ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

A Secured Content Unobservable on Demand Routing Protocol For Mobile Ad-hoc Network

[I]Vinothini.V, [II]Yuvaraj.R, [III]Dr. P.S.K.Patra
[I]Dept. of CSE, Agni College of Technology, Anna University, Chennai, Tamilnadu, India
[II]Research Scholar, Anna University,Chennai, Tamil Nadu, India
[III]Head of the Dept., Dept. of CSE, Agni College of Tech., Anna University/ Chennai, Tamil Nadu, India

Abstract
Security in communication is becoming an essential requirement in ad-hoc networks. Secure communication is decisive due to mobility of nodes and its wireless nature. Various schemes are proposed for stronger privacy protection in Mobile ad-hoc network. These schemes offer Disassociativity and obscurity, since no other protocols has a property of complete imperceptibility, since data packets and control packets are still linkable and distinguishable in these schemes. In this paper, we define a stronger privacy scheme that provides a secure routing in MANET. We propose a new efficient routing scheme that provides complete Disassociativity and content imperceptibility. This protocol uses the combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that SCURP (Secure Content Unobservable on demand Routing Protocol) can well protect user privacy against both inside and outside attackers. SCURP is implemented on ns2, and evaluate its performance by comparing with AODV. The simulation results show that SCURP not only has satisfactory performance compared to AODV, but also achieves stronger privacy protection.

Keywords
Obscurity,Privacy preserving,Security

I. Introduction

Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ''ad-hoc'' network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure, e.g., disaster recovery environments. . The independent mobile nodes communicated to each other directly or indirectly through radio waves. In MANET environment the security of each individual network node is very important due to pervasive nature of MANETs. A network node will not always be under the control of their owners and as a result physical security of the node becomes a very important issue.

Secrecy preserving in mobile ad-hoc networks is more essential than in wired environment because of its both static and dynamic topologies with increased dynamics due to node motion or other factors. Comparing with wired networks it is hard to gain the access of the cable and there is no mobility in the network. Providing secrecy preservation in MANET is a very challenging task.

In mobile ad-hoc networks, preserving the secret during the communication of nodes in the network are empathize to three terms. They are as follows

1. OBSCURITY
2. DISASSOCIAITIVITY
3. IMPERCEPTIBILITY

OBSCURITY: In the network, the node are not identifiable which refers to the obscurity. The sender, receiver and intermediate nodes are not known to other nodes.

DISASSOCIATIVITY: The nodes are protected from the outsider.

IMPERCEPTIBILITY: Data packets from all nodes are similar and they are not distinguishable from other packet.

Secured routing in MANET is accomplished by implementing the above factor in all the nodes of the network. In MANET all the nodes act as the host as well as the routers and nodes are interdependent to each other. Thus secured routing is one of the tor importances for the structure of MANET. Mostly mobile ad-hoc networks are used in military communication by soldiers, planes, tanks etc, operations, automated battlefields, emergency management teams to rescue, search, fire fighters or by police and replacement of a fixed infrastructure in case of earthquake, floods, fire etc, quicker access to patient data about record, status, diagnosis from the hospital database, remote sensors for weather, personal area network, taxi cab network, sports stadiums, mobile offices, yachts, small aircraft, electronic payments from anywhere, voting systems ,vehicular computing, education systems with set-up of virtual classrooms, conference rooms, meetings, peer to peer file sharing systems ,collaborative games with multi users. Several routing schemes were proposed to achieve the disassociativity and Imperceptibility identity in mobile Ad-hoc networks. A number of secret preserving routing schemes have been proposed. However, existing obscure routing protocols mainly consider obscurity and partial disassociativity. Most of the scheme uses the feature of asymmetric public key cryptosystems to achieve secure communication .Complete disassociativity and imperceptability are not guaranteed due to incomplete content protection. These protocol fail to protect content of packets and also the header information from attackers,so that the attacker can obtain information like packet type, sender id,receivers id and sequence number etc. This information associates the link between two packets, which breaks disassociativity property and may lead to trace the source for attacks. Since , the header information like unprotected packet type ,sender id, and sequence number also perceptible in these schemes. So, still now we don't have a defined solution to achieve complete disassociativity and imperceptibility. These schemes offer partial disassociativity alone which is not enough in hostile environments. The attackers are still able to know the important information like packet type etc.[2]. This protocol makes the traffic content completely imperceptible to outside attackers ,so that a passive attacker only overhears some random noises. It is difficult to hide information on packet header and the identity of the nodes. The main drawback of most previous schemes is that they all highly depends on public key cryptography, and thus a very high computation overhead. Imperceptibility is the strongest requirement for achieving not

