# Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing *

Jiejun Kong†, Xiaoyan Hong‡, M. Y. Sanadidi†, Mario Gerla†
†Department of Computer Science
University of California
Los Angeles, CA 90095
‡Department of Computer Science
University of Alabama
Tuscaloosa, AL 35487
jkong@cs.ucla.edu, hxy@cs.ua.edu, {medy,gerla}@cs.ucla.edu

## Abstract

*Introducing node mobility into the network also introduces new anonymity threats. Nevertheless, this important change of the concept of anonymity has not been studied in state-of-art network security research. This paper presents the needed study. Then we show that anonymous routing in mobile networks has great impact on routing performance. We calls for the attention to devise new and efficient anonymous routing schemes for mobile ad hoc networks.*

## 1 Introduction

A mobile ad hoc network (MANET) can establish an instant communication structure for many time-critical and mission-critical applications. Nevertheless, the innate characteristics of MANET, such as node mobility and wireless transmissions, make it very vulnerable to security threats. Even though many security protocol suites have been designed and deployed to protect wireless communications, they unfortunately do not consider anonymity protection and leave mobile nodes traceable by wireless traffic analysts. Providing mobile anonymity supports for MANET is critical. This poses challenging constraints on secure routing and data forwarding.

The purpose of this paper is to identify new anonymity requirements for mobile wireless networks. Our study has two folds: (1) We show that mobility has changed the underlying assumption of existing anonymity research, thus mobile anonymity cannot be ensured by existing proposals designed for fixed networks; (2) Meanwhile we study design principles of new countermeasures. For mobile wireless networks, our study suggests that a hybrid approach of *identity-free routing* and *on-demand routing* provides better anonymity support than other approaches. The contributions of our study are listed below:

*Part of the work is funded by ONR MINUTEMAN grant N00014-01-C-0016 and NSF NRT grant ANI-0335302.

- We show that anonymity research in fixed networks does not address the new threats identified in this paper. Since mobility dissociates node identities from a topological or physical location, now mobile nodes need more anonymity supports to protect their location privacy and to hide their motion patterns. Various anonymity attacks studied in this paper effectively break existing anonymity schemes designed for fixed networks.
- Given a reasonable assumption that adequate physical protection is not feasible for all mobile nodes, we argue that *identity-free routing* is needed to hide a node's identity from its neighboring forwarders. In addition, since MIX-Net [5] and proactive routing approach are vulnerable to single point of compromise if used in mobile wireless networks, we also show that *on-demand routing* is a better approach to protect mobile wireless networks.

The rest of the paper is organized as follows. Section 2 explains related work including anonymous schemes used in fixed networks and on-demand routing used in mobile networks. In Section 3 we illustrate that how the concept of anonymity is significantly changed by the introduction of node mobility into the network. Then Section 4 shows that ad hoc anonymous routing schemes may have great impact on routing performance. It is an open challenge to serve security needs and performance needs at the same time. Finally Section 5 summarizes the paper.

## 2 Background and related work

**Anonymity in fixed networks** A set of informal notions introduced by [20] characterizes anonymity guarantee in fixed networks. In a distributed system or computer network, the *anonymity set* is the set of all (uncompromised) network members that are identified by unique IDs. Network transmissions are treated as the *items of interest* (IOIs). The concept of *anonymity* is defined as the state of being not identifiable within the anonymity set. More formally, it is defined

in an information theoretic model [27][8] similar to Shannon's classic notion of secrecy [28].

**Definition 1** *For a set as event space $S$, let $X_S$ be a discrete random variable with probabilistic distribution $p(i) = Pr[X_S = i]$ where $i$ represents each possible value that $X_S$ can take. If the event space $S$ denotes an anonymity set, then $X_S$ represents the identity pseudonyms. If the event space $S$ denotes the set of all IOIs, then $X_S$ represents the end-to-end routing path (being eavesdropped) between any sender and any recipient.*

*The adversary's a priori knowledge about the sender/recipient is measured by the uncertainty entropy before any IOI occurs:*

$$H(X_{AS}) = -\sum_{i \in X_{AS}} p(i) \cdot \log\, p(i)$$

*where $AS$ is the anonymity set.*

*The adversary's a posteriori knowledge about the sender/recipient is measured by the uncertainty entropy after all IOIs occur (which are intercepted by the adversary):*

$$H(X_{AS}|C) = -\sum_{i \in X_{AS},\, j \in C} p(i,j) \cdot \log\, p(i|j)$$

*where $C$ is the set of intercepted IOIs, and conditional probability $p(i|j) = \frac{p(i,j)}{\sum_{i \in X_{AS}} p(i,j)}$.*

