# ACHIEVING ANONYMITY AND TRACEABILITY IN WIRELESS MESH NETWORKS WITH A SECURED ARCHITECTURAL DESIGN

Jahnavi Priyadarshini V H Srikoo[1], and Johng Chern[2]
Department of Mathematics and Computer Science
Chicago State University
9501 South King Drive, HWH332, Chicago, IL 60628
[1]jsrikoo@csu.edu, and [2]jchern@csu.edu

## Abstract

Now-a-days, users have a huge awareness on their privacy which is resulting in increase of the anonymity. Anonymity is the quality or state of being unknown or unacknowledged. It provides protection for the users to use the network services without being traced. Even the tracing does not happens, sometimes if any conditional anonymity like misbehaving entities in the network occurs, the network authority keeps such entities traceable.

In this project, security architecture is proposed to ensure the unconditional anonymity for the honest users and tracing the misbehaving users by trusted authorities in WMNs (Wireless *Mesh Networks*). The proposed system architecture can be used to resolve the problems faced between the anonymity and traceability. It also provides fundamental security requirements like authentication, confidentiality, data integrity and nonrepudiation. A thorough analysis has done on security and efficiency that has incorporated which demonstrates the feasibility and effectiveness of the proposed system architecture.

Keywords: *payment based systems, anonymity, wireless mesh networks, confidentiality, authentication, integrity, non-repudiation, security, feasible design;*

# 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).

Recently, new proposals on WMN security have emerged. An attack-resilient security architecture (ARSA) is proposed for WMNs, addressing counter measures to a wide range of attacks in WMNs. Due to the fact that security in WMNs is still in its infancy as very little attention has been devoted so far, a majority of security issues have not been addressed.

Anonymity and privacy issues have gained considerable research efforts in the literature, which have focused on investigating anonymity in different context or application scenarios. 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 this research we take anonymity and un-traceability as our area of interest. 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.

# 2 Literature Review

A WMN is meant to be a communications network which is made up of radio nodes that is organized in a mesh topology. These networks mostly consist of mesh clients, mesh routers and gateways *[1]*. The mesh clients are called as laptops, cell phones and any other wireless devices. The mesh routers will forward the packets or data to and from the gateways which is needed to connect to the internet. Each node operates not only as a host but also as a router.

A WMN is dynamically self-organized and self-configured, with the nodes in the network by automatically establishing and maintaining the mesh connectivity among themselves (creating, in effect, an ad hoc network). This feature brings many advantages

to WMNs such as low up-front cost, easy network maintenance, robustness, and reliable service coverage *[2]*. The mesh connectivity significantly enhances network performance, such as fault tolerance, load balancing, throughput, protocol efficiency; and dramatically reduces cost.

Most of the existing standard wireless networks like Wi-Fi and WIMAX do not have such capabilities. The mesh network is created through the connection of access points installed at each network user's locale. Each network is also a provider that forwards data to the next node. The infrastructure of this network is decentralized and simplified as the data is just transmitted to the next node.

Wireless mesh networks can be easily, effectively and wirelessly connect entire cities using inexpensive, existing technology. In a wireless mesh network, only one node needs to be physically wired to a network connection like a DSL Internet modem *[3]*. That one wired node then shares its Internet connection wirelessly with all other nodes in its vicinity. Those nodes then share the connection wirelessly with the nodes closest to them. The more nodes, the further the connection spreads, creating a wireless "cloud of connectivity" that can serve a small office or a city of millions.

Wireless Mesh Network (WMN) is the promising technology and is expected to be widespread due to its low investment feature and wireless broadband services it supports, which is attractive to both the 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 *[4]*. 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).

A wireless LAN (or WLAN, for wireless local area network, sometimes referred to as LAWN, for local area wireless network) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. The IEEE 802.11 group of standards specifies the technologies for wireless LANs. 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wired Equivalent Privacy algorithm *[5]*. It uses high-frequency radio waves rather than wires to communicate between nodes.

