowledged. It has received increasing attention in the literature due to the users' awareness of their privacy nowadays. It provides security by providing protection for users to enjoy network services without being traced. The issues were mainly used in the field of ecommerce mainly in the peer to peer systems.Moreover the computer network authority requires conditional anonymity such that misbehaving entities in the network remain traceable. In this paper, we propose a security architecture to ensure unconditional anonymity for honest to trace out the unauthorized and legitimate users.This security 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. Thorough analysis on security and efficiency is incorporated, demonstrating the feasibility and effectiveness of the proposed architecture.

Keywords

Anonymity, Traceability, Confidentiality,Ticket Granting, Access Privelage

I. 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. In [8], the authors describe the specifics of WMNs and identify three fundamental network operations that need to be secured. We [9] 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

II. IBC from Bilinear Pairings

ID-based cryptography (IBC) allows the public key of an entity to be derived from its public identity information such as name and e-mail address, which avoids the use of certificates for public key verification in the conventional public key infrastructure (PKI) . 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:

Bilinear: eðaP;bQÞ¼eðP;QÞ^{ab}, 8P ; Q 2 G$_1$, and 8a; b 2 Z$_{p,}$, where Z$_p$, denotes the multiplicative group of Z$_p$, the integers modulo p. In particular, Z$_p$ ¼ fx j 1 x p 1g since p is prime.

1. Nondegenerate: 9P; Q 2 G$_1$ such that eðP; QÞ ¼ 1.
2. Computable: there exists an efficient algorithm to compute eðP; QÞ; 8P; Q 2 G$_1$.

A. Blind Signature

Blind signature is first introduced by Chaum. We refer the readers to for a formal definition of a blind signature scheme, which should bear the properties of verifiability, unlink ability, and enforceability.

III. System Model

A. Notation and Definitions

First, we give a list of notation and definitions that are frequently used in this paper.

1. Notation

!,!!, and k: denote single-hop communications, multihop communications, and concatenation, respectively.

CL, MR, GW, and TA: abbreviations for client, mesh router, gateway, and trusted authority, respectively. ID$_x$: the real identity of an entity x in our WMN system PS$_x$: the pseudonym self-generated by a client x by using his real identity ID$_x$. H^{1}ðMÞ and H^{1}ðMÞ: f0; 1g ! G$_1$, cryptographic hash functions mapping an arbitrary string M to G$_1$.H$_2$:a cryptographic secure has function: G$_1$ G$_2$! Z$_p$ .H$_3$: a cryptographic secure hash function: G2G2 IDGW date=time! Z$_p$.H^{1}ðID$_x$Þ/ x and H^{1}ðIDT$_x$Þ/ $_x$: the public/private key pairs assigned to an entity x in the standard IBC and HIBC, respectively. P Sx/f$_x$ and P ST$_x$/^{f}x: the self-generated pseudo-nym/ private key pairs based on the above public/ private key pairs. SIG x ðmÞ: the ID-based signature on a message musing the signer x's private key $_{\text{x.VERðSIGÞ}}$: the verification process of the above signature, which returns "accept" or "reject." HI DS x; sx ðmÞ: the hierarchical ID-based signature on a message m

2. Definitions

(i). Anonymity (Intractability)

The anonymity of a legitimate client refers to the untraceability of the client's network access activities.

(ii). Traceability

A legitimate client is said to be traceable if the TA is able to link the client's network access activities.

(iii). Ticket Reuse

one type of misbehavior of a legitimate client that refers to the client's use of a depleted ticket (Val ¼ 0).

(iv). 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.

(v). 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).

(vi). 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.

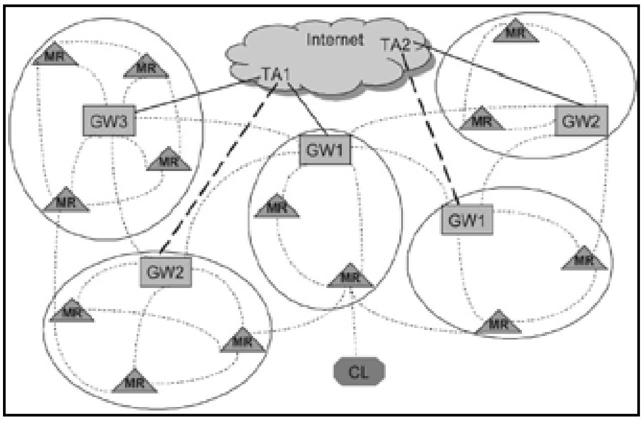

Fig. 1:

B. Network Architecture

Consider the network topology of a typical WMN depicted in Fig. 1. The wireless mesh backbone consists of mesh routers (MRs) and Gateways (GWs) interconnected by ordinary wireless links.

