Toward Efficient Solutions to Resist Mobile Traffic Sensors: How Much Performance Cost is Paid by On-demand Anonymous Routing Protocols

Jiejun Kong†, Jun Liu*, Xiaoyan Hong*, Mario Gerla‡
†Department of Computer Science
University of California
Los Angeles, CA 90095
‡Department of Computer Science
University of Alabama
Tuscaloosa, AL 35487

Abstract
The recent progress in embedded real-time system development has realized mobile traffic sensors, for example, embedded systems carried by palm-size Unmanned Aerial Vehicles (UAV). This has great impact on privacy design in mobile ad hoc networks because mobility introduces new privacy targets for the traffic sensors. In a mobile network, a node’s motion pattern, traffic pattern, standing venue and route-driven packet flows, and even the dynamic network topology, all become new interests of the mobile traffic sensors, bringing in new privacy challenges in addition to conventional identity privacy and message privacy. In particular, in wireless ad hoc networks mobile nodes must rely on ad hoc routing in communication. As the wireless medium is open to anyone within the transmission range, the baseline of the mobile traffic sensors is to exploit this routing opportunity to conduct various attacks threatening the network security and privacy.

Recently, the on-demand routing approach has been used by several anonymous routing schemes to prevent mobile nodes from being traced by mobile traffic sensors[29]. In this paper we seek to compare the overhead incurred by security and anonymity operations of two recently proposed on-demand anonymous routing schemes, namely ANODR [28][27] (with an enhanced variant ASR [50]) and SDAR [8]. We use the standard on-demand scheme AODV [37] in the comparison to show how much overhead is paid by each anonymous on-demand scheme. Our simulation study shows that various design choices in anonymous routing trade performance with security protection. We conclude that extensive performance study is needed to evaluate the practicality of the existing and new anonymous routing schemes and their enhancements.

Keywords—Performance study, Mobile traffic sensor, Anonymous routing, On demand routing

1 Introduction
An ad hoc network can establish an instant communication structure for many time-critical and mission-critical applications. However, the intrinsic characteristics of ad hoc networks, such as wireless transmission and node mobility, make it very vulnerable to security threats. Even though many security protocol suites have been proposed to protect wireless communications, they nevertheless do not consider anonymity protection and leave identity information intercepted by nearby passive eavesdroppers. The goal of passive attacks is very different from other related routing security problems such as resistance to route disruption or prevention of “denial-of-service” attacks. In fact, the passive enemy will avoid such aggressive schemes, in the attempt to be as “invisible” as possible, until it traces, locates, and then physically destroys legitimate assets. Consider for example a battlefield scenario with ad hoc, multi-hop wireless communications support. The adversary could deploy reconnaissance and surveillance sensor networks in the battlefield and maintains communications among them. Via intercepted wireless transmissions, they could infer the location, movement, number of participants, and even the goals of our task forces. Anonymity and location privacy guarantees for our ad hoc networks are critical, else the entire mission may be compromised. This poses challenging constraints on routing and data forwarding.

1.1 Mobile traffic sensor network
Recent advances in manufacturing technologies have enabled the physical realization of small, light-weight, low-power, and low-cost miniature aerial vehicles (MAVs) [22][21]. These MAVs refer to a new breed of unmanned aerial vehicles (UAVs) or aerial robots that are significantly smaller than currently available UAVs. Figure 1 illustrates the WASP MAV recently tested by DARPA. It is a 32 cm “flying wing” made of a plastic lithium-ion battery material that provides both electrical power and wing structure. The wing utilizes synthetic battery materials that generate an average output of more than nine watts during flight — enough power to propel the miniature aircraft for one hour forty-seven minutes. Such aerial robots, equipped with information sensing and trans-
mission capabilities, extend the sphere of awareness and mobility of human beings, and allow for surveillance or exploration of environments too hazardous or remote for humans.

The MAV research group of our collaborator has established a long track record in designing, building, and test-flying autonomous MAVs. The next-generation MAVs to be developed are expected to serve as an enabling technology for a plethora of civilian and military applications, including homeland security, reconnaissance, surveillance, tracking of terrorists/suspects, rescue and search, and highway/street patrol. With signal processing techniques (and other out-of-band techniques like visual perception which will not be discussed in this paper), one can use three MAVs to locate the position of a target such as a person’s or a car’s communication interface. Due to the small size of MAVs, the tracking of MAVs is almost unnoticed by the target being tracked. The velocity of an MAV is from 10 to 30 miles per hour, which is fast enough to track a human being or an automobile on local roads. In regard to ad hoc routing schemes, the mobile traffic sensors carried by MAVs can trace where a mobile wireless sender node is, infer the motion pattern of the mobile node, or identify a multi-hop path between a pair of nodes.