Peer-to-peer is a communications model in which each party has same capabilities and either party can initiate a communication session *[6]*. Other models with which it might be contrasted include the client/server model and the master/slave cases, peer-to-peer communications is implemented by giving each communication node both server and client capabilities. In recent usage, peer-to-peer has come to describe applications in which users can use the Internet to exchange files with each other directly or through a mediating server. This differs from client/server architecture in which some computers are dedicated to serving the others. Peer-to-peer networks are generally simpler, but they

usually do not offer the same performance under heavy loads. Peer-to-peer systems often implement an abstract overlay network, built at Application Layer, on top of the native or physical network topology. Such overlays are used for indexing and peer discovery and make the P2P system independent from the physical network topology.

A MANET (mobile ad-hoc network) is a type of ad-hoc network where the locations can be changed and configured itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. The main purpose of MANETs working group is to standardize IP routing protocol functionality that is suitable for wireless routing application within both static and dynamic topologies with the increased dynamics due to node motion or other factors [7].

The improvement of the network technologies has provided the use of them in several different fields. One of the most emergent applications of them is the development of the Vehicular Ad-hoc Networks (VANETs), one special kind of Mobile Ad-hoc Networks (MANETs) in which the communications are among the nearby vehicles. Participating cars become a wireless connection or router through VANET and it allow the cars almost to connect 100 to 300 meters to each other and in order to create a wide range network, other vehicles and cars are connected to each other so the mobile internet is made. It is supposed that the first networks that will incorporate this technology are fire and police mobiles to interact with one another for security reasons. These products include remote keyless entry devices, personal digital assistants (PDAs), laptops and mobile telephones. As mobile wireless devices and networks become increasingly important, the demand for Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I) Communication will continue to grow.

# 3 Problem Statement

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. Electronic cash (E-*cash*) is an attempt to construct an electronic payment system model. Paper cash has such features as being: portable (easily carried), recognizable (as legal tender) hence readily acceptable, transferable (without involvement of the financial network), untraceable (no record of where money is spent), anonymous (no record of who spent the money) and has the ability to make "change". E-cash is used over the Internet, email, personal computer, or mobile to other workstations in the form of secured payments of "cash" that is virtually untraceable to the user. It is backed by real currency from real banks. Electronic payment systems can come in many forms including digital checks, debit cards, credit cards, and stored value cards. The usual security features for such systems are privacy (protection from eavesdropping), authenticity (provides user identification and message integrity), and non-repudiation (prevention of

later denying having performed a transaction). Therefore, traceability is highly desirable such as in e-cash systems where it is used for detecting and tracing double-spenders. Thus it is required to achieve anonymity for trusted users and traceability for untrusted users in the network.

In existing system, 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

# 4 Proposed System

The security conflicts namely anonymity and traceability are resolved in the emerging WMN communication systems. An initial design of the security architecture has been proposed, where the feasibility and applicability of the architecture were not fully understood. So, a detailed efficiency analysis has been given in terms of small program, to shows how our anonymity and traceability is achieved in WMNs with a secured architectural design. This is a practically viable solution to the application scenario of interest.

A multi-hop wireless network is analyzed with multiple source-destination pairs, given routing and traffic information. Each source injects packets in the network, which traverses through the network until it reaches the destination. For example, a multi-hop wireless network with three flows. The exogenous arrival processes correspond to the number of packets injected in the system at time. A packet is queued at each node in its path where it waits for an opportunity to be transmitted. Since the transmission medium is shared, concurrent transmissions can interfere with each other's transmissions. The set of links that do not cause interference with each other can be scheduled simultaneously, and can call them *activation vectors* (matchings'). There is no priori restriction on the set of allowed activation vectors, i.e., they can characterize any combinatorial interference model. For example, in a K-hop interference model, the links scheduled simultaneously are separated by at least K hops. Each link has unit capacity; i.e., at most one packet can be transmitted in a slot. For the above example, we assume a 1-hop interference model. The delay performance of any scheduling policy is primarily limited by the interference, which causes many bottlenecks to be formed in the network. The use of exclusive sets is demonstrated for the purpose of deriving lower bounds on delay for a wireless network with single hop traffic.

