ACHIEVING USER PRIVACY AND ANONYMITY IN WIRELESS MESH NETWORKS USING ANONYMOUS PROTOCOL

Phani babu Komarapu[1], and Loshma Gunisetti[2]

[1] M.Tech Student ,Department of CSE Sri Vasavi engineering College Tadepalli Gudem,W.G(D),Andhra Pradesh

[2]Associate professor,Department of CSE Sri Vasavi Engineering College,Tadepalli Gudem,W.G(D),Andhra Pradesh.

ABSTRACT:
Wireless Mesh Network (WMN) is a capable technology and is expected to be prevalent due to its low investment feature and the wireless broadband services it supports, attractive to both service providers and users. Ticket based security architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users for network authorities in WMNs Using anonymous Routing protocol. The existing 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. By incorporating anonymous routing protocols 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. Anonymous routing achieves user privacy.

KEYWORDS: Wireless Mesh Network, Anonymity, User privacy, Unlinkability

1. INTRODUCTION: 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 wireless mesh router. Multiple mesh routers communicate with one another to form a multi-hop wireless backbone that forwards user traffic to a few gateways connected to the Internet[1]. Some perceived benefits of WMN include enhanced resilience against node failures and channel errors, high data rates, and low costs in deployment and maintenance.

Privacy has been a major concern of Internet users. It is a particularly critical issue in the context of WMN-based Internet access, where users' traffic is forwarded via multiple mesh routers. In a community mesh network, this means that the traffic of a residence can be observed by the mesh routers residing at its neighbors. Wireless security has been the hot topic in the literature for various network technologies such as cellular networks[21], wireless local area networks (WLANs)[22], wireless sensor networks mobile ad hoc networks (MANETs) and vehicular ad hoc networks (VANETs)[9].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. We propose an attack-resilient security architecture (ARSA) for WMNs[8], 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, a majority of security issues have not been addressed and are surveyed in. Anonymity and privacy issues have gained considerable research efforts in the literature which have focused on investigating anonymity in different context or application scenarios. One requirement for anonymity is to unlink a user's identity to his or her specific activities, such as the anonymity fulfilled in the untraceable e-cash systems[14] and the P2P payment systems where the payments cannot be linked to the identity of a payer by the bank or broker. Anonymity is also required to hide the location information of a user to prevent movement tracing, as is important in mobile networks and VANETs[1]. 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. In this paper, we are motivated by resolving the above security conflicts, namely anonymity and traceability, in the emerging WMN communication systems. Our system borrows the blind signature technique from payment systems[14], 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[21] 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

ISSN: 2278 – 1323

payment systems among bank, customer, and store cannot be directly applied. In addition to the anonymity scheme, other security issues such as authentication, key establishment, and revocation are critical in WMNs to ensure the correct application of the anonymity scheme. Moreover, although we employ the widely used pseudonym approach to ensure network access anonymity and location privacy, our pseudonym generation does 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..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 interdomain authentication avoiding domain parameter certification. 4) Incorporating Anonymous Routing protocol.

2. PRELIMINARIES: The Wireless Mesh backbone consists of mesh routers and gateways interconnected by ordinary wireless links. 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. Each WMN [21]domain, or trust domain (to be used interchangeably) is managed by a domain administrator that serves as a trusted authority (TA), e.g., the central server of a campus WMN. The TA and associated gateways are connected by high-speed wired or wireless links, displayed as solid and bold dashed lines, respectively. TAs and gateways are assumed to be capable of handling computationally intensive tasks. 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 domains can be building blocks of an even larger metropolitan WMN domain.

2.1 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.

2.2 Blind Signature: Blind signature is first introduced by Chaum[14]. 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. From formal definition of a blind signature scheme, which should bear the properties of verifiability, unlink ability, and unforgeability. Brands developed 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 traceability in the restrictive blind signature systems

2.3 Anonymity (Untraceability): the anonymity of a legitimate client refers to the untraceability of the client's network access activities. The client is said to be anonymous if the TA, the gateway, and even the collusion of the two cannot link the client's network access activities to his real identity.

2.4 Traceability: a legitimate client is said to be traceable if the TA is able to link the client's network access activities to the client's real identity if and only if the client misbehaves, i.e., one or both of the following occurs: ticket reuse and multiple deposit.

