Performance Evaluation of Anonymous Routing Protocols in MANETs

Jun Liu*, Jiejun Kong†, Xiaoyan Hong*, Mario Gerla†
*Department of Computer Science
University of Alabama
Tuscaloosa, AL 35487
{jliu,hxy}@cs.ua.edu
†Department of Computer Science
University of California
Los Angeles, CA 90095
{jkong,gerla}@cs.ucla.edu

***Abstract*—**
Mobile ad hoc networks require anonymous communications in order to thwart new wireless passive attacks; and to protect new assets of information such as nodes' locations, motion patterns, network topology and traffic patterns in addition to conventional identity and message privacy. In particular, in wireless ad hoc networks mobile nodes must rely on ad hoc routing to keep network functional for communication. The transmitted routing messages and cached active routing entries leave plenty of opportunities for eavesdroppers. To address the new challenges, several anonymous routing schemes have been proposed recently. However, in various network scenarios, how the different cryptographic operations impact the routing performance remains unclear. In this paper we investigate the impact from cryptographic operations needed for the anonymous features. The overhead considered includes both increased control packet size and prolonged processing delay. The protocols taken into account include ANODR, AnonDSR, ASR, MASK, and SDAR. We present results based on extensive simulation study. We use the standard/unprotected on-demand scheme AODV in the comparison to show how much cost is paid by each anonymous on-demand scheme. Our simulation study shows that various design choices in anonymous routing indeed trade performance with anonymity protection. We conclude that extensive performance study is needed to evaluate the practicality of any enhancement of these proposed schemes and any new anonymous routing schemes.

I. Introduction

Mobile ad hoc networks (MANETs) are envisioned to support many time-critical and mission-critical applications due to the ability in establishing communication structure instantly without the need for an infrastructure network. Nevertheless, the intrinsic characteristics of ad hoc networks, such as wireless transmission and node mobility, make it very vulnerable to security threats. Many security protocol suites have been proposed to protect wireless communications, but they do not consider anonymity protection and leave identity information freely available to nearby *passive* eavesdroppers. The goals of passive attacks are to gather network information, such as node identities, node locations, network topology, and traffic flows, etc., as much as possible, until it traces, locates, and then physically destroys legitimate assets. The passive enemy will avoid aggressive actions as performed in routing security attacks, such as route disruption or "denial-of-service" attacks, in order to keep themselves to be as "invisible" as possible. Under such an attack model, anonymity and location privacy guarantees for the deployed ad hoc networks are critical, otherwise the entire mission may be compromised. This poses challenging constraints on MANET routing and data forwarding.

Many anonymous routing schemes have been proposed for MANET recently. Most of them use the on-demand routing approach following the MANET on-demand routing paradigm. The operations of an on-demand protocol are triggered by the communication demand at sources. Typically, an on demand routing protocol has two components: *route discovery* and *route maintenance*. In route discovery phase, the source seeks to establish a route towards the destination by flooding a route request (RREQ) message, then waits for the route reply (RREP) which reverses the receiving RREQ path and sets up the route. 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 active routing entries, if revealed to the adversary, will leak large amount of private information about the network. The proposed anonymous on-demand routing protocols use various cryptographic operations to anonymize both the transmission events and stored data. However, for battery and CPU power limited mobile devices, how the incurred cryptographic operation overhead affects the performance in general is an important issue that needs to be studied to gain a better understanding on the protocol design and applicability.

Generally, cryptographic operation affects the performance of an on-demand routing protocol in two ways: one is the routing control packet size and the other is the computational latency. Typically, routing packet RREQs and RREPs now contain additional fields for keys, nonces or other cryptographic structures (see Section II); sending and receiving those packets incur encryption, decryption or hashing operations. For handhold device, the computation time could be none trivial. In this paper, we carry out a systematic performance study of several recently-proposed anonymous routing protocols, namely ANODR [10][9], AnonDSR [16], ASR [19], MASK [18], and SDAR [3]. For every protocol we study its design framework , and analyze its computational and communication overhead. We also compare the advantage and disadvantage of these protocols. While the overhead can be studied analytically, this paper takes the simulation approach, which allows us to tune many network conditions for a variety of network scenarios, hence provides us a rich set of results. In the evaluation, especial attempts to reach a balance between the assumptions

The work was supported in part by the ONR MINUTEMAN project under contract N00014-01-C-0016, and in part by University of Alabama RAC 2005 award.