C. Trust Model

The trust model comprising trust relationships and the trust domain initialization will be described in this section.

1. Trust Relationship

In general, the TA is trusted within the WMN domain. There is no direct trust relationship between the client and the gateway/mesh router. We will use standard IBC for authentication and secure communications both at the backbone and during network access inside a trust domain (i.e., intradomain).

All the TAs in the SDE's domain are at level 1 and all gateways, mesh routers and clients in each TA's domain are at level 2.

2. Trust Domain Initialization

We apply the domain initialization of the hierarchical IBC.

(i). Input security parameter 2 Zþ into domain para-meter generator PG and output the parameter tuple ðp; G_1; G_2; e; P_0; H_1Þ.

(ii). Randomly select a domain master secret s_0 2 Z_p and calculate the domain public key P_{pub} ¼ s_0P_0. The root PKG (e.g., the SDE or SDH) publishes the domain parameters ðp; G_1; G_2; e; P_0; H_1; P_{pub}Þ and maintains s_0 confidential. Suppose that a child CH_j is located at level j. The lower level setup is performed by the parent as follows:

- 1. compute K_j ¼ H_1ðID_1; :::; ID_jÞ;
- 2. compute CH_j's private keys $_j$ ¼ $_j$ 1 þ s_j $_1K_j$ ¼ j i¼1 s i 1Ki, and j ¼ H_1ðID_jÞ;
- 3. distribute QT ¼ fQ_l : 1 l<jg to CH_j, where Q_l ¼ s_lP_0.

In the above private key assignment, ðID_1; . :::;ID_iÞ for 1 i j is the ID tuple of CH_j's ancestor at level i. The private keys j and j are generated for the interdomain and intradomain authentication, respectively, where s_j 1 is the parent's secret and is the master secret of the trust domain.

IV. SAT Security Architecture

A. Ticket-Based Security Architecture

First, we restrict our discussion to within the home domain.

1. Ticket Issuance

In order to maintain security of the network against attacks and the fairness among clients, the home TA may control the access of each client by issuing tickets based on the misbehavior history of the client, which reflects the TA's confidence about the client to act properly.It generates a valid ticket ticket ¼ fT_N ; W ; c; ðU^0; V ^{0}; X^0; ; 00 g at the output, unique serial number of the ticket that can be computed from the client's account number(cf., Section 4.1.1), ðU^0;V ^{0};X^0; is the signature on ðT_N ; W ;

It is necessary for verifying the validity of the signature in the ticket deposit protocol.

The TA publishes the domain parameters to be used within its trust domain as ðp; G_1; G_2; e; P; P_1 ;P_2; H_1; H_2; H_3;P_{pub}Þ using the standard IBC domain initialization.Where ðP;P_1;P_2Þ are random generators of G_1, and Ppub ¼ P. Since the scheme in is selected for demonstration, G_1 here should be a Gap Diffie-Hellman (GDH) group, where the computational Diffie-Hellman problem (CDHP is assumed to be intractable. In addition, theTAchoosesr2_RZ_p and Q2_RG_1, and the client chooses ; ; ; ; ; ; 2_R Z_p. Note that if the scheme in is adopted, the TA publishes ðp; G_1; G_2; e; g; g_1;g_2;H; H_0; H_1Þ, where G_1 should be a GDH in which the RCDHP (reversion CDHP) is assumed to be intractable We will demonstrate the following protocols based on the scheme.