*An anonymous communication scheme ensures* perfect anonymity *for sender or recipient if $H(X_{AS}) = H(X_{AS}|C)$. Otherwise the compromise of anonymity is measured by the difference or the ratio between these two quantities.* ∎

**Example 2** *Consider a fully connected network of four nodes $AS = \{v_1, v_2, v_3, v_4\}$. Suppose during the entire network lifetime, the only communication event is a unicast from $v_1$ to $v_3$. The adversary's a priori knowledge about the sender and the recipient is $H(X_{AS}) = 2$. The adversary's a posteriori knowledge about the sender and the recipient is $H(X_{AS}|C) = 0$.* ∎

In fixed networks, this information theoretic notion only covers node identity. And nearly all anonymous schemes designed so far assume that the entire network topology is fixed, while many of them also assume the entire topology is known *a priori*. In DC-Net [6], the network topology is suggested as a closed ring and routing is not needed. In Crowds [25] and sorting network [23], pairwise communication has uniform cost (i.e., all nodes are one logical hop away). Thus the protocol can randomly select any member to be next forwarder. This assumption is *not* applicable to mobile ad hoc networks where multi-hop routing is completely different from local forwarding. In MIX-Net [5], a data sender solves the problem of routing by selecting a random path from the known network topology. All subsequent MIX-Net designs [22][21] inherit this assumption. But static and *a priori* topology knowledge is no longer available in mobile ad hoc networks where topology dynamically changes due to mobility, frequent route outage, and node joining/leaving. Maintaining the same topology knowledge that is identical to fixed networks is very expensive and reveals the private knowledge to node intruders. In PipeNet and Onion Routing [24], virtual circuit based routing is introduced. However, they assume that network nodes do not move, do not go offline (as no solution is proposed to address offline nodes), and the topology is fixed after initialization. These assumptions are also inapplicable to mobile ad hoc networks. In a nutshell, these schemes treat the underlying network as a simple fixed graph with abundant *a priori* topological information. They do not address mobile routing and do not fit in highly dynamic multi-hop wireless networks.

**Anonymity in wireless networks** Existing anonymity schemes for wireless networks fall into a spectrum of classes. Deng et al. [7] study how to protect privacy for fixed sinks in a stationary sensor network. *Phantom routing* [18] protects location privacy for mobile sources in a stationary sensor network. Both Location-Base Services [10] and Mix Zones [2] study how to use middleware service to ensure location anonymity with respect to time accuracy and position accuracy. These literatures do not focus on mobility's impact on anonymity.

Various proposals [11][1][26] protect anonymity for mobile users of last-hop wireless networks, where the fixed base stations help to protect identity anonymity. Here mobile nodes does not require anonymous routing because the problem is reduced to fixed network anonymity research after a one-hop wireless forwarding to based stations.

In terms of routing schemes, ANODR [14][16][13] is the first *identity-free* and purely *on-demand* protocol proposed, but we are concerned with its performance in highly mobile networks. ASR[1] is based on ANODR, with several crypto-functions slightly changed (e.g. AES is replaced by one-time pad). Other research efforts include MASK [29] and SDAR [4]. They protect mobile nodes from conventional identity anonymity attacks. Both of them also follow the same *on-demand* approach. But unlike the purely on-demand ANODR using "boomerang onion", MASK seeks to gain better performance by adding a proactive neighbor detection protocol to set up anonymous links prior to on-demand route discovery. And SDAR is different from both ANODR and MASK in key management: (1) In ANODR and MASK, symmetric session keys are needed to implement ACI (Anonymous Circuit Identifier [24]), which only requires pairwise key agreement between *neighboring* nodes; (2) But in SDAR, the destination shares a symmetric session key with each intermediate forwarder (who has paid the key agreement cost in the route request message). Then the destination sends back "onion"-like messages similar to Chaum's MIX-Net design [5]. SDAR packets are ex-

[1]ASR is a variant of ANODR, but not vice versa. Please see our new technical report [17] for more details. The timeline of the related events is: (i) The camera ready version of MOBIHOC'03 [14] was due on April 7, 2003. At this moment we filed UCLA CSD technical report [16] as a backup. (ii) The first author's Ph.D. thesis [13] was filed on June 4, 2004. ANODR was finalized in [13]. In addition to ANODR, notions like "strong/weak location privacy" were also defined in [13] to illustrate ANODR's power. (iii) The camera ready version of LCN'04 where ASR [30] is published was due on August 25, 2004.

cessively long and incur large communication overhead, as demonstrated in the associated simulation study.

