International Journal of Scientific & Engineering Research, Volume 8, Issue 4, April-2017
ISSN 2229-5518

Ticket-Based Security Architecture for Achieving Obscurity and Ascribable in Mobile Ad Hoc Networks

Nagaraj.C, and Sandhya.K

Abstract- Obscurity has received increasing attention in the literature due to the users' awareness of their privacy nowadays. Obscurity provides protection for users to enjoy network services without being traced. While Obscurity-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 Connectionless mesh networks (WMNs). On the other hand, the network authority requires conditional Obscurity such that misbehaving entities in the network remain traceable. In this paper, we propose a security architecture to ensure unconditional Obscurity for honest users and Ascribable of misbehaving users for network authorities in WMNs.
Key Words-Ad-hoc netwrok

---

1. INTRODUCTION

The main objective is resolving the security conflicts, namely systems.Connectionless Mesh Network (WMN) is a promising technology and is expected to be widespread due to its low investment feature and the Connectionless broadband services it supports, attractive to both service providers and users. However, security issues inherent in WMNs or any Connectionless 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. Connectionless security has been the hot topic in the literature for various network technologies such as cellular networks, Connectionless local area networks (WLANs), Connectionless sensor networks, mobile ad hoc networks (MANETs), and vehicular ad hoc networks (VANETs).

Recently, new proposals on WMN security have emerged. In the authors describe the specifics of WMNs and identify three fundamental network operations that need to be secured. An attack security architecture (ARSA) for WMNs, addressing countermeasures to a wide range of attacks in WMNs. -resilient security architecture (ARSA) for WMNs, addressing countermeasures to a wide range of attacks in WMNs. Obscurity and privacy issues have gained considerable research efforts in the literature which have focused on investigating Obscurity in different context or application scenarios. One requirement for Obscurity is to unlink a user's identity to his or her specific activities, such as the Obscurity 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. Obscurity is also required to hide the location information of a user to prevent movement tracing, as is important in mobile networks and VANETs.

In Connectionless 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 Obscurity is indispensable, which conceals the confidential communication relationship of two parties by building an anonymous path between them. Nevertheless, unconditional Obscurity may incur insider attacks since misbehaving users are no longer traceable is highly desirable such as in e-cash systems where it is used for detecting and tracing double-spenders.

In this project, we are motivated by resolving the above security conflicts, namely Obscurity and Ascribable, in the Emerging WMN communication systems. We have proposed the initial design of our security architecture in, 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 project to show that our scri is a practically viable solution to the application scenario of interest. Our system borrows the blind signature technique from payment systems and hence, can achieve the Obscurity of unlinking user identities from activities, as well as the Ascribable of misbehaving users. Furthermore, the proposed Obscurity and Ascribable, in the emerging WMN communication pseudonym technique renders user location information unexposed. Our work differs from previous work in that WMNs have unique hierarchical topologies and rely heavily on Connectionless links, which have to be considered in the Obscurity design. As a result, the original Obscurity

NAGARAJ.C, SANDHYA.K
Assistant Professor,
c.nagaraj91@gmail.com, ksandhya.hsr@gmail.com
Spurthy College of Science and Management Studies, Bangalore.

scheme for payment systems among bank, customer, and store cannot be directly applied. In addition to the Obscurity scheme, other security issues such as authentication, key establishment, and revocation are critical in WMNs to ensure the correct application of the Obscurity scheme. Moreover, although we employ the widely used pseudonym approach to ensure network access Obscurity and location privacy, our pseudonym generation does not rely on a central authority, e.g., the broker in, the domain authority in, the transportation authority or the manufacturer in, and the trusted authority in, who can derive the user's identity from his pseudonyms and illegally trace an honest user. Note that our system is not intended for achieving routing Obscurity, which can be incorporated as an enhancement. Specifically, our major contributions in this project include,

- Design of a ticket-based Obscurity system with Ascribable property.
- Bind of the ticket and pseudonym which guarantees anonymous access control (i.e., anonymously authenticating a user at the access point) and simplified revocation process.
- Adoption of the hierarchical identity-based cryptography (HIBC) for inter-domain authentication avoiding domain parameter certification.

2 SYSTEM ANALYSIS

2.1Existing System

Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads to a very demanding environment to provide security. Public-key cryptography is too expensive to be usable, and even fast symmetric-key ciphers must be used sparingly. Communication bandwidth is extremely dear: each bit transmitted consumes about as much power as executing 800–1000 instructions [13], and as a consequence, any message expansion caused by security mechanisms comes at significant cost.

2.1.1Disadvantages

One requirement for Obscurity is to unlink a user's identity to his or her specific activities, such as the Obscurity 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.
Unconditional Obscurity may incur insider attacks since misbehaving users are no longer traceable. Therefore Ascribable is highly desirable such as in e-cash systems where it is used for detecting and tracing double-spenders.

2.2Proposed System

Security architecture to ensure unconditional Obscurity for honest users and Ascribable of misbehaving users for network authorities in WMNs. The proposed architecture strives to resolve the conflicts between the Obscurity and Ascribable 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.

2.2.1 Advantages

- Design of a ticket-based Obscurity system with Ascribable property.
- Bind of the ticket and pseudonym which guarantees anonymous access control (i.e., anonymously authenticating a user at the access point) and simplified revocation process.
- Adoption of the hierarchical identity-based cryptography (HIBC) for inter-domain on avoiding domain parameter certification.

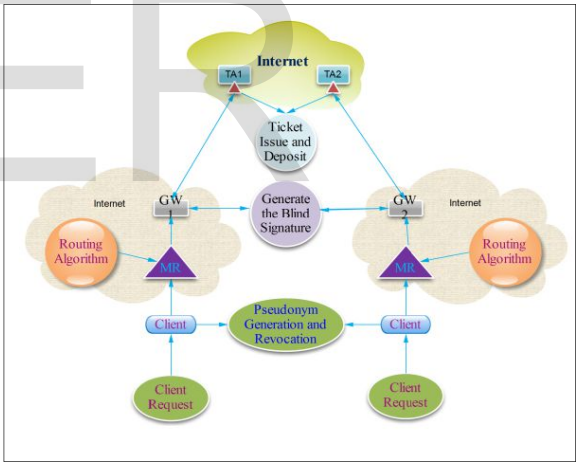


Figure 2.2.1 System Architecture

The Connectionless mesh backbone consists of mesh routers (MRs) and gateways (GWs) interconnected by ordinary Connectionless 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. 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 Connectionless links, displayed as solid and bold dashed lines, respectively. 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.

