UnObservable BATMAN Routing for Fast and Secure Transmission in Comparison with USOR

[I]Sujatha Gaini, [II]Md. Abdul Azeem
[I]M.Tech (CSE), [II]Associate Professor
[I,II]Dept. of CSE, MVSREC, Nadegul, Hyderabad, India

Abstract

A Mobile ad hoc network (MANET) is a self-configurable, self-organizing, infrastructure less multi-hop wireless network. Routing in MANET is a critical issue due to mobility. So an efficient routing protocol makes the MANET reliable and secure. USOR is a privacy preserving routing protocol deals with the concept of anonymity, unlinkability and unobservability. This can be achieved by combining group signature and ID-based encryption. USOR has latency in finding route since it uses on demand routing. Every node maintains network topology information which consumes time. We know that ad-hoc network has limited battery power. Already half of the power used in security, remaining power has to be used efficiently to calculating route and data transmission. So apart from security, there should be efficient delivery of data. BATMAN (Better Approach to Mobile Ad hoc Network) is proactive routing protocol in which every node has knowledge of best hop details instead of maintaining entire network topology. It takes less time to calculate best hop details. Route may be readily available in the routing table so reduce delay in finding route. BAMAN periodically updates routing information that avoids failure node rate. This technique eliminates time delay and achieves fast and secure transmission of data.

Keywords

Anonymity, Unlinkability, Unobservability, USOR, Privacy, BATMAN.

I. Introduction

Mobile ad-hoc networks (MANETs) are rapidly evolving as an important area of mobility. MANET is infrastructure less and wireless network contains several nodes which are free to move arbitrarily and can manage themselves. The node in the network not only acts as host, but also acts as routers, that route data to/from other nodes in network. An ad hoc network has the capability of making communication possible even between two nodes that are not in direct range with each other: packets to be exchanged between these two nodes are forwarded by intermediate nodes using a routing algorithm.

Mostly mobile ad hoc networks are used in military communication by planes, soldiers etc, automated battlefields, emergency management teams uses MANET to rescue, disaster relief, commercial sector, quicker access to patient data for record and check status of patient, diagnosis from the hospital database, remote sensors for weather, personal area network, taxi cab network, sports stadiums, collaborative games with multi users, mobile offices, electronic payments from anywhere, voting systems, vehicular computing, education systems with set-up of virtual classrooms, conference rooms, meetings, and peer to peer file sharing systems.

Routing protocols are required due to the dynamic topology maintenance. They are classified into three types:

- Reactive routing protocols(Non-table driven, on demand)
- Proactive routing protocols(Table driven)
- Hybrid routing protocols

In reactive routing protocol, routes are discovered only when data needs to be sent. Route is discovered by route request and reply messages Ex: Ad-hoc On Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR). In proactive routing protocol, every node maintains the network topology information in the form of routing tables, by periodically sending/receiving HELLO packet to/from its neighbour nodes. Ex: Destination Sequenced Distance Vector Routing (DSDV), OLSR (Optimized Link State Routing). The combination of reactive and proactive routing protocol is a hybrid routing protocol which takes advantages of these two protocols and as a result, routes are found quickly in the routing zone. Hybrid routing protocol requires the following three properties Adaptive, Flexible, Efficient and Practical for successful deployment Ex: Zone Routing Protocol (ZRP).

With regard to privacy-related notions in communication networks, we follow the terminology on anonymity, unlinkability, and unobservability discussed in [2]. Anonymity, unlikability, unobservability are possible by combing group signature [3] and ID-based encryption [4].

A group signature is a method which allows a member of a group to anonymously sign a message on behalf of the group. Here it is known that the sign is done by a member of that group but could not identify the individual member who signed. This scheme has a group manager who is in charge of adding group members. And also group manager has the ability to reveal the original signer in the event of disputes.

ID-Based encryption is a type of public key encryption in which the public key of a user is some unique information about the identity of the user. Identity based system allows any party to generate a public key from a known identity value such as ASCII string. A trusted third party called the Private Key Generator (PKG) generates the corresponding private keys. To operate the PKG first publishes a master public key and retains the corresponding master private key (master key). By providing the master key, any party can compute a public key corresponding to the identity ID by combining master public key with the identity value.

II. Related Work

In normal AODV, it uses on demand method to find route. When malicious node is present in the network, packet delivery ratio becomes less. So to avoid attacking malicious node to the network privacy has to be maintained.

