Achieving Anonymity in Mobile Ad Hoc Networks Using Fuzzy Position Information *

Xiaoxin Wu[1], Jun Liu[2], Xiaoyan Hong[2], and Elisa Bertino[3]

[1] Intel Communication Technology Beijing Lab, Beijing, 100080, P. R. China,
[2] Dept. of Computer Science,University of Alabama, Tuscaloosa, AL 35487, USA,
[3] Dept. of Computer Science, Purdue University, West Lafayette, IN 47907, USA

Abstract. Traditionally the anonymity of an entity of interest can be achieved by hiding it among a group of other entities with similar characteristics, i.e., an anonymity set. In mobile ad hoc networks, generating and maintaining such an anonymity set for any ad hoc node are challenging because of the node mobility and consequently of the dynamic network topology. In this paper, we address the problem of the destination anonymity. We propose protocols that use fuzzy destination position to generate a geographic area called *anonymity zone (AZ)*. A packet for a destination is delivered to all the nodes in the AZ, which, consequently, make up the anonymity set. The size of the anonymity set may decrease because nodes are mobile, yet the corresponding management on anonymity set is simple. We design techniques to further improve node anonymity. We use extensive simulation to study the node anonymity and routing performance, and to determine the parameters that most impact the anonymity level that can be achieved by our protocol.

1 Introduction

Privacy is a major concern for today's network users. An important privacy requirement is represented by anonymity, which is becoming increasingly important in a large variety of application domains. At the same time, mobile ad hoc networks are envisioned as an effective solution for extending the last-hop network communications to any party at any time and anywhere. Therefore, communication privacy, especially anonymity for communicating parties in ad hoc networks, is highly desired. In this work we investigate the application scenario where an ad hoc node receives sensitive data from well-known servers. This receiver may not wish its identity to be revealed to the network; we refer to this requirement as *destination anonymity.*

Traditional anonymous communication protocols may not be directly applied to mobile ad hoc networks. MIX [12] and Onion routing [13] require that security associations among entities be set up and stably maintained, which is

* Work from Xiaoxin Wu was performed at Purdue University with a support from Information Infrastructure Protection (I3P) Fellowship. *Part of the work was also supported by University of Alabama RAC 2005 award.

very difficult in MANET because of the lack of fixed infrastructure and of its dynamic nature. Approaches based on broadcast [2] or multicast [3] are not applicable because the network has limited bandwidth. In addition, multicast in MANETs is itself a challenging research issue. The obstacles against achieving communication-end privacy, especially destination anonymity, also depend on the fact that in on-demand routing protocols, such as AODV [4] and DSR [5], a global flooding is required in the route discovery stage. The destination identity is carried in the request, therefore, it has to be revealed to the entire network. All nodes in the network may thus become aware of the communications being established.

A widely investigated class of routing protocols for ad hoc networks is based on geographic (i.e., positioning) routing algorithms [6], where node positions are used for routing. A commonly proposed positioning routing algorithm is the Greedy Perimeter Stateless Routing (GPSR) [7]. GPSR has a better potential to achieve communication privacy because of its local and stateless route discovery protocol. More importantly, the routing information required by GPSR is the node position, not the node ID. Therefore, the real identity of a node, e.g., a destination, can be hidden. Node positions can also be used as pseudonyms for routing purposes, as in the private positioning routing algorithm AO2P[8]. However, position information is sensitive data in many applications. By probing, attackers can easily break the privacy of node locations. Thus, attackers could trace down to a destination according to its position and then identify the destination in a face-to-face manner.

The goal of our paper is to explore the advantages of geographic assisted routing while at the same time to address the privacy problem connected with the use of the aforementioned sensitive position data. We propose an anonymous geographic routing algorithm that uses fuzzy destination positions. The notion of fuzzy position has been used in privacy-preserving location-based services [9] [10]; under such an approach, a mobile user intentionally provides inaccurate positions for services to protect its real positions. Here, we use a fuzzy position to prevent adversaries from discovering the real position of a node and a destination ID based on its position. A pseudo destination that has a position near that of the real destination is generated, toward which packets are sent. The successful delivery in such a routing algorithm relies on the broadcast nature of wireless communication, where a transmission can always be received by all the nodes within the transmission range of the sender. Therefore, if the real destination is located in a geographic area that is not far away from the pseudo destination, it will receive the packets. Such a geographic area, that we refer to as an *anonymity zone (AZ)*, is the key concept in our design. The destination anonymity is determined by the number of nodes that are located in the AZ, and the protocol is thus called *zone-based anonymous positioning routing (ZAP) protocol.*

ZAP is based on the same principle of the Crowds protocol [1], under which a receiver hides among a group of entities, referred to as anonymity set. The difference, however, is that in ZAP, the size of such anonymity set, is affected by many network conditions and varies with time. For example, the number of nodes located in an AZ depends on the size of the AZ and the node distribution. In addition, once the AZ is built, the size of the group will decrease because of the node mobility. On the other hand, if one allows a fixed anonymity set, e.g., a group consisting of some fixed ad hoc nodes, reaching every node in the anonymity set requires MANET multicast, which may result in anonymity breaches.

