JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

A Secure payment System for banking transactions

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 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 norepudiation. Thorough analysis on security and efficiency is incorporated, demonstrating the feasibility and effectiveness of the proposed architecture.

JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

OBJECTIVE:

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). 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.

EXISTING SYSTEM:

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.

JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

Disadvantages of Existing Systems:

In the existing Systems, there exists Conflicts between the anonymity and traceability.

The fundamental security requirements including authentication, confidentiality, data integrity, and non-repudiation are not achieved in the existing systems.

PROPOSED SYSTEM:

We are motivated by resolving the above security conflicts, namely anonymity and traceability, in the emerging WMN communication systems.

We have proposed the initial design of our security architecture, where the feasibility and applicability of the architecture were not fully understood. As a result, we provide detailed efficiency analysis in terms of storage, communication, and computation in this paper to show that our SAT is a practically viable solution to the application scenario of interest.

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

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.

Advantages of proposed System:

Our work differs from previous work in that WMNs have unique hierarchical topologies and rely heavily on wireless links, which have to be considered in the anonymity design. As a result, the original anonymity scheme for payment systems among bank, customer, and store cannot be directly applied.

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.

Moreover, although we employ the widely used pseudonym approach to ensure network access anonymity and location privacy, our pseudonym generation does

JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

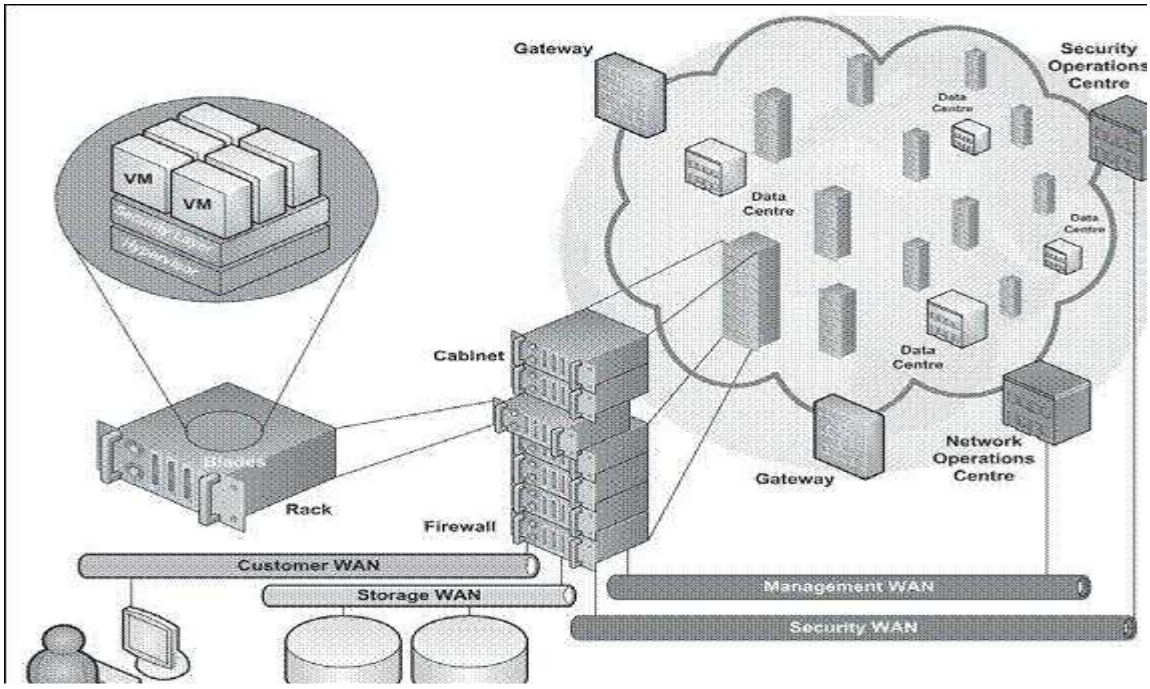
Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

not rely on a central authority, e.g., the broker , the domain authority , the transportation authority or the manufacturer, and the trusted authority , who can derive the user's identity from his pseudonyms and illegally trace an honest user.

Our system is not intended for achieving routing anonymity, which can be incorporated as an enhancement.

Architecture:



JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.
jpinfotechprojects@gmail.com

MODULES:

- ✓ Wireless mesh networks (WMNs)
- ✓ Blind Signature
- ✓ Ticket Issuance
- ✓ Fraud Detection
- ✓ Fundamental security objectives

MODULE DESCRIPTION:

Wireless mesh networks (WMNs)

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 the central server of a campus WMN.

JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

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. We refer the readers for a formal definition of a blind signature scheme, which should bear the properties of verifiability, unlinkability, and unforgeability. 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.

Ticket Issuance

In order to maintain security of the network against attacks and the fairness among clients, the home server manager may control the access of each client by issuing tickets based on the misbehavior history of the client, which reflects the server manager’s confidence about the client to act properly. Ticket issuance occurs when

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

the client initially attempts to access the network or when all previously issued tickets are depleted. The client needs to reveal his real ID to the server manager in order to obtain a ticket since the server manager has to ensure the authenticity of this client.

Fraud Detection

Fraud is used interchangeably with misbehavior in this paper, which is essentially an insider attack. 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 server manager to constrain his ticket requests.

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, message authentication code, and encryption, in our system. We are only left with the proof of non-repudiation in this category. A fraud can be repudiated only if the client can provide a different representation, he knows of message from what is derived by the server manager. If the client has misbehaved, the representation he knows will

be the same as the one derived by the server Manager which ensures non-repudiation.

SYSTEM SPECIFICATION:

HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 256 Mb.

SOFTWARE REQUIREMENTS:

- Operating system : Windows XP Professional
- Front End : JAVA, Swing(JFC),J2ME
- Tool : Sun Java Wireless Toolkit 2.5.2 (J2ME Code)