Safety Measures For Achieving Anonymity and Traceability in Wireless Mesh Networks

[1]V. Redya Jadav, [2]N. S. S Durga Vanama
[1,2]Dept. of CSE, Bomma Institute of Technology and Science, Khammam, AP, India

Abstract
Due to the users' awareness of their privacy nowadays Anonymity has received increasing attention in the literature 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). Anonymity provides protection for users to enjoy network services without being traced. On the other hand, the network authority requires conditional anonymity such that misbehaving entities in the network remain traceable. In this paper, we propose a security architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users for network authorities in WMNs. The proposed architecture strives to resolve the conflicts between the anonymity and traceability objectives, in addition to guaranteeing fundamental security requirements including authentication, confidentiality, data integrity, and non-repudiation. Thorough analysis on security and efficiency is incorporated, demonstrating the feasibility and effectiveness of the proposed architecture.

Keywords
Anonymity, Traceability, Pseudonym, Misbehavior, Revocation, Wireless Mesh Network (WMN)

I. Introduction

Wireless Mesh Network (WMN) is a promising technology and is expected to be widespread due to its low investment feature and the wireless broadband services it supports, attractive to both service providers and users. 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 [1], wireless local area networks (WLANs) [2], wireless sensor networks [3-4], mobile ad hoc networks (MANETs) [5-6], and vehicular ad hoc networks (VANETs) [7]. Recently, new proposals on WMN security [8-9] have emerged. In [8], the authors describe the specifics of WMNs and identify three fundamental network operations that need to be secured. We [9] propose an Attack-Resilient Security Architecture (ARSA) for WMNs, addressing countermeasures to a wide range of attacks in WMNs. Due to the fact that security in WMNs is still in its infancy as very little` attention has been devoted so far [8], a majority of security issues have not been addressed and are surveyed in [10].

In this paper, 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 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 paper to show that our SAT is a practically viable solution to the application scenario of interest. Our system borrows the blind signature technique from payment systems [10-11,13], 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 we employ the used pseudonym approach to ensure network access anonymity and location privacy, our pseudonym generation does not rely on a central authority, e.g., the broker in [9], the domain authority in [14], the transportation authority or the manufacturer in [7], 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 anonymity, which can be incorporated as an enhancement. Specifically, our major contributions in this paper include, (1) design of a ticket-based anonymity system with traceability property; (2) 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; (3) adoption of the hierarchical identity based cryptography (HIBC) for inter-domain authentication avoiding domain parameter certification.

II. Preliminaries

A. IBC from Bilinear Pairings

ID-based cryptography (IBC) allows the public key of an entity to be derived from its public identity information such as name and e-mail address, which avoids the use of certificates for public key verification in the conventional public key infrastructure (PKI). Boneh and Franklin introduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically, let G1 and G2 be an additive group and a multiplicative group, respectively, of the same prime order p. The Discrete Logarithm Problem (DLP) is assumed to be hard in both G1 and G2. Let P denote a random generator of G1 and e: G1G1! 2 denote a bilinear map constructed by modified Weil or Tate pairing with the following properties:

1. Bilinear: eðaP;bQÞ¼eðP;QÞab, 8P ; Q 2 G1, and 8a; b 2 Zp, where Zp denotes the multiplicative group of Zp, the integers modulo p. In particular, Zp ¼ fx j 1xp1g since p is prime.
2. Nondegenerate: 9P ; Q 2 G1 such that eðP ; QÞ ¼ 1.
3. Computable: there exists an efficient algorithm to compute eðP ; QÞ; 8P ; Q 2 G1.