2.5 Ticket reuse: one type of misbehavior of a legitimate client that refers to the client's use of a depleted ticket.

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

ISSN: 2278 – 1323

2.7 Collusion: the colluding of malicious TA and gateway to trace a legitimate client's network access activities in the TA's domain (i.e., to compromise the client's anonymity).

2.8 Framing: A type of attack mounted by a malicious TA in order to revoke a legitimate client's network access privilege. In this attack, the TA can generate a false account number and associate it with the client's identity. The TA can then create valid tickets based on the false account number and commit fraud (i.e., misbehave). By doing so, the TA is able to falsely accuse the client to have misbehaved, and thus, to revoke his access right.

3. TICKET BASED SECURITY ARCHITECTURE: 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.

3.1. 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 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 unlinkable to a specific execution of the ticket generation algorithm (the core of ticket issuance protocol), while maintaining the verifiability of the ticket.

3.2 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.

3.3 Fraud Detection: Fraud [1] 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 -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. 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). 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. 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. 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.

3.4 Ticket revocation: Ticket revocation[1] 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.

ISSN: 2278 – 1323

3.5 Random Walk Algorithm: In addressing privacy and anonymity on the Internet, Dingle dine[16] argues that cryptography alone will not hide the existence of confidential communication relationships and implemented an anonymous communication overlay network, Tor based on the anonymous routing protocol, i.e., the onion routing[2]. In addressing the privacy preserving issue in vehicular ad hoc networks (VANETs) where the vehicles enjoy various VANET applications, Raya and Hubaux 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. This is one problem which we have identified in previous work.For overcoming this drawback in existed System we will include anonymous routing protocol concept to previous work.In order to protect both the privacy and anonymity of Internet communication against both eavesdropping and traffic analysis, Onion Routing employs a route selection algorithm to generate random routes for communicating endpoints. The goal of the route selection algorithm is to produce a route for a source to reach its destination, while keeping the length within a pre-specified minimum and maximum number of hops. Further, the algorithm must be non-deterministic, such that given the same input on subsequent invocations the algorithm should return different paths with an evenly distributed probability of repeating routes. Access control lists will be used to select an eligible destination point. Selecting a destination site is likely to be a recursive function that utilizes a hash table.

At this point the communicating source node knows adjacency list information of the entire system and the destination point for sending data. Using the adjacency list information, each of our potential route selection algorithms requires that the source node computes (and maintains) single-source shortest-path (the path from itself to every other node in the system). Currently, single-source-shortest-path is calculated using randomly assigned edge weights. The route selection algorithm will most likely be called with the parameters: *src, dest, hardMin, softMin, hardMax and softMax*. The *src* parameter is the node initiating communication and the *dest* parameter is the destination selected as a suitable exit point from the network. The parameters *hardMin* and *hardMax* correspond to the absolute minimum and maximum number of hops in the route from *src* to *dest*. Typically, we will want a route that is at least 6 hops (hardMin), because fewer than 6 hops yields a higher probability of determining the communicating end points. Likewise, we will want to impose a limit on the number of hops (hardMax), because an enormously long route hinders performance. The *softMin* and *softMax* parameters correspond to the "desired" bounds of the length of the route. Thus, if the route generated is not within the bounds of *softMin* and *softMax*, then it will only be discarded if it exceeds our absolute bounds. The goal is to generate the "bulk" of routes within the confines of the specified *softMin* and *softMax*, and few will fall outside of these bounds. The specification of these bounds can be viewed as a tradeoff between performance and security. Note, the parameters of this algorithm may change and suggestions are welcome. The pseudocode of the algorithms below will only utilize the parameters: *src, dest, min,* and *max* (*i.e.,* the soft and hard bounds are equal).It is likely that the graph will be fairly dense (edge-rich), however, our simulations utilize five graphs with different topologies. This allows us to investigate the behavior of each route selection algorithm under other circumstances which may occur due to link or node failures in the network. Currently, we have two algorithms to generate random targeted routes. Random Walk Algorithm is one which combines random walking of the graph with a shortest-path segment to keep the total number of hops under the pre-specified maximum.