The WMNs of interest here are those where the TA provides free Internet access but requires the clients (CLs) to be authorized and affiliated members generally for a long term use in WMNs.

2.3 Feasibility study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

2.3.1 Economical feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

2.3.2 Social feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity.

The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

2.3.3 Technical feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources.

This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system

3Problem Definition

Security issues inherent in WMNs or any Connectionless 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.

Our system borrows the blind signature technique from payment systems and hence, can achieve the Obscurity of unlinking user identities from activities, as well as the Ascribable of misbehaving users. Furthermore, the proposed pseudonym technique renders user location information unexposed. Our work differs from previous work in that WMNs have unique hierarchical topologies and rely heavily on Connectionless links, which have to be considered in the Obscurity design. As a result, the original Obscurity scheme for payment systems among bank, customer, and store cannot be directly applied. In addition to the Obscurity scheme, other security issues such as authentication, key establishment, and revocation are critical in WMNs to ensure the correct application of the Obscurity scheme. Moreover, although we employ the widely used pseudonym approach to ensure network access Obscurity and location privacy, our pseudonym generation does not rely on a central authority.

4 Overview of SOA

In this project, we are motivated by resolving the above security conflicts, namely Obscurity and Ascribable, in the emerging WMN communication systems. We have proposed the initial design of our security architecture in, 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 project to show that our SOA is a practically viable solution to the application scenario of interest. Our system borrows the blind signature technique from payment systems, and hence, can achieve the Obscurity of unlinking user identities from activities, as well as the Ascribable of misbehaving users.

Furthermore, the proposed pseudonym technique renders user location information unexposed. Our work differs from previous work in that WMNs have unique hierarchical topologies and rely heavily on Connectionless links, which have to be considered in the Obscurity design. As a result, the original Obscurity scheme for payment systems

among bank, customer, and store cannot be directly applied. In addition to the Obscurity scheme, other security issues such as authentication, key establishment, and revocation are critical in WMNs to ensure the correct application of the Obscurity scheme. Moreover, although we employ the widely used pseudonym approach to ensure network access Obscurity and location privacy, our pseudonym generation does not rely on a central authority, e.g., the broker in, the domain authority in, the transportation authority or the manufacturer in, and the trusted authority in , who can derive the user's identity from his pseudonyms and illegally trace an honest user. Note that our system is not intended for achieving routing Obscurity, which can be incorporated as an enhancement.

5 Module Description

- Client & Trusted Node deployments
- Ticked issuance and deposit process
- Generate pseudonym and revocation process
- Blind Signature generation
- Fraud Detection & Ticket Revocation process
- Accessing the Network from Foreign Domains
- Inter-Domain Authentication from Mesh-Router.

5.1.1 Client & Trusted Node Deployments

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., intra domain). We further assume the existence of pre-shared keys and secure communication channels between entities (TAs, gateways, mesh routers) at the backbone 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.

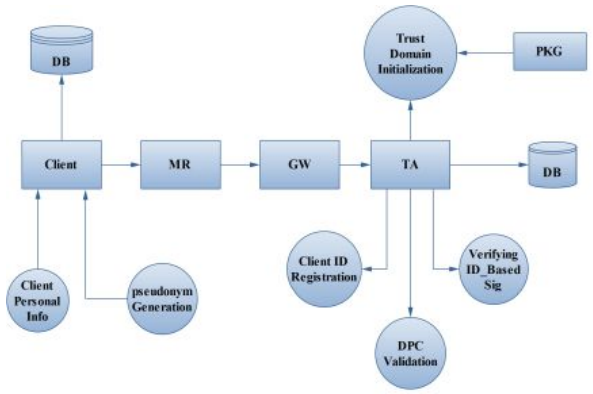


Figure 5.1.1 Client & Trusted Node Deployments

The client selects a unique account number computed by a randomly chosen secret number u1. 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 stem from the direct authentication of the clients traveling among gateways/mesh routers in the same domain, which reduces network access latency and communication overhead that is expected to be overwhelming in future WMNs due to the large user population and high mobility. The domain initialization of the hierarchical IBC. Specifically, the root public key generator (PKG) at level 0 in the HT performs the following domain initialization algorithm when the network is bootstrapped, where P0 is a generator of G1.

5.1.2 Ticked Issuance and Deposit Process

Ticket issuance occurs when 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 TA in order to obtain a ticket since the TA has to ensure the authenticity of this client. Moreover, the TA should be unable to link the ticket it issued to the clients' real identities. The client thus employs some blinding technique to transform the ticket to be un-linkable to a specific execution of the ticket generation algorithm (the core of ticket issuance protocol), while maintaining the verifiability of the ticket. The ticket generation algorithm, which can be any restrictive partially blind signature scheme in the literature, takes as input the client's and TA's secret numbers, the common agreement c, and some public parameters, and generates a valid ticket = {TN;W; C; (U'; V';X';)} gat the output, where TN is the unique serial number of the ticket that can be computed from the client's account number We opt for a partially restrictive blind signature scheme with two desired features: partial blindness and restrictiveness for the proposed WMN

framework. Partially blind signatures alone allow the blind signature to carry explicit information on commonly agreed terms (i.e., ticket value, expiry date, misbehavior, etc.) which remains publicly visible regardless of the blinding process.

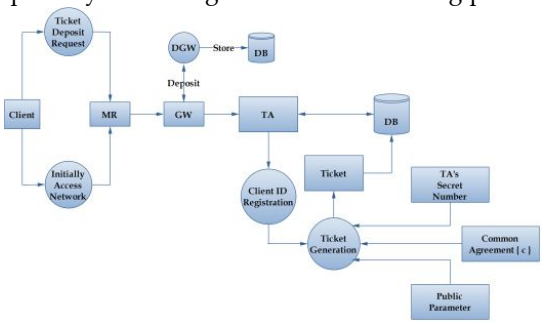


Figure 5.1.2 Ticked Issuance and Deposit Process

Restrictive blind signatures place restrictions on the client's selection of messages being signed which contain encoded identity information (in TN) instead of completely random numbers, allowing the TA to recover the client's identity by computing if and only if misbehavior is detected. A design issue to be pointed out is the commonly agreed information c negotiated at the beginning of the ticket generation algorithm. We define c as (Val; exp; misb), where Val, exp, and misb denote the ticket value, expiry date/time, and the client's misbehavior level, respectively. The ticket value confines the total amount of traffic that the client is allowed to generate and receive before the expiry date of the ticket. Tickets bear different values. The value val is issued by the TA and will be deducted by the gateway in the ticket deposit protocol. The client's misb field conveys information on the misbehavior history of the client in the network.