1.2 On-demand routing

Most routing protocols in ad hoc networks fall into two categories: proactive routing and reactive routing (aka., on-demand routing) [9]. In proactive ad hoc routing protocols like OLSR, TBRPF and DSDV, mobile nodes constantly exchange routing messages which typically include node identities and their connection status to other nodes (e.g., link state or distance vector), so that every node maintains sufficient and fresh network topological information to allow them to find any intended recipients at any time. On the other hand, on demand routing has become a major trend in ad hoc networks. AODV [36] and DSR [25] are common examples. Unlike their proactive counterparts, on-demand routing operation is triggered by the communication demand at sources. Typically, an on-demand routing protocol has two components: route discovery and route maintenance. In the route discovery phase, the source establishes a route towards the destination by first flooding a route request (RREQ) message, and then receiving a route reply (RREP) sent by the destination. In the route maintenance phase, nodes on the route monitor the status of the forwarding path, and report to the source about route errors. Optimizations could lead to local repairs of broken links.

Clearly, transmitted routing messages and cached routing tables, if revealed to the adversary, leak a large amount of private information about the network. When this happens, proactive protocols and on-demand protocols show different levels of damages by design. With proactive routing, a compromised node has fresh topological knowledge about other proactive nodes during the entire network lifetime. It can also translate the topological map to a physical map using several anchor points (e.g., by techniques similar to sensor network’s localization service [33][46]). This way, a single-point of intrusion allows the adversary to visualize the entire network and know where each node is. On the other hand, with on-demand routing, the adversary has reduced chance in tracing the mobile network in the sense that only active routing entries are in cache and in transmission, and the traffic pattern is probabilistic (depending on application needs) and expires after a predefined timeout.

1.3 Contributions

In this paper, our goal is to carry out a systematic performance study of anonymous routing protocols following the on-demand approach. We illustrate the security overhead incurred by two recently-proposed on-demand anonymous routing schemes, namely ANODR [28][27] (enhanced by ASR [50]) and SDAR [8]. We use the standard on-demand scheme AODV [37] in the comparison to show how much overhead is paid by each anonymous on-demand scheme. Our simulation study shows that various design choices in anonymous routing trade performance with security protection. So far no anonymous routing scheme is able to surpass other competing schemes in all ad hoc scenarios studied. We conclude that extensive performance study is needed to evaluate the practicality of existing and new anonymous routing schemes.

The rest of the paper is organized as follows. In Section 2 we describe ANODR, ASR and SDAR protocols in details. In Section 3 we evaluate their routing performance. Section 4 describes related work in wireless networks. Finally Section 5 summarizes the paper.

2 Anonymous routing revisited

In this section we briefly review anonymous routing approaches that do not use an on-demand design style first. We then revisit the two recently-proposed on-demand anonymous routing schemes. We show the idiosyncrasies of each scheme and how the design choices affect routing protocol performance.

2.1 Anonymous routing not based on the on-demand approach

Before ANODR [28], ASR [50] and SDAR [8], global-knowledge-based routing approach and proactive routing ap-
proach were the dominant choices in anonymous routing design.

In global-knowledge-based routing approach, the network topology is fixed and pre-stored on each node. This includes the following designs. (i) In Chaum’s DC-net [12], the network topology is suggested as a fixed and closed ring. (ii) In Chaum’s MIX-net [11], each message sender pre-stores the entire network topology, and then selects a random path from the known network topology in message routing. All subsequent MIX-net designs [39][23][26][6] inherit this assumption. (iii) In Crowds [43] and sorting network [41], all nodes are one logical hop away, pairwise communications exist with uniform cost. Anonymous messages are forwarded to the next node which is selected in a random manner. If this node is unavailable due to mobility or system crash, then another selection must be made following the same probabilistic method. In other words, every Crowds node (named as “jondo” in [43]) or sorting network node is a member of an overlay network. Although at the network IP layer every node-to-node (or jondo-to-jondo) route is comprised of multiple IP routers, at the anonymized overlay layer such a node-to-node route is a single-hop logical link. This overlay anonymous network assumes either a global routing design or a proactive routing design at the IP network layer. In contrast, static and global topology knowledge is no longer available in mobile ad hoc networks where the network topology constantly changes due to mobility, frequent route outage, and node joining/leaving. Maintaining the same global topology knowledge that is identical to fixed networks is very expensive and reveals the changing topological knowledge to node intruders.

