ISSN: 2321-7782 (Online)
Volume 3, Issue 8, August 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Efficient Key Authentication and Network Lifetime Enhancement Schemes for MANET

S. Yuvabarathi[1]
M.Phil-Full Time Research Scholar
Department of Computer Science & Applications,
Vivekanandha College of Arts and Sciences for Women (Autonomous),Ellayampalayam, Tamil Nadu, India

C. Theebendra[2]
M.Sc.,M.Phil, Asst. Professor Department of Computer Science & Applications, Vivekanandha College of Arts and Sciences for Women (Autonomous), Ellayampalayam, Tamil Nadu India

Abstract: ***To achieve security in MANET, it is important to be able to encrypt and authenticate messages sent between sensor nodes. Before doing so, keys for performing encryption and authentication must be agreed upon by the communicating parties. Many key agreement schemes used in general networks, such as public-key based schemes, are not suitable for most MANET infrastructure due to the limited computational abilities of the mobile nodes. Existing protocol, i.e., authenticated anonymous secure routing (AASR), to satisfy the requirement and defend the attacks. In this project, we provide a framework in which to study the security of key pre-distribution schemes, propose a new key pre-distribution scheme which substantially improves the resilience of the network compared to previous schemes, and give an in-depth analysis of our scheme in terms of network resilience and associated overhead. A major requirement on the network is to provide unidentifiability and unlinkability for mobile nodes and their traffics. The route request packets are authenticated by a group signature, to defend the potential active attacks without unveiling the node identities. The key-encrypted onion routing with a route secret verification message, is designed to prevent intermediate nodes from inferring a real destination.***

Keywords: Anonymous Routing, Authenticated Routing, Onion Routing, Mobile Ad hoc Networks, Group Signature, Secure Efficient Trusted Authority Routing

I. INTRODUCTION

The history of wireless networks started in the 1970s and the interest has been growing ever since. During the last decade, and especially at its end, the interest has almost exploded probably because of the fast growing Internet. At present, this sharing of information is difficult, as the users need to perform administrative tasks and set up static, bi-directional links between the computers. This motivates the construction of temporary networks with no wires, no communication infrastructure and no administrative intervention required. Such interconnection between mobile computers is called an Ad hoc Network. In such environment, it may be necessary for the mobile computers to take help of other computers in forwarding a packet to the destination due to the limited range of each mobile host's wireless transmission. A self-configuring infrastructure less network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Mobile Ad Hoc Networks (MANETs) are an emerging type of wireless networking, in which mobile nodes associate on an extemporaneous or ad hoc basis.

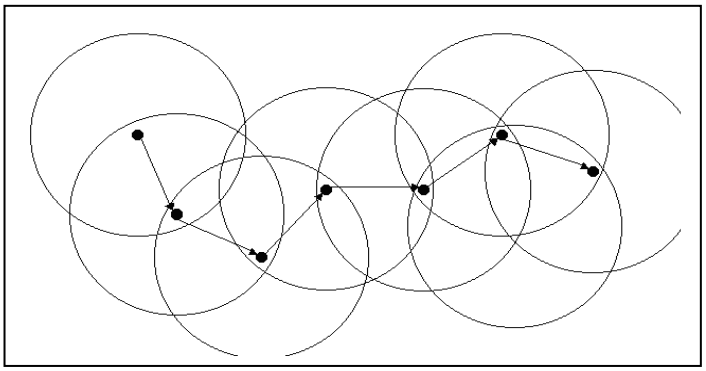


Figure 1.1 Basic Structure of Ad hoc Network.

Ad hoc networks are emerging as the next generation of networks and defined as a collection of mobile nodes forming a temporary (spontaneous) network without the aid of any centralized administration or standard support services. In Latin, ad hoc literally means "for this," further meaning "for this purpose only", and thus usually temporary. An ad hoc network is usually thought of as a network with nodes that are relatively mobile compared to a wired network.

II. PROPOSED WORK

We focus on the MANETs in adversarial environments, where the public and group key can be initially deployed in the mobile nodes. We assume that there is no online security or localization service available when the network is deployed. We propose an authenticated anonymous secure routing (AASR) to overcome the pre-mentioned problems. We adopt a key encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage. Group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet.

