www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 2 Issue 9 Sept., 2013 Page No. 2677-2681*

# Achieving Anonymity and Traceability in Wireless Networks

***R. Manasa Annapurna, G.Sowmya***

Assistant Professor MLR Institute of Technology Hyderabad.
manasaannapurna06@gmail.com gonuru_sowmya@yahoo.co.in

***Abstract:*** *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 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. In this paper, 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*.

## 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, wireless local area networks (WLANs), wireless sensor networks, mobile ad hoc networks (MANETs) and vehicular ad hoc networks (VANETs).

In the present system we are proposing an attack-resilient security architecture (ARSA) for WMNs, addressing countermeasures to a wide range of attacks in WMNs. Anonymity and privacy issues have gained considerable research efforts in the literature, 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 and the P2P payment systems where the payments cannot be linked to the identity of a payer by the bank or broker. 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. Thus, routing anonymity is indispensable, which conceals the confidential communication relationship of two parties by building an anonymous path between them. Nevertheless, unconditional anonymity may incur insider attacks since misbehaving users are no longer traceable. Therefore, traceability is highly desirable such as in e-cash systems, where it is used for detecting and tracing double-spenders.

This system is a practically viable solution to the application scenario of interest and this 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. This work differs from previous work in that WMNs have unique hierarchical topologies and rely heavily on wireless links. In addition to the anonymity scheme, other security issues such as authentication, key establishment, and revocation are critical in WMNs to ensure the correct application of the anonymity scheme. Although we use the widely used pseudonym approach to ensure network access anonymity and location privacy, pseudonym generation does not rely on a central authority. Specifically, the major contributions are 1) Design of a ticket-based anonymity system with traceability property; 2) Bind of the ticket and pseudonym which guarantees anonymous access control and simplified revocation process;3) Adoption of the Hierarchical Identity-Based Cryptography (HIBC) for inter-domain authentication avoiding domain parameter certification.

## 2. PRELIMINARIES

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

### Blind Signature

Blind signature is first introduced by Chaum. 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.

Brands developed the first restrictive blind signature scheme, where the restrictiveness property is incorporated into the blind signature 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 information into what is being signed by the bank. Such that this secret can be recovered by the bank to identify a user if and only if he/she double-spends. The restrictiveness property is essentially the guarantee for traceability in the restrictive blind signature systems.

Partial blind signature scheme allow the resulting signature to convey public 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.

Restrictive partially blind signature schemes are essentially blind signature schemes with restrictiveness and partial blindness property.

## 3. SYSTEM MODEL

Here list of definitions that are used in this paper are mentioned.

### Definitions

### A. 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, the gateway, and even the collusion of the two cannot link the client's network access activities to his real identity.

### B. 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

### C. Ticket reuse

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

### D. Multiple deposits

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

### E. Collusion

The colluding of malicious TA and gateway to trace a legitimate client's network access activities in the TA's domain.

### F. 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 thus, to revoke his access right.

**Network Architecture**

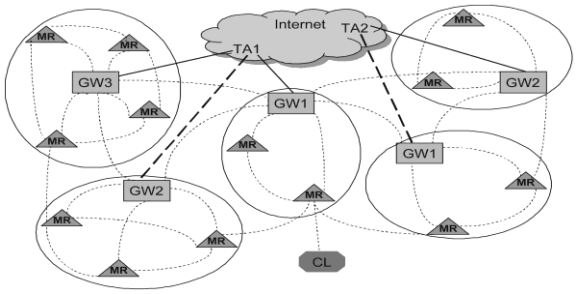



Fig 1.Network topology of a typical WMN

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 (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. The TA and associated gateways are connected by high-speed wired or wireless links, displayed as solid and bold dashed lines, respectively. TAs and gateways are assumed to be capable of handling computationally intensive tasks.