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 c, the TA successfully informs gateways about the client's past misbehavior when the ticket is deposited. 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. Our scheme restricts the ticket to be deposited only once at the first encountered gateway that provides network access services to the client according to val before exp. The ticket is deemed valid if both the signature verification and the above equality check succeed. 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 TA may decrease the value of the issued tickets or reduce the frequency of approving the client's ticket requests based on the misbehavior level indicated in misb.

5.1.3. Generate Pseudonym and Revocation Process

The use of pseudonyms has been shown in the ticket-based protocols. This section copes with the pseudonym generation technique and the related revocation issue. 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 intra-domain authentication in our system, the client generates his own pseudonym by selecting a secret number $2 and computing the pseudonym PSCL {H1, IDCL, and P}. The corresponding private key can be derived as g=CL, CL_H1, IDCL, PSCL a batch of pseudonyms are 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 (with tickets) to enhance Obscurity by using this inexpensive method. As a final note on the self-generation algorithm, it would render the pseudonym revocation impossible by using the pseudonym alone.

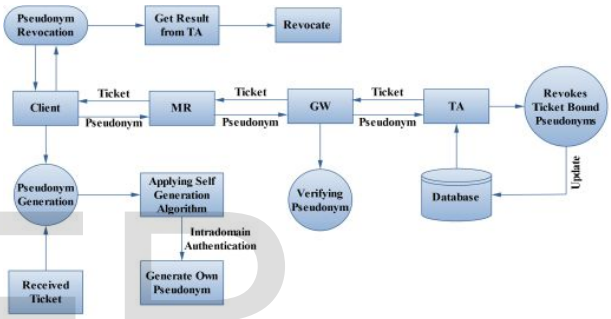


Figure 5.1.3 Generate Pseudonym and Revocation Process

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). in addition to the ticket-related operations, the TA will be required to generate and update the pool of pseudonyms for the client and to distribute the revocation list for revoking all effective pseudonyms in the active pool during a specific period, which induces significantly higher signaling overhead. The TA will also be able to derive the real identity corresponding to the assigned pseudonyms, which destroys the Obscurity for honest clients.

5.1.4Blind Signature Generations

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 for a formal definition of a blind signature scheme, which should bear the properties of verifiability, un-link-ability, and un-forge-ability 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 Ascribable in the restrictive blind signature systems. This is useful when certain information in the signature needs to be reviewed by a third party.

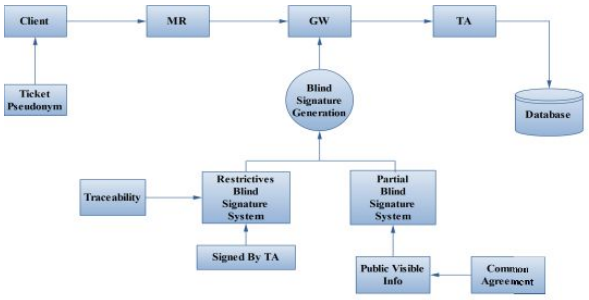


Figure 5.4 Blind Signature Generations

One example is the common agreements, the visibility of which enables the intermediate parties who examine the signature to check the compliance of the signee to the items specified in the agreements, before proceeding to the verification of the signature and other operations.

Restrictive partially blind signature schemes were derived from the aforementioned work. They are essentially blind signature schemes with restrictiveness and partial blindness properties. In the restrictive partially blind signature schemes that serve as a building block for our architecture, the two key concepts, namely restrictiveness and partial blindness A signature scheme is partially blind if, for all probabilistic polynomial-time algorithm A, A wins the game in the signature issuing protocol with probability at most 1 2 þ 1 k for sufficiently large k and some constant. The probability is taken over coin flips of KG, U0, U1, and A, where KG is the key generation function defined in, U0 and U1 are two honest users following the signature issuing protocol. Due to the space limitation, interested readers are referred to for complete description of the game in the signature issuing protocol.

5.1.5Fraud Detection & Ticket Revocation Process

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. Note, however, that since a client is able to obtain multiple tickets in one ticket issuance protocol and self-generate multiple pseudonyms,

he can distribute these pseudonym/ticket pairs to other clients without being traced as long as each ticket is deposited only once. This approach, in general, requires synchronization. Another solution is to adopt the tamper-proof secure module so that a client cannot disclose his secrets to other parties since the secure module is assumed to be expensive and impractical to access or manipulate. In the following discussion, we will still consider multiple deposit as a possible type of fraud (e.g., in case that secure modules are unavailable).

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. When the TA detects duplicate deposits using the ticket records reported by gateways, the TA will have the view of at least two different challen34ges from gateways and two corresponding sets of responses from the same client.

By solving the equation sets below based on these challenges and responses, the TA is able to obtain the identity information encoded in the message, and hence, the real identity of the misbehaving client.

1. Revocation of new tickets: the client may store a number of unused tickets, as mentioned previously. When revoking these tickets that have not been deposited, the client sends PScl,TN,t10, in the revocation request to any SIG TCL ~(TN)||t10 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 PSCL, IDDGW, t11, SIG, in the revocation request to the DGW. The DGW authenticates the client and marks the associated ticket revoked.

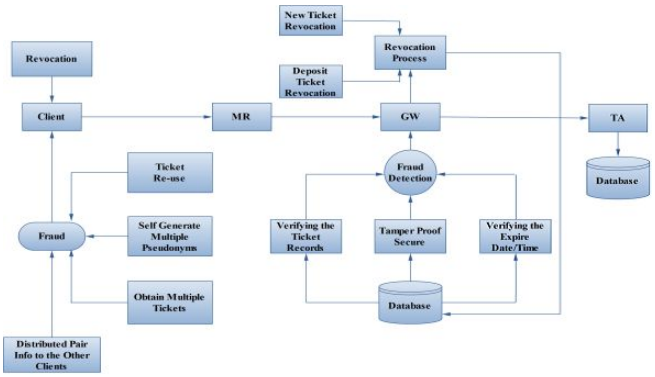


Figure 5.1.5 Fraud Detection & Ticket Revocation Process

5.1.6 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.