1-4244-0270-0/06/$20.00 (c)2006 IEEE

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2006 proceedings.

and overhead are made for fairness.

The rest of the paper is organized as follows. In Section II we briefly summarize protocols ANODR, AnonDSR, ASR, MASK, and SDAR. In Section III we describe the methodology and simulation models we use for the evaluations. In Section IV we report results for different sets of network scenarios. Finally Section V summarizes the paper.

II. Anonymous routing revisited

In this section we briefly revisit several on-demand anonymous routing schemes recently proposed for MANETs. We show the major features of each scheme and how the design choices affect routing protocol performance.

A. ANODR and ASR

ANODR [10][9] and ASR [19] are on-demand anonymous routing protocols. They have some common features and mechanisms. In general, they both use *anonymous virtual circuit* in routing and data forwarding. Each ANODR and ASR node does *not* know its immediate upstream node and immediate downstream node. Instead, the node only knows the physical presence of neighboring ad hoc nodes. This is achieved by a special anonymous signaling procedure. The per-hop pairwise session key of the route is determined when a node forwards RREP to its upstream node.

Route discovery The source node initiates the anonymous signaling procedure. It creates an anonymous *global trapdoor*. For ANODR, an *onion* [4][14] is included in an one-time route request (RREQ) flood packet. For ASR, a long random number generated by the source is used as a hop counter during RREQ to record the number of hops RREQ travels from the source.

1) *Anonymous global trapdoor*: The global trapdoor is a (semantically secure [6]) encryption of a well-known tag message that can only be decrypted by the destination. The design of global trapdoor requires anonymous end-to-end key agreement between the source and the destination.
2) *Onion*: For ANODR, 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 anonymous virtual circuit is established during the RREP phase.

At RREQ phase, an RREQ upstream node (which is later the RREP downstream) puts a one-time temporary public key or key negotiation material (if Key Pre-distribution Schemes (KPS) are used [11], see also Section III) in the RREQ packet. The RREQ downstream node records this one-time public key or key negotiation material for the source/destination session and overrides the field with its own temporary public key.

At RREP phase, the RREP upstream node (earlier the RREQ downstream) uses the stored one-time public key or the negotiated secret key to encrypt the contents of RREP packet with a pairwise per hop session key included. If key negotiation is required, the RREP upstream node will include the key negotiation material in the RREP packet. An en route one-hop RREP receiver will be able to decrypt the encrypted contents and identify a unique route discovery session and get the per hop session key. A random number is selected at each intermediate node to be sent to the next hop toward the source. Each node records the incoming random number together with the outgoing random number and insert the nonce pair to the route table.The anonymous virtual circuit is established when the source node receives the RREP with route discovery session information confirmed.

B. SDAR and AnonDSR

SDAR [3] and AnonDSR [16] are anonymous routing protocols with a combination of proactive MIX-net [4][13][8][2] and on-demand route discovery.

Trust Management SDAR node uses a *proactive* and *explicit* neighbor detection protocol to constantly see the snapshot of its one-hop mobile neighborhood. It periodically sends out a HELLO message holding the certified public key of the node, and at the same time collects other nodes' public keys. By observing behaviour of one-hop neighboring nodes or using other approaches, a node classifies its one-hop neighbors into different trust levels. Keys corresponding to these levels are negotiated among same-level nodes. They are later used to enforce trust-based secure communication. For AnonDSR protocol, a security parameter establishment (SPE) protocol is used before the anonymous routing. SPE establishes a shared key (and key index) between the source and the destination, which then, is used to set up a trapdoor between the two nodes.