An anonymous routing protocol is ANODR [5], in this two problems were addressed. It prevents strong adversaries from tracing packet flow from source or destination through *route anonymity.* It ensures that adversaries cannot discover real identities of nodes through *location privacy.* This design is completely based on *broadcast* *with trapdoor information* to provide node anonymity, encryption and authentication schemes. Main aim of ANODR is to present untraceable and intrusion tolerant routing protocol for MANET.

A new cryptography technique called *pairing* is introduced to propose anonymous neighbour authentication protocol which enables neighbouring nodes to authenticate each other without revealing their identities. This is possible with dynamic changing pseudonym of nodes instead of real identities. MASK [6] allows neighbour nodes to establish pair wise secrete key for anonymous route discovery and data forwarding. MASK outperforms than AODV under heavy traffic load.

Later, one time public/private key pair concept is introduced to achieve anonymity and unlinkability. ASR [10] is designed to achieve stronger location privacy. It ensures nodes on the route have no information on their distance to the source/destination node. It also achieves anonymity and unlinkabilty. It abandons the onion routing to reduce computation overhead. In this method small size packet TAG has included with data packet during transmission. All nodes have to decrypt TAG, if successful it would decrypt entire packet. ASR ensures identity privacy, location privacy as well as route anonymity. The generation of public/private key for each RREQ is expensive.

In previous anonymous routing protocols one time public/private key generation is used for anonymity and unlikability but it increases the computation overhead. To solve this problem, ARM [11] is introduced. It is a novel anonymous on demand routing scheme for MANET. Anonymity is the important part of overall security as it allows users to hide their activities. This enables the private communication between nodes while making it harder for adversaries to focus their attacks. This protocol makes use of secrete key and pseudonym to solve previously proposed tasks.

The combination of public key cryptography and group signature helps to preserve privacy of network. Group signature has very good privacy preserving feature in that everyone can verify the group signature but cannot identify who is the server. ALARM [12], Anonymous Location Aided Routing protocol for MANET makes use of public key cryptography and group signature. It uses nodes current location to construct a secure MANET map. Based on the current map, each node can decide to which node it wants to make the communication. Node privacy under this framework is preserved even if portion of node are stationary, or if speed of the motion is not very high. But ALARM leaks lot of sensitive information such as network topology and location of every node.

Earlier anonymous routing protocols achieve complete anonymity and partial unlinkability. But unobsevability is not achieved due to this attacker can easily trace routing packets and packet headers. To address the problem USOR [1] is introduced, is privacy preserving on demand routing protocol achieved content unobservability in MANET for the first time. Complete anonymity and unlinkability is maintained at every node in MANET. Group signature used for anonymity through which anonymous key establishment is done. It uses ID based encryption and pseudonyms for unobservability. In this both control packets like route request and route replay packets and data packets were encrypted which were indistinguishable from dummy packets of outside adversaries. So USOR achieves strong privacy protection as well as more resistant against attacks.

In a Simple pragmatic approach to routing using BATMAN [7], includes comparison of BATMAN and OLSR. For static wireless mesh networks BATMAN performance is good by considering all performance metrics than OLSR. Traffic overhead of OLSR is almost 90% higher than BATMAN since BATMAN only maintains control packet of OGM but OLSR has to maintain HELLO message as well as topology control messages.

The B.A.T.M.A.N. routing protocol is used in Android Application [8] which operates on the Android Operating System. This method has four scenarios; those were single hop scenario, Join/Leave scenario, multi hop scenario, and network reconfiguration scenario. This approach divides the knowledge about the best path between nodes in the network to all participating nodes.

III. Proposed Work

UnObservable BATMAN technique incorporates unobservable security and proactive routing scheme. B.A.T.M.A.N (Better Approach to Mobile Ad hoc Network) is a proactive routing protocol has knowledge of best hop details. This technique executes in two phases to achieve fast, secure transmission and: Anonymous key establishment and route discovery scheme.