## 3 Mobility changes anonymity

In this section we study various *new* anonymity threats in mobile ad hoc networks. We limit our research scope in network layer routing. In other words, anonymity problems at the physical layer or the application layer are *not* studied here. For instance, it is beyond the scope of this paper to study how to trace a network node using signal delay, signal strength index, triangulation and trilateration at the physical layer. Various transmission techniques, such as spread spectrum, MIMO and UWB, have addressed the complementary LPI/LPD/LPE issues. They can be used with anonymous routing schemes to realize an untraceable and unobservable mobile network.

### 3.1 Differentiate *identity anonymity* and *venue anonymity*

The existing set of anonymity definitions described in the previous section does not characterize some unique anonymity threats in mobile wireless networks.

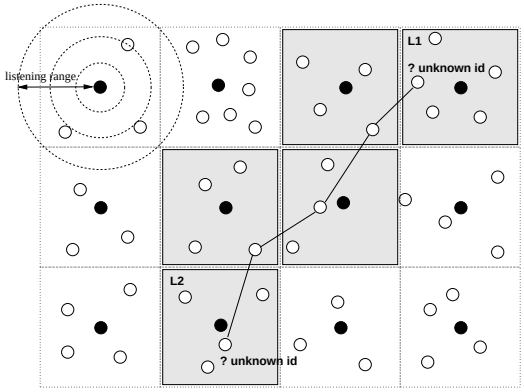


**Figure 1. Underlying graph $G = \langle V, E \rangle$ (Traffic analysts are depicted as solid black nodes. A sender in cell $L1$ is communicating with a recipient in cell $L2$. Identified active routing cells are depicted in shade.)**

Figure 1 illustrates an adversary's network which is comprised of a number of eavesdropping cells. Each cell corresponds to a vertex in an undirected graph $G = \langle V, E \rangle$, where adversarial eavesdropping nodes form a vertex/venue[2] set $V$, and topological links amongst the nodes form an edge set $E$. This grid structure demonstrates several possible attacks. On one hand, it characterizes the capability of a collection of collaborative traffic analysts from multiple cells. On the other hand, it also characterizes the capability of a mobile traffic analyst traveling along the grids to launch anonymity attacks anywhere and anytime.

In fixed networks, a sender (or recipient) and its venue are synonyms, that is, identifying a sender's (or recipient's) venue implies the compromise of sender (or recipient) anonymity. But in mobile networks, a node's identity is dissociated from a specific venue. However, at each traffic analyst's vertex/venue, the adversarial analyst can correlate node identities with its own exact location (e.g., obtained via a positioning system like GPS).

Example 3, 4 and 5 show that *identity anonymity* and *venue anonymity* are different concepts in mobile networks. While identity anonymity is still an issue, venue anonymity is a new problem that should be addressed separately. In particular, **the new *venue anonymity set* is comprised of all vertexes/venues, and the sender/recipient venue should not be identifiable within the new anonymity set given all intercepted IOIs.**

**Example 3** *(Sender or recipient identity anonymity attack in on-demand route request flooding) In common on-demand ad hoc routing schemes like DSR [12] and AODV [19], identities of the source/sender and the destination/recipient are explicitly embedded in route request (RREQ) packets. Any external adversary who has intercepted such a flooded packet can uniquely identify the sender's and the recipient's identities, but may not know the venue/vertex of the sender or the recipient.* ∎

**Example 4** *(Per-hop encryption may not protect sender or recipient identity anonymity against internal adversary) A seemingly-ideal cryptographic protection is to apply pairwise key agreement on every single hop, so that a single-hop transmission is protected by an ideal point-to-point secure channel between the two ends of the hop. The secure channel also protects every packet including the packet header.*

*This solution prevents external adversary from understanding routing messages and network topology, but unfortunately does not prevent any internal DSR/AODV network member from identifying the sender's and the recipient's identities upon receiving a flooded RREQ packet.* ∎