ONION ROUTING*:* It is a mechanism to provide private communications over a public network. The source node sets up the core of an onion with a specific route message. During a route request phase, each forwarding node adds an encrypted layer to the route request message. The source and destination nodes do not necessarily know the ID of a forwarding node. The destination node receives the onion and delivers it along the route back to the source. The intermediate node can verify its role by decrypting and deleting the outer layer of the onion. Eventually an anonymous route can be established.

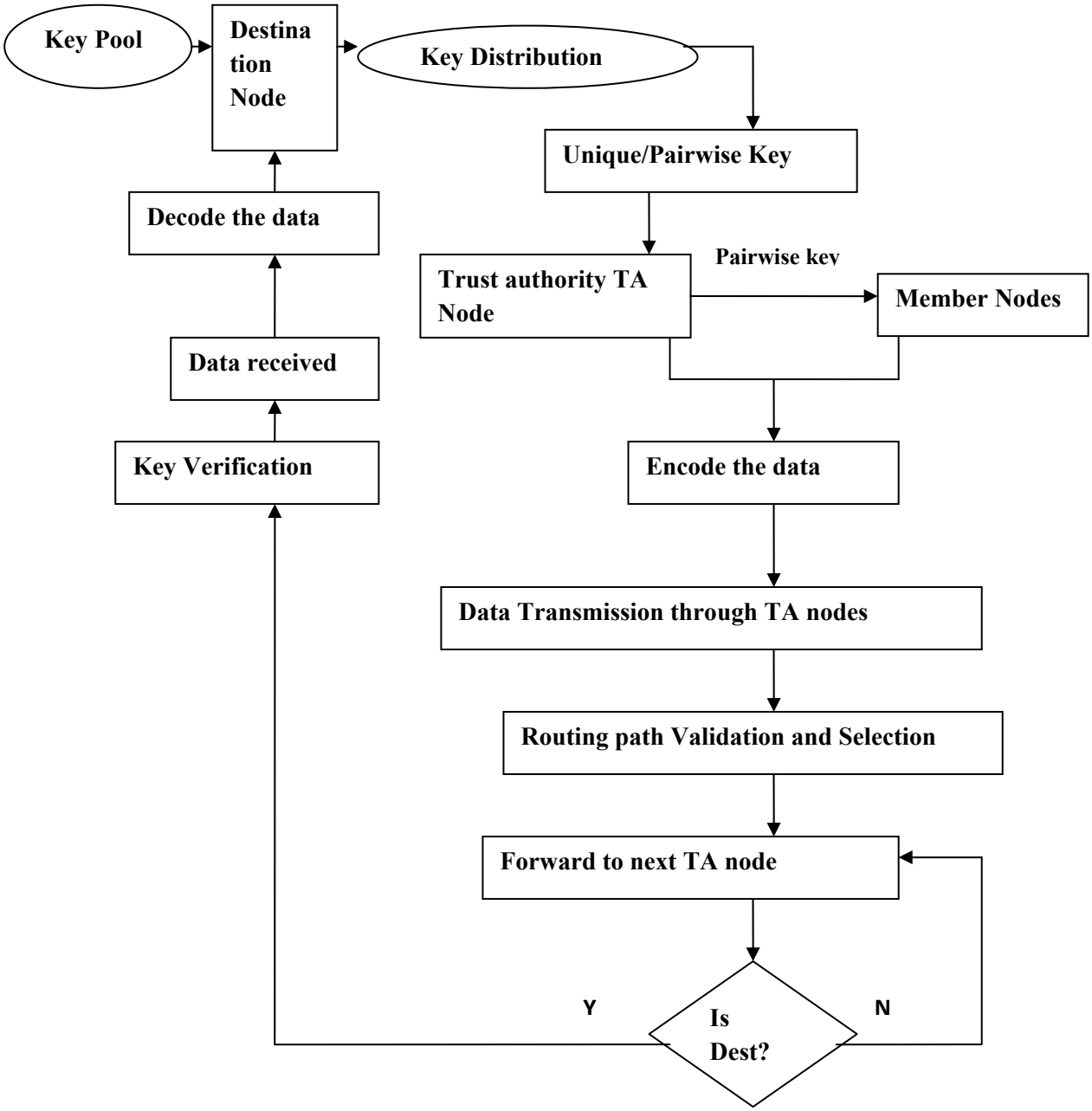
GROUP SIGNATURE: Group signature scheme can provide authentications without disturbing the anonymity. Every member in a group may have a pair of group public and private keys issued by the group trust authority (i.e., group manager). The member can generate its own signature by its own private key, and such signature can be verified by other members in the group without revealing the signer's identity. Only the group trust authority can trace the signer's identity and revoke the group keys.