Route discovery SDAR and AnonDSR employ *on-demand* route discovery procedures to establish ad hoc routes. Similar to ANODR and ASR, a 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 ID-free global trapdoor, SDAR uses the destination D's ID in the global trapdoor. AnonDSR also uses global trapdoor. However, as it assumes the source node shares secret key with the destination, the trapdoor is encrypted by using symmetric cryptography. Like SDAR, AnonDSR also uses destination's clear ID in the trapdoor.

SDAR's RREQ flooding phase does not form any onion. Instead, 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 global trapdoor. Each RREQ forwarder records TPK, chooses a random symmetric key K, and uses TPK to encrypt this per-stop K. This encrypted block is appended to the current RREQ packet. Finally the destination D opens the global trapdoor and knows TSK, then uses TSK to decrypt every TPK-encrypted block and thus shares a symmetric key with every forwarder of the received RREQ packet. This process is just like transferring a locked $SuggestionBox$. Both source and destination can open the box. While the intermediate nodes can inject information into this suggestion box, they can't open it. After the destination opens the $SuggestionBox$ it gets all information added by intermediate nodes.

AnonDSR uses onion in RREQ. However, unlike the onion used by ANODR, it consists of two parts. The first part is

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2006 proceedings.

the secret key selected at each hop encrypted by the one-time public key handed from the source node, and the other part is the onion received from RREQ upstream node with a nonce encrypted all together using that secret key.

Similar to MIX-net , for both of SDAR and AnonDSR, the destination D has the l (symmetric) keys to form an RREP packet in the form of MIX-net onion, where l is the number of hops from the source to the destination. The destination D puts all symmetric key Ks' 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.

In contrast with other protocols, for SDAR and AnonDSR, the overhead of public key coding the desination node has to perform is proportional to the hop count en route from the source to the destination. This is because at each hop, public key encryption is used for packing pairwise session key. Furthermore, decoding using public key is expensive. It's obvious that when the number of hops is large for a source-destination pair, it takes huge overhead for the destination to extract intermediate nodes' session keys.

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 payload to each other.

C. MASK

MASK [18] relies on a *proactive* neighbor detection protocol to constantly see the snapshot of its one-hop mobile neighborhood. The proactive neighbor detection protocol is ID-free. Each MASK node only knows the physical presence of neighboring ad hoc nodes. This is achieved by a pairing-based anonymous handshake [1] between any pair of neighboring nodes. MASK uses three-stage handshake for key exchanges among a node and its new neighboring nodes. After the handshake, each pair of nodes shares a chain of secret key and locally unique LinkID pair which corresponds to the Pseudonyms used during handshake. In general, every MASK node periodically sends out a HELLO message holding the pairing cryptographic materials. The MASK HELLO messages are not necessarily being too long, since it could only consist a 8-byte pseudonym and a 4-byte nonce.

Route discovery Like ANODR, MASK employs an on-demand signaling procedure to establish virtual circuit for later data delivery. The source node S assembles an RREQ flood packet which is similar to AODV in format. Unlike ANODR and SDAR, MASK does *not* use global trapdoor. In the MASK's RREQ packet S *explicitly* puts in the destination node D's network ID. This saves the processing overhead to open the global trapdoor, thus spares the need of end-to-end key agreement and results in a more efficient RREQ procedure. However, the security tradeoff is that recipient anonymity is compromised by every RREQ receiver [12].

Besides the removal of global trapdoor, MASK is more efficient because the proactive neighbor detection protocol has already established every anonymous link needed by the virtual circuit. During RREQ phase, every RREQ forwarder remembers which outgoing Pseudonym is used to forward the RREQ packet from an incoming LinkID. During RREP phase, a node looks up its Pseudonym corresponding to the incoming LinkID included in RREP packet, finds out the incoming LinkID received during RREQ corresponding to that Pseudonym, and insert this two LinkID pair into its route table. When the source receives RREP, the anonymous virtual circuit is established.

III. Evaluation Methodology

In this section, we use simulation to evaluate and compare the aforementioned anonymous ad-hoc routing protocols. Our evaluation concerns the influence from both the processing time needed to perform the crypto operations and the increased sizes of routing control packets on network performance.