In proactive routing approach, every node proactively and periodically exchanges routing messages with other nodes. Similar to the global routing approach, every node maintains fresh topology knowledge by paying routing communication overheads. In mobile ad hoc networks, various optimized proactive routing schemes, such as OLSR [1] and TBRPF [34], have been proposed to reduce the incurred routing communication overheads. However, like their wired counterparts, the proactive ad hoc routing schemes let every message sender maintain fresh topology knowledge about the network (even though the incurred communication overhead is less than their wired counterparts). Based on the proactively collected fresh routing knowledge, it is then possible to route anonymous messages to the next stop, which in turn routes the messages toward the final destination. This includes the following designs. (i) All MIX-nets leverage proactive routing protocols at the IP layer to acquire network topology knowledge, which is then used at the anonymized overlay MIX layer to route messages. (ii) Like MIX-nets, an overlay of Crowds [43] or sorting network [41] leverages proactive routing information as well. (iii) In wired Internet,PipeNet [13] and Onion Routing [42] employ anonymous virtual circuit in data forwarding. After a connection establishment procedure, a sequence of routing tables are created on the forwarding nodes to deliver data packets.

Each route table holds two columns of virtual circuit identifiers (VCI) in the form of $VCI_x \rightarrow VCI_y$. If a node receives a packet and the packet is stamped with a $VCI_x$ stored in its routing table, the node then accepts the packet, overrides the stamp with the corresponding $VCI_y$, and sends the changed packet to next stop. Both PipeNet and Onion Routing assume that the underlying proactive routing scheme has already provided the needed routing service. Besides, every node in the anonymous network knows its immediate previous stop (upstream node) and immediate next stop (downstream node). (iv) In MIX route [24], a backbone network is formed to cover a mobile network. Every backbone node is a MIX, which uses proactive routing protocols to maintain fresh network topology of the backbone MIX-net.

In a nutshell, these global-knowledge-based routing and proactive routing schemes treat the underlying network as either a stationary graph, or fresh snapshots that can be treated as stationary graphs per proactive period. A shortcoming of applying these approaches in mobile networks comes from node intrusions. If adequate physical protection cannot be guaranteed for every mobile node, intrusion is inevitable within a long time window. The adversary can compromise one mobile node, gather fresh network topology from the node’s knowledge, then use network localization schemes (e.g., distance vector based APS [33]) to pinpoint every mobile node in the network.

Therefore, although various anonymous mechanisms, such as anonymous virtual circuit [13], MIX-net onion and backbone-style MIX-net [24] remain feasible in ad hoc networks, the global routing topology caching and proactive routing topology acquisition approaches are gradually replaced by the on-demand routing approach. Now we describe the recently-proposed on-demand anonymous routing schemes following the order of publication.

2.2 ANODR and ASR

Like PipeNet [13] and Onion Routing [42], ANODR [28][27] and ASR [50] uses anonymous virtual circuit in routing and data forwarding. But unlike infrastructure-based PipeNet and Onion Routing, every ANODR and ASR node does not know its immediate upstream node and immediate downstream node in a mobile environment. Instead, the node only knows the physical presence of neighboring ad hoc nodes. This is achieved by a special anonymous signaling procedure.

Route discovery The source node initiates the anonymous signaling procedure. It creates an anonymous global trapdoor and an onion in a one-time route request (RREQ) flood packet.

1. Anonymous global trapdoor: The global trapdoor is a (semantically secure [17]) encryption of a well-known tag message (e.g., a pre-determined bit-string “You are the destination”) that can only be decrypted by the destination. Once the destination receives the flooded RREQ packet, it decrypts the global trapdoor and sees the well-known tag. But all other nodes see random bits after
decryption. The design of global trapdoor requires anonymous end-to-end key agreement between the source and the destination.

2. Onion: As the RREQ packet is flooded from the source to the destination, each RREQ forwarding node adds a self-aware layer to the onion. Eventually the destination receives an onion that can be used to deliver a route reply (RREP) unicast packet back to the source. The signaling procedure ends when the source receives RREP, and the anonymous virtual circuit is established during the RREP phase.

RREQ flood is a very expensive procedure, while public key crypto-processing is also expensive. According to measurement reports [10] on low-end mobile devices, common public key cryptosystems require 30–100 milliseconds of computation per encryption or per signature verification, 80–900 milliseconds of computation per decryption or per signature generation. Therefore, combining public key crypto and RREQ flood likely degrades routing protocol’s performance. ASR [50] does not study how to establish the shared symmetric key between the source and the destination. ANODR [27] proposes to avoid public key crypto except in the first RREQ flood between a pair of communicators. In ANODR [27], each node is capable of doing encryption and decryption in both symmetric and public key cryptosystems. To establish the symmetric key shared between the source and the destination, the source must cache the certified public key of the intended destination prior to communication. (1) This implies that every network node must acquire a signed credential from an offline authority $\Psi$ prior to network operations. The credential can be verified by the well-known $PK_\Psi$. The credential is in the form of “[id, pk$_{id}$, validtime]$_{SK_\Psi}$” signed by $SK_\Psi$, where a unique network address $id$ is assigned to a node. $pk_{id}$ is the certified public key of the $id$, and validtime limits the valid period of the credential. Instead of using the unprotected plain $id$, the source remembers the credential and avoids using $id$ in communication. (2) The credentials are not secret messages. They can be freely exchanged in the network to facilitate source nodes’ caching experience. In contrast, the selection of a destination’s $pk_{id}$ is a secret random choice of the source node. (3) The selected $pk_{id}$ of the destination is the global trapdoor key used in the first RREQ flood between the source and the destination. For better performance, a symmetric key is piggybacked in the first global trapdoor. Then the source would use the symmetric key in later global trapdoors between the same pair of source and destination. This spares the need of public key decryption in later RREQ floods.