only the obscurity and also the disassociativity property.To achieve imperceptibility, a routing scheme should provide imperceptible communication for both content and control pattern. The paper is organized as follows: Section 2 describes the related works . The details of SCURP protocol are explained in Section 3. The performance evaluation and simulation results are presented, and Section V concludes the work.

II. Related Work

Various obscure schemes are proposed for mobile ad-hoc network, most of these schemes uses public key cryptography that offers different level of security with different cost. These public key cryptosystem has expensive operation on computing the keys and hence have more communication overhead.

Some of following schemes uses public key cryptosystem for routing in the network.

A. ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks.

ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. We address two closely related problems: For route obscurity, ANODR prevents strong adversaries from tracing a packet flow back to its source or destination; for location privacy, ANODR ensures that adversaries cannot discover the real identities of local transmitters. The design of ANODR is based on "broadcast with trapdoor information", a novel network security concept which includes features of two existing network and security mechanisms, namely "broadcast" and "trapdoor information".

B. ARM: Anonymous routing protocol for mobile ad hoc networks.

A novel anonymous on demand routing scheme for MANETs and propose an efficient solution that provides obscurity in a stronger adversary model. It also make use of one-time public/private key pairs to achieve obscurity and disassociativity.

C. ODAR: On-Demand Anonymous Routing in Ad Hoc Networks.

An On-Demand Anonymous Routing protocol for wireless ad hoc networks to enable complete anonymity of nodes, links and source-routing paths/trees using Bloom filters.It provides node, link and path anonymities in ad hoc networks based on Bloom filters. The use of Bloom filters additionally gives ODAR the storage, processing and communication efficiencies, making it suitable in the ad hoc network environments. The mechanisms to efficiently store source routes anonymously, and to forward data packets anonymously. A key management mechanism is described in order provide strong anonymity for end-to-end communications.

D. SDAR: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks.

Self- Organized Public-Key Management scheme allows users to generate their public-private key pairs, to issue certificates, and to perform authentication. This scheme provides different level of privacy protection at different cost [1].Secure Distributed Anonymous Routing Protocol(SDAR) guarantees security, obscurity and high reliability of the established route in a hostile environment. It requires more computation effort because more scalable to network size [2].

E. MASK Protocol.

Anonymous Communications using new cryptography scheme based on pairing.It provides obscurity tp sender and also receiver. The protocol gives a wide range of adversarial attacks and the setup of MASK is quite expensive [3].

F. ALARM: Anonymous location-aided routing in suspicious manets.

A anonymous routing framework (ALARM) uses nodes' current locations to construct a secure MANET map. Based on the current map, each node can decide which
other nodes it wants to communicate with. ALARM takes advantage of some advanced cryptographic primitives to achieve node authentication, data integrity, anonymity and untraceability (tracking-resistance). It also offers resistance to certain insider attacks. To provide secure communication in hostile and suspicious MANETs. To this end, we construct a framework for Anonymous Location-Aided Routing in MANETs (ALARM) which demonstrates the feasibility of obtaining, at the same time, both strong privacy and strong security properties. By privacy properties we mean node anonymity and resistance to tracking. Whereas, security properties include node/origin authentication and location integrity.