SECURE EFFICIENT TRUSTED AUTHORITY ROUTING ALGORITHM

In typical two-tier architecture, individual source nodes forward information to their respective trusted authority's (TAs). At the TA the information is aggregated and then sent to a destination by the TA. The TAs and the destination usually form a single hop or multi-hop network, for which energy-efficient on demand routing protocols need to be applied. Nodes are spited according to the radio range and form a group of trusted members, each trusted group indicates a network thus form heterogeneous networks.

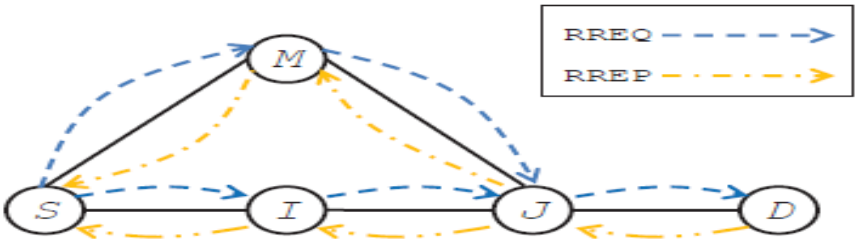
The random pair-wise keys scheme randomly picks groups and assigns each pair a unique random key and also assign common key for TA's. In the random solutions, key chains are randomly selected from a key-pool and distributed to sensor nodes. Our proposed protocol called SETAR aims at minimizing the overall network overhead, delay and energy expenditure associated with the secure data retrieval process while also ensuring balanced energy consumption among nodes and prolonged network lifetime. Finally, we demonstrate how the protocol can be made secure, efficient data transmission and energy efficient.

III. Architecture Diagram



IV. Algorithm

In the route discovery phase, the source node broadcasts an RREQ packet to every node in the network. If the destination node receives the RREQ to itself, it will reply an RREP packet back along the incoming path of the RREQ. In order to protect the anonymity when exchanging the route information, we redesign the packet formats of the RREQ and RREP, and modify the related processes.



The routing algorithm SETAR

1) During route discovery, a source node broadcasts an RREQ packet.

2) If an intermediate node receives the RREQ packet, it verifies the RREQ by using its group public key, and adds one layer on top of the key-encrypted onion. This process is repeated until the RREQ packet reaches the destination or expired.

3) Once the RREQ is received and verified by the destination node, the destination node assembles an RREP packet, and broadcasts it back to the source node.

4) On the reverse path back to the source, each intermediate node validates the RREP packet and updates its routing and forwarding tables. Then it removes one layer on the top of the key-encrypted onion, and continues broadcasting the updated RREP.

5) When the source node receives the RREP packet, it verifies the packet, and updates its routing and forwarding tables. The route discovery phase is completed.

6) The source node starts data transmissions in the established route. Every intermediate node forwards the data packets by using the route pseudonym.

SOURCE NODE

We assume that S initially knows the information about D, including its pseudonym, public key, and destination string. The destination string dest is a binary string, which means "You are the destination" and can be recognized by D. If there is no session key, S will generate a new session key KSD for the association between S and D.Then, S will assemble and broadcast an RREQ packet in the format of (1). To simplify the notation, we ignore the timestamp information in the RREQ packet.