**Example 5** *(Packet flow tracing attack) This attack reveals the relationship between a sender's venue and its recipient's venue. On a (multi-hop) forwarding path, timing correlation and content correlation analysis can be used to trace a packet flow. (1)* Timing correlation analysis: *The adversary can use timing information between successive transmission events to trace a victim message's forwarding path. With no background traffic, a packet forwarded to node $X$ at time $t$ and a packet forwarded from the same node at time $(t + \epsilon)$ are very likely on the same packet flow. (2)* Content correlation analysis: *A control/data flow can be traced by content correlation (e.g., comparing data field contents and length amongst local transmissions).*

*In Figure 1, collaborative adversarial analysts can trace an ongoing packet flow to the sender's venue $L1$ and the recipient's venue $L2$, thus break sender (or recipient) venue anonymity. But they may not be able to identify the sender's (or recipient's) identity. This is possible in ANODR [14] where routing is completely free of sender's and recipient's identities.* ∎

[2] Throughout the paper the term "venue" means an identifiable location that is defined by the one-hop receiving range of an adversarial analyst.

### 3.2 Privacy of location and motion pattern

In fixed networks, a fixed node's topological location and related physical location are determined *a priori*. Besides, the motion pattern of a fixed node is not a network security concern. In other words, there is no need to ensure privacy for a network node's location and motion pattern. Therefore, in anonymity solutions proposed for fixed networks, a network node is allowed to know its neighborhood. For example, a Chaumian MIX knows its immediate upstream and downstream MIXes, a jondo in Crowds [25] knows its next jondo or the destination recipient. If directly ported from the fixed networks, these schemes do not ensure location privacy near any internal adversary, which can launch attacks described in Example 6.

**Example 6** *(One-hop location privacy attack) Given any cell L depicted in Figure 1, the inside wireless traffic analyst may gather and quantify (approximate) information about active mobile nodes, for example, (a) enumerate the set of currently active nodes in L; (b) related quantities such as the size of the set; (c) traffic analysis against L, e.g., how many and what kind of connections in-and-out the cell.* ∎

Ensuring privacy for mobile nodes' motion pattern is a new expression. Example 7 gives a brief overview of the attack. If the network fails to ensure one-hop location privacy, we [15] have showed that a mobile node's motion pattern privacy can be compromised by a dense grid of traffic analysts, or even by a sparse set of internal adversarial nodes under certain conditions, for example, when (1) a node is capable of knowing neighbors' relative positions (clockwise or counter-clockwise), and (2) in DSR/AODV's on-demand route discovery, RREP traffic of the same source-destination pair is correlatable.

**Example 7** *(Motion pattern inference attack) As implied by the name, the goal of this passive attack is to infer (possibly imprecise) motion pattern of mobile nodes. For example, collaborative adversaries can monitor wireless transmissions in and out a specific mobile node, they can combine the intercepted data and trace the motion pattern of the node. In some cases, a network mission may require a set of legitimate nodes to move towards the same direction or a specific spot. Motion pattern inference attack can effectively visualize the outline of the mission. In a network with dense adversarial analysts, motion pattern inference attack can be trivially implemented on top of one-hop location privacy attack using stored historical records.* ∎

Mobile networks could be deployed in severe environments, where nodes with inadequate physical protection are susceptible to being captured and compromised. Any node in such a network must be prepared to operate in a mode that allows no gullibility. In the network, the combination of infrastructureless networking and location privacy presents a dilemma described in Example 8.

**Example 8** *(Location privacy dilemma in infrastructureless networks with internal adversary) In mobile routing schemes without infrastructure support, a node must rely on at least one of its neighbors to forward its packets. When anonymity service is concerned, a node is facing a dilemma. On one hand, it must forward its packets to one of its neighbors, so that the neighbor(s) can further forward the packets towards the destination. On the other hand, the node does not know whether there is an adversarial node amongst its neighbors, and if yes, which neighbor is adversarial. This dilemma calls for* ***identity-free routing*** *that does not reveal a node's identity information to its neighbors.* ∎

### 3.3 Privacy of ad hoc network topology

As shown by Shannon [28], privacy is defined by the difference between *a priori* and *a posteriori* knowledge. In a fixed network, network topology is physically determined *a priori*. Hence there is no such difference (and associated privacy concerns). However, in mobile networks network topology constantly changes due to mobility. Once the adversary knows fresh network topology, it can break the network's anonymity protection given other out-of-band information like geographic positions and physical boundaries of the underlying mobile network. Privacy of network topology becomes a new anonymity aspect in mobile networks.