G. Other Schemes

ARM fails to protect all content of packets from attackers Privacy offered by hiding routes in limited broadcast groups, and padding messages [4]. Anonymous Dynamic Source Routing protocol (AnonDSR) provides a strong security and obscurity protection. This protocol fails to protect associativity or observability of messages [5]. On-Demand Anonymous Routing protocol enables complete obscurity, this protocol fails to provide disassociativity, and also the entire RREQ/RREP packets are not protected with session keys [6]. PRISM reveals less topology and more privacy-friendly [7]. Anonymous Location-Aided Routing in MANET (ALARM) still leaks a lot sensitive privacy information network topology and Location of every node [8].

III. SCURP : Secure Content Unobservable Routing Protocol .

In this part, we define an efficient imperceptible routing scheme for mobile ad-hoc networks. The data packets and control packet in this protocol were random and these protocol are not distinguishable from dummy packets in the network by the attackers. The authentic nodes can only be able to distinguish the valid packets from the dummy packets which uses symmetric key for encryption and decryption. The SCRUP protocol initiates a key to share with its neighbor and such a key is used to encrypt the packet for the neighbor nodes. The receiving nodes with key and makes a trial decryption and finds whether the packet is intended to itself, if the nodes is not the desired destination then the packet are forwarded to the other nodes in the network. It supports both the unicast and multicast broadcast with a group key and a paired session key. With a source as two keys, SCRUP embraces of two phases : anonymous key establishment and imperceptible route discovery.

The SCRUP properties are as follows:

1) Obscurity: the senders, receivers, and intermediate
nodes are not known to other nodes within the whole network.

2) Disassociativity: the link between any two or more nodess from the senders, the receivers, the intermediate

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

nodes, and the messages is protected from outsiders.
3)Imperceptibility: A valid packets and dummy packets are not distinguishable from other packet.Both the content and the control packet are protected from both the inside and outside attackers
An efficient secret preserving routing protocol SCURP that achieves content imperceptibility by employing anonymous key establishment based on group signature. The setup of SCURP is simple: each node only has to obtain a group signature signing key and an ID-based private key from an offline key server or by a key management scheme. The unobservable routing protocol is then executed in two phases. First, an anonymous key establishment process is performed to construct secret session keys. Then an perceptible route discovery process is executed to find a route to the destination. SCURP is to protect all parts of a packet's content, and it is independent of solutions on traffic pattern imperceptibility. And it can be used with appropriate traffic padding schemes to achieve truly communication imperceptibility.
SCRUP model uses a group signature scheme and a ID based scheme . We use a elliptic curve cryptography and a bilinear diffie hellman for solving these keys.
In this network, all nodes have the same communication range, and each node can move around within the network. A node can communicate with other nodes within its transmission range, and these nodes are called its neighbors. For nodes outside of one's transmission range, one has to communicate via a multi-hop path. We assume the ad hoc network is all connected, and each node has at least one neighbor. Nodes do not use physical addresses like MAC addresses in data frames to avoid being identified by others. Instead, they set their network interfaces in the promiscuous mode to receive all the MAC frames that can be detected in the neighborhood.
Group signature Scheme: The key was generated by the node itself. It generates a group public key gpk which is publicly known by everyone, and it also generates a private group signature key gskX for each node X. The group signature scheme ensures full-obscurity, which earns a signature does not reveal the signer's identity but everyone can verify its authenticity.
ID based scheme: ID based scheme uses the elliptic curve cryptography. Let G1, G2 be an elliptic curve group of order q. An admissible bilinear mapping e : G1 ×G1 → G2 is defined as in [13].The key server chooses a master secret s ∈ Z*q and generates the ID-based private key for node X as KX = s · H1(X). A random generator P is also selected by the server.

A. Imperceptible Routing Scheme

The imperceptible routing scheme comprises of two phases: anonymous key establishment and the secret preserving route discovery process.Each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbours in first phase. Then under protection of these session keys, the route discovery process can be initiated by the source node to discover a route to the destination node in the second phase.