B. IBC from Bilinear Pairings

Blind signature is first introduced by Chaum. In general, a blind signature scheme allows a receiver to obtain a signature on a message such that both the message and the resulting signature

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

III. System Model

A. Network Architecture

Consider the network topology of a typical WMN depicted in fig. 1. The wireless mesh backbone consists of Mesh Routers (MRs) and Gateways (GWs) interconnected by ordinary wireless links (shown as dotted curves). Mesh routers and gateways serve as the access points of the WMN and the last resorts to the Internet, respectively. The hospital, campus, enterprise, and residential buildings are instances of individual WMN domains subscribing to the Internet services from upstream service providers, shown as the Internet cloud in Fig. 1. Each WMN domain, or trust domain (to be used interchangeably) is managed by a domain administrator that serves as a trusted authority (TA), e.g., the central server of a campus WMN.

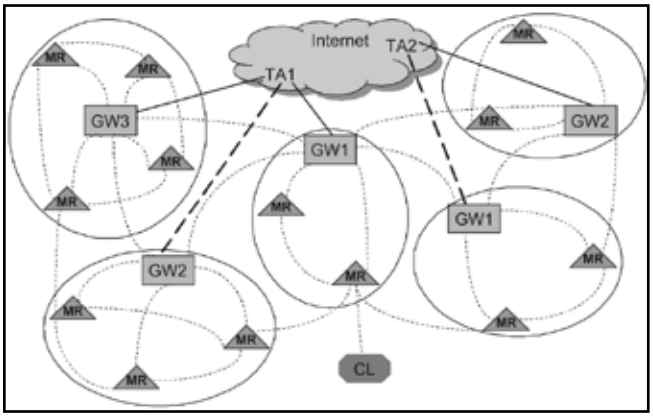

Fig. 1: Network Topology of a Typical WMN

The TA and associated gateways are connected by high-speed wired or wireless links, displayed as solid and bold dashed lines, respectively. TAs and gateways are assumed to be capable of handling computationally intensive tasks. 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, as the employees or students in the case of enterprise and hospital WMNs or campus WMNs. Such individual WMN domains can be building blocks of an even larger metropolitan WMN domain.

B. Trust Model

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

1. Trust Relationship

In general, the TA is trusted within the WMN domain. There is no direct trust relationship between the client and the gateway/mesh router. We will use standard IBC for authentication and secure communications both at the backbone and during network access inside a trust domain (i.e., intradomain). We further assume the existence of preshared keys and secure communication channels between entities (TAs, gateways, mesh routers) at the back-bone and will solely consider the authentication and key establishment during the network access of the clients.

IV. SAT Security Architecture

A. Ticket Based Security Architecture

First, we restrict our discussion to within the home domain. The inter-domain protocols in our security architecture, which are executed when the client roams outside his home domain, will be presented in Section IV A. 5. The ticket-based security architecture consists of ticket issuance, ticket deposit, fraud detection, and ticket revocation protocols. In what follows, we will describe these protocols in detail, together with the fulfillment of authentication, data integrity, and confidential communications that may take place during the execution of these protocols.

1. Ticket Issuance

In order to maintain security of the network against attacks and the fairness among clients, the home TA may control the access of each client by issuing tickets based on the misbehavior history of the client, which reflects the TA's confidence about the client to act properly. Ticket issuance occurs when the client initially attempts to access the network or when all previously issued tickets 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 TA publishes the domain parameters to be used within its trust domain as ðp; G1; G2; e; P; P1; P2; H1; H2; H3;PpubÞ using the standard IBC domain initialization where ðP;P_1;P_2Þ are random generators of G1, and Ppub ¼ P . Since the scheme in is selected for demonstration, G1 here should be a Gap Diffie-Hellman (GDH) group, where the computational Diffie-Hellman problem (CDHP) is assumed to be intractable. In addition, the TA chooses r 2_R Z_p and Q 2_R G_1, and the client chooses ; ; ; ; ; ; 2_R Z_p. Note that if the scheme is adopted, the TA publishes ðp; G_1; G_2; e; g; g_1; g_2; H; H_0; H_1Þ, where G_1 should be a GDH in which the RCDHP (reversion CDHP) is assumed to be intractable for detailed definitions). We will demonstrate the following protocols based on the scheme. The application of the scheme to our protocols is straightforward following a similar procedure. The ticket issuance protocol is demonstrated as follows:

CL !! TA: IDCL;m;t1, HMAC ðm k t1Þ;

TA!!CL:IDTA; X¼eðm; TAÞ; Y ¼eðP;QÞ; Z¼eðm;QÞ; U ¼rH1ðIDTAÞ; V ¼rP;t2;HMAC ðXkY kZkU kV kt2Þ;

CL !! TA : IDCL; B¼1H2ðm0 kU0 kV0 kRkW kX0 kY0 kZ0Þ þ ;t3;HMAC ðBkt3Þ; and

TA!!CL:IDTA; 1 ¼QþB TA; 2 ¼ðrþBÞ TA þrH1ðcÞ;t4; HMAC ð 1 k 2 k t4Þ:

2. Ticket Deposit

After obtaining 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.

CL !! GW : PSCL;m0;W;c;

0

0

¼ ðU^0; V ^{0}; X^0; ;1;$_2$Þ; t_5;

SIG ðm0 k W k c k k t5Þ;
tcl
1. GW !! CL : IDGW , d ¼ H3ðR k W k IDGW k T Þ, t6, HMAC 0ðd k t6Þ;
2. CL !! GW : PSCL, r1 ¼ dðu1 Þ þ v1, r2 ¼ d þ v2, t7, HMAC 0 ðr1 k r2 k t7Þ; and
3. GW !! CL : IDGW ; misb; exp; t8; SIG ðPSCL k IDGW k misb k exp k t8Þ; gw

3. 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 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. A possible remedy to this situation is to specify the nonoverlapping 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. 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).

4. Ticket Revocation

Ticket revocation is necessary when a client is compromised, and thus, all his secrets are disclosed to the adversary. In our system, the adversary is motivated by gaining network services using tickets once the ticket-associated secrets are obtained from the compromised clients. Therefore, the compromised client needs to be able to revoke the ticket and prevent the adversary from acquiring benefits. The compromised client and the adversary are the only two parties that are in possession of the ticket-related secrets, a valid revocation request must be sent by the compromised client for genuine revocation purpose since the adversary gains nothing in doing so. The ticket revocation protocol consists of two cases as follows:

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 P SCL, TN , t10, SIG fðCLTN k t10Þ in the revocation request to any encountered gateway. This gateway authenticates the client using P SCL and records the ticket serial number TN as revoked.

2. Revocation of Deposited Tickets

the client simply sends P SCL, IDDGW, t11, SIG fðCLIDDGW k t11Þ in the revocation request to the DGW. The DGW authenticates the client and marks the associated ticket revoked.

When gateways have records in the revocation database, they immediately report the revocations to the home TA, which will update and distribute the revocation list for all gateways in the trust domain to reference.

5. Accessing the Network from Foreign Domains

The access services the visiting (foreign) trust domain provided the ticket-based security architecture can take place in two ways including the following:

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

1. CL !! MR : PSTCL;aP0;t12;
   HI DS CL;sCL ðH1ðPSTCL k aP0 k t12ÞÞ;
2. MR!CL:IDTMR;bP0;t13;
   HI DS MR;sMRðH1ðIDTMR k bP0 k t13ÞÞ; and
3. CL !! MR: PSTCL, PSCL, SKE ðIDCL k mÞ, t14, HMAC ðP SCL k SKE k t14Þ.

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. The first two steps of the procedure are exactly the same as the above. The last step in this case will be CL !! MR: P STCL, P SCL, ticket, t15, HMAC ðP SCL k ticket k t15Þ.

B. Pseudonym Generation and Revocation

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 $ 2R Zp and computing the pseudonym P SCL ¼ $H1ðIDCLÞ. The corresponding private key can be derived as g CL¼$CL¼$ H1ðIDCLÞ ¼ P SCL, in a similar way to that of compared to [7, 9, 15] where 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 anonymity by using this inexpensive method.

V. Security Analysis

In this section, we analyze the security requirements our system can achieve as follows: Again, we use theorems for demonstration and the analysis using theorems can be carried out in a similar fashion.