A. Implementation details

The implementation of ANODR, ASR, MASK and SDAR are based on AODV, and AnonDSR on DSR. Route optimizations used by the original AODV and DSR do not apply in anonymous routing, so they are not enabled in the implementations. In addition, we have made a few more justifications in order to make the results comparable and fair among all the protocols.

First of all, in our implementation and evaluation, assumptions made by each protocol are preserved. Overhead incurred in pre-configure phase or bootstrap phase is not counted in the evaluation. Secondly, for ANODR, an improved version [11] using Key Pre-distribution Schemes (KPS) (in RREP unicasts) is also implemented and evaluated in our simulation study. It is denoted as ANODR-KPS and uses the probabilistic KPS scheme proposed by Du et al. [5]. Thirdly, for AnonDSR protocol, the security parameter establishment (SPE) protocol is considered as a precondition, the overhead is not calculated. This is equivalent to assumptions made by other protocols on pre-existing source-destination security agreements (ANODR, ASR, and SDAR) or leave the destination as plain text (MASK). Further, periodical broadcast among neighbors in protocols MASK and SDAR are modified from HELLO messages in AODV. For MASK, besides periodical HELLO (first stage in its three-stage neighborhood key exchanges), two more broadcast packets are added to complete the rest two stages of the handshake among a newcomer and its neighbors. Taking into consideration that one can use adaptive frequencies to reduce the overhead from the periodical updates, and to improve performance (compared to the results generated from our implementations), in our evaluation, we separate the evaluation of the periodic overhead from the evaluation on the main on-demand route discovery principles.

Moreover, assumptions implied by crypto-systems in use are also preserved, e.g., using 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; using a KPS scheme, the network needs an offline authority to load every node with personal key materials. In ANODR-KPS, the probability of achieving a successful key agreement at each hop is 98%. In other words,

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2006 proceedings.

per hop key agreement fails with 2% at every RREP hop. A new route discovery procedure will be invoked eventually by the source. Finally, in our implementation, cryptographical operations over data packet transmission is not calculated since all the protocols use symmetric key systems.

B. Crypto-processing performance measurement

The processing overhead used in our simulation is based on actual measurement on a low-end device. Table I shows the measurements performed by Gupta et al. [7] on the performance of different cryptosystems. For public key cryptosystems, the table shows processing latency per operation. For symmetric key cryptosystems, it shows encryption/decryption bit-rate.

TABLE I

PROCESSING OVERHEAD OF VARIOUS CRYPTOSYSTEMS (ON INTEL STRONGARM 200MHZ CPU BASED POCKET PC RUNNING LINUX)

Cryptosystem	decryption	encryption
ECC (163-bit key)	24.5ms	46.5ms
RSA (1024-bit key)	188.7ms	10.8ms
AES/Rijndael (128-bit key & block)	29.2Mbps	29.1Mbps

Clearly, different cryptosystems introduce different processing and link overhead, thus have different impact on anonymous routing performance. Taking consideration of the cryptosystems proposed by original authors, we practically choose the cryptosystem in favor of performance. For public key cryptographic operations in the simulation, AnonDSR uses RSA and rest of the protocols use ECIES with 163-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 $24.5 + 46.5 = 71$ms for RREP packets. In general, longer delay is required for asymmetric key encryption/decryption compared with the symmetric cryptography. The KPS based ANODR trades link overhead for processing time, i.e., ANODR-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 processing packets.

C. Evaluation Metrics

We evaluate the performance of these protocols in terms of the overall network performance (delivery matric) and the influence from processing delay (delay metric) and packet size (overhead metric). We use the following metrics: *packet delivery fraction*, *average end-to-end data packet delay*, and *normalized routing load* in *bytes* of total control packets per data packet delivered.

D. Simulation model

The simulation is performed in QualNet^{TM} [15], 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. The radio uses the *two-ray ground reflection* propagation model. The channel capacity is 2Mbps. The network field is 2400m×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 [17]). CBR sessions are used to generate network data traffic. For each session, data packets of 512 bytes are generated in a rate of 4 packets per second. The source-destination pairs are chosen randomly from all the nodes. During the simulation time, a constant, continuously renewed load of short-lived pairs is maintained.