A. Anonymous key establishment

In this phase, every node in the ad hoc network communicates with its direct neighbours within its radio range for anonymous key establishment. Suppose there is a node S with a private signing key gsk_S and a private ID-based key K_S in the ad hoc network and it is surrounded by a number of neighbours within its power range. S does the following anonymous key establishment procedure:

1. S generates a random number $r_S \in Z^*$ q and computes r_SP, where P is the generator of G1. It then computes a signature of r_SP using its private signing key gsk_S to obtain $SIGgsk_S(r_SP)$. Anyone can verify this signature using the group public key gpk. It broadcast (r_SP, $SIGgsk_S$ (r_SP)) within its neighbourhood.
1. A neighbour X of S receives the message from S and verifies the signature in that message. If the verification is successful, X chooses a random number $r_X \in Z^*q$ and computes r_XP. X also computes a signature $SIGgsk_X$ ($r_SP|r_XP$) using its own signing key gsk_X. X computes the session key $k_{SX} = H_2(r_Sr_XP)$, and replies to S with message (r_XP, $SIGgsk_X$ ($r_SP|r_XP$), E_{kSX} (k_X*|$r_SP|r_XP$)), where k_X* is X's local broadcast key.
2. Upon receiving the reply from X, S verifies the signature inside the message. If the signature is valid, S proceeds to compute the session key between X and itself as $k_{SX} = H_2$ (r_Sr_XP). S also generates a local broadcast key k_S*, and sends E_{kSX} (k_S*|k_X*|$r_SP|r_XP$) to its neighbour X to inform X about the established local broadcast key.
3. X receives the message from S and computes the same session key as $k_{SX} = H_2$ (r_Sr_XP). It then decrypts the message to get the local broadcast key k_S*.

The output of this phase is session keys and local broadcast key, these are used to encrypt HELLO packets and data packets.

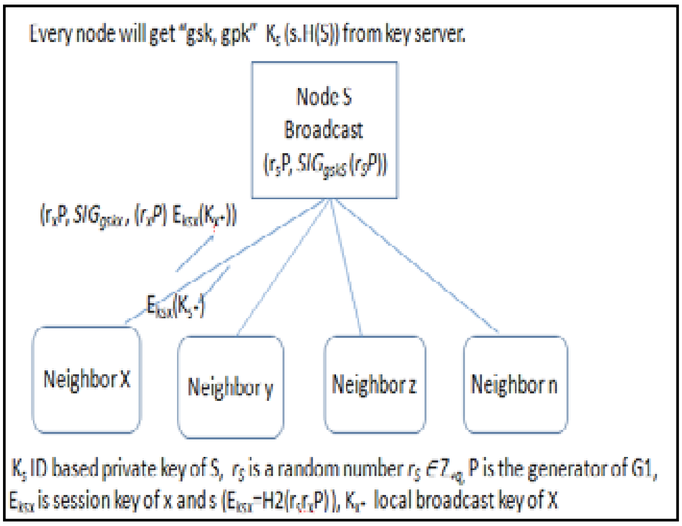
Every node will get "gsk, gpk" K_S (s.H(S)) from key server.
Node S
Broadcast
$(r_SP, SIG_{gskS}(r_SP))$
$(r_xP, SIG_{gskx}, (r_xP)\ E_{ksx}(K_x-))$
$E_{ksx}(K_S-)$
Neighbor X
Neighbor y
Neighbor z
Neighbor n
K_S ID based private key of S, r_S is a random number $r_S \in Z_{*q}$, P is the generator of G1,
E_{ksx} is session key of x and s (E_{ksx}=H2(r_sr_xP)), K_x- local broadcast key of X

Fig. 1: Process of anonymous key establishment

B. Route discovery scheme

Route discovery is done by BATMAN routing protocol. The objective is to maximize the probability of delivering messages. BATMAN checks the existence of the link not the quality of it. The links are compared in terms of the number of originator messages that have been received within the current sliding window.

In B.A.T.M.A.N, all the participating nodes periodically broadcast originator messages (OGMs) to its neighbours. It maintains one routing table to keep track of OGM. In this paper HELLO message is calling as OGM.

Initiation of Nodes:

- In BATMAN all nodes periodically broadcasts hello packets, also known as originator messages, to its neighbours.
- Each originator messages consists of an originator address, sending node address, unique sequence number and hop count.
- Each neighbour changes the sending address to its own address and re-broadcast the OGM.
- On receiving its own message the originator does a bidirectional link check to verify that the detected link can be used in both directions.
- The sequence number is used to check the currency of the message.

BATMAN does not maintain the full route to the destination, each node along the route only maintains the information about the existence of next link through which it can find the best route.

