IOSR Journal of Computer Engineering (IOSRJCE)
ISSN : 2278-0661 Volume 1, Issue 4 (May-June 2012), PP 33-38
www.iosrjournals.org

An Architecture to Achieve Anonymity and Traceability

S. Reshma[1], K. S. Masthan Vali[2]
[1]*PG Student M.Tech,* [2]*Associate Professor*
Department of Computer Science, Madina College of Engineering

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. On the other hand, the 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 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 nonrepudiation.*

Index Terms: *Anonymity, traceability, pseudonym, misbehavior, revocation, wireless mesh network (WMN).*

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. Wireless security has been the hot topic in the literature for various network technologies such as cellular networks [1], wireless local area networks (WLANs) [2], wireless sensor networks [3], [4], mobile ad hoc networks (MANETs) [5], and vehicular ad hoc networks (VANETs). We 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

Anonymity [6] and privacy issues have gained considerable research efforts in the literature [6]. One requirement for anonymity is to unlink a user's identity to his or her specific activities. Anonymity is also required to hide the location information of a user to prevent movement tracing, as is important in mobile networks and VANETs . In wireless communication systems, it is easier for a global observer to mount traffic analysis attacks by following the packet forwarding path than in wired networks. Therefore, traceability [6] is highly desirable such as in e-cash systems where it is used for detecting and tracing double-spenders.

In this paper, we are motivated by resolving the above security conflicts, namely anonymity and traceability, in the emerging WMN communication systems. Our system borrows the blind signature technique from payment systems and hence, can achieve the anonymity of unlinking user identities from activities, as well as the traceability of misbehaving users. Furthermore, the proposed pseudonym technique renders user location information unexposed.

II. PRELIMINARIES

2.1 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). Specifically, let G1 and G2 be an additive group and a multiplicative group, respectively, of the same prime order p. The 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},∀P, Q ƐG1, and
∀ a, b ƐZ^*_p, where Z^*_p denotes the multiplicative group of Zp, the integers modulo p. In particular
Z^*_p= {x|a≤x≤p-1} since p is prime.
2. Nondegenerate: ∃P, Q Ɛ G1 such that e(P,Q)≠1.
3. Computable: there exists an efficient algorithm to
compute e(P,Q),∀P,Q Ɛ G1.

2.2 Blind Signature

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. A blind signature scheme should bear the

properties of verifiability, unlinkability, and unforgeability. 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. Partial blind signature schemes 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.

III. SYSTEM MODEL

3.1 Notation and Definitions

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

3.1.1 Notation

1. $\rightarrow$, $\rightarrow\rightarrow$ *and* $||$: denote single-hop communications, multihop communications, and concatenation, respectively.
2. CL, MR, GW, and TA: abbreviations for client, mesh router, gateway, and trusted authority, respectively.
3. IDx: the real identity of an entity x in our WMN system.
4. PSx: the pseudonym self-generated by a client x by using his real identity IDx.
5. H1 (M) and $H1^{1}$ (M): $\{0; 1\}^{*} \rightarrow G1$, cryptographic hash functions mapping an arbitrary string M to G1.
6. H2: a cryptographic secure hash function: $G1^{3} * G2^{5} \rightarrow Z^{*}_{p.}$
7. H3: a cryptographic secure hash function: G2 * G2* IDGW *date/time $\rightarrow Zp^{*}$.

3.1 Definitions

Anonymity (Untraceability): the anonymity of a legitimate client refers to the untraceability of the client's network access activities.

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.

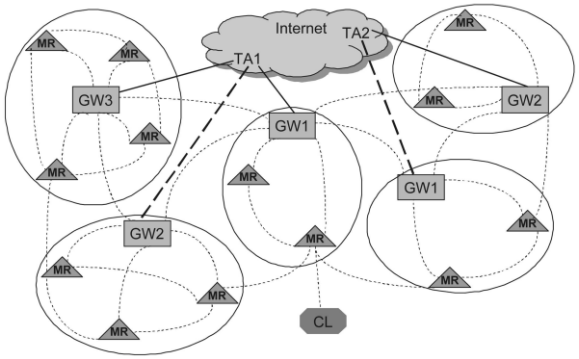
Ticket reuse: one type of misbehavior of a legitimate client that refers to the client's use of a depleted ticket (val = 0).

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.

Framing: a type of attack mounted by a malicious TA in order to revoke a legitimate client's network access privilege.

3.2 Network Architecture



The wireless mesh backbone consists of mesh routers (MRs) and gateways (GWs) 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. 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. TAs and gateways are assumed to be capable of handling computationally intensive tasks. In addition, they are assumed to be protected in private places and cannot be easily compromised due to their important roles in the WMN.

IV. SAT SECURITY ARCHITECTURE

4.1 Ticket-Based Security Architecture

The ticket-based security architecture consists of ticket issuance, ticket deposit, fraud detection, and ticket revocation protocols.