The ticket issuance protocol is demonstrated as follows:

1. CL !! TA: ID_{CL};m;t_1, HMAC ðm k t_1Þ;
2. TA!!CL:ID_{TA}; X¼eðm; $_{TA}$Þ; Y ¼eðP; Q Z¼eðm;QÞ; U ¼rH_1ðID_{TA}Þ; V ¼rP;t_2;HMAC ðXkY kZkU kV kt_2Þ;
3. CL !! TA : ID_{CL}; B¼1H_2ðm^0 kU^0 kV^0 kRkW kX^0 kY^0 kZ^0Þ þ ;t_3;HMAC ðBkt_3Þ; and
4. TA!!CL:ID_{TA}; 1¼QþB TA; 2¼ðrþBÞ TA þrH1ðcÞ; t4 HMAC ð$_1$k$_2$kt_4Þ:

At the end, the client checks if the following equalities hold: eðP; 1Þ ¼ y^BY and eðm; 1Þ ¼ X^BZ, where y ¼ eðP_{pub}; H1ðIDT AÞÞ. If the verification succeeds, the client calculates ∞β1 ¼ 1 þ H1ðIDTAÞ, 2 ¼ 2,¼ B, and outputs the signature ðU^0; V^0; X^0; ;0 0 on ðT_N ; W ; cÞ,1; 2Þ where T_N ¼ m^0.

In Step 3 above, m ¼ u_1P_1 þ u_2P_2 ¼ þ u_2P_2 ¼ 0, where u_1 2_R Z_p and u_2 ¼ 1; m^0 ¼ m; U^0 ¼ U þ H_1ðID_{TA}Þ H_1ðcÞ; V^0 ¼ Vþ P_{pub}; R¼eðm^0;H_1ðID_{TA}ÞÞ; W ¼$g^1$1$g^2$2; where g_1 ¼ eðP_1; H_1ðID_{TA}ÞÞ; g_2 ¼ eðP_2; H_1ðID_{TA}ÞÞ; and v_1; v_2 2_R Z_p ; X^0 ¼ X , Y ^{0} ¼ Y g, where g ¼ eðP ; H_1ð$ID_{T A}$ÞÞ, Z^0 ¼ Z R. In the above protocol, the TA and the client can locally derive a symmetric key ¼ eð $_{TA}$;H_1ðID_{CL}ÞÞ, and ¼ eðH_1ð$ID_{T A}$Þ; $_{CL}$Þ, respectively, assuming that IDT A is known to all the entities in the TA's domain.

A time stamp ti is included in each message exchanged to prevent the message replay attack.

2. Ticket Deposit

After obtaining a valid ticket, the client may deposit it anytime the network service is desired before the ticket expires, using the ticket deposit protocol shown below.

1. CL !! GW : PS_{CL};m^0;W;c;
0 0¼ ðU^0; V ^{0}; X^0; ;1;2Þ; t5;SIGðm^0 k W k c k k t_5Þ;fCL
2. GW !! CL : ID_{GW}, d ¼ H_3ðR k W k IDGW k T Þ, t_6,HMAC

0ðd k t$_{6}$Þ;

3. CL !! GW : PS$_{CL}$, r$_{1}$ ¼ dðu$_{1}$ Þ þ v$_{1}$, r$_{2}$ ¼ d þ v$_{2}$,t$_{7}$, HMAC 0 ðr$_{1}$ k r$_{2}$ k t$_{7}$Þ; and

4. GW !! CL : ID$_{GW}$; misb; exp; t$_{8}$;SIGðPSCL k IDGW k misb k exp k t$_{8}$Þ; GW

At the end, the gateway checks if the equality g^{1}1 g^{2}2 ¼ R^{d}W holds. At the end of Step 1, the gateway will perform VERð Þ before Steps 2 and 3 can be proceeded, and R can be derived as R ¼ eðm^{0}; H$_{1}$ðID$_{T A}$ÞÞ from the received information. T is the date/time when the ticket is deposited. A symmetric key can be derived locally by the gateway and the client as 0¼eð$_{GW}$;PS$_{CL}$Þ,and CLÞ, respectively, after learning each other's ID

B. Fraud Detection

Fraud is used interchangeably with misbehavior in this paper, which is essentially an insider attack.