At route reply (RREP) phase, the onion\(^1\) is decrypted to establish routing tables en route. When the onion comes back from the destination in the reverse order of encryption. The RREP upstream node chooses a random number $vci$ and places it with the onion. The RREP downstream node receives this $vci$, then functions as the successive upstream node to choose its own $vci$ and overrides the same field in the packet. As the RREP packet is processed and forwarded towards the source node, each route table on a forwarder $Y$ holds two columns of virtual circuit identifiers (VCI) in the form of $vci_y \rightarrow vci_x$, where $vci_x$ is chosen by $Y$’s RREP upstream node $X$, and $vci_y$ is chosen by $Y$ itself. Later in data packet delivery, if a node receives a packet and the packet is stamped with a $vci_x$ stored in its routing table, the node then accepts the packet, overrides the stamp with the corresponding $vci_y$, and sends the changed packet to next stop (the source and the destination are denoted with special VCI tags $vci_{src}$ and $vci_{dst}$).

Data delivery ANODR and ASR seek to make every data packet computationally one-time. This prevents traffic analysis and replay attacks. Hence a $vci$ must be a secret shared on a forwarding hop. It is used as the cipher key to encrypt the link frame payload (i.e., IP header and payload). Besides, the explicit VCIs stamped on data packets are computationally one-time. They are cryptographically strong pseudorandom sequences generated from the shared $vci$, which is now used as the shared secret seed. To share the secret $vci$ on a hop, a per-hop key exchange scheme is needed. (1) At RREQ phase, an RREQ upstream node (which is later the RREP downstream) must put a one-time temporary public key in the RREQ flood packet. This one-time temporary public key is recorded by the RREQ downstream node (which is later the RREP upstream) for the source/destination session. The RREQ downstream node then overrides the field with its own temporary public key. (2) At RREP phase, the RREP upstream node (earlier the RREQ downstream) uses the stored one-time public key to encrypt the contents of RREP packet including the $vci$ and the coming-back onion. If a one-hop RREP receiver decrypts the encrypted contents and sees the onion it sent out previously at RREQ phase, then this receiver (earlier the RREQ upstream) is en route. The anonymous virtual circuit is established when the source node receives the onion core it sent out a while ago. This way, the one-time public keys are plain data bits during RREQ floods. Per-hop key agreement overhead (using public key encryption/decryption) is paid during RREP unicasts.

Performance impact ANODR and ASR have to pay expensive public key crypto-processing overhead during the first RREQ flood between a pair of communicators and all RREP unicasts. This significantly affects their routing performance. In addition, all the anonymous routing schemes reviewed in this section, i.e., ANODR, ASR and SDAR, have not implemented route optimization techniques specified in AODV and DSR (e.g., gratuitous route reply, proactive route fix using constrained flooding, etc.).

2.3 SDAR

SDAR [8] is a combination of proactive and on-demand route discovery. Unlike the purely on-demand ANODR and ASR,
every SDAR node uses a proactive and explicit neighbor detection protocol to constantly see the snapshot of its one-hop mobile neighborhood. Every SDAR node periodically sends out a HELLO message holding the certified public key of the node. The SDAR HELLO messages are significantly longer than regular beacon messages because it holds long public keys (typically $\geq 1024$-bit in a common public key cryptosystem like RSA and El Gamal).

An SDAR node is named as the central node as it sits at the center of its own one-hop transmission circle. A central node $X$ explicitly sees its neighbors’ network IDs and verifies associated credentials. $X$ classifies its neighbors into three trust levels according to their behavior. Routing preference is given to the higher level nodes. This is implemented by group key management. $X$ randomly chooses a key for all neighbors in the same trust level (except the lowest level, which is not protected by cryptoschemes). The key is then shared by $X$ and these nodes. Routing messages intended for the highest level is encrypted with the group key corresponding to the highest level. Routing messages intended for the medium level is encrypted with either the group key corresponding to the medium level or the one corresponding to the highest level. Routing messages intended for the lowest level is not encrypted and thus seen by all listening nodes.