In our approach, we tolerate some losses in privacy but provide simpler protocols and network management and increased efficiency. Challenges in ZAP design include how to deliver a data packet given only pseudo location information; how to increase the degree of anonymity protection, i.e., the size of the anonymity set, even though it is a probabilistic protocol; and what are the required security properties. The factors that most impact our solution, and thus must be taken into account in an analytical or simulation model of our approach, include node density, mobility and communication patterns.

2 Zone-Based Anonymous Positioning Routing Protocol

2.1 Assumptions

With respect to the network, we assume that nodes are uniformly distributed with a node density not too low. A node moves toward a random direction at a variable speed. The wireless channel is bi-directional. Each node knows its own position, e.g., through a GPS system. Nodes exchange their positions locally through "hello" messages.

With respect to privacy, we assume that each node has a public key that is known to all the other nodes. The public key is assigned by a certificate authority before a node joins the network. For data delivery, the identity of the destination is not revealed to the network. Each node has an equal probability to be a receiver (client).

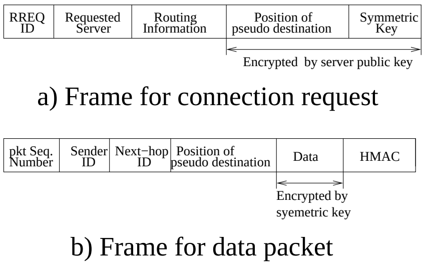
The attacker models that we consider in our work are as follows. There are internal attackers that trace or monitor the behavior of other nodes for malicious purposes. These attackers follow the protocols. They do not act aggressively (that is, do not interrupt the correct network functioning) to obtain additional information because they would like to stay in the network without being noticed. An attacker is able to eavesdrop the communication channel. It can collect position information of its neighbors by intercepting hello messages. An attacker or colluding attackers therefore can discover the *local* network topology. Finally, if a transmission lasts long enough, attackers can locate the transmitter, e.g., through directional antenna techniques, and identify it by moving to the transmitter.

2.2 ZAP with Pseudo Destination (PD-ZAP): A Basic Approach

ZAP preserves destination anonymity through anonymity zones, under which a destination is located with a number of other nodes. The protocol operates in the following steps.

A client (*destination*) sends a server (*source*) a connection request for data downloading. The request indicates parameters for setting up a private route, which includes the fuzzy position information (i.e., the pseudo destination) and, if necessary, the range of the anonymity zone. The connection request can be sent by traditional routing algorithms or flooding. To assure data confidentiality and integrity, the destination can generate a symmetric key and carry it in the connection request. Concerning the destination anonymity of this request message, our claim is that the probability of intercepting a sporadic request at its initiating location by an attacker is very small. In addition, the identity of the request originator is not carried in the message.

The message frames for connection requests and data packets can be structured as shown in Fig. 1. The routing information in a connection request is determined by the routing algorithm to be used for sending the request.


RREQ ID
Requested Server
Routing Information
Position of pseudo destination
Symmetric Key
Encrypted by server public key
pkt Seq. Number
Sender ID
Next−hop ID
Position of pseudo destination
Data
HMAC
Encrypted by syemetric key

a) Frame for connection request

b) Frame for data packet

Fig. 1. Data frame for the packet.

The source retrieves the AZ information after receiving the connection request. It then initiates the greedy geographic forwarding to deliver data packets. Any forwarder (including the source) forwards the data packet to a neighboring node that is closest to the pseudo destination, which also is the geographic center of the AZ. Once a data packet reaches the AZ, a node in the AZ that first receives the packet becomes a *proxy*. The proxy then uses different local packet distribution mechanisms to deliver the packet to the destination, according to the size of AZ. The source uses the symmetric key to encrypt data, and uses HMAC [11] for data integrity. As data packets are delivered toward the AZ, not the real destination, such an approach is called ZAP with pseudo destination, or PD-ZAP.

PD-ZAP is illustrated in Fig. 2. The position of the pseudo destination is randomly selected, and is not too far from that of the real destination. This position is also the routing information carried in each data packet. Therefore, the connection request does not have to carry the real identity of the destination, as it is not required for routing. This guarantees the destination anonymity even if the source is compromised.

In PD-ZAP, a packet will finally be received by a node that is closest to the pseudo destination [4]. This node then acts as a *proxy* and broadcasts the received packet to all of its neighbors. In this paper, a broadcast is defined as the process that a node transmits a message to all of its neighboring nodes that are within its radio coverage. In Fig. 2, the solid circular represents the transmission range of the proxy, which has a radius of r. r is the maximum ad hoc channel coverage. If the real destination is within the proxy's radio coverage, it will receive the

[4] It is not necessary that a node is located at that position.

data packet. If an ACK is required, the proxy sends its neighbor list back to the source. The neighbor list has been obtained by exchanging “hello” messages.