In fixed Internet, proactive routing schemes like BGP, OSPF and RIP are widely used in inter-domain routing and intra-domain routing. Every router possesses abundant knowledge about network topology if the underlying routing scheme is hierarchical, or complete knowledge about the entire network topology if the underlying routing scheme is flat. This is not a problem for the fixed Internet. In proactive ad hoc routing protocols like DSDV, OLSR and TBRPF, mobile nodes also constantly exchange routing messages, so that each sender node knows enough network topological information to find any intended recipient. In a typical network with pairwise end-to-end communication pattern, this means at each moment every sender node knows abundant network topological information about all other nodes. Thus a single adversarial sender can break anonymity protection of the underlying mobile network. This remark is justified in the following Example 9 and 10.

**Example 9** *(A compromised sender tries to locate where a specific node is) An anonymous routing protocol should prevent a sender from knowing a (multi-hop) forwarding path towards any specific mobile node. Otherwise, a compromised network member can simply function as a sender to trace any mobile node at its convenience. This example shows that pre-computed routing schemes, in particular proactive routing schemes that accumulate a posteriori network topology knowledge on each sender, directly conflicts with anonymity protection in mobile networks.*

*Any equivalence of proactive routing scheme, such as enforcing requirement to let node send out unsolicited advertisements to other nodes so that network topology can be well-known in the network, also directly conflicts with mobile anonymity protection. The network topology knowledge collected on mobile nodes can be used by the adversary to fight against the network. If node compromise is feasible, such design indeed establishes a lot of single points of compromise in the network.* ∎

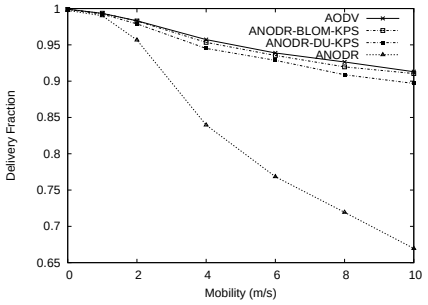


**Figure 2. Data Packet Delivery Fraction**

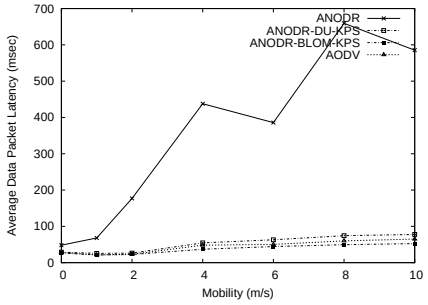


**Figure 3. End-to-end Data Packet Latency**

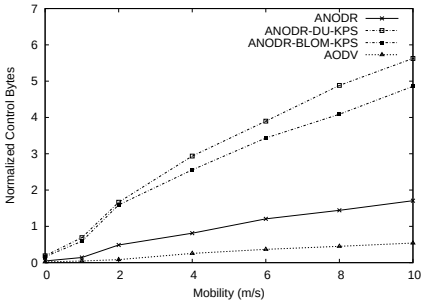


**Figure 4. Normalized Control Bytes**

**Example 10** *(Vulnerabilities of MIX-Net in mobile networks) In MIX-Net, the entire forwarding path must be determined on the sender prior to anonymous data delivery. Proactive routing schemes may be used in MIX-Nets to let sender gather the needed network topology knowledge, but this design choice is not resilient to internal threats. If we directly port Chaumian MIX-Net into a mobile network by treating all or some mobile nodes as Chaumian MIX nodes, then any adversarial sender knows the entire topology of the MIX-Net.* ■

Compared to source routing, link state routing and distance vector routing, virtual circuit [24] based schemes only store information about next link ID for each session. With appropriate design, it is not necessary to reveal a node's identity to neighbors. This *identity-free routing* strategy minimizes information leakage in spite of node intrusions. On the other hand, compared to proactive schemes, on-demand schemes are less vulnerable to internal threats since they do *not* require mobile nodes to acquire fresh network topology knowledge. Based on these observations, we believe that a hybrid of **identity-free routing** and **on-demand routing** provides better anonymity support in mobile ad hoc networks.