$$S \rightarrow * : [RREQ, Nsq, VD, VSD, Onion(S)]GS^{-} \quad (1)$$

Onion(S) is a keyencrypted onion created by S. The whole RREQ packet is finally signed by S with its group private key GS−. The combination of VD and VSD works similarly to the global trapdoor used in ANODR. We introduce

$$VSD: VSD = (Nv)Kv \quad (2)$$

where Nv and Kv are two parameters created by S and sent to D for future route verification; Nv is a one-time nonce for the route discovery; and Kv is a symmetric key. The secret message VD is defined as:

$$VD = \langle Nv, Kv, dest\rangle KSD, \{KSD\}KD+ \quad (3)$$

If D is the receiver of the message, D can decrypt the second part of VD by its private key KD−, and then decrypt the first part by the obtained KSD. Otherwise, the receiver knows that it is not the intended destination. If S and D have already established KSD in a previous communication, the costly public encryption in the second part of VD can be eliminated, and then VD is defined as:

$$VD = \langle Nv, Kv, dest\rangle KSD, pad \quad (4)$$

where pad is a pre-defined bit-string that pads the message to a constant length. VSD and VD are separated in the RREQ format (1). For a non-destination node, it can use VSD as a unique identity for the route request. Now we describe the encrypted onion Onion(S). S creates the onion core as follow:

$$Onion(S) = OKv (NS) \quad (5)$$

INTERMEDIATE NODE

Then I tries to decrypt the part of VD with its own private key. In case of decryption failure, I understands that it is not the destination of the RREQ. I will assemble and broadcast another RREQ packet in the following format:

I → ∗ : [RREQ, Nsq, VD, VSD, Onion(I)]GI− (6)

where Nsq , VD, and VSD are kept the same as the received RREQ packet; the key-encrypted onion part is updated to Onion(I). The complete packet is signed by I with its group private key GI−. I updates the onion in the following way:

Onion(I) = OKSI (NI , Onion(S)) (7)

where NI is a one-time nonce generated by I to indicate itself; Onion(S) is obtained from the received RREQ packet; this layer of onion is encrypted with the symmetric key KSI . When I's RREQ reaches the next hop J, J will perform the same procedures and update the onion in the RREQ with one more layer, which is: **Onion(J) = OKIJ (NJ , Onion(I)) (8)**

DESTINATION NODE

When the RREQ packet reaches D, D validates it similarly to the intermediate nodes I or J. Since D can decrypt the part of VD, it understands that it is the destination of the RREQ. D can obtain the session key KSD, the validation nonce Nv, and the validation key Kv. Then D is ready to assemble an RREP packet to reply the S's route request.

V. EXPERIMENTAL RESULT

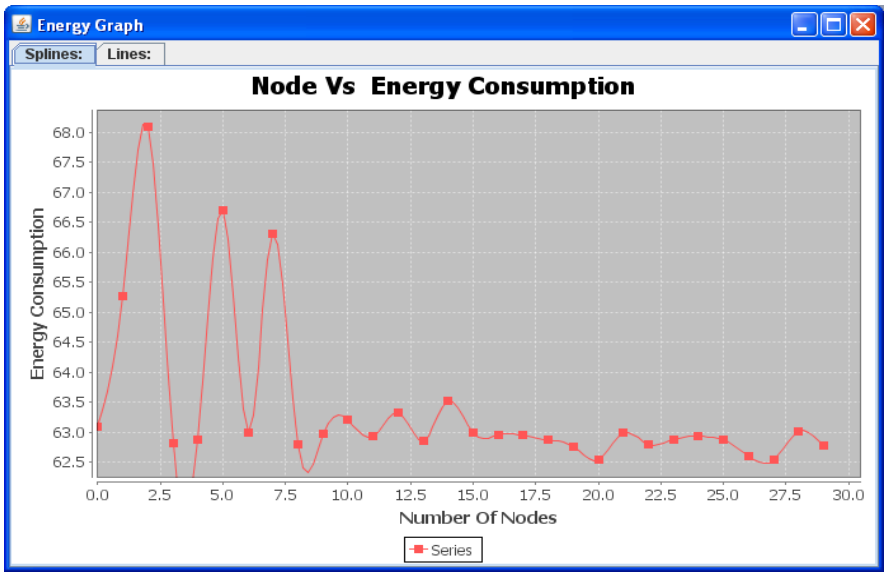
Establish a secure link between a leader node (LN) and a sensor node and to improve network resilience to node captures. Propose scheme that combines the polynomial pool-based key pre-distribution with the probabilistic generation key pre-distribution scheme to establish a pairwise key between FN and any sensor node.