To focus on influence from anonymous design and cryptographic operation, we do not introduce attacks in the simulation. We present two sets of simulations. One set is to show routing performance variation under different mobility conditions, where mobility is increased from 0 to 10 m/sec in different runs. The pause time is fixed to 30 seconds. 5 CBR pairs is constantly maintained. In the other series of simulation, showing the impact of performance due to different traffic load, we fix the mobility at 2 m/sec and vary the number of concurrent short-lived CBR communication from 5 to 25. Each of these series of simulation are conducted in identical network scenarios (mobility, communication traffic and node density) and routing configurations across all schemes (except the one to be varied) in comparison.

IV. PERFORMANCE RESULTS

In this section, we give simulation results for different network scenarios, namely, increasing mobility and increasing traffic load.

A. Impact from mobility

Figure 1 shows the comparison of packet delivery ratio. The original AODV protocol indicates the best performance possible on this metric as expected since the environment has no attackers. MASK and ANODR-KPS have similar performance with the original AODV, as they both use efficient symmetric cryptography only when exchanging routing packets, effectively accelerating the route discovery process and making the established routes more durable. ANODR and ASR experience moderate delivery ratio degression. Both of them use public key cryptography in RREP. The AnonDSR and SDAR show significant degradation delivery ratio. The reasons are that the two protocols need hop-related public key encryption/decryption at the destination nodes. In a mobile environment, excessive delay in route discovery process makes it harder to establish and maintain routes. All the curves show a more or less yet steady descendant when mobility increases. This is natural as increasing mobility will cause more packet losses.

Figure 2 illustrates the data packet latency. Because of the public key cryptographical overhead, SDAR and AnonDSR show significant longer end-to-end latency. ANODR and ASR have similar average data packet latency. ANODR-KPS and MASK have the lowest and nearly the same data packet delay with original AODV, thanks to the efficient symmetric encryption algorithms and hash functions used. When there is

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2006 proceedings.

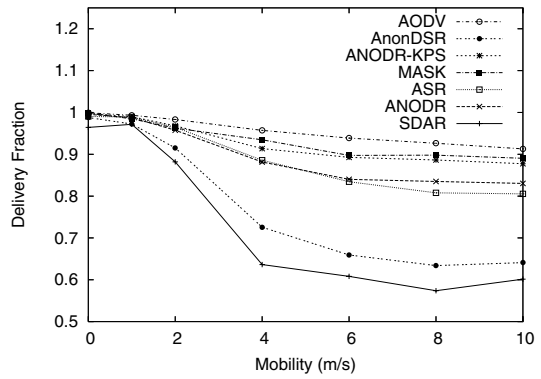

Fig. 1. Delivery Fraction

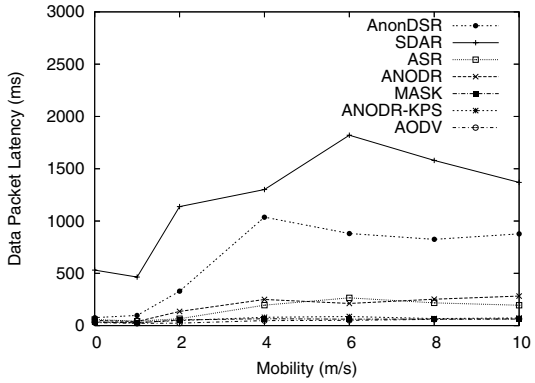

Fig. 2. Data Packet Latency (ms)