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 proposed system 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 anonymity of unlinking user identities from activities, as well as the traceability of misbehaving users. i.e., if the users in the network are malfunctioning the resources or transactions, they can be traced by this system. This can be shown by misuses option and is viewed only by the admin. He has to login first and can view the blind messages between the clients and also the misuse transaction which has been traced. Furthermore, the proposed pseudonym technique renders user location information unexposed.

The structure for proposed system is as shown in Figure 1. Pseudonym manager is responsible for creating new users. It checks whether a created user already exists or not. If the user does not exist then it stops and creates the new user. After creating a fresh new user/ existing user, the behavior is checked. If the user has good behavior, (s)/he can access network features like unconditional anonymity. Otherwise, misbehaving user details are sent to pseudonym manager. The pseudonym manager intern sends misbehaving alerts to mobile manager if the mobile server is on.

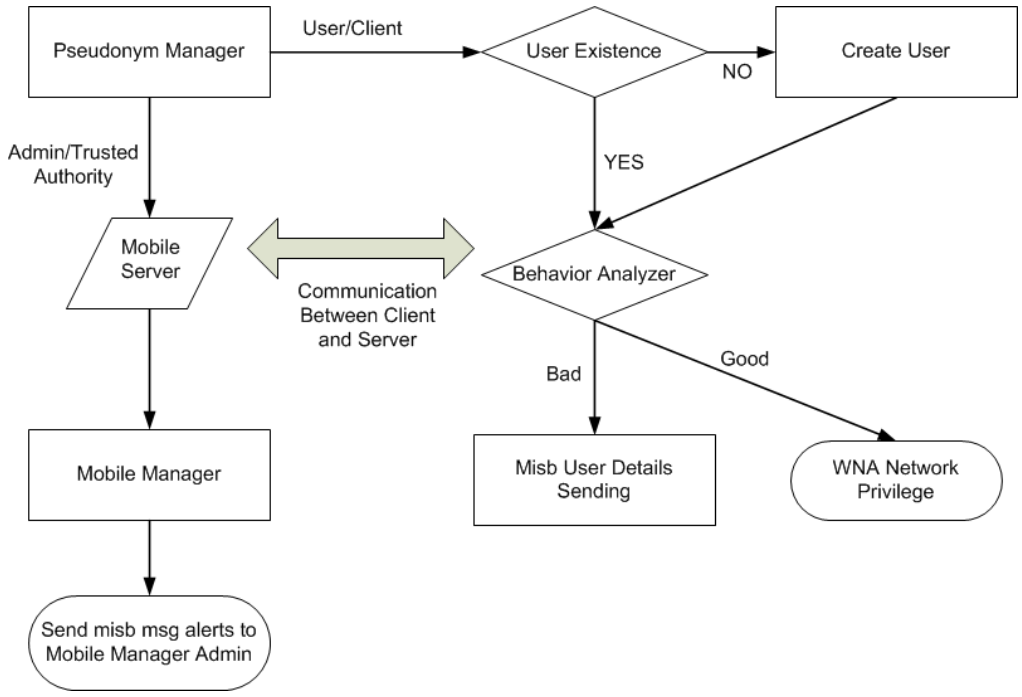


Figure 1: Structure for Implemented System

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. 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 the widely used pseudonym approach has been employed to ensure network access anonymity and location privacy, the pseudonym generation does not rely on a central authority. e.g., the broker, the domain authority in the transportation authority or the manufacturer and the trusted authority 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 anonymity, which can be incorporated as an enhancement. We wrote a program based on the ticket-based security architecture, which consists of *ticket issuance*, *ticket deposit*, and *fraud detection* to achieve anonymity and intractability.