MR will forward the network access request consisting of the symmetric key between the client and his home TA, or PSCL; ticket to an access point (a gateway or mesh router) in the client's home domain k QT outputs "accept" in Steps 1 and 2. The symmetric key between the client and MR is a P0, where a; b p and P0 are the public domain parameter of the root PKG. It is noted that the above triangular traffic forwarding via the home domain can be cumbersome if the client will stay at a foreign domain for a long term (e.g., not temporarily visiting). Consequently, all the network access-related operations including ticket issuance, deposit, revocation, and fraud detection will follow the same procedures as in the home domain case, which greatly reduces the communication overhead in the system.

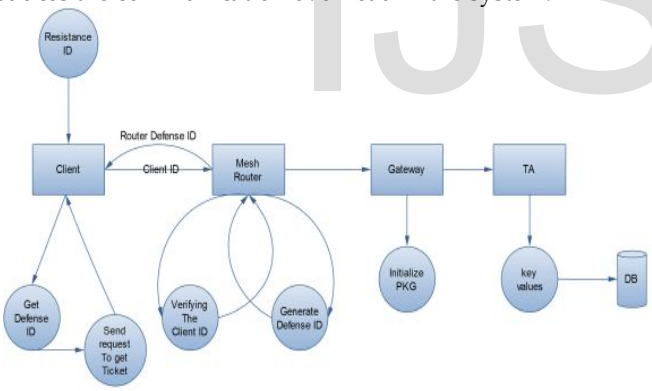


Figure 5.1.6 Accessing the Network from Foreign Domains

5.1.7 Inter-Domain Authentication from Mesh Router

Inter-domain authentication is more important for Connectionless peer-to-peer authentication networks in this module give the inter-domain authentication. The mesh router generate and initialize the Defense ID for each client. The client very first process generates the Resistance ID and gives the resistance ID to mesh router.

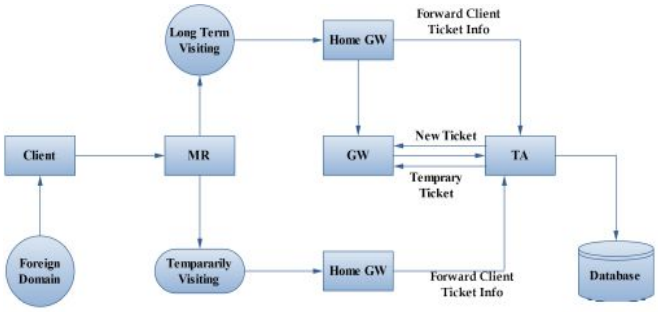


Figure 5.1.7 Inter-Domain Authentication from Mesh Router

The mesh router receives that ID and registers the client resistance ID and send to home domain mesh routers. The mesh router sends the defense ID to client.

5.2 Literature Review

5.2.1 Anonymous Connections and Onion Routing

Onion Routing is an infrastructure for private communication over a public network. It provides anonymous connections that are strongly resistant to both eavesdropping and track analysis. Onion routing's anonymous connections are bidirectional and near real time, and can be used anywhere a socket connection can be used. Any identifying information must be in the data stream carried over an anonymous connection. An onion is a data structure that is treated as the destination address by onion routers; thus, it is used to establish an anonymous connection.

Onions themselves appear differently to each onion router as well as to network observers. The same goes for data carried over the connections they establish. Proxy aware applications, such as web browsing and e-mail, require no modification to use onion routing, and do so through a series of proxies. A prototype onion routing network is running between our lab and other sites. This project describes anonymous connections and their implementation using onion routing. This project also describes several application proxies for onion routing, as well as configurations of onion routing networks.

Is Internet communication private? Most security concerns focus on preventing eaves dropping outsiders listening in on electronic conversations. But encrypted messages can still be tracked, revealing who is talking to whom. This tracking is called trace analysis and may reveal sensitive information. For example, the existence of inter-company collaboration may be Confidential. Similarly, e-mail users may not wish to reveal who they are communicating with to the rest of the world. In certain cases Obscurity may be desirable also: anonymous e-cash is not very anonymous if delivered with a return address.

This project describes anonymous connections, their realization in onion routing, and some of their applications. Anonymous connections are resistant to both eavesdropping

and tra analysis. They separate the Obscurity of the connection from the Obscurity of communication over that connection. For example, two parties controlling onion routers can identify themselves to each other without revealing the existence of a connection between them. This project demonstrates the versatility of anonymous connections by exploring their use in a variety of Internet applications. These application include standard Internet services like Web browsing, remote login, and electronic mail. Anonymous connections can also be used to support virtual private networks with connections that are resistant to analysis and that can carry connectionless traffic.

5.2.2 Selfish MAC Layer Misbehavior in Connectionless Networks

Connectionless Medium Access Control (MAC) protocols such as use distributed contention solution mechanisms for sharing the Connectionless channel. In this environment, selfish hosts that fail to there to the MAC protocol may obtain an unfair throughput share. For example, requires sis competing for access to the channel to wait for a "back off" internal, randomly selected from a specified range, before initiating a transmission. Selfish hosts may wait for smaller back off intervals than all-behaved hosts, thereby obtaining an unfair advantage.

Simulation results under these misbehavior models indicate to our detection and penalty schemes are successful in handling MAC layer misbehavior. Wireless Medium Access Control (MAC) protocols such as use distributed contention resolution mechanisms for sharing the Connectionless channel. The contention resolution mechanism is typically based on cooperative protocols (e.g., random back off before transmission) that attempt to ensure a reasonably fair throughput share for all the participating hosts. In environments where hosts in the network are entrusted, some hosts may misbehave by failing to adhere to the network protocols, with the intent of obtaining an unfair share of the channel. The presence of *selfish* hosts that deviate from the contention resolution protocol can reduce the throughput share received by well-behaved hosts.

Handling MAC layer misbehavior is an important requirement in ensuring a reasonable throughput share for well-behaved hosts in the presence of misbehaving hosts. In this project, we have presented modifications to MAC protocol that simplifies misbehavior detection. Simulation results have indicated that our scheme provides fairly accurate misbehavior diagnosis. The penalty scheme we have proposed is effective in restricting the throughput of selfish hosts to a fair share. We plan to extend the proposed scheme for detecting other types of host misbehavior, such as a host using multiple MAC addresses for obtaining higher throughput, with the support of higher layers. Designing strategies for combining information from multiple observers, as well as optimally placing the observers are part of future work. We also plan to incorporate adaptive selection of protocol parameters into the proposed scheme.