System model: A network is modelled as G = (N, E), where N represents a set of nodes and E represents a set of links between node pairs. For each node i ∈ N in BATMAN, there exist a set of one-hop neighbours, K. The message from a source s ∈ N to a destination d is transmitted along a link (s, d) ∈ E if d is also an element of K otherwise it is transmitted along a multi-hop route made up of a link (s, i) and a route [i, d], where i is a node in K and (s, i) is a link in E. The route [i, d] represents a route from node i to node d.

Algorithm to find best hop

- Consider routing message m from s to d on network G. Eliminate all links (s, i) ∀ I != K to reduce the graph.
- Associate each link with weight w_{si} where w_{si} is the number of originator messages received from the destination through neighbour node i within the current sliding window.
- Find the link with largest weight w_{si} in the sub-graph and send m along the link (s, i).
- If i != d repeat Steps 1 to 4 for routing message from i to d in the sub-graph S

Suppose source S wants to send data to the destination D with A is an intermediate node. The following are the secure packet formats of HELLO and DATA respectively.

$Nonce_S$, $Nym_{S,}$ E_{Ks*}(HELLO, N_S , E_S(S D r_SP), Org, SA, seqno, H)
$Nonce_S$, $Nym_{S,}$ E_{KsA*}(DATA, N_S, seqno, E_{SD}(Payload))

Here $Nonce_S$ is the alternative name of node S, Nym_S = H_3(K_{S*}|$Nonce_S$), RREQ is packet type, N_S is another random number as route pseudonym, which is used as index to specific route entry, Org is originator address of HELLO packet, SA is sending address and H is hop count. As BATMAN uses these secures packets to achieve anonymity, unlinkability, and unobservability.

Considering privacy in BATMAN, it achieves anonymity and unobservability by combining group signature and ID-based encryption. Every data packet and control packet (HELLO) along with its header will be encrypted before sending to other nodes. As mentioned in USOR [1] authorized node can only decrypt packet using key.

The following algorithm is the procedure to implement unobservable BATMAN routing protocol in NS2.

C. BATMAN Algorithm Algorithm

```
1. Initialize the nodes as follows
     a. Key server: (it can share the key at initial time)
     b. Normal node: (normal mobile node)
2. Key server node initially sends the Group ID key to all then
   mobile node
3. If normal node receives the GID then stores into memory
4. If node having GID
     a. Request key server for private key
     b. key server sends private key, public key,
        pseudonym
5. If not
     a. Can't access the request
6. Checks for the secure session availability
     a. If session available
          i. Start the communication with LB Key
     b. If no secure session
          i. Send the session request to neighbour with
             Digital sign
          ii. Neighbour checks the sign and establish the
              session key to requester
          iii. Receives the session key from number of
               neighbours and wait for small interval
          iv. Establish local broad-cast key and send to
              secured neighbours
7. After authentication is over node digitally signs on HELLO
   packet and periodically broadcast to find best hop and stores
   in routing table.
8. If node (i) wants to communicate with another node
     a. It checks in the routing table
     b. if route is found
```

```
        i.    sends data
    c.  if not found
        i.    node i waits for another periodic
              interval till route to the destination
              found
```

VI. Performance Analysis

We have tested MANET with AODV and malicious AODV, implemented USOR, and BATMAN compared the performance of them in NS2.

Scenarios for packet delivery fraction

Table1: Packet Delivery Fraction

No of nodes	AODV	AODV mali	USOR	BATMAN
10	66.63 %	22 %	34.58 %	63.02 %
20	66.35 %	16 %	25.66 %	40.96 %
30	65.35 %	15 %	7.98 %	57.32 %