## 4.1 Ticket Issuance

In order to maintain security of the network against attacks and the fairness among clients, the home *TA (trusted authority*) 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 client needs to reveal his real *ID (real identity)* 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*} at the output, where *TN* is the unique serial number of the ticket that can be computed from the client's account number Ω. 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. 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. 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.

As a result, the anonymity of an honest client is unconditionally ensured. Restrictive partially blind signature schemes can be adopted as the building block of the ticket generation algorithm in this ticket issuance protocol. 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 (ticket value, expiry date, misbehavior, etc.*)},

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.

Note that the presence of misbehavior information in *c* will not leak the client's identity to any entity in the network, since *misb* is just a quantitative level indicating the severity of the misbehavior and is not specific to a particular client. The incorporation of the *misb* field has several merits. One possible merit would be to punish clients with misbehavior history by higher network access latency. The gateway 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 (i.e., the *TA* performs ticket fraud detection to check if this ticket has been deposited before). Since we assume an offline *TA* in our scheme, the network access delay cannot be bounded and depends on the work load of the *TA*. Moreover, 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*.

## 4.2 Ticket Deposit

After obtaining a *valid ticket*, the client may deposit it anytime the network service is desired before the ticket expires. This 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 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. This is the reason why the client is not allowed to change his pseudonym while still using a deposited ticket to which the pseudonym is associated, since the *DGW* will refuse to offer access services to the client if the present pseudonym mismatches the one recorded with the ticket.

As a result, the ticket value needs to be set to a relatively small quantity in order to allow frequent update of the pseudonym if the client has high requirement on his anonymity. It

will not place extra signaling overhead into the system since the TA can grant a batch of small valued tickets during one single ticket issuance protocol. Due to the limited ticket value, the client is expected to have minimal mobility during the usage of the deposited ticket. However, there are also cases where the client moves to other gateways after the ticket is deposited.

## 4.3 Fraud Detection

Fraud is used interchangeably with misbehavior, 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 *TA* to constrain his ticket requests. Multiple deposits 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.*

However, that since a client is able to obtain multiple tickets in one ticket issuance protocol and self-generated multiple pseudonyms; he can distribute these pseudonym/ticket pairs to other clients without being traced as long as each ticket is deposited only once. A possible remedy to this situation is to specify the no overlapping active period of a ticket instead of merely the expiry date/time such that each time, only one ticket can be valid. 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. This approach will eliminate the multiple deposit fraud but requires the deployment of secure modules.

Let us consider multiple deposits as possible types of fraud (e.g., in case that secure modules are unavailable). These 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. Specifically, when the *TA* detects duplicate deposits using the ticket records reported by gateways, the *TA* will have the view of at least two different challenges from gateways and two corresponding sets of responses from the same client.

In Figure 2, we explain a scenario on how our system works. Authority will request a Server access by logging into it by client. Manager/Trusted Authority (MTA) monitors on the Client/User messages and transactions and send alert message in case of fraud and MTA also checks for the User's real identity when it receives a request to authenticate. On the client side, user will request the server to start and authenticate. (S)/He will be able to do transactions if their conduct is good or will receive alert message if there is some fraud detection.