5.2.3 Provably Secure Partially Blind Signatures

Partially blind signature schemes are an extension of blind signature schemes that allow a signer to explicitly include necessary information (expiration date, collateral conditions, or whatever) in the resulting signatures under some agreement with the receiver. This project formalizes such a notion and presents secure and efficient schemes based on a widely applicable method of obtaining witness indistinguishable protocols. We then give a formal proof of security in the random oracle model. Our approach also allows one to construct secure fully blind signature schemes based on a variety of signature schemes.

Digital signature schemes are essential for electronic commerce as they allow one to authorize digital documents that are moved across networks. Typically, a digital signature comes with not just the document body but also attributes such as \date of issue" or \valid until", which may be controlled by the signer rather than the receiver. One cans ¯and more about those attributes in PKCS for instance. Blind signature schemes, ¯rest introduced by Chaum are a variant of digital signature schemes. They allow a receiver to get a signature without giving the signer any information about the actual message or the resulting signature. This blindness property plays a central role in applications such as electronic voting and electronic cash schemes where Obscurity is of great concern.

We have presented formal dentitions of partially blind signature schemes and constructed an enceinte scheme based on the Scanner signature scheme. We then have a proof of security in the random oracle model assuming the intractability of the discrete logarithm problem. Although we have shown a particular construction based on Scanner signature, the basic approach of constructing WI protocols and the proof of security do not substantially rely on the particular structure of the underlying signature scheme. Accordingly, a signature scheme derived from public-coin honest varied zero-knowledge can be plugged into our scheme if it can be blinded. It covers, for instance, signature and some variants of muddied Algoma Signature schemes. As we mentioned, one can easily transform fully blind signature schemes from partially blind ones. We have shown that the reverse is possible; partially blind signature scheme.

5.2.4 ID-based restrictive partially blind signatures and applications

Restrictive blind signatures allow a recipient to receive a blind signature on a message not known to the

signer but the choice of message is restricted and must conform to certain rules. Partially blind signatures allow a signer to explicitly include necessary information (expiration date, collateral conditions, or whatever) in the resulting signatures under some agreement with receiver. Restrictive partially blind signatures incorporate the advantages of these two blind signatures.

The existing restrictive partially blind signature scheme was constructed under certificate-based (CA-based) public key systems. In this project we follow Brand's construction to propose the first identity-based (ID-based) restrictive blind signature scheme from bilinear pairings. Furthermore, we first propose an ID-based restrictive partially blind signature scheme, which is provably secure in the random oracle model. As an application, we use the proposed signature scheme to build an untraceable off-line electronic cash system followed the Brand's construction.

5.2.5Identity-based identification and signature Schemes using correcting codes

The most critical point of classical public key cryptography (RSA, El gamely...) is in the management of the authenticity of the public key. In fact, if Alice manages to take Bob's identity by cheating her own public key as Bob's one, she would be able to decipher all messages sent to Bob and to sign any message using the stolen identity. Shamir introduced the concept of Identity-based Public Key Cryptography in order to simplify the management and the authentication of the public key, which, time passing by, had become more and more complex. In the ID-PKC scheme of Shamir, the public key of an user is undeniably linked to his identity on the network (user-id): it can be a concatenation of any publicly known information: his name, his e-mail, his phone number, etc ...

Hence it is not necessary to verify a certificate for the public key or to contact a data base to obtain it. At first glance it seems simple but producing private keys becomes more complex. And since a private user cannot derivate his own private key by himself, it is necessary to introduce trusted third party which derivate the private key from the public key and sends it to the user (at least it has to be done once for each user).

In this project we presented an IBI and a related IBS scheme based on error correcting code. This scheme is the first non-number theory based identity based scheme. The scheme combines two well-known schemes and inherits from bad properties of these schemes: the public data is large, the communication cost for the IBI scheme is large and the signature length for the IBS scheme is also very large but besides these weaknesses our scheme presents the first alternative to number theory for ID-based cryptography and may open a new area of research.

5.2.6 Obscurity in Connectionless Broadcast Networks

Systems that provide network traffic Obscurity typically focus on wide-area network topologies, and exploit the infeasibility of eavesdropping on all links to prevent attackers from determining communication peers. This approach is inappropriate for high-security Connectionless local area networks, since it does not obscure the traffic volume, allowing attackers to identify critical nodes (e.g., a military HQ) and, given the ability of an attacker to obtain a global view of all communications, the relative ease of identifying the source and destination of traffic flows. These weaknesses derive from the fact that, whereas in wide-area networks the sender, the receiver and the adversary are on different physical links, in Connectionless networks they may share a single broadcast link.

Moreover, the adversary can easily and the physical location of the transmitter and thereby identify the entity sending the track, not just its network identity. We introduce Connectionless Anonymous Routing (war), an approach to achieve Obscurity in a broadcast network. We describe a formal threat model for war and compare it to the traditional Obscurity approaches. We show that these are inadequate when applied to the broadcast model, and describe new protocols that preserve security with better performance, adequately addressing the requirements of security-critical environments.

We provide analytical and some preliminary experimental evidence that our protocols achieve Obscurity at a reasonable cost. Obscurity and resistance to traffic analysis is an interesting and difficult problem in computer networking. In most modern networks, including IP-based ones, communication peers inherently identify the sources and destinations of traffic to routers, gateways, and ancillary servers. In packet-switched networks, the network-level addresses are visible to anyone with access to any link over which the traffic flows. An especially difficult aspect of this problem involves hiding various aspects of the identity of peers from each other.

Obscurity has many potentially interesting applications in Connectionless networks, but conventional protocols do not work well in these environments. We have introduced a security model for Connectionless Obscurity as well as a suite of protocols that provides basic Obscurity functions in local broadcast networks. Our analytical and experimental results suggest that the protocols are realistic and sufficiently efficient to be useful in practice for many applications. A number of interesting and significant problems re-main, however. Admission control and network management is perhaps the most significant area here: how do we control network membership, especially in ad-hoc public networks, and how can we best link such networks together? How do Obscurity networks perform under, and how can they adapt to, highly dynamic and difficult radio conditions (especially where there are many, mostly disjoint, users with only a few links between them)? And, of course, issues of scale

are likely to be especially difficult. Believe the model and analysis we presented in this project will serve as a useful launching pad to answering these interesting questions.

5.2.7 Preserving Traffic Privacy in Connectionless Mesh Networks

Multi-hop Wireless mesh network (WMN) has attracted increasing attention and deployment as a low-cost approach to provide last-mile broadband Internet access. Privacy is a critical issue in WMN, as traffic of an end user is relayed via multiple Wireless mesh routers. Due to the unique characteristics of WMN, the existing solutions applied in Internet are either ineffective at preserving privacy of WMN users, or will cause severe performance degradation. In this project, we propose a light-weight privacy preserving solution aimed to achieve well-maintained balance between network performance and traffic privacy preservation.