### Route discovery
SDAR also employs an on-demand route discovery procedure to establish ad hoc routes. Similar to ANODR and ASR, an SDAR source node $S$ puts a global trapdoor in its RREQ flood packet. While the global trapdoor is encrypted with the destination $D$’s certified public key, a symmetric key is piggybacked into the global trapdoor to fulfill end-to-end key agreement. Nevertheless, unlike ANODR/ASR which uses identity-free tags, SDAR uses the destination $D$’s ID in the global trapdoor. This differentiates ANODR/ASR’s identity-free global trapdoor from SDAR’s ID-based global trapdoor.

Unlike ANODR and ASR, SDAR’s RREQ forwarding events do not form any onion. Instead, a sequence of key agreement operations are implemented. The source node $S$ puts its one-time public key $TPK$ in the RREQ flood packet. $S$ also piggybacks the corresponding one-time private key $TSK$ in the RREQ flood packet. While the global trapdoor is encrypted with the destination $D$’s certified public key, a symmetric key is piggybacked into the global trapdoor to fulfill end-to-end key agreement. Nevertheless, unlike ANODR/ASR which uses identity-free tags, SDAR uses the destination $D$’s ID in the global trapdoor. This differentiates ANODR/ASR’s identity-free global trapdoor from SDAR’s ID-based global trapdoor.

Similar to MIX-net, now the SDAR destination $D$ has the $l$ (symmetric) keys to form an RREP packet in the form of MIX-net onion. The destination $D$ puts all symmetric key $K$’s in the innermost core so that only the source $S$ can decrypt the onion core and share $D$’s symmetric key with every RREP forwarder.

Once the source $S$ receives the coming-back RREP, both the source $S$ and the destination $D$ have made a symmetric key agreement with every intermediate forwarder. Like the way RREP packet is delivered, $S$ and $D$ use MIX-net onion to deliver data payloads to each other.

### Data delivery
The SDAR literature [8] claims that the data delivery design is similar to Onion Routing [42] (which uses anonymous virtual circuit), but its data delivery protocol description matches MIX-net onion rather than Onion Routing’s virtual circuit. In fact, as described below in Section 3, adopting virtual circuit in data delivery has great impact on routing performance.

### Performance impact
Compared to the purely on-demand ANODR, SDAR incurs extra neighbor detection overhead. Each neighbor detection message is significantly longer than short beacon messages, and also incurs a number of public key authentication and key exchange operations in the changing mobile neighborhood.

In on-demand route discovery, SDAR incurs large cryptographic and communication overheads. Every RREQ forwarding must pay the cost of a public key encryption using $TPK$. This incurs expensive public key encryption overhead in the entire network per RREQ flood. SDAR’s RREQ and RREP packets are very long. Each RREQ packet holds $l'$ $TPK$-encrypted blocks where $l'$ is the hop count from the source $S$ to the current RREQ forwarder, each of the blocks is as long as the public key length (typically $\geq 1024$-bit in a common public key cryptosystem like RSA and El Gamal). Every RREP packet and DATA packet has $l$ MIX-net onion layers, each of the layers is at least 128-bit long (a typical symmetric key length).

### 2.4 Summary

Table 1 compares several design choices that may have significant impact on routing protocol performance and on security/performance tradeoffs.

<table>
<thead>
<tr>
<th></th>
<th>ANODR</th>
<th>ASR</th>
<th>SDAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully on-demand?</td>
<td>Fully</td>
<td>Fully</td>
<td>Proactive neighbor detection</td>
</tr>
<tr>
<td>PKC in RREQ flood</td>
<td>First contact</td>
<td>First contact</td>
<td>All the time</td>
</tr>
<tr>
<td>Data delivery</td>
<td>Virtual circuit</td>
<td>Virtual circuit</td>
<td>MIX-net onion</td>
</tr>
<tr>
<td>Neighbor exposure</td>
<td>No</td>
<td>No</td>
<td>Exposed</td>
</tr>
</tbody>
</table>

We compare the above aspects due to the following reasons: (1) Proactive neighbor detection incurs periodic communication and computational overheads on every mobile node. (2) Using expensive public key cryptography (PKC
encryption/decryption) with expensive RREQ flood incurs intensive communication and computational overheads per flood. (3) In terms of data delivery performance, virtual circuit based schemes are more efficient than MIX-net’s onion based schemes. The latter one incurs / real-time encryption delay on the source node and then a single real-time decryption delay on every packet receiving nodes. (4) In MIX-net, a one-hop neighborhood is exposed to an internal (and possibly external) adversary. This is not a security problem in fixed networks. But in mobile networks, this reveals the changing local network topology to mobile traffic sensors, which could quickly scan the entire network for once and assemble every neighborhood together to obtain an estimation of the entire network topology. (5) Recipient anonymity (of the destination’s network ID) is a critical security concern. Otherwise, every RREQ packet receiver (i.e., every node participating in the RREQ flooding) can see how busy a destination node is from the received RREQ packets. This traffic analysis can be used by the mobile traffic sensors to define the priority in node tracing.