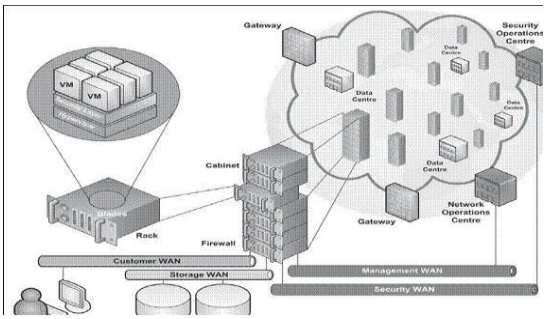
**Trust Model**

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

**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. We further assume the existence of preshared keys and secure communication channels between entities at the back- bone and will solely consider the authentication and key establishment during the network access of the clients. The client presents his ID upon registration at the TA, which assigns a private key associated with the client's ID. The client selects a unique account number computed by a randomly chosen secret number. The account number is stored with the client's ID at the TA. The TA also assigns an ID/private key pair to each gateway and mesh router in its trust domain before deployment. Advantages of this general trust relationship with the TA system from the direct authentication of the clients.

**4. SECURITY ARCHITECTURE**




The above figure shows the security architecture.

**Ticket-Based Security Architecture**

The ticket-based security architecture consists of ticket issuance, ticket deposit, fraud detection and ticket revocation protocols. These are also fulfilled with authentication, data integrity and confidential communication that take place during execution of these protocols.

**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 ticket generation, which can be restrictive partially blind signature scheme in the literature, takes as input clients and TA's secret numbers, the common agreement and some public parameters generates a valid ticket. The serial no. of client is based on clients account no. This information is summarized at the TA by performing the fraud detection based on the ticket records reported by gateways that have serviced this client. By placing the misbehavior information in tickets, the TA successfully informs gateways about the client's past misbehavior when the ticket is deposited. At the same time we

do not leak any information of misbehavior to any entity in the network.

The merit of this system is to punish clients with misbehavior history with higher network access latency. The gate way may intend to service well-behaved clients immediately upon receiving the ticket, and report ticket records to the TA at a later time. If the client appears to have misbehaved previously, and thus, may cast a threat on network operations, the gateway will first report the ticket record to the TA and will service the client only if the TA returns positive feedback.

**Pseudonym Generation and Revocation**

This technique is used to hide the location of user. Where a batch of pseudonyms is assigned to each client by the TA, the self –generation method vastly reduces the communication overhead in the system. Moreover, the client is able to frequently update his pseudonyms to enhance anonymity by using this inexpensive method.

The pseudonym ticket is active only when its associated ticket is actively in use. The revocation process automatically revokes the ticket-bound pseudonyms.

## 5. SECURITY ANALYSIS

In this section, we analyze the security requirements that can be in this system as follows:

**Fundamental Security Objectives**

It is trivial to show that this 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, messaged authentication code and encryption in this system. We are only left with the proof of non-repudiation in the above category. A fraud can be repudiated only if the client provided a different representation he knows from what is derived by the TA. If the client has misbehaved, the representation he knows will be the same as the one derived by the TA which ensures known repudiation.

**Anonymity**

First of all, it can be easily shown that 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 clients 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 clients deposit gateway (DGW) cannot deduce the client's ID from the deposited ticket, which has been blinded by the client and doesn't reveal any identification information unless misbehavior occurs.

**Traceability (**Conditional anonymity**)**

According to its definition, this requirement is to fold: 1) Anonymity for honest client's is unconditional 2) A misbehaving client is traceable where the identity can be revealed.

**Framing resistance**

If the client is honest, with overwhelming probability, the representation the user 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. Therefore, innocent clients exculpate themselves to prevent malicious TAs from revoking their network access privilege.

**Unforgeability**

The proof of unforgeability is essentially the proof of the adopted restrictive partially blind signature scheme is existentially unforgeable against adoptively chosen message and ID attacks.

By this system we can conclude that the proposed security architecture satisfies the security requirements for anonymity, traceability, framing resistance and unforgeability, in addition to the fundamental objectives including authentication, data integrity, confidentiality and non-repudiation.

## CONCLUSION

In this paper, we propose, a security 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 hierarchical identity-based cryptography, the proposed architecture is demonstrated to achieve desired security objectives and efficiency.

## 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, September 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] 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.

[5] 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.

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

[7] M. Raya and 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 and J-P. Hubaux,"Securing Wireless Mesh Networks", IEEE Wireless Comm.,vol. 13, no. 2,pp. 50-55, Apr. 2006.

[9] Y. Zhang and 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 and W.Wang,"Wireless mesh networks a survey", computer networks, vol.47,no.4,pp.445-487,mar.2005.