## 4 Simulation study

ANODR [14][16][13] is the first *identity-free* and purely *on-demand* ad hoc routing protocol proposed. In ANODR, node identities are never used in routing and thus never revealed to adversary. Nevertheless, in this section we will show how the adoption of various cryptosystems has great impact on anonymous routing performance. We have implemented the following ANODR variants.

1. ANODR, where pairwise key agreement between two consecutive RREP forwarders is implemented by key exchanges using one-time public keys.
2. ANODR-KPS, where the needed key agreement is implemented by Key Pre-distribution Schemes (KPS) instead of public key cryptography. In particular, ANODR-BLOM-KPS uses Blom's deterministic KPS [3] and ANODR-DU-KPS uses Du's probabilistic KPS [9]. In ANODR-DU-KPS, the probability of a successful key agreement per hop is 98%, which means during RREP phase the probability of establishing the anonymous virtual circuit per hop is 98%. With 2% at every hop, key agreement fails and new route discovery procedure must be invoked.

Figure 2 gives the packet delivery fraction as a function of increasing mobility. The figure shows that ANODR-KPS's perform almost as good as optimized AODV. This result can be justified by the following reasons: (1) The onion and/or the key agreement material used in ANODR's and/or ANODR-KPSs' control packets, and the route pseudonym field used in data packets are not big enough to incur noticeable impact to the packet delivery fraction. (2) The 0.02ms/1ms cryptographic computation overhead for the two schemes is too small to make a difference in route discovery. The latter reason also explains why the performance of ANODR degrades faster than ANODR-KPSs – the long encryption/decryption computation time of ANODR prolongs the route acquisition delay, which reduces the accuracy of the newly discovered route, leading to more packet losses. (3) The route optimization of AODV has less effect when a network is at a medium size - 150 nodes. Further, the figure shows that ANODR-DU-KPS has lower delivery ratio than ANODR-BLOM-KPS. The reason for the degradation is the failed probabilistic key agreement along the RREP path. The source only has $0.98^k$ ($k$ is the path length, here, the average is 4-5 hops) chances of receiving a RREP, which may be small for some paths. The source has to initiate a new route discovery in the absence of an expected RREP, resulting in higher control overhead and lower performance. Clearly, the figure shows the tradeoff concern between the performance and the degree of protection.

Figure 3 shows the average end-to-end data packet latency when mobility increases. ANODR-KPS's and AODV exhibit very close end-to-end packet latency as they require very small processing time. ANODR has much longer latency than the aforementioned three due to additional public key processing delay during RREP phase. ANODR-DU-KPS has a little longer end-to-end packet delay than the other two due to probabilistic failures. The delay trend of all the protocols increases when mobility increases, leading to increasing buffering time in waiting for a new route

discovery.

Figure 4 gives the number of control bytes being sent in order to deliver a single data byte. All ANODR variants send more control bytes than AODV, because they use larger packets due to global trapdoors, cryptographic onions, and KPS key agreement materials. In particular, either ANODR-KPS uses long key agreement materials. When mobility increases, the lack of optimization in ANODR variants demonstrates here a faster increasing trend as more recovery are generated from sources.

## 5 Summary

In this paper we have studied unique anonymity threats in mobile ad hoc networks. Unlike a fixed network, a mobile ad hoc network should prevent its *mobile* network members from being traced by passive adversary. The network needs more anonymity protections like (1) venue anonymity in addition to conventional identity anonymity, (2) privacy of node's location and motion pattern, and (3) privacy of ad hoc network topology. Many anonymous schemes designed so far have not considered at least one of these new threats, thus must be re-investigated before they are ported into mobile ad hoc networks. We use ANODR and its KPS-based variants to show that the efficiency of anonymous routing is an open challenge. ANODR employs *on-demand routing* and *identity-free routing* to provide anonymity protection for mobile nodes. Nevertheless, our simulation study shows that routing performance changes significantly when different cryptosystems are used to implement the same function (i.e., pairwise key agreement per-hop). We call for the attention to realize efficient and anonymous routing in mobile ad hoc networks.

## References


[1] G. Ateniese, A. Herzberg, H. Krawczyk, and G. Tsudik. Untraceable Mobility or How to Travel *Incognito*. *Computer Networks*, 31(8):871–884, 1999.

[2] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 2(1):46–55, 2003.