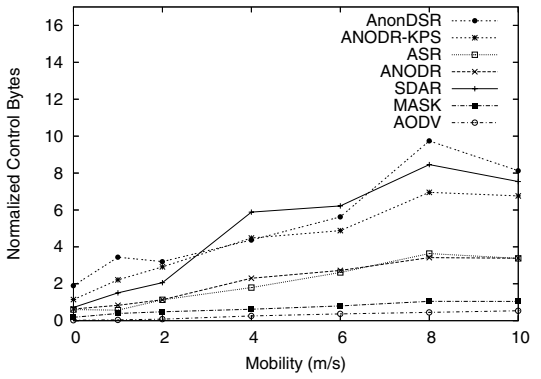

Fig. 3. Normalized Control Bytes

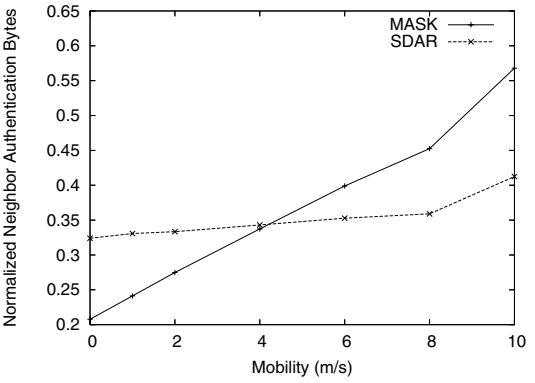

Fig. 4. Normalized Neighbor Authentication Bytes

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.

Figure 3 compares the normalized control overhead in terms of bytes. ANODR-KPS, AnonDSR and SDAR generate the most normalized control bytes, ASR and ANODR less. The result is expected because SDAR and AnonDSR both have large RREQ and RREP packet sizes for carrying keys. ANODR-KPS also includes key negotiation material in RREQ and RREP messages, making them significantly larger than original ANODR control packets. In addition, AnonDSR and SDAR are low in the number of successfully delivered packets. Finally, MASK has closer values with AODV, because in route discovery MASK relies on existing pairwise keys. The background key exchange overhead is not counted here (Figure 4).

Figure 4 reports the overhead of the proactive key establishment of MASK and SDAR. It shows the normalized *bytes* of neighbor authentication packets under different mobility condition. SDAR uses periodical hello messages containing public keys for community management, which is not affected by mobility. But as the number of packets delivered decreases as mobility increases, Figure 4 shows an increasing trend of SDAR when mobility increases. MASK's three-stage handshake is triggered by new neighbors, thus is more affected by mobility. This behavior results in higher packet overhead of MASK compared to SDAR, and faster increasing trend when mobility increases as more handshakes are needed. Other results from our simulation (not included in the paper) show that the number of packets increases. And especially, when the network is static, MASK and SDAR have almost the same number of the control packets. The figure also shows an interesting crossing phenomenon. This is because that the size of SDAR's HELLO message, which carries a public key, is much larger than that of MASK who typically only needs to carry an 8 byte pseudonym. Thus, when mobility is low, SDAR incurs more normalized neighbor authentication bytes. As the mobility increases, a node tends to encounter more other nodes, and handshake with more newly met neighbors. Thus at one point, the normalized neighbor authentication bytes of MASK will exceed that of SDAR, as the overhead of MASK increases much faster.

B. Impact from traffic load

The network traffic load is increased by increasing the number of communication pairs. Figure 5 compares the delivery ratio performance under different traffic load. It displays an unanimous degradation trend of delivery fraction for all protocols. This is typically because of the increasing congestions and communication collisions when traffic load increases.

Figure 6 shows the impact of traffic load on end-to-end data packet latency. No surprise, the data latency is extended as the traffic load increases. This is caused by longer queueing delay in contenting the wireless medium, and more needs for route re-discovery. Protocols with longer computation delay always suffer more under heavy traffic load.

Figure 7 shows the normalized control overhead in terms of bytes. More control overhead are generated when traffic becomes heavier. Again the performance deteriorates in a

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2006 proceedings.

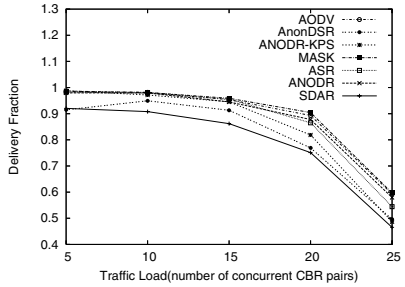

Fig. 5. Delivery Fraction

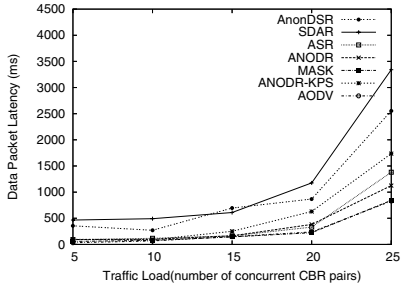

Fig. 6. Data Packet Latency (ms)