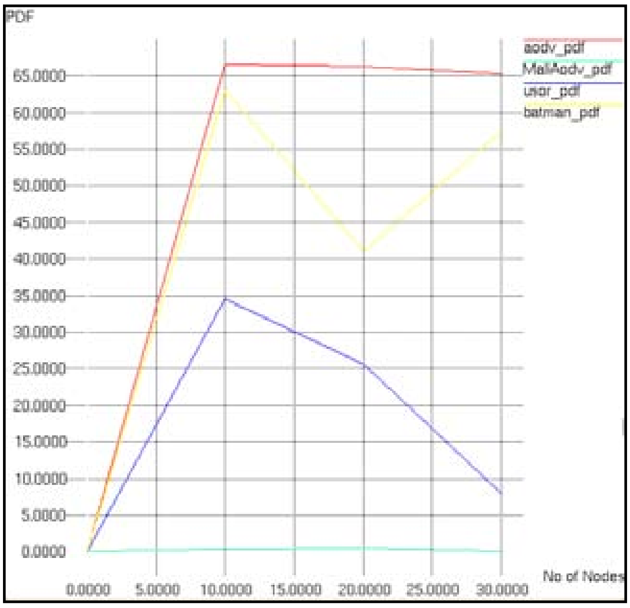

Fig. 2: Packet Delivery Ratio Comparison of AODV, malicious AODV, USOR and BATMAN

Packet delivery ration that is the ratio of received packets to the sent packets, of normal AODV is high among all. But due to lack of security if malicious node enters, PDF is very low as shown in figure2. To avoid this privacy preserving routing is implemented i.e. USOR which is implemented against all attacks but due to on demand in nature, delay and PDF are less compared to BATMAN. PDF is improved in BATMAN than USOR. So now BATMAN is almost reaching to the AODV with security.

Scenarios for packet delay

Table 2: Packet Delay Comparison

No of Nodes	AODV	AODV mali	USOR	BATMAN
10	0.02 s	4.73 s	0.18 s	0.03 s
20	0.03 s	4.28 s	0.21 s	0.05 s
30	0.03 s	50.51 s	0.27 s	0.04 s

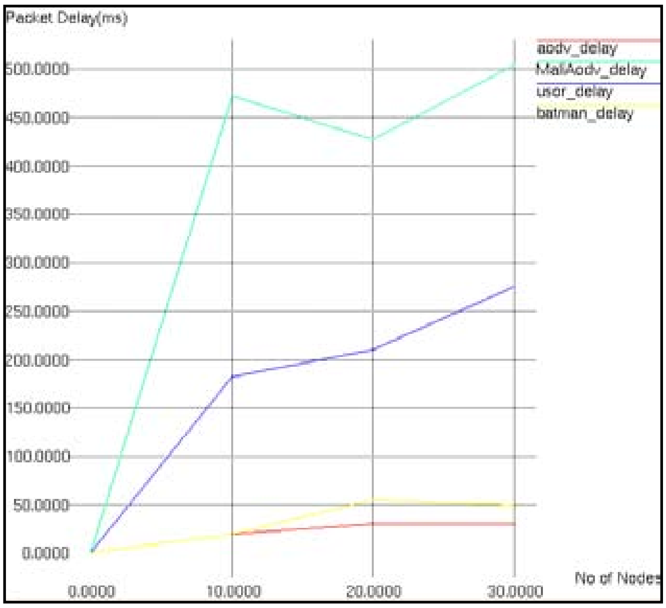

Fig. 3: Packet Delay Comparison AODV, malicious AODV, USOR, and BATMAN

The graphical representation of table2 is figure3. In AODV, packet delay is very less since security is not there in that, but if malicious node is present in the network; delay become high as shown in the figure3 which decreases the performance of the network. So to avoid that, secured privacy preserving routing protocol USOR is implemented. Due to the packet encryption and decryption delay becomes high compared to AODV. There is latency in route discovery, unobservable BATMAN is introduced to make pre route discovery and to reduce latency.

The graphical representation of table3 is figure4. Figure4 shows that AODV, malicious AODV, and USOR contains less overhead compared to BATMAN since it uses on demand routing as route is discovered whenever communication required, but in BATMAN updates its routing table for every periodic interval so routing overhead is high.

Scenarios for Routing Overhead

Table 3: Routing Overhead Comparison

No of Nodes	AODV	AODV mali	USOR	BATMAN
10	52 Pkts	51 Pkts	121 pkts	11600 pkts
20	139 pkts	78 pkts	222 pkts	37311 pkts
30	811 pkts	260 pkts	370 pkts	145583 pkts