At the center of this solution is a novel metric called "traffic entropy", which quantifies the amount of information required to describe the traffic pattern and is used to characterize the performance of traffic privacy preservation. We further present a penalty-based shortest path routing algorithm that maximally preserves traffic privacy by minimizing the mutual information of "traffic entropy" observed at each individual relaying node, meanwhile controlling performance degradation within the acceptable region. Extensive simulation study proves the soundness of our solution.

Recently, multi-hop Wireless mesh network (WMN) has attracted increasing attention and deployment as a low-cost approach to provide last-mile broadband Internet access In a WMN, each client. Accesses a stationary Connectionless mesh router. Multiple mesh routers communicate with one another to form a multi-hop Connectionless backbone that forwards user traffic to a few gateways connected to the Internet. Some perceived benefits of WMN include enhanced resilience against node failures and channel errors, high data rates, and low costs in deployment and maintenance.

This project identifies the problem of traffic privacy preservation in Wireless mesh networks (WMN). To attack this problem, we start by introducing a lightweight architecture for WMN, then propose "traffic entropy", an information theoretic metric to quantify how well a solution performs at preserving the traffic pattern confidentiality, all of which pave the way to our penalty-based shortest path routing algorithm. Simulation results show that our algorithm is able to maximally preserve the traffic privacy, meanwhile managing the network performance degradation within the acceptable region. For the future work, we will focus on the following problems. First, multiple observing nodes may collude to analyze the traffic pattern of a destination node. Besides new routing solutions to defend collusion, we also need to extend the "traffic entropy" concept by applying the chain rules in information theory. Second, although our algorithm is evaluated in a single-radio, single-channel setting, it can be easily enhanced to exploit the advantage of multiple radios and multiple channels available in WMNs. Performance evaluation of the enhanced algorithm in such settings will be an interesting future work.

5.3 Data Flow Diagram

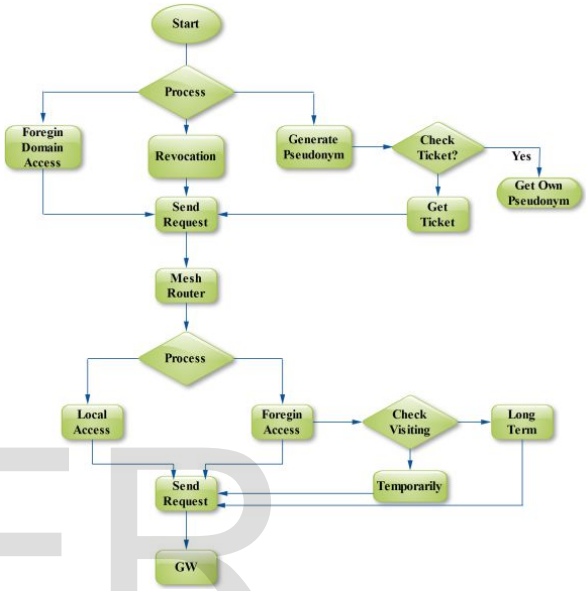


Figure 5.3.1 Data Flow Diagram 1

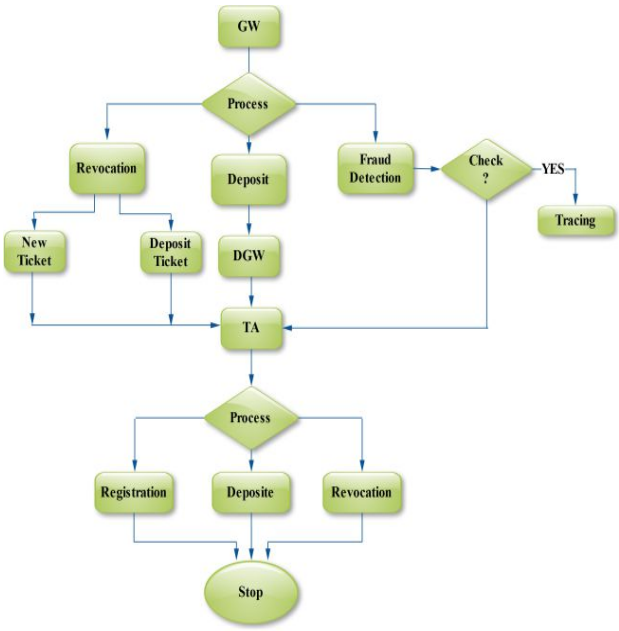


Figure 5.3.2 Data Flow Diagram 2

In the above Data Flow Diagram, Initial process client send the personal information to Trusted Authority, The process for foreign domain access request and revocation process request send to mesh router. After receiving the ticket from TA the client node generate pseudonym and then send to GW. In mesh router check the accessing process. If local accesses send the request to GW otherwise check the visiting. If long term visiting get a new ticket otherwise get temporally ticket from DGW. In Gateway handle the three processes in first ticket deposit request verifying the ticket, pseudonym and then generate the blind signature. Revocation for new ticket, deposit ticket and send to TA. Third fraud detection check the every request to fraud detection if any problem to tracing requested users. In TA getting the request from GW, the request is client personal information so the trusted authority register the personal information and also handle the deposit request and revocation process.

Data Flow Diagram:
Level Data Flow Diagram:

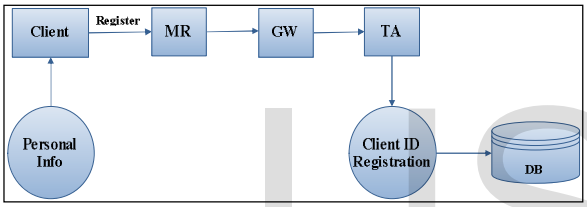


Figure 5.3.3 Level 0

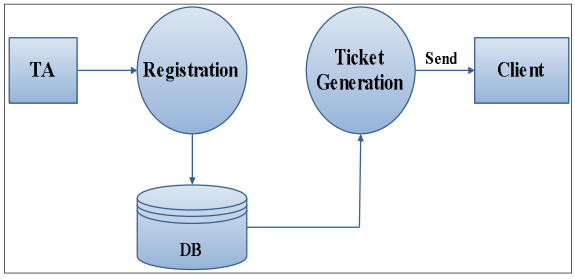


Figure 5.3.4 Level 1

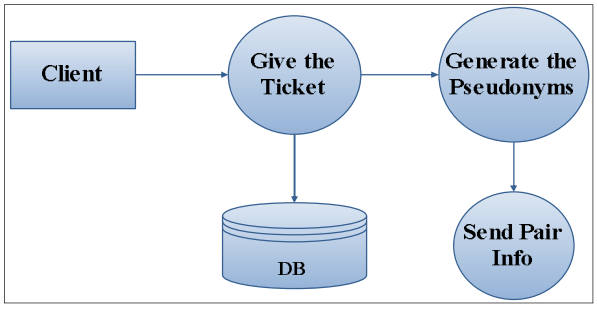


Figure 5.5.5 Level 2

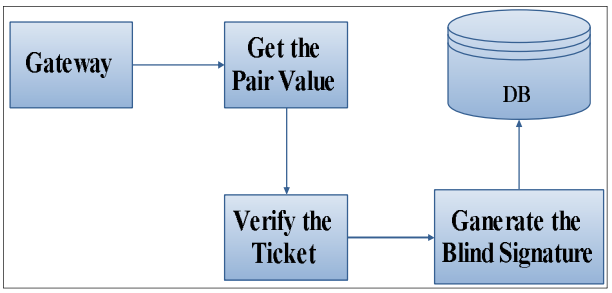


Figure 5.3.6 Level 3

5.4 E-R Diagram

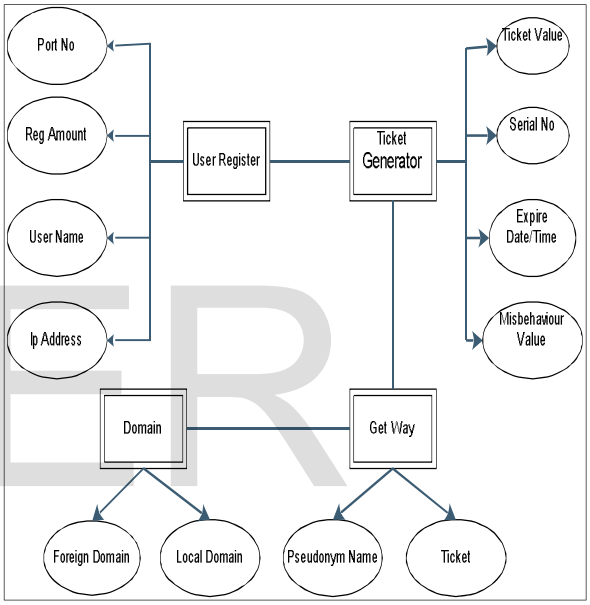


Figure 5.4.1 E-R Diagram

5.5 Database Design

securitydatabase.trusted_authority: 1 records total

Client_Name	Address	PortNo	AccountType	Amount
UserA	Localhost	2000	Current Account	5000

5.5.1 Trusted Authority Table

securitydatabase.address: 1 records total

Name	Address	Port
Gateway	localhost	2001

5.5.2 Address Table

securitydatabase.ticket_details: 22 records total

Ticket_SerialID	Ticket_Value	Ticket_Expire	Ticket_MisbeValue
22222OOOOOO888	3477136	9:1:2012/17:23:30	0
AAAAABBVT40JBUU	8802593	9:1:2012/17:30:45	5
AA991199FFF33GG	1139311	9:1:2012/22:41:41	0
AAAAQQQLLLLLLMM	8277331	9:1:2012/22:49:14	6
AAAAAA8333333666	979728	10:1:2012/11:23:44	4
AR88888888HHB666	2971373	10:1:2012/18:38:57	5
AAIIBODV3IIIIIII	8943630	10:1:2012/18:45:33	3
AAAAAAAA888888T	9415347	14:1:2012/11:3:34	6
TTTJJJE9666CCCC6	9320736	14:1:2012/11:26:58	0
AAA8EEEB0000000L	5791386	14:1:2012/11:31:45	3
HHHH19999TBBBB0C	4324090	14:1:2012/11:35:38	5
AA777QQQQCCS0JJ	1410142	14:1:2012/12:52:45	5
A5ICCJJJJJJ61999	8329134	14:1:2012/12:55:31	4
ALL44FZZZZZFF555	6811617	14:1:2012/13:30:18	6
000008999XX88R22	4606990	14:1:2012/13:34:1	0
AAAAAUUK8833999	5799995	14:1:2012/17:37:25	8
AAUUUU667770077	7001542	14:1:2012/17:42:57	0
AAATTNO744911222	9115021	24:1:2012/12:25:47	8
A9JJJJ24RRQQ0TTT	437656	29:1:2012/1:14:25	9
AAAAAVVVVVHKKKKI	9462521	29:1:2012/1:17:9	6
AAAAAAAAS9000DC	6209103	29:1:2012/11:37:6	4
AHH0002BBA666111	4239762	31:1:2012/15:13:17	2

5.7.3 Ticket Table

securitydatabase.signature: 1 records total

Name	Signature
UserA	16E0785A9B6500F4D8FAE049

5.7.4 Signature Table

The database design is a must for any application developed especially more for the data store projects. Since the chatting method involves storing the message in the table and produced to the sender and receiver, proper handling of the table is a must.

5.8 Input Design

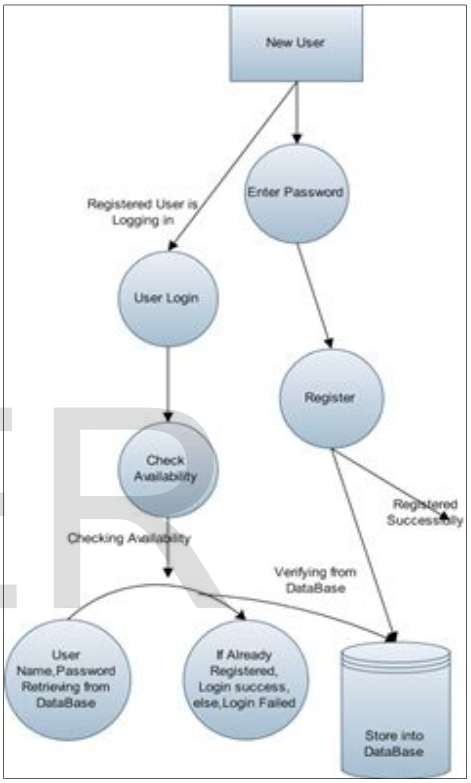
Input design is the process of converting user-originated inputs to a computer-based format. Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system. In the project, the input design is made in various window forms with various methods.