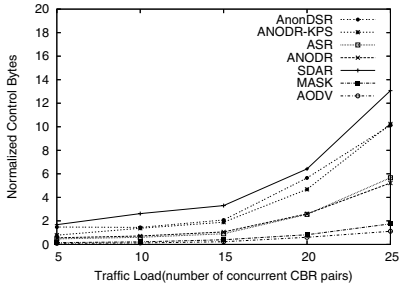

Fig. 7. Normalized Control Bytes

regular fashion according to the computational overhead each protocol requires respectively.

C. Performance summary

After all, our main findings are: (i) Control packet size, if controlled within a reasonable size, has less impact on performance. E.g., Figure 1 and Figure 5 show almost the same delivery ratio of MASK and ANODR-KPS. But ANODR-KPS has much higher control bytes as shown in Figure 3 and Figure 7. (ii) Processing delay has great impact on delivery ratio in a mobile environment. E.g., ANODR-KPS and SDAR have similar combined packet size, while as Figure 1 and Figure 5 show, their delivery ratios have large difference.

On the other hand, the simulation results 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. Our results show while ANODR and ASR could be suitable for low-end nodes and medium mobility, AnonDSR and SDAR are better be used by high-end nodes that can run public key cryptography efficiently. In order to design a practical anonymous ad hoc routing scheme, we must find out the optimal balance point that can both avoid expensive cryptographic processing and provide needed security protection at the same time.

V. Conclusion

In this paper we have presented a comprehensive survey and performance evaluation of the five recently-proposed on-demand anonymous routing schemes, namely ANODR, AnonDSR, ASR, MASK, 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. The simulation results show that control packet size has less impact on performance, while processing delay has great impact on delivery ratio in a mobile environment. The results also suggest that public key cryptography based protocols are better be used at high-end nodes. We conclude that extensive performance study is needed to evaluate the practicality of these proposed schemes, any enhancement of them, and any new anonymous routing schemes. Our future work will further study the anonymous communication demand, scalability demand and the routing performance demand together.

References

[1] D. Balfanz, G. Durfee, N. Shankar, D. K. Smetters, J. Staddon, and H.-C. Wong. Secret Handshakes from Pairing-Based Key Agreements. In *IEEE Symposium on Security and Privacy*, pages 180–196, 2003.

[2] O. Berthold, H. Federrath, and S. Köpsell. Web MIXes: A system for anonymous and unobservable Internet access. In H. Federrath, editor, *DIAU'00, Lecture Notes in Computer Science 2009*, pages 115–129, 2000.

[3] 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.

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

[5] 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.

[6] S. Goldwasser and S. Micali. Probabilistic Encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[7] V. Gupta, S. Gupta, S. Chang, and D. Stebila. Performance Analysis of Elliptic Curve Cryptography for (SSL). In *Proc. ACM Workshop on Wireless Security 2002*, September 2002.

[8] D. Kesdogan, J. Egner, and R. Buschkes. Stop-and-go MIXes Providing Probabilistic Security in an Open System. *Second International Workshop on Information Hiding (IH'98), Lecture Notes in Computer Science 1525*, pages 83–98, 1998.

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

[10] 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.

[11] J. Kong, X. Hong, M. Sanadidi, and M. Gerla. Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing. In *The Tenth IEEE Symposium on Computers and Communications (ISCC)*, 2005.

[12] A. Pfitzmann 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.

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

[14] 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.

[15] Scalable Network Technologies (SNT). QualNet. `http://www.qualnet.com/`.

[16] R. Song, L. Korba, and G. Yee. AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks. In *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2005.

[17] J. Yoon, M. Liu, and B. Noble. Sound Mobility Models. In *ACM MOBICOM*, pages 205–216, 2003.

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

[19] 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.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2006 proceedings.