Fundamental security objectives. It is trivial to show that our security architecture satisfies the security requirements for authentication, data integrity, and confidentiality, which follows directly from the employment of the standard cryptographic primitives, namely digital signature, message authentication code, and encryption, 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 ðu1; u2Þ he knows of m from what is derived by the TA. If the client has misbehaved, the representation he knows will be the same as the one derived by the TA which ensures non-repudiation.

Anonymity. First of all, it can be easily shown that a gateway cannot link a client's network access activities to his real identity. Due to the use of pseudonyms in authentication, which reveals no information on the real ID, the

gateway learns nothing about the identity of the client requesting network access. Since the pseudonym is generated by the client using his secret number, solving for the real identity from the pseudonym is equivalent to solving the DLP. Furthermore, the client's deposit gateway (DGW) cannot deduce the client's ID from the deposited ticket, which has been blinded by the client and does not reveal any identification information unless misbehavior occurs.

VI. Efficiency Analysis

Most pairing-based cryptosystems need to work in (1) a subgroup of the elliptic curve EðFq Þ of sufficiently large prime order p, and (2) a sufficiently large finite field Fqk, where q is the size of the field over which the curve is defined and k is the embedding degree. For current minimum levels of security, we require $p > 2^{160}$ and $q^k > 2^{1;024}$ to ensure the hardness of the DLP in G_1 and G_2. To improve the computation and communication efficiency when working with EðFq Þ, we tend to keep q small while maintaining the security with larger values of k. According to a popular choice is to work with points in EðFq Þ, where $q2^{170}$, and to have a curve with embedding degree k ¼ 6 so that $qk2^{1;024}$. In the following analysis, we will use the parameter values given above, resulting in the elements in G_1 and G_2 to be roughly 171-bit (using point compression) and 1,024-bit, respectively. We further assume that SHA-1 is used to compute the keyed-hash message authentication code (HMAC), which yields a 160-bit output.

A. Communication

Our ticket-based security architecture consists of four intra-domain protocols in which ticket deposit involves only clients and gateways. This protocol is distributed in nature, and thus, the communication cost incurred is more affordable. In contrast, protocols involving interactions with the centralized TA contribute largely to the expensive communication costs in the system. In the fraud detection protocol, gateways report accumulated ticket records to the TA periodically instead of in real time. Reports from gateways can be scheduled at different time intervals, avoiding a sudden increase in the communication overhead caused by simultaneous transmissions. For each record, a gateway transmits roughly 443 bytes, including five G1 elements, two G2 elements, and four 160-bit elements. Other parameters in the record transmission are negligible compared to the above elements. Assuming that the communication channel between gateways and the TA has a bandwidth of 10 Mbps, each record takes 0.35 ms to be transmitted.

Ticket issuance and revocation may take place in real time. The associated communication overhead depends on how frequent 1) the clients use up issued tickets and 2) the clients misbehave. One can expect minimal real-time interaction with the TA for systems where ticket issuance is based on the client's usage trend (such that ticket requests other than scheduled will be infrequent) and there is a well-behaving majority. Since multiple tickets are issued to the client at each scheduled interval, the average communication cost can be further reduced because some parameters need only be transmitted once. In a single ticket issuance, the client sends roughly 60 bytes (i.e., three 160-bit elements) to the TA. The TA sends to the client approximately 128 bytes (i.e., four G1 elements and two 160-bit HMACs).

Note that we have excluded the information that need only be transmitted once. In the ticket revocation protocol, the gateway sends revocations in real time to the TA to ensure a timely update and distribution of the ticket revocation list.

B. Storage

As mentioned above, the TA may consist of several servers to store necessary information from all clients during protocol executions. The storage capability of these high-end servers is usually not a concern, and therefore, we focus on the storage overhead encountered at the low-end client side. Note that there is a trade-off between storage and computation overhead. In our protocols, the client has to perform pairing computations frequently, which is impractical due to the high cost of pairings and limited power of clients. Fortunately, many pairing operations in the protocols can be computed once and stored for future use. Furthermore, some stored information remains unchanged for all instances of protocol execution (e.g., all tickets issued in the ticket issuance protocol). As a result, we need merely take into account the effective storage overhead (i.e., information that is changed and has to be stored at each protocol instance).