Module Description:

- ✓ User Registration
- ✓ Working Type
- ✓ Connecting to SAT Server
- ✓ Avoiding/Blocking Users

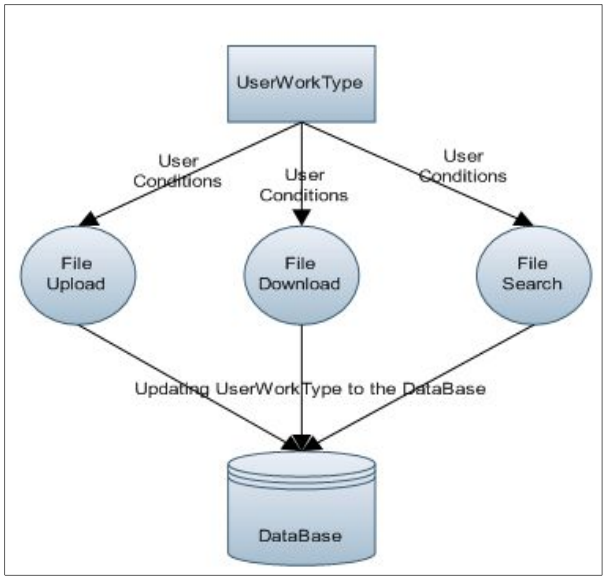
User Registration:

1. New User is registered first, then entering the password.
2. If the user is registered then the message will be displayed,"Registered successfully".
3. Then the details will be stored to Database.
4. The user is trying to login, then it checks the availability.
5. If the user is already registered, it retrieves from database.
6. If you're User Name and password is already registered, you will be allowed to login.
7. You're User Name and password is not correct, then your login will be failed.



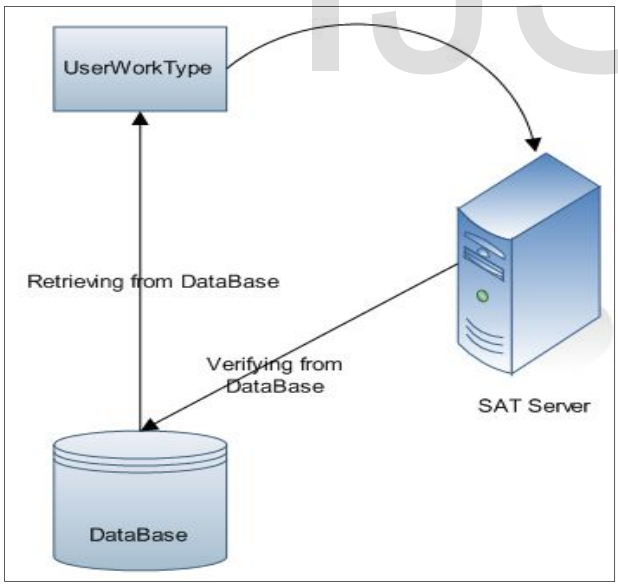
Working Type:

1. The User has some conditions to work in this SAT Server.
2. The User's conditions are, "**File Upload, File Download, and File Search**".
3. Then the User has to use that condition only to the further works.
4. Then the User conditions have to be updating to the Database.



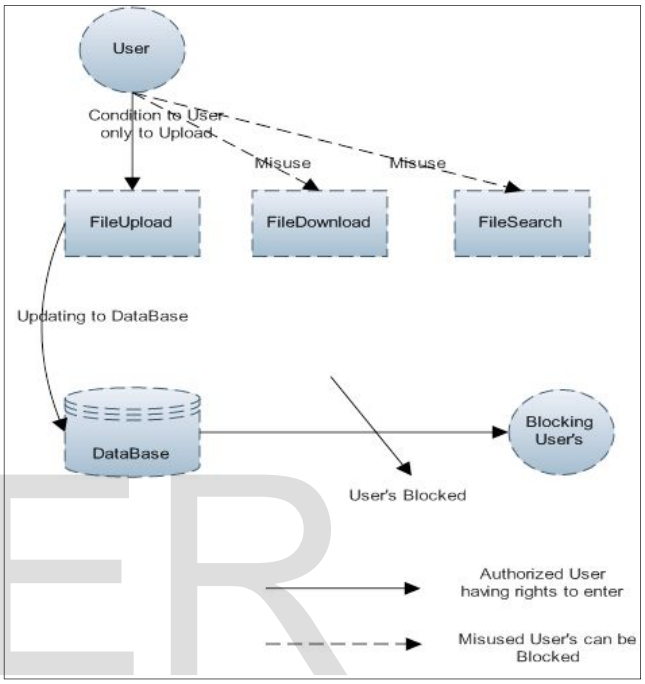
Connecting to SAT Server:

1. If the User's conditions are given by the user, then, the users conditions to be retrieved from Database.
2. If the User gives the condition without permission, then the SAT Server should be verifying from the Database.



Avoiding/Blocking Users:

1. The User is registered to the condition for ex : (File Upload), then they works with any other conditions for ex :(File Download or File Search), then the user can be blocked or avoided.
2. If the User gives the correct condition then the user should be considered as "**Authorized User**".
3. Else, the User is considered as "**Anonymity".**
4. Then the User should be "**Traced**" by the "**SAT Server**".
5. Then the "**UN Authorized User"** should be avoided or blocked.



5.9 Output Design

Output design generally refers to the results and information that are generated by the system for many end-users; output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application.

6 Conclusion

This project identifies the problem of traffic privacy preservation in Wireless mesh networks (WMN). To attack this problem, we start by introducing a lightweight architecture for WMN, then propose "traffic entropy", an information theoretic metric to quantify how well a solution performs at preserving the traffic pattern confidentiality, all of which pave the way to our penalty-based shortest path routing algorithm. Simulation results show that our algorithm is able to maximally preserve the traffic privacy, meanwhile managing the network performance degradation within the acceptable region. For the future work, we will focus on the following problems. First, multiple observing nodes may collude to analyze the traffic pattern of a

destination node. Besides new routing solutions to defend collusion, we also need to extend the "traffic entropy" concept by applying the chain rules in information theory. Second, although our algorithm is evaluated in a single-radio, single-channel setting, it can be easily enhanced to exploit the advantage of multiple radios and multiple channels available in WMNs. Performance evaluation of the enhanced algorithm in such settings will be an interesting future work.

10 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] 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 WirelessMesh 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.