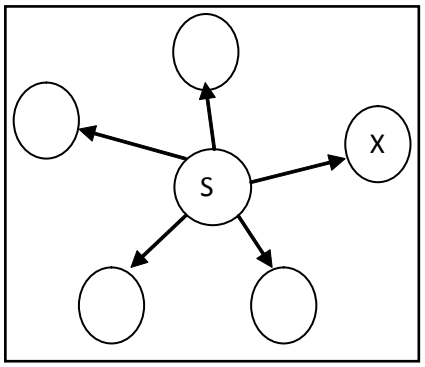


Fig. 1:

1. Anonymous Key Establishment

For anonymous key establishment the node communicates with its direct neighbors within its radio range in the network. Let us assume the source node S with a private signing key gskS and a private ID-based session key KS in the network. The procedure is as follows.
(i). S generates a random number $r_S \in Z^* q$ and computes $r_S P$, where P is the generator of G1. It then computes a signature of $r_S P$ using its private signing key gskS to obtain $SIG_{gskS}(r_S P)$. Anyone can verify this signature using the group public key gpk. It broadcast $r_S P$, $SIG_{gskS}(r_S P)$ within its neighborhood.
(ii). A neighbor 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 $r_X P$. X also computes a signature $SIG_{gskX}(r_S P | r_X P)$ using its own signing key g_{skX}. X computes the session key $k_S X = H_2(r_S r_X P)$, and replies to S with message $\{r_X P, SIG_{gskX}(r_S P | r_X P), E_{kSX}(\bar{k}_X * | r_S P | r_X P)\}$, where $\bar{k}_X *$ is X's local broadcast key.
(iii). 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 $k_S X = H_2(r_S r_X P)$. S also generates a local roadcast key $\bar{k}_S *$, and sends $E_{kSX}\bar{k}_S * | \bar{k}_X * | r_S P | r_X P)$ to its neighbor X to inform X about the established local broadcast key.
(iv). X receives the message from S and computes the same session key as $k_{SX} = H_2(r_S r_X P)$. It then decrypts the message to get the local broadcast key $\bar{k}_S *$.
At the end of this phase the pairwise ID based session key is shared between two nodes in a secure way . The source establishes the local broadcast key and it transmit to its neighbor nodes in the ad-hoc network. It uses Diffie- Hellman key exchange algorithm which generates the key using random number and keys are not shared between the nodes. Hence it is prevented from replay attack and disclosure of key.

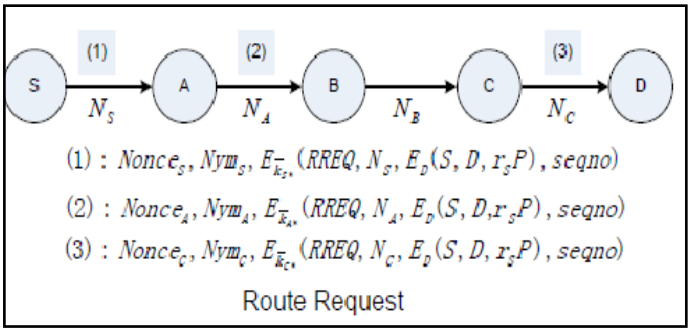
2. Secret Preserving Route Discovery:

Secret preserving route discovery is the normal route discovery that comprises of RouteRequest(RREQ) and RouteReply(RREP). The route request message floods the whole network to reach the destination whereas the route reply traverse directly to the source.

Route Request:

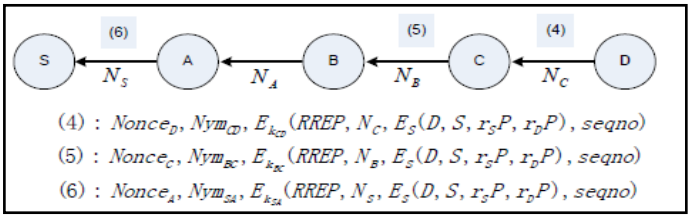
(i). S chooses a random number rS, and uses the identity of node D to encrypt the using the ID based key, which yields ED(S,D, rSP). S then selects a sequence number seqno for this route request, and another random number NS as the route pseudonym To achieve