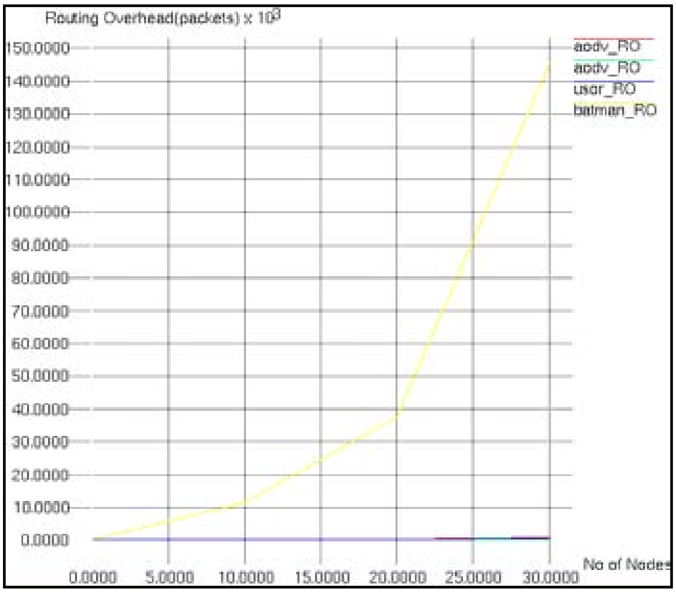

Fig. 4 : Routing Overhead Comparison AODV, malicious AODV, USOR, and BATMAN

V. Conclusion and Future work

In this paper, we proposed an unobservable BATMAN routing scheme. This proposed system achieves efficient transmission of data without delay in finding the route to the destination. Data delivery ration of proposed scheme is increased compared to USOR. Through anonymous key establishment, session key and local broadcast keys were generated, with those keys packets were encrypted before transmitting to another node in a network. Hence, unobservability, anonymity and unlinkability are maintained in the network.

We can enhance this scheme by testing with wormhole attack as well as block hole attack.

VI. Acknowledgement

Authors would like to thank all anonymous reviewers for their valuable comments. We also thank all technical staff of CSED, MVSREC for extending their support and giving valuable suggestions. And also thanks to parents for their support. Finally thanks to almighty god for being with me in each and every moment.

References

[1] *Zhiguo Wan, Kui Ren, and Ming Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks", in IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 11, NO. 5, MAY 2012.*

[2] *A. Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology," draft, July 2000.*

[3] *D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology–Crypto '04, Lecture Notes in Computer Science, vol. 3152, 2004, pp. 41–55.*

[4] *D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology–Crypto '01, Lecture Notes in Computer Science, vol. 2139, 2001, pp. 213–229.*

[5] *J. Kong and X. Hong, "ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM MOBIHOC' 03, pp. 291–302.*

[6] *Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in 2005 IEEE INFOCOM.*

[7] *David Johnson, Ntsibane Ntlatlapa, and Corinna Aichel Simple pragmatic approach to mesh routing using BATMAN", 2nd IFIP International Symposium on Wireless Communications andvInformation Technology in Developing Countries, 2008*

[8] *Leo Sicard, Matyas Markovics, Giannakis Manthios, "An Ad hoc Network of Android Phones Using B.A.T.M.A.N.", in the Pervasive Computing Course, Fall 2010. The IT University of Copenhagen.*

[9] *S. Balaji, Manicka Prabha "UOSPR: UnObservable Secure Proactive Routing Protocol for Fast and Secure transmission using B.A.T.M.A.N" in IEEE international conference on Green High Performance Coputing, may 14-15, 2013.*

[10] *B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anonymous secure routing in mobile ad-hoc networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108.*

[11] *S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications, pp. 133–137.*

[12] *K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, 2011.*

Author's Profile

Sujatha Gaini is currently pursuing M.Tech in Computer Science and Engineering at M.V.S.R Engineering college, Hyderabad, India. Her area of interests are Mobile ad hoc Nerworks, Network Security, Privacy preserving routing protocols, Anonymity, Digital Signature, and Cloud Computing. She has presented papers and poster in national level technical fests.

Md Abdul Azeem is working as an Associate Professor in CSE department at M.V.S.R Engineering College, Hyderabad, since 1999 after having worked in industry for 1 year. He did his B.E and M.Tech in Computer Science & Engineering from Osmania University and pursuing his Ph.D in wireless Ad hoc Sensor Networks from JNTU Hyderabad. His area of specialization includes Mobile Ad hoc Networks, Sensor Networks, Network Security, and Information Security. He has published 2 papers in international journals and 2 papers presented in national conferences. He has graduated 5 M.Tech students. He is a member of CSI.