3 Performance evaluation

The performance of the anonymous ad-hoc routing protocols discussed in this paper is evaluated through simulation in our empirical study. In the evaluation, the aforementioned anonymous ad-hoc routing protocols are presented for comparison together with the original AODV. Our evaluation concerns the influence from processing overhead incurred by the cryptosystems in use and also the influence of routing control overhead caused by different size of routing control packets. The simulation of the protocols are all implemented based on AODV. Each of them implements the main principles but uses different cryptosystems in establishing the secret hop key $vci$. The cryptosystems include the public key cryptography and a variant of efficient Key Pre-distribution Schemes (KPS). In a public key scheme, the network needs an offline authority to grant every network member a credential signed by the authority’s signing key, so that any node can verify a presented credential with the authority’s well-known public key. The standard ANODR, SDAR and ASR described in Section 2 uses public key cryptography. In a KPS scheme, the network needs an offline authority to load every node with personal key materials. Afterward, any two nodes can use their key materials and agree on a symmetric key. If the underlying KPS scheme is a probabilistic one [16][15] rather than a deterministic one [7], then the key agreement succeeds with a high probability. Besides the original public key based ANODR, a variants of ANODR using KPS (in RREP unicasts) is tested in our simulation study. It uses the probabilistic KPS scheme proposed by Du et al. [15] (denoted as ANODR-DUKPS). In ANODR-DU-KPS, the probability of achieving a successful key agreement at each hop is 98%. In other words, key $vci$ agreement fails with 2% at every RREP hop. A new route discovery procedure will be invoked eventually by the source.

3.1 Crypto-processing performance measurement

The processing overhead used in our simulation is based on actual measurement on low-end devices. Table 2 shows our measurements on the performance of different cryptosystems. For public key cryptosystems, the table shows processing latency per operation. For symmetric key cryptosystems (the five AES final candidates), the table shows encryption/decryption bit-rate.

Table 2: Processing overhead of various cryptosystems (on iPAQ3670 pocket PC with Intel StrongARM 206MHz CPU)

<table>
<thead>
<tr>
<th>Cryptosystem</th>
<th>decryption</th>
<th>encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECAES (160-bit key)</td>
<td>42ns</td>
<td>160ms</td>
</tr>
<tr>
<td>RSA (1024-bit key)</td>
<td>900ms</td>
<td>30ms</td>
</tr>
<tr>
<td>El Gamal (1024-bit key)</td>
<td>80ms</td>
<td>100ms</td>
</tr>
<tr>
<td>AES/Rijndael (128-bit key &amp; block)</td>
<td>29.2Mbps</td>
<td>29.1Mbps</td>
</tr>
<tr>
<td>RC6 (128-bit key &amp; block)</td>
<td>53.8Mbps</td>
<td>49.2Mbps</td>
</tr>
<tr>
<td>Mars (128-bit key &amp; block)</td>
<td>36.8Mbps</td>
<td>36.8Mbps</td>
</tr>
<tr>
<td>Serpent (128-bit key &amp; block)</td>
<td>15.2Mbps</td>
<td>17.2Mbps</td>
</tr>
<tr>
<td>TwoFish (128-bit key &amp; block)</td>
<td>30.9Mbps</td>
<td>30.8Mbps</td>
</tr>
</tbody>
</table>

Clearly, different cryptosystems introduce different processing overhead, thus have different impact on anonymous routing performance. For all public key cryptographic operations in the simulation, we use ECAES with 160-bit key. For the symmetric cryptography, we use AES/Rijndael with 128-bit key and block. The coding bandwidth is about 29.2Mbps. As an example, in ANODR, computational delay is approximately 0.02ms for each onion construction during each RREQ and RREP forwarding, and another public key processing time 160 + 42 = 202ms for RREP packets. The KPS based ANODR trades link overhead for processing time, i.e., ANODR-DU-KPS uses 1344 bits and 1288 bits key agreement material for RREQ and RREP packets respectively. Each of them requires only 1ms extra time in symmetric key crypto-processing.