In ticket issuance, the client stores for each protocol instance 621 bytes pre-computed information (3 jG1jelement þ 4 jG2jelement þ jZp jelement) and 43 bytes (2jG1jelement) after protocol information for future use. Information such as the symmetric key , and other protocol parameters m, X, Y , Z, g, g1, g2, etc., will only be stored once by the client for all protocol instances. The ticket issuance protocol contributes to most of the storage over-head at the client side, since all ticket-related information necessary for the remaining protocols will be stored by the end of ticket issuance. The only requirement left for intradomain protocols is the storage of the 43-byte pseudonym/private key pair and the corresponding symmetric keys (128 bytes each) with gateways and mesh routers. The size of this storage depends on the frequency of the client's pseudonym update. The trade-off between storage and computation overhead arises again where the symmetric key storage can be eliminated if digital signatures replace HMAC for integrity check in our protocols.

VII. Security Enhancements

In addressing privacy and anonymity on the Internet, Dingledine argues that cryptography alone will not hide the existence of confidential communication relationships and implemented an anonymous communication overlay network, based on the anonymous routing protocol, i.e., the onion routing. In addressing the privacy preserving issue in vehicular ad hoc networks (VANETs) where the vehicles enjoy various VANET applications, Raya and Hubaux [7] claim that all vehicle identifiers, in particular, the MAC and IP addresses, must change over time, in addition to the frequent update of the anonymous keys (pseudonyms). Analogously, the proposed ticket-based anonymity system relies on effective anonymous routing protocols to construct anonymous communication paths and guarantee unlinkability. Unlinkability is a requirement for preserving user privacy in addition to anonymity. It refers to the property that multiple packets cannot be linked to have originated from a same client. For instance, if the network ID (i.e., IP address, MAC address) of a client's device is fixed and exposed in packet forwarding, the packets sent by a same client can be linked, which will enable the attackers to profile the client through traffic analysis attacks. By incorporating anonymous routing protocols suitable for WMNs into our system, the real network ID will be effectively concealed rendering it difficult to profile the client and to discover the confidential

relationship of the communicating parties. Note that anonymous routing serves as an enhancement to user privacy. The anonymity guarantee of our architecture will not be undermined even if anonymous routing protocols are absent.

VIII. Conclusion

In this paper, we propose SAT, a security architecture mainly consisting of the ticket-based protocols, which resolves the conflicting security requirements of unconditional anonymity for honest users and traceability of misbehaving users. By utilizing the tickets, self-generated pseudonyms, and the hierarchical identity-based cryptography, the proposed architecture is demonstrated to achieve desired security objectives and efficiency.

References

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

[2] P. Kyasanur, 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, D. Wagner,"Security in Wireless Sensor Networks," Comm. ACM, Vol. 47, No. 6, pp. 53-57, 2004.

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

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

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

[9] Y. Zhang, 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, W. Wang,"Wireless Mesh Networks: A Survey", Computer Networks, Vol. 47, No. 4, pp. 445-487, Mar. 2005.

[11] S. Brands,"Untraceable Off-Line Cash in Wallets with Observers", Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cyptology (CRYPTO '93), pp. 302-318, Aug. 1993.

[12] K. Wei, Y.R. Chen, A.J. Smith, 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.

[13] D. Chaum, A. Fiat, M. Naor,"Untraceable Electronic Cash,"Proc. Conf. Advances in Cryptology (CRYPTO '88), 2002.

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

V.Redya Jadav M.Tech(cs), Head of the Department Department of CSE, I am having 12 years of experience in teaching Computer Technologies published various research articles in National and International Journals.

N.S.S Durga Vanama, Pursuing M.Tech (C.S.E) in Bomma institute of technology And Science, Khammam, AP, India.