[3] R. Blom. An Optimal Class of Symmetric Key Generation System. In T. Beth, N. Cot, and I. Ingemarsson, editors, *EUROCRYPT'84, Lecture Notes in Computer Science 209*, pages 335–338, 1985.

[4] 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 *29th IEEE International Conference on Local Computer Networks (LCN'04)*, pages 618–624, 2004.

[5] D. L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[6] D. L. Chaum. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

[7] J. Deng, R. Han, and S. Mishra. Intrusion Tolerance and Anti-Traffi c Analysis Strategies for Wireless Sensor Networks. In *IEEE International Conference on Dependable Systems and Networks (DSN)*, pages 594–603, 2004.

[8] C. Díaz, S. Seys, J. Claessens, and B. Preneel. Towards measuring anonymity. In R. Dingledine and P. Syverson, editors, *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002), Lecture Notes in Computer Science 2482*, pages 54–68, 2002.

[9] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A Pairwise Key Predistribution Scheme for Wireless Sensor Networks. In *ACM CCS*, pages 42–51, 2003.

[10] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *MobiSys03*, 2003.

[11] Q. He, D. Wu, and P. Khosla. Quest for Personal Control over Mobile Location Privacy. *IEEE Communications Magazine*, 42(5):130–136, 2004.

[12] D. B. Johnson and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In T. Imielinski and H. Korth, editors, *Mobile Computing*, volume 353, pages 153–181. Kluwer Academic Publishers, 1996.

[13] J. Kong. *Anonymous and Untraceable Communications in Mobile Wireless Networks*. PhD thesis, University of California, Los Angeles, July 2004.

[14] J. Kong and X. Hong. ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks. In *ACM MOBIHOC'03*, pages 291–302, 2003.

[15] J. Kong, X. Hong, and M. Gerla. A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks. In *IEEE MILCOM*, 2003.

[16] J. Kong, X. Hong, and M. Gerla. An Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks. Technical Report CSD-TR030020, Dept. of Computer Science, UCLA, 2003.

[17] J. Kong, X. Hong, and M. Gerla. ASR is a variant of ANODR. Technical Report CSD-TR050014, Dept. of Computer Science, UCLA, April 2005.

[18] C. Ozturk, Y. Zhang, and W. Trappe. Source-Location Privacy in Energy-Constrained Sensor Network Routing. In *ACM SASN*, pages 88–93, 2004.

[19] C. E. Perkins and E. M. Royer. Ad-Hoc On-Demand Distance Vector Routing. In *IEEE WMCSA'99*, pages 90–100, 1999.

[20] A. Pfi tzmann and M. Köhntopp. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In H. Federrath, editor, *DIAU'00, Lecture Notes in Computer Science 2009*, pages 1–9, 2000.

[21] A. Pfi tzmann, B. Pfi tzmann, and M. Waidner. ISDNMixes: Untraceable Communication with Very Small Bandwidth Overhead. In *GI/ITG Conference: Communication in Distributed Systems*, pages 451–463, 1991.

[22] A. Pfi tzmann and M. Waidner. Networks Without User Observability: Design Options. In F. Pichler, editor, *EUROCRYPT'85, Lecture Notes in Computer Science 219*, pages 245–253, 1986.

[23] C. Rackoff and D. R. Simon. Cryptographic defense against traffi c analysis. In *Symposium on the Theory of Computation (STOC)*, pages 672–681, 1993.

[24] M. G. Reed, P. F. Syverson, and D. M. Goldschlag. Anonymous Connections and Onion Routing. *IEEE Journal on Selected Areas in Communications*, 16(4), 1998.

[25] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for Web Transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.

[26] D. Samfat, R. Molva, and N. Asokan. Untraceability in Mobile Networks. In *ACM MOBICOM*, pages 26–36, 1995.

[27] A. Serjantov and G. Danezis. Towards an Information Theoretic Metric for Anonymity. In R. Dingledine and P. Syverson, editors, *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002), Lecture Notes in Computer Science 2482*, pages 41–53, 2002.

[28] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[29] Y. Zhang, W. Liu, and W. Lou. Anonymous Communications in Mobile Ad Hoc Networks. In *IEEE INFOCOM*, 2005.

[30] B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng. Anonymous Secure Routing in Mobile Ad-Hoc Networks. In *29th IEEE International Conference on Local Computer Networks (LCN'04)*, pages 102–108, 2004.