3.2 Simulation model

The simulation is performed in QualNet$^{TM}$ [45], a packet level simulator for wireless and wired networks developed by Scalable Network Technologies Inc. The distributed coordination function (DCF) of IEEE 802.11 is used as the MAC layer in our experiments. It uses Request-To-Send (RTS) and Clear-To-Send (CTS) control packets to provide virtual carrier sensing for unicast data packets to overcome the well-known hidden terminal problem. Each unicast data transmission is followed by an ACK. The radio uses the two-ray ground reflection propagation model and has characteristics similar to commercial radio interfaces (e.g., WaveLAN). The channel capacity is 2Mbps.

The network field is 2400m$\times$600m with 150 nodes initially uniformly distributed. The transmission range is 250m. Random Way Point (RWP) model is used to simulate node mobility. In our simulation, the mobility is controlled in such a way that minimum and maximum speeds are always the same (to
fix a recently discovered problem [48]), but increase from 0 to 10 m/sec in different runs. The pause time is fixed to 30 seconds. CBR sessions are used to generate network data traffic. For each session, data packets of 512 bytes are generated at a rate of 4 packets per second. The source-destination pairs are chosen randomly from all the nodes. During 15 minutes simulation time, a constant, continuously renewed load of 5 short-lived pairs is maintained. All simulations are conducted in identical network scenarios (mobility, communication traffic) and routing configurations across all schemes in comparison. All results are averaged over multiple runs with different seeds for the random number generator.

### 3.3 Routing performance measurement

We evaluate the performance of these protocols in terms of five metrics: packet delivery ratio, average end-to-end data packet delay, average route acquisition delay, and normalized routing load in bytes and number of packets per data packet delivered. SDAR requires each node to periodical broadcast messages to neighboring one hop nodes. When we compare the five performance metrics, we leave out the periodical routing control overhead for SDAR and study it in a separate discussion.

All of the curves show a more or less yet steady descendant when mobility increases. This is natural as increasing mobility will cause more packet loss.

**Figure 2: Delivery Fraction**

Figure 2 shows the comparison of packet delivery ratio. No doubt that under an environment without any attackers, the original AODV protocol indicates the best performance possible on this metric. ANODR-DU-KPS has the similar performance with the original AODV, as it only uses efficient symmetric cryptography when exchanging routing packets, effectively accelerating the route discovery process and making the established routes more durable. The other three protocols result in significant degradation in delivery ratio, primarily caused by the longer delay required for asymmetric key encryption/decryption. In a mobile environment, excessive delay in route discovery process makes it harder to establish and maintain routes. SDAR has the worst performance, because SDAR requires public key encryption/decryption to forward both route request messages and route reply messages, while the other two protocols only run public key encryption/decryption when forwarding route reply messages.

**Figure 3: Data Packet Latency (ms)**

Figure 3 illustrates the data packet latency. Again, as SDAR uses public key cryptography throughout the round trip of route discovery, a node needs to wait longer time before a route is established. ANODR and ASR have similar average data packet latency and both of them only use public key encryption/decryption when forwarding route reply messages. ANODR-DU-KPS has nearly the same data packet delay with the original AODV, thanks to the efficient symmetric encryption algorithms and hash functions used. When there is little mobility, all protocols display small data packet latency, because once a route is established, a stable network allows a longer average route lifetime. When mobility increases, data packet latency increases accordingly. It generally stops increasing at some point and starts to decrease because beyond the summit, more and more data packets are lost due to mobility, thus only the routes with relatively small hop counts can survive and be used to transmit data packets efficiently.

**Figure 4: Average Route Acquisition Delay (ms)**

Figure 4 shows the average route acquisition delay under different node mobility. The overall trend is similar with figure 3, with the exception that unlike data packet latency, when mobility is small, the route acquisition delay is at a very high level. This can be explained by the fact that when nodes are
moving, it’s easier for them to encounter other nodes either closer to the destination or moving in the direction of the destination.

Figure 5: Normalized Control Packets

Figure 5 compares the number of normalized control packets over all of the protocols. All of the anonymous ad-hoc protocols have similar normalized control packets. They are all significantly higher than that of the original AODV, as the added cryptographic delay results in more route error messages and route repairs. Also, as the mobility increases, more route error will be generated.

Figure 6: Normalized Control Bytes

Figure 6 compares the normalized control overhead in terms of bytes. The trend of the curves is about the same with figure 5, however it’s clear that ANODR-DU-KPS incurs much more overhead. This is expected because having a similar number of normalized control packets, the comparison of normalized control bytes will be determined by the control packet size. As we can see, the size of the control packets (RREQ and RREP, primarily) of ANODR-DU-KPS is about two times or more as that of ANODR, SDAR and ASR, three times or more as that of the original AODV.