The two proposed schemes guarantee that node can establish a pairwise key with a FN with high probability and without sacrificing security. Security analyses indicate that the two schemes proposed here provide a higher probability for non compromised sensors to establish a secure communication with the LN than previous schemes.The network performance of SETAR routing protocol is discussed and compared with the existing protocol AASR routing protocol.

ENERGY CONSUMPTION

The performance of energy consumption is a measure of energy spent for forwarding a packet to the destination via neighbor nodes and key generation and distribution basis. AASR devour more energy and each time it sends signal to all the available nodes in the path to the destination to send the data packets, key distribution, hop by hop authentication and consumes more energy when recover from attacks. AASR could not cope up with the large group size and network size. This problem is overcomes in the proposed research work SETAR.

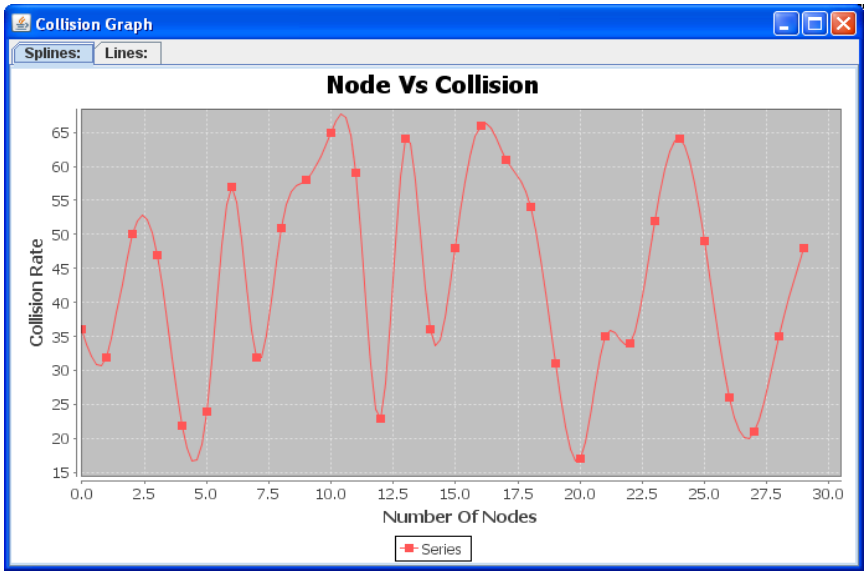
The energy consumption is calculated by the cost of transmitting packet, receiving of packets and discarding of the packets during the period of link error. The energy consumption of existing protocol is average of 64mWhr. The energy consumption for the proposed protocol is average of 89mWhr. The energy consumption is highly reduced by the proposed method.



COLLISION RATE

In a network, when two or more stations attempt to transmit a packet across the network at the same time, a packet collision occurs. When a packet collision occurs, the packets are either discarded or sent back to their originating stations and then retransmitted in a timed sequence to avoid further collision.

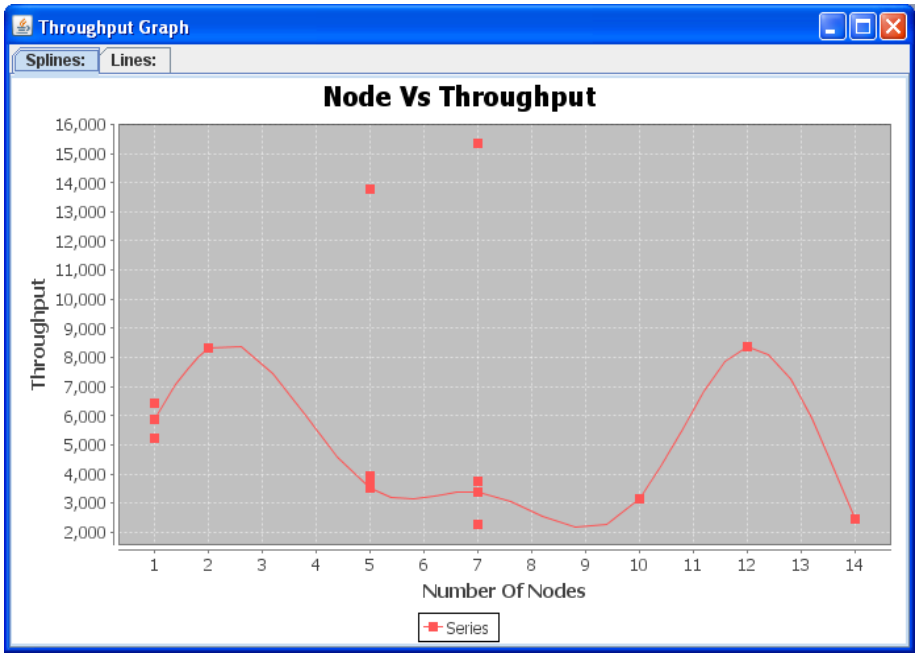
Packet collisions can result in the loss of packet integrity or can impede the performance of a network. The collision rate is calculated by dividing the number of packet collisions detected by the number of packets transmitted. The collision rate factor of SETAR is extremely very low when compared with the AASR.