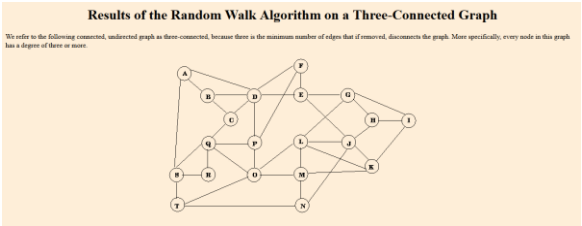
The algorithm[2] is as follows. A route length is randomly selected. In our algorithm below, we selected a number, *Length*, between *Min* and *Max*, where *Min* is equal to 6 and *Max* is equal to twice the number of nodes in the graph (2*20). Then, a coin is tossed to determine whether the random walk from the source or the random walk from the destination takes one random hop to an adjacent node. The coin may or may not be a fair coin. That is, it may be desirable to have more random walking close to the source node or close to the destination node. In either case the coin toss can easily reflect this preference. In the algorithm below, we use a fair coin to select which random walk proceeds. After an adjacent node is selected, the total number of hops including this

ISSN: 2278 – 1323

new node plus the shortest-path to connect the two random walks is computed before the node is incorporated into the route. The above steps continue until the route length is reached or once the next random step exceeds the route length. If the later occurs, then we simply back up one hop (do not include the last random hop in the route). The pseudocode for this algorithm is below (for simplicity, storing the actual route in a data structure has not been included).

```
LengthFromSrc  = 0;
LengthFromDest = 0;
TotalNumberHops = 0;
X = SRC; /*Last Node Visited from Random
                        walk starting at SRC;*/
Y = DEST; /*Last Node Visited from Random
                        walk starting at DEST;*/
          /* Randomly select a route length */
do {
  Length = rand( ) % Max;
  while( Length < Min );
  while ( TotalNumberHops < Length )
      {
        Next = Toss Coin to Pick Random Walk
                        From Src or from Dest;
        if( Next == RandWalkFromSrc )
                        {
Z = Randomly select an adjacent node to X;
TotalNumberHops=1+LengthFromSrc+
      LengthFromDest+ shortest-path from Z to Y;
       if( TotalNumberHops > Length )
          break;
           X = Z;  /*include the node in the route*/
       Store X in the route data structure
         LengthFromSrc++;
          }
else
     {  /* Next = RandWalkFromDest */
        Z = Randomly select an adjacent node to Y;
        TotalNumberHops = 1 + LengthFromSrc +
                        LengthFromDest+
                        Shortest-path from Z to X;
          if( TotalNumberHops > Length )
                        break;
                        Y = Z;
                Store Y in the route data structure
                        LengthFromDest++;
                }
}
```

4. RESULTS: In order to analyze Random Walk algorithm, we view the system as a graph, where all nodes and edges in the system are known.



1) L K L K L G E G H I H I H G L K M O Q R S T O L O T N T S T O T O
2) L K L K L J K J L G H I G H G E G L G L M L J L J E D A S T S T O T O
3) L K L K L J N J K L K J H J N T O M O…….

The number of unique paths generated by this algorithm is approximately 13 times the length of routes generated by any other algorithm. In many cases, the Random Walk Algorithm did not repeat any routes over 1000 executions for every source and destination pair. Due to the larger number of routes generated by this algorithm, we only displayed two communicating pairs for each graph.

5. SECURITY ANALYSIS: In this section, we analyze the security requirements our system can achieve as follows: Again, we use theorems in 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.

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

ISSN: 2278 – 1323

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. Next, we will show that the client's home TA cannot perform such linking either, which follows directly that the restrictive partially blind signature scheme used as a building block for our security architecture is partially blind. , which is equivalent to random guessing.. Traceability (conditional anonymity). According to its definition, this requirement is twofold: 1) Anonymity for honest clients is unconditional, which can be proved following 2) A misbehaving client is traceable where the identity can be revealed. The proof of point 2 follows from that the adopted restrictive partially blind signature scheme in our security architecture achieves restrictiveness. In other words, point 2 states that the client can only obtain signatures on messages of which the client knows a representation for which the structure in the representation (where the identity information is encoded) remains, proved by using and two extra requirements on the representations the client knows ofmandm0 for detailed description of the two requirements).Framing resistance. We conclude that the proposed security architecture satisfies the security requirements for anonymity, traceability, framing resistance, and unforgeability, in addition to the fundamental objectives including authentication, data integrity, and confidentiality. By including Random walk algorithm in existed system we are giving solution to the problem which has been identified in previous work. Using this algorithm[2] we can generate different paths for multiple packets transfer using network id.Because of using different routes for packets transfer, attackers are unable to do traffic analysis technique for getting user real identify information, by doing so we can prevent user information from attackers.