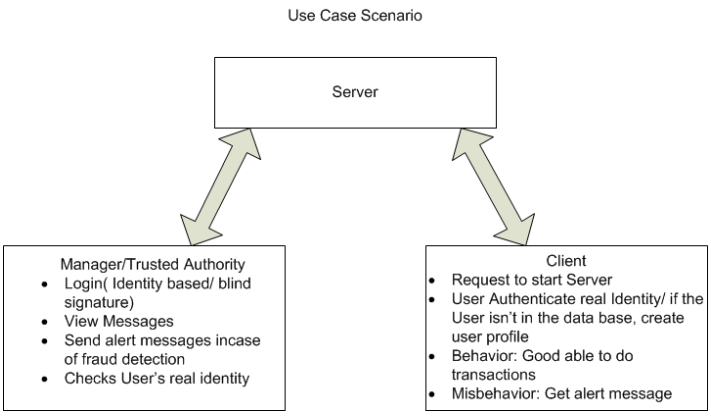


Figure 2: User Case Scenario

# 5 Conclusion

A security architecture designed here is 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 anonymity and intractability and efficiency. Here we are motivated by resolving the above security conflicts, namely anonymity and traceability, in the emerging WMN communication systems through a small program of ours [7]. Various security and privacy characteristics, such as e-coin integrity, authenticity, un-forgetability, un-reusability, intractability and anonymity are also satisfied. The proposed scheme proved to be resistant to various threats and attacks against its security and reliability.

# 6 Future Enhancement

In the WMNs considered here, the uplink from the client to the mesh router may rely on multichip communications. Peer clients act as relaying nodes to forward each other's traffic to the mesh router, which forms a P2P network. The notorious problem common in P2P communication systems is the free-riding, where some peers take advantage of the system by providing little or no service to other peers or by leaving the system immediately after the service needs are secured. Our design for achieving anonymity and in traceability in WMNs with a secured architectural design which satisfies the service needs. Peer cooperation is thus the fundamental requirement for P2P systems to operate properly. Since peers are assumed to be selfish, incentive mechanisms become essential to promote peer cooperation in terms of both cooperativeness and availability. Typical incentive mechanisms for promoting cooperativeness include reputation and payment-based approaches. In the reputation-based systems, peers are punished or rewarded based on the observed behaviour. However, low availability remains an unobservable behaviour in such systems, which hinders the feasibility of the reputation-based mechanism in

improving peer availability. By contrast, the payment-based approach provides sufficient incentives for enhancing both cooperativeness and availability, and thus, is ideal to be employed in multichip uplink communications among peer clients in our WMN system. In future, this work can be used to extend wireless LAN with more security. It can help in better utilization of bandwidth as in this work overhead is reducing as it is helping in reducing the number of nodes for achieving security and privacy.

# REFERENCES


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

[2] 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.

[3] N.B. Salem and J-P. Hubaux, "Securing WirelessMesh Networks," IEEE Wireless Comm., vol. 13, no. 2, pp. 50-55, Apr. 2006.

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

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

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

[7] Paramjeet Rawat and Dr. M.S.Aswal "INTEGRATED SECURITY FRAMEWORK FOR HYBRID WIRELESS MESH NETWORKS ", IJCSE: International Journal on Computer Science and Engineering, Vol. 02, No. 04, 2010, 1136- 1141

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

[9] Taojun Wu, Yi Cui and Yuan Xue, "Preserving Traffic Privacy in Wireless Mesh Networks", Department of Electrical Engineering and Computer Science Vanderbilt University

[10] Yong Guan, Xinwen Fu, Riccardo Bettati, Wei Zhao, "An Optimal Strategy for Anonymous Communication Protocols", IEEE ICDCS 2002

[11] Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Avi Rubin, "Anonymity in Wireless Broadcast Networks", International Journal of Network Security, Vol.8, No.1, PP.37–51, Jan. 2009

[12] Marco Casassa Mont, Pete Bramhall , "IBE Applied to Privacy and Identity Management, " HP Labs, HPL-2003- 101, 2003.

[13] Xiaoxin Wu, Ninghui Li, "Achieving Privacy in Mesh Networks", ACM 1-59593-554-1/06/0010, 2006

[14] Shams Qazi, Yi Mu, Willy Susilo, "Securing Wireless Mesh Networks with Ticket-Based Authentication", 978-1- 4244-4242-3/018, IEEE 2008 [15] Yanchao Zhang, Wei Liu and Wenjing Lou, "Anonymous Communications in Mobile Ad Hoc Networks", In IEEE Infocom 2005, Miami, USA, March 13-17, 2005.