Figure 7 reports the overhead of the proactive key establishment of SDAR. It shows the normalized number and bytes of neighbor authentication packets under different mobility condition. SDAR uses periodical hello messages containing public keys for community management. Thus the number of periodical control packets are not affected by mobility. However, since the number of packets delivered decreases as the mobility increases, the overhead packets increases gradually when mobility increases (the scale is given at the left side of Figure 7). Similar trend for overhead measured in bytes is observed (the scale is shown at the right side of Figure 7). On the other hand, the number of authentication packets are determined by the frequency of the Hello message. In this simulation we use the default AODV Hello frequency, i.e., one Hello message per second. Compared with the normalized routing overhead presented in Figures 5 and 6, the current periodic packet overhead close to the overhead generated by the route discovery and maintenance (Figure 5). Reduction of this neighbor authentication overhead could be achieved through possible adaption on Hello interval. However, SDAR has a lower lever of normalized authentication bytes than its routing control bytes (Figure 6). This is because that the size of Hello message is smaller than the sizes of RREQ and RREP packets in SDAR.

In summary, the simulation results explicitly demonstrate the existence of trade-offs between routing performance and security protection. Because the ad hoc route discovery (RREQ/RREP) procedure is time critical in a mobile network, excessive crypto-processing latency would result in stale routes and hence devastated routing performance. In order to design a practical anonymous ad hoc routing scheme, we must find the optimal balance point that can both avoid expensive cryptographic processing and provide needed security protection at the same time. Our results show that ANODR and ASR are suitable in mobile ad hoc networks with heterogeneous nodes (including low-end nodes) and medium mobility. SDAR is only suitable in mobile ad hoc networks with high-end nodes that can run public key cryptography efficiently. In addition, compared to ANODR’s anonymous virtual circuit design, SDAR’s onion-based data delivery design incurs significant routing overhead per data packet. The anonymous communication demand and the routing performance demand together call for the future work to study more anonymous ad hoc routing proposals in regard to their routing performance and security guarantee.
4 Related Work

Existing anonymity schemes for wireless networks fall into a spectrum of classes. In “last hop” wireless networks (including cellular networks and wireless LANs), the demand of user roaming requires more promising assurance on the privacy of mobile users. The network participants considered in related research are typically the mobile users, the home servers of the users, the foreign agent servers local to the users, and the eavesdroppers (could be other mobile users). In [44][2], mobile users are associated with dynamic aliases that appear unintelligible to anyone except the home server. Then the foreign agent server accepts the user’s connections upon the home server’s request. In [19], mobile users employ Chaum’s blind signature to establish authenticated but anonymous connections to the foreign agent server. Hu and Wang [20] propose to use anonymous rendezvous, an anonymous bulletin board, to let mobile nodes anonymously connect to their communicators. These efforts provide unlinkability protections between node identities and their credentials during anonymous transactions. This design goal is orthogonal to anonymous on-demand routing.

In wireless sensor networks, distributed sensor nodes monitor target events, function as information sources and send sensing reports to a number of sinks (command center) over multi-hop wireless paths. The sensor nodes and sinks are typically stationary in WSN. Deng et al. [14] propose to use multi-path routes and varying traffic rates to protect recipient anonymity for the network sinks. Ozturk et al. [35] prevent a mobile adversary (e.g., a poacher) from tracing a sensor report packet flow back to a mobile target’s location (e.g., a panda). The sensor nodes must report the mobile target’s status to the sinks via phantom flooding, which is a sequential combination of random walk and controlled flooding. Both proposals seek to prevent the adversary from tracing network packet flows back to the sources or the sinks. In these proposals, routers (i.e., forwarding nodes) are stationary. They are not applicable to a network where every router is mobile.

In geographic services, both Location-Base Services [18] and Mix Zones [5] study how to use middleware service to ensure location privacy with respect to time accuracy and position accuracy. They study user anonymity protection in static “geographic regions” with boundary lines. The regions are fixed during the network lifetime, and anonymity protection degrades in a single region. Besides, since the anonymity protection stops at the middleware layer (typically above the network IP layer), the adversary can trace a mobile node using network identities/addresses at the network layer and the link layer, or radio signatures at the physical layer. These middleware services protect upper layer user identities that are different from routing identities.

5 Conclusion

In this paper we have illustrated the connections amongst the two recently-proposed on-demand anonymous routing schemes, namely ANODR (and its variant ASR) and SDAR. We analyze various factors that affect their routing performance and security. We further demonstrate that tradeoffs exist between the performance and the degree of protection. Our simulation study verifies that various choices in anonymous routing design have significant impact on anonymous routing protocol performance. Our results show that ANODR and ASR are suitable in mobile ad hoc networks with heterogeneous nodes (including low-end nodes) and medium mobility. SDAR is only suitable in mobile ad hoc networks with high-end nodes that can run public key cryptography efficiently. We conclude that more extensive performance study is needed to evaluate the practicality of the proposed anonymous proposals, the enhancements of them, and the new anonymous routing schemes.

References