The fraud detection protocol is shown as follows:

GW! T A : ID$_{GW}$; m^{0}; W ; c;¼ ðU^{0};V ^{0};X^{0}; ; 1; 2Þ;r$_{1}$;r$_{2}$;T;t$_{9}$; HMAC 00 ðm^{0} k W k c k k r$_{1}$ k r$_{2}$ k T k t$_{9}$Þ; where 00 is the preshared symmetric key between the gateway and the TA, which we have assumed for the WMN backbone.:

r$_{1}$ ¼ dðu$_{1\ Þþv1}$; r2 ¼d þv2; ð1Þ

r1 ¼ d^{0}ðu$_{1\ Þþv1}$; r2 ¼d^{0} þ v2: ð2Þ

1. Ticket Revocation

Ticket revocation is necessary when a client is compromised, and thus, all his secrets are disclosed to the adversary.

The ticket revocation protocol consists of two cases as follows:

1. Revocation of new tickets: the client may store a number of unused tickets, as mentioned previously.
2. Revocation of deposited tickets: the client simply sends P S$_{CL}$, ID$_{DGW}$, t$_{11}$, SI G fðIDDGW k t11Þ in the revocation request to the DGW. The DGW authenticates the client and marks the associated ticket revoked.

2. Accessing the Network from Foreign Domains

The access services the visiting (foreign) trust domain provided the ticket-based security architecture can take place in two ways including the following:

CL!!MR: PST$_{CL}$; aP$_{0}$; t$_{12}$; HI DS CL; s CL ðH1^{ðPST}CL $^{k\ aP}$0 ^{k} ^{t}12^{ÞÞ};

MR!CL:IDT$_{MR}$;bP$_{0}$;t$_{13}$;

HI DS MR;sMRðH1^{ðIDT}MR $^{k\ bP}$0 $^{k\ t13}$ÞÞ; and

CL !! MR: PST$_{CL}$, PS$_{CL}$, SKE ðID$_{CL}$ k mÞ,t$_{14}$, HMAC ðP SCL k SKE k t$_{14}$Þ.

MR (or an access point) forwards the client's ticket deposit request to the home domain when the client owns available new tickets issued by the home TA.

C. Pseudonym Generation and Revocation

The use of pseudonyms has been shown in the ticket-based protocols. After obtaining the private key j associated with the ID tuple IDT$_{j}$ ¼ ðID$_{1}$; . . . ; ID$_{j}$Þ as $_{j}$ ¼ $_{j\ 1}$ þ s$_{j\ 1}$H1ðIDTjÞ from the parent (i.e., the home TA), the client CL$_{j}$ derives the self-generated pseudonym tuples fP ST$_{i}$: 1 i jg as follows: CL$_{j}$ selects a random secret $ 2 Z$_{p}$ and computes the pseudonym tuples PST$_{i}$ ¼ K_{i}$ ¼ H_{1}$ðIDT$_{i}$Þ (1 I j). The associated private key can be computed as ej ¼ $ j ¼ $ P^{i}P$_{j}$ ¼1 si 1Ki ¼ P^{i¼1} si 1 K_{i}$ ¼ i¼1 si 1 $H1ðIDT$_{i}$Þ ¼ P$_{i¼1}$ si 1 PSTi. By substituting PST$_{j}$= ej for H$_{1}$ðIDT$_{j}$Þ= j in the HIDS scheme, the signing and verification can be correctly performed.

V. Security Analysis

In this section, we analyze the security requirements our system can achieve as follows. Fundamental security objectives. It is trivial to show that our security architecture satisfies the security requirements for authentication, data integrity, and confidentiality, Anonymity. First of all, it can be easily shown that a gateway cannot link a client's network access activities to his real identity. Specifically, any view of the ticket issuance protocol ðU; V ; X; Y ; Z; B; 1; 2;mÞ is un-linkable to any valid signature ðU^{0} V 0;X^{0}; ; 0 0 m^{0}Þ

IV. Efficiency Analysis

To improve the computation and communication efficiency when working with EðF$_{q}$ Þ, we tend to keep q small while maintaining the security with larger values of k.

A. Communication

Our ticket-based security architecture consists of four intradomain protocols in which ticket deposit involves only clients and gateways. This protocol is distributed in nature, and thus, the communication cost incurred is more affordable.

B. Storage

As mentioned above, the TA may consist of several servers to store necessary information from all clients during protocol executions.