imperceptibility,
S chooses a nonce NonceS and calculates a pseudonym asNymS = H3(¯kS∗|NonceS).
(ii). S encrypts these items using its local broadcast key ¯kS* to obtain E¯kS* (RREQ,NS,ED(S,D, rSP)). Finally, S broadcast the following unobservable route request to its neighbors: NonceS,NymS,E¯kS*(RREQ,NS,ED(S,D, rSP), seqno).
Each node maintain a temporary routin table for tha packet traverse though it.
(iii). Upon receiving the route request message from S, A tries all his session keys shared with all neighbors to calculate H3(¯kX*|NonceS) or H3(kXA|NonceS) to see which one matches the received NymS. Then A would find out ¯kS*satisfies NymS = H3(¯kS*|NonceS), so he uses ¯k* todecrypt the ciphertext. After finding out this is a route request packet, A tries to decrypt ED(S,D, rSP) using his private IDbased key to see whether he is the destination node.
(iv). A prepares and broadcast the following message to all its neighbors: NonceA,NymA,E¯kA* (RREQ,NA,ED(S,D, rSP), seqno).
(v). Finally, the destination node D receives the following message from C: NonceC,NymC, E¯kC*(RREQ,NC,ED(S,D, rSP), seqno).



Route Reply

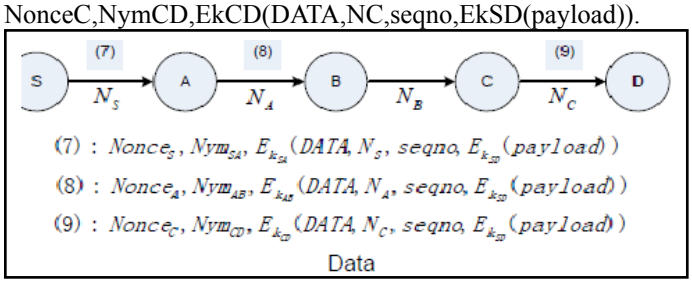
When a destination node D,finds that it is an authentic node to receive the packet, node decrypt the packet and it prepares the reply message to the source node. To reduce communication computation overhead it uses unicast reply instead of broadcast message.



(1) D chooses a random number rD and computes a ciphertext ES(D, S, rSP, rDP) to show that D is the authentic destination. A session key kSD = H2(rSrDP|S|D)
is computed for data protection. Then he generates a new pairwise pseudonym NymCD = H3(kCD|NonceD). At the end, using the pairwise session key kCD, he computes and sends the following message to C: NonceD, NymCD,EkCD(RREP,NC,ES(D, S, rSP, rDP), seqno).
(2) Finally, the following route reply is sent back to the source node S by A in our example illustrated in the Fig. 2: NonceA,NymSA,EkSA(RREP,NS, ES(D, S, rSP, rDP), seqno).
S has successfully found a route to the destination node D, and the route discovery phase is completed successfully.

Imperceptible Packet Delivery: The source node S find its route to destination D efficiently. The source node S now start its imperceptible data packet transmission with the secret key as follows.
(1) The data packets sent by S take the following format NonceS,NymSA, EkSA(DATA,NS, seqno,EkSD(payload)).
(2) A on receiving the above message from S, A knows that this message is for him according to the pseudonym NymSA.
(3) A knows this message is a data packet and should be forwarded to B according to route pseudonym NS.
NonceA,NymAB,EkAB(DATA,NA, seqno,EkSD(payload)).
(4) At the end, the following data packet is received by D:

NonceC,NymCD,EkCD(DATA,NC,seqno,EkSD(payload)).



B. Implementation and Analysis

The difference between the SCURP and AODV relies on the key established between the nodes for secret preserving communication. By the implementation the SCURP protocol is well in protecting all the content in the data packets.