4.1.1 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. Ticket issuance occurs when the client initially attempts to access the network or when all previously issued tickets are depleted. The clien employs some blinding technique to transform the ticket to be unlinkable to a specific execution of the ticket generation algorithm while maintaining the verifiability of the ticket. The ticket generation algorithm, takes as input the client's and TA's secret numbers, the common agreement c as (val, exp, misb), and some public parameters, and generates a valid ticket ticket = { TN,W, c, (U^1, V^1, X^1,^{p},$\sigma 1, \sigma 2$)} at the output, where TN is the unique serial number of the ticket that can be computed from the client's account number Ώ (U^1, V^1, X^1, ^{p},$\sigma 1, \sigma 2$) is the signature on (T_N,W, c) where W is necessary for verifying the validity of the signature in the ticket deposit protocol. We opt for a partially restrictive blind signature scheme with two desired features: partial blindness and restrictiveness, for the proposed WMN framework.

4.1.2 Ticket Deposit

After obtaining a valid ticket, the client may deposit it anytime the network service is desired before the ticket expires. The deposit gateway (DGW), where the ticket is initially deposited, will then generate a signature on the client's pseudonym, the DGW's ID, and the associated misb and exp values extracted from c. The signature is required to be present in order for other access points in the trust domain to determine whether and where to forward the client's access requests, if the deposited ticket will be further used from other access points. The DGW creates a record for the deposited ticket as: record = (ticket, r1, r2, T, rem, log), where rem and log denote the remaining value of the ticket and the logged data of the client's noncompliant behavior, respectively.

4.1.3 Fraud Detection

Ticket reuse generally results from the client's inability to obtain tickets from the TA when network access is desired, primarily due to the client's past misbehavior, which causes the TA to constrain his ticket requests. Multiple -deposit can also be termed client coalition, which is beneficial when the coalescing parties are unauthorized users or clients with misbehavior history having difficulty in acquiring tickets from the TA.

These two types of fraud share a common feature, that is, a same ticket (depleted or valid) is deposited more than once such that our one-time deposit rule is violated. This is where the restrictiveness of the blind signature algorithm takes effect on revealing the real identity of the misbehaving client.

GW ->TA: IDGW, m^1, W, c,

σ = (U^1, V^1, X^1, ^{p},$\sigma 1, \sigma 2$) r1, r2, T, t9;

$HMAC_{k11}$ (m^1 || W || c || σ || r1 || r2 || T || t9)

4.1.4 Ticket Revocation

Ticket revocation is necessary when a client is compromised, and thus, all his secrets are disclosed to the adversary. In our system, the adversary is motivated by gaining network services using tickets once the ticket associated secrets are obtained from the compromised clients. Therefore, the compromised client needs to be able to revoke the ticket and prevent the adversary from acquiring benefits.

1. Revocation of new tickets: The client may store a number of unused tickets. When revoking these tickets that have not been deposited, the client sends PS_{CL}, TN, t10, $SIG_{\Gamma CL}$ (TN || t10) in the revocation request to any encountered gateway. This gateway authenticates the client using PSCL and records the ticket serial number TN as revoked.

2. Revocation of deposited tickets: The client simply sends PS_{CL}, ID_{DGW}, t11, $SIG_{\Gamma CL}$ (ID_{DGW} || t11) in the revocation request to the DGW. The DGW authenticates the client and marks the associated ticket revoked. When gateways have records in the revocation database, they immediately report the revocations to the home TA, which will update and distribute the revocation list for all gateways in the trust domain to reference.

4.1.5 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:

. A foreign mesh router MR (or foreign access point) forwards the client's new ticket request to the home domain when there is no available ticket for accessing the network from the foreign domain.
. 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.

4.2 Pseudonym Generation and Revocation

The pseudonym is used to replace the real ID in the authentication, which is necessary for both anonymous network access and location privacy. In the intradomain authentication in our system, the client generates his own pseudonym by selecting a secret number $\bar{w} \in R Z^{*}p$ and computing the pseudonym $PS_{CL} = \bar{w}$ $H1(ID_{CL})$. The corresponding private key can be derived as $\Gamma_{CL} = \bar{w}\Gamma_{CL} = \bar{w}\pi H1(IDCL) = \pi$.

The pseudonym revocation is impossible by using the pseudonym alone. The reason is that any adversary who has compromised a client can generate valid pseudonym/ key pairs that are only known to the adversary by running the self-generation algorithm. However, this pseudonym self-generation technique is appropriate in our system because the pseudonym revocation can be realized via revoking the associated ticket since the pseudonym is active only when its associated ticket is actively in use (deposited and not depleted).

V. SECURITY ANALYSIS

Fundamental security objectives. It is trivial to show that our security architecture satisfies the security requirements for authentication, data integrity, and confidentiality, which follows directly from the employment of the standard cryptographic primitives, namely digital signature, message authentication code, and encryption. A fraud can be repudiated only if the client can provide a different representation (u1, u2) he knows of m from what is derived by the TA.