C. Computation

Following the claims from the storage analysis, we are mainly interested in the computation overhead experienced at the client side and will count solely the effective overhead(i.e., the overhead that is varying for each protocol instance or cannot be precomputed).

VII. Security enhancements

In addressing privacy and anonymity on the Internet, Dingle dine argues that cryptography alone will not hide the existence of confidential communication relationships.

VIII. Conclusion

In this paper, we propose SAT, a security architecture mainly consisting of the ticket-based protocols.

References

[1] European Telecomm. Standards Inst. (ETSI),"GSM 2.09: Security Aspects", June 1993.

[2] P. Kyasanur, N.H. Vaidya,"Selfish MAC Layer Misbehavior in Wireless Networks", IEEE Trans. Mobile Computing, Vol. 4, No. 5, pp. 502-516, Sept. 2005.

[3] A. Perrig, J. Stankovic, D. Wagner,"Security in Wireless Sensor Networks", Comm. ACM, Vol. 47, No. 6, pp. 53-57, 2004.

[4] S. Zhu, S. Setia, 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.

[5] W. Lou, Y. Fang, X. Chen, X. Huang, D.-Z. Du, "A Survey on Wireless Security in MobileAd Hoc Networks: Challenges and Possible Solutions", Kluwer Academic Publishers/ Springer, 2004.

[6] L. Zhou, Z.J. Haas,"Securing Ad Hoc Networks", IEEE Network Magazine, Vol. 13, No. 6, pp. 24-30, Dec. 1999.

[7] M. Raya, J-P. Hubaux,"Securing Vehicular Ad Hoc Networks", J. Computer Security, special issue on security of Ad-Hoc and sensor networks, Vol. 15, No. 1, pp. 39-68, 2007.

[8] N.B. Salem, J-P. Hubaux,"Securing Wireless Mesh Networks", IEEE Wireless Comm., Vol. 13, No. 2, pp. 50-55, Apr. 2006.

[9] Y. Zhang, Y. Fang,"ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks", IEEE J. Selected Areas Comm., Vol. 24, No. 10, pp. 1916-1928, Oct. 2006.

[10] I.F. Akyildiz, X. Wang, W. Wang,"Wireless Mesh Networks: A Survey", Computer Networks, Vol. 47, No. 4, pp. 445-487, Mar.2005.

[11] S. Brands,"Untraceable Off-Line Cash in Wallets with Observers", Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cyptology (CRYPTO '93), pp. 302-318, Aug. 1993.

[12] K. Wei, Y.R. Chen, A.J. Smith, B. Vo,"Whopay: A Scalable and Anonymous Payment System for Peer-to-Peer Environments", Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS), July 2006.

[13] D. Chaum, A. Fiat, M. Naor,"Untraceable Electronic Cash", Proc. Conf. Advances in Cryptology (CRYPTO '88), 2002.

[14] D. Figueiredo, J. Shapiro, D. Towsley,"Incentives to Promote Availability in Peer-to Peer Anonymity Systems", Proc. IEEE Int'l Conf. Network Protocols (ICNP), pp. 110-121, Nov. 2005.

[15] G. Ateniese, A. Herzberg, H. Krawczyk, G. Tsudik, "Untraceable Mobility or How to Travel Incognito", Computer Networks, Vol. 31, No. 8, pp. 871-884, Apr. 1999.

[16] Q. He, D. Wu, P. Khosla,"Quest for Personal Control over Mobile Location Privacy", IEEE Comm. Magazine, Vol. 42, No. 5, pp. 130-136, May 2004.

[17] A.R. Beresford, F. Stajano,"Location Privacy in Pervasive Computing," IEEE Pervasive Computing, Vol. 2, No. 1, pp. 46-55, Jan.-Mar. 2003.

Md.Razia Sultana pursuing M.Tech in the department of Computer Science and Technology. Her research areas include computer networks,information security,data mining and data warehousing.

B.Rajeshwar Singh working as an Associate Professor in the department of computer science and engineering. His research areas include cloud computing,data mining and data warehousing, Java.

M.Srinivas ,Head of Department and working as an Associate Professor in the department of computer science and engineering.His research areas include network security,data mining and data warehousing.