6. CONCLUSION:

This project deals with achieving security in WMNS by protecting user privacy from Traffic analysis attackers by implementing anonymous routing protocol. By incorporating anonymous routing protocols 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. In this way we can protect user details. Through this we can achieve Security in Wireless Mesh Networks

7. REFERENCES:

[1] Jinyuan Sun, Member, IEEE, Chi Zhang, Student Member, IEEE, Yanchao Zhang, Member, IEEE, and Yuguang Fang, Fellow, IEEE SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks.

[2]http://www.onionrouter.net/Archives/Route/Alg2/ThreeConnected.html.

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

[4] 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.

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

[6] 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.

[7] A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55, Jan.-Mar. 2003.

[8] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," IEEE Trans.Wireless Comm., vol. 5, no. 9, pp. 2376-2385, Sept. 2006.

[9] S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks," Proc. 20th Int'l Conf. Advanced Information Networking and Applications (AINA), pp. 133-137, Apr. 2006.

[10] M.G. Reed, P.F. Syverson, and D.M. Goldschlag, "Anonymous Connections and Onion Routing," IEEE J. Selected Areas Comm., vol. 16, no. 4, pp. 482-494, May 1998.

[11] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," Proc. USENIX Security Symp., pp. 303-320, Aug. 2004.

[13] J. Sun, C. Zhang, and Y. Fang, "A Security Architecture Achieving Anonymity and Traceability

ISSN: 2278 – 1323

in Wireless Mesh Networks," Proc. IEEE INFOCOM, pp. 1687-1695, Apr. 2008.

[14] D. Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology—Crypto '82, pp. 199-203, Springer-Verlag,1982.

[15] S.M.M. Rahman, A. Inomata, T. Okamoto, M. Mambo, and E. Okamoto, "Anonymous Secure Communication in Wireless Mobile Ad-Hoc Networks," Proc. First Int'l Conf. Ubiquitous Convergence Technology, pp. 131-140, Dec. 2006.

[16] R. Dingledine, "Tor: An Anonymous Internet Communication System," Proc. Workshop Vanishing Anonymity, the 15th Conf. Computers, Freedom, and Privacy, Apr. 2005.

[17] M. Blaze, J. Ioannidis, A.D. Keromytis, T. Malkin, and A. Rubin, "Anonymity in Wireless Broadcast Networks," Int'l J. Network Security, vol. 8, no. 1, pp. 37-51, Jan. 2009.

[18] X. Wu and N. Li, "Achieving Privacy in Mesh Networks," Proc Fourth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '06), pp. 13-22, Oct. 2006.

[19] T. Wu, Y. Xue, and Y. Chi, "Preserving Traffic Privacy in Wireless Mesh Networks," Proc. Int'l Symp. World of Wireless, Mobile and Multimedia Networks (WoWMoM '06), 2006.

[20] Z. Wan, K. Ren, B. Zhu, B. Preneel, and M. Gu, "Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks," Proc. ASIAN ACM Symp. Information, Computer and Comm. Security (ASIACCS '09), pp. 368-371, Mar. 2009.

[21] European Telecommunications Standards Institute (ETSI), "GSM 2.09: Security Aspects.," June 1993.

[22] 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.

[23] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Comm. of the ACM , vol. 47, no. 6, pp. 53–57, 2004.

[24] 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

AUTHORS PROFILE

Phanibabu Komarapu did his BTech (Computer Science and Engineering) in SRKR engineering College, Bhimavaram, and West Godavari District. Now he is pursuing his M.Tech (Computer Science and Engineering) in Sri Vasavi Engineering College, pedatadepalli, Tadepalligudem, west Godavari, and Andhra Pradesh, India.His area of interest is Network security.

Gunisetti Loshma did her B.Tech (Computer Technology) and M.Tech (Computer Science and Engineering) and is currently working as an associate Professor in CSE Department at Sri Vasavi EngineeringCollege,Pedatadepalli,Tadepalligudem,West Godavari, and Andhra Pradesh,India.She has 13 years of experience in teaching. She has published number of papers in various journals and conferences.

ISSN: 2278 – 1323