Anonymity. A gateway cannot link a client's network access activities to his real identity. Due to the use of pseudonyms in authentication which reveals no information on the real ID, the gateway learns nothing about the identity of the client requesting network access. Since the pseudonym is generated by the client using his secret number, solving for the real identity from the pseudonym is equivalent to solving the DLP. Furthermore, the client's deposit gateway (DGW) cannot deduce the client's ID from the deposited ticket, which has been blinded by the client and does not reveal any identification information unless misbehavior occurs.

Traceability (conditional anonymity). According to its definition, this requirement is twofold:
1) Anonymity for honest clients is unconditional
2) A misbehaving client is traceable where the identity can be revealed. The adopted restrictive partially blind signature scheme in our security architecture achieves restrictiveness.

Framing resistance. If the client is honest, with overwhelming probability, the representation (u1, u2) he knows is different from that the malicious TA falsely generated. Since the client could not have come up with this representation by himself, it proves that the TA attempts to frame the client.

nforgeability. Unforgeability defines that the adopted restrictive partially blind signature scheme is existentially unforgeable against adaptively chosen message and ID attacks under the assumption of the intractability of CDHP in G1 and the random oracle.

VI. EFFICIENCY ANALYSIS

Most pairing-based cryptosystems need to work in 1) a subgroup of the elliptic curve E(Fq) of sufficiently large prime order p, and 2) a sufficiently large finite field Fqk , where q is the size of the field over which the curve is defined and k is the embedding degree. For current minimum levels of security, we require $p > 2^{160}$ and $qk > 2^{1024}$ ensure the hardness of the DLP in G1 and G2. To improve the computation and communication efficiency when working with E (Fq), we tend to keep q small while maintaining the security with larger values of k.

The communication and computation efficiency is best achieved using the Dual-HIDS. The client transmits approximately 148 bytes (5* |G1|element + 160bit HMAC output) and 446 bytes (5 * |G1|element + 2 * |G2|element þ 160bit HMAC output), respectively, for a new ticket request and a ticket deposit request. In the new ticket request, the client needs to perform an HIDS signing and verification, a symmetric-key encryption, and an HMAC, among which the HIDS operations dominate the computation costs.

6.1 Communication

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. In contrast, protocols involving interactions with the centralized TA contribute largely to the expensive communication costs in the system. In the fraud detection protocol, gateways report accumulated ticket records to the TA periodically instead of in real time. For each record, a gateway transmits roughly 443 bytes, including five G1 elements, two G2 elements, and four 160-bit elements.

Ticket issuance and revocation may take place in real time. The associated communication overhead depends on how frequent 1) the clients use up issued tickets and 2) the clients misbehave. In a single ticket issuance, the client sends roughly 60 bytes (i.e., three 160-bit elements) to the TA. The TA sends to the client approximately 128 bytes (i.e., four G1 elements and two 160-bit HMACs).

6.3 Computation

The computation tasks for clients include pairing operations (basic pairing and finite field exponentiation), point multiplications and additions, hash operations, etc., among which pairing operations are undoubtedly the most time-consuming task.

In ticket issuance, the client only computes two basic pairings in real time for each protocol instance. The remaining pairing operations can either be computed once or be precomputed and stored for all protocol instances. Several HMAC operations also need to be performed in real time, which is considered computationally efficient. In ticket deposit, one signing, one verification, and two HMAC operations are performed in real time by the client for each ticket deposited. In ticket revocation, a client has to compute one signature in real time for each revoked ticket, which requires no basic pairings but a finite field exponentiation.

VII. SECURITY ENHANCEMENTS

Addressing the privacy preserving issue in vehicular ad hoc networks (VANETs) where the vehicles enjoy various VANET applications. The proposed ticket-based anonymity system relies on effective anonymous routing protocols to construct anonymous communication paths and guarantee unlinkability. Unlinkability is a requirement for preserving user privacy in addition to anonymity. It refers to the property that multiple packets cannot be linked to have originated from a same client.

Another possible enhancement is to incorporate peer-to-peer cooperation. In the WMNs, the uplink from the client to the mesh router may rely on multihop communications. Peer clients act as relaying nodes to forward each other's traffic to the mesh router, which forms a P2P network.

VIII. CONCLUSION

In this paper, we propose An Architecture mainly consisting of the ticket-based protocols, which resolves 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.

IX. ACKNOWLEDGMENT

I express my profound sense of gratitude and indebtedness to my guide, Sri S.K..Mashtan vali, Associate Professor, Department of Computer Science, Madina College of Engineering, Kadapa, for his valuable guidance and suggestions to do my research and the help he provided to me in the formulation of ideas for my Thesis. I owe a lot to him and I sincerely feel that without his guidance, it would have been difficult for me to carryout my work.

Finally, Rigorous hard work has been put in this project to ensure that it proves to be the best project ever made & it is hoped that this project will prove to be a breeding ground for the next generation of students and will guide them in every possible way.

REFERENCES

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

[2] 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.

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

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

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

[6] SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2011.