THROUGHPUT

The amount of data transferred from one place to another or processed in a specified amount of time. Data transfer rates for networks are measured in terms of throughput. The Throughput measures the number of packets received per second at the sink node.

In the proposed routing protocol SETAR the throughput rate is highly increased when compared to the existing protocol AASR. Network throughput performance refers to the average data rate of successful data or message delivery over a specific communications link. Network throughput is measured in bits per second (bps). The throughput factor of SETAR is extremely very high when compared with the AASR.



COMPARATIVE STUDY OF AASR AND SETAR

Performance Metrics	AASR	SETAR
When compared to AASR, SETAR gives better result in terms of pre key distribution and introduction of pair wise key distributio		
Energy Utilization	High	Reduced
Collision Rate	High	Reduced
Throughput	Low	Improved
Security	Weak	Strong

VI. CONCLUSION AND FUTURE ENHANCEMENT

Key management has become a challenging issue in the design and deployment of secure wireless sensor networks. A common assumption in most existing distributed key management schemes is that all sensor nodes have the same capability.The connectivity and lifetime of a sensor network can be substantially improved if some nodes are given greater power and transmission capability. Therefore, how to exploit those heterogeneity features in design of a good distributed key management scheme has become an important issue. In sensor nodes should use pre-distributed keys directly, or use keying materials to dynamically generate pair wise keys. An efficient way of distributing keys and keying materials to sensor nodes prior to deployment with better QOS. It is well-known that Secure Efficient Trusted Authority Routing (SETAR) architecture enables better security and helps to improve power control and QOS. It also scales well to different network sizes and node densities under energy constraints.

In the random solutions, key chains are randomly selected from a key-pool and distributed to sensor nodes. Extensive simulation results show that, even with a small/large number of heterogeneous nodes, the performance of a wireless sensor network can be improved. Investigate the impact of different partitioning strategies (of the target field), such as hexagon shapes, on the performance and security. Assign polynomial shares and seek the optimal solution. Optimizing public-key protocols for sensor networks.

References

1. D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila, "Towards a taxonomy of wired and wireless anonymous Networks," in Proc. IEEE WCNC'09, Apr. 2009.
2. C. Perkins, E. Belding-Royer, S. Das, et al., "RFC 3561 - Ad hoc On- Demand Distance Vector (AODV) Routing," Internet RFCs, 2003.
3. D. Johnson, Y. Hu, and D. Maltz, "RFC 4728 - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," Internet RFCs, 2007.
4. J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in Proc. ACM MobiHoc'03, Jun. 2003, pp. 291–302.
5. J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," IEEE Trans. on Mobile Computing, vol. 6, no. 8, pp. 888– 902, Aug. 2007.
6. A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad hoc Networks," in Proc. IEEE Int'l Conf. Local Computer Networks (LCN'04), Nov. 2004, pp. 618–624.
7. R. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad hoc networks," in Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN'05), Nov. 2005.
8. Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in Proc. IEEE INFOCOM 2005, vol. 3, Mar. 2005, pp. 1940–1951.
9. Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On- Demand Routing in Mobile Ad hoc Networks," IEEE Trans. on Wireless Comms., vol. 5, no. 9, pp. 2376–2386, Sept. 2006.
10. L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," in Proc. Int. Conf. on SECURECOMM'06, Aug. 2006.