1. Obscurity

User obscurity is implemented by group signature which can be verified without disclosing one's identity. Group signature is used to establish session keys between neighboring nodes, so that they can authenticate each other obscurely. And subsequent routing discovery procedure Is built on top of these session keys. Hence it is easy to see that SCURP fulfills the obscurity requirement under both passive and active attacks, as long as the group signature is secure.

2. Disassociativity

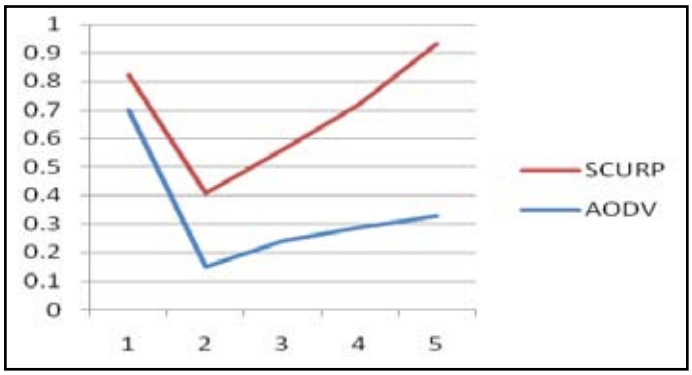
The nonces are only used once and never reused, and so are the pseudonyms. Except the random nonce and the pseudonym, the remaining part of the message, including the trapdoor information in the route request, is decrypted and encrypted at each hop. Hence even for a global adversary who can eavesdrop every transmission within the network, it is impossible for him to find linkage between messages without knowing any encryption key. He even has no idea of the type of the packet being transmitted in the network, and he cannot relate different packets in terms of packet type. The only way to gain information on relationship between transmissions is that the attacker has access to some encryption keys, i.e., he has compromised one or more valid nodes.

3. Imperceptibility

In SCURP, RREQ, RREP and data packets are indistinguishable from dummy packets to a global outside adversary. Meanwhile, nodes involved in the routing procedure are anonymous to other valid nodes. Consequently, SCURP provides imperceptibility as defined for ad hoc networks.
We analyze computation cost of SCURP, and compare it with existing well known schemes AODV. We then describe

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

theperformance evaluation of our protocol. SCURP requires a signature generation in the first phase. In the route discovery process, one ID-based decryption in the second phase.



The performance of the SCURP protocol is evaluated and it is compared with the AODV protocol. As a result AODV has its higher packet delivery ratio when compared with SCRUP because of trusted packet forwarding, frequent mobility of nodes and non applicability route repair technique due to secret preserving communication. Since the Secured Content Unobservable Routing Protocol (SCURP) achieves all three properties for secret preserved communication. The above graph shows the delay in packet delivery ratio.

IV. Conclusion

SCURP –A Secured Content Unobservable Routing Protocol is proposed for a secure communication of data packet in adhoc network. The protocol proposed is based on group signature and ID-based cryptosystem for ad hoc networks. The design of SCURP offers strong privacy protection complete disassociativity and content Imperceptibility—for ad hoc networks. We implemented the SCURP on ns2 and the security analysis demonstrates that the protocol not only provides strong privacy protection, it is also has more resistant against attacks due to node compromise. Future work is to increase the delay in the imperceptible routing mechanism. The protocol not only increases the delay it also improves the overall performance of the system and to defend against the DoS attack and wormhole attack.

References

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

[2] *S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Comput., vol. 2, no. 1, pp. 52–64, Jan.-Mar. 2003.*

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

[4] *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.*

[5] *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.*

[6] *Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR:anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1536–1550, 2009.*

[7] *A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a secure distributed anonymous routing protocol or wireless and mobile ad hoc networks," in Proc. 2004 IEEE LCN, pp. 618–624.*

[8] *D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems.*

[9] *J. Ren, Y. Li, and T. Li, "Providing source privacy in mobile ad hoc networks," in Proc. IEEE MASS'09, pp. 332–341.*

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

[11] *"Privacy-preserving location-based on-demand routing in MANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 10, pp. 1926– 1934, 2011.*