A new session has to be started if the destination can no longer receive data packets, typically when the destination has moved away from the AZ. In this case the destination has to send a new connection request along with the updated AZ information, based on which the source initiates another private route.

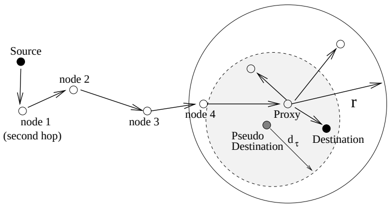


Fig. 2. The PD-ZAP approach.

The generation of the pseudo destination is the key part of the algorithm. The maximum distance (or the distance threshold value) between the pseudo destination and the real destination, denoted as d_τ, determines both the node anonymity and the success of a packet delivery. The distance cannot be too long, otherwise the real destination may not receive the data packet from the proxy. It cannot be too short either, because a short distance results in a small anonymity set. As shown in Fig. 2, the destination anonymity zone (D-AZ) in PD-ZAP is the shaded circular area that is centered at the pseudo destination and has a radius of d_τ. For the attackers, only a node located in that area can be the destination. The pseudo destination selection depends on node density and node mobility.

In PD-ZAP, the position of the pseudo destination is also used as the session ID, according to which a node receiving the packet from the proxy knows whether it is the destination. Only the destination will be able to decrypt the packet using the established symmetric key. The other nodes simply drop the packet. However, since upon different packet arrivals, the node that is closest to the pseudo destination may be different, proxies can be different for the same session.

2.3 Anonymity, Weaknesses, and Mitigation Techniques

In this subsection we discuss the protocol anonymity at high level. We determine possible privacy attacks, and propose mechanisms as counter measures.

Anonymity Our anonymity goal is to hide a destination among a number of ad hoc nodes. In ZAP, the destination anonymity depends on the size of the group formed by the nodes that are located in the D-AZ. The determining factors are node distribution, size of D-AZ, and node mobility.

Intercepting a connection request may not help attackers too much in identifying the destination. As the identity of the request originator is not carried in the message, upon intercepting a request, the attacker cannot even tell whether the node from which it intercepted the message is the originator or just a forwarder. Even if an attacker knows that such node is the originator, the transmission happens too soon so that it is difficult for the attacker to locate the originator and thereafter to identify it. For the same reason, when a destination sends an ACK back using an alternative private route and the ACK is intercepted by attackers, the identity of the destination will not be discovered.

Because a node has to locally disclose its position, an attacker can stay close to its target node and monitor its behavior. Under such a target-oriented attack, communication privacy cannot be preserved by just using ZAP protocol. To mitigate such an attack, background noise is needed. A node can occasionally send out dummy packets that have the same pattern as requests and ACKs. In this case, when a real request or ACK is sent, the attacker cannot be certain.

The goal of the destination anonymity achieved by PD-ZAP can be achieved using earlier work on untraceable and anonymous routing presented in ANODR [14]. The routing protocol ANODR serves as an untraceable and anonymous signaling procedure that establishes VCIs (Virtual Circuit Identifiers) for data communication. It uses an onion structure for route discovery where the destination identity is protected by using the *global trapdoor*. The construction and propagation of the *Trapdoor Boomerang Onions* in the route discovery ensures the identities of nodes and relationships between upstream and downstream nodes not being revealed. The route discovery also assigns pseudo-random numbers as temporary VCIs for links en route. Each node only knows the pseudo numbers about its previous hop and next hop. Using the VCIs and mixing techniques, ANODR can create one-time packet content at each forwarding hop to further defend against packet tracing. The destination receives data through the VCI of its upstream link. Thus in routing operation and in data forwarding, no identities and no linkage towards the destination are revealed.

In both PD-ZAP and ANODR, the real destination hides within the radio range of the last hop towards the destination. The two protocols also share a similar way of establishing a credential between the source and the destination. The global trap door used by ANODR can be implemented the same way as in PD-ZAP given the available public keys. The difference relies on the location information. Geographic position (could be pseudo) allows a destination node (client) in PD-ZAP to send an initial request to the source (server) directly through geo-forwarding, and in return, allows the server to geo-forwarding data packets to the destination. While in ANODR, without location information, a destination has to flood its initial request and then use the signaling route discovery to establish a route. In addition, the ZAP protocols can be used in applications that favor geographic information assisted routing. However using geo-forwarding, an internal passive attacker can learn the approximate area of the destination from any hop. When that happens, destination anonymity relies on the protection within the zone. In order to increase the anonymity zone and to defend attacks against destination anonymity, we present a ZAP variant (RR-ZAP, in Section 2.4) that expands the anonymity zone towards an area other than the receiving range of the last hop.

Intersection Attack: The Impact of Node Mobility on Anonymity Node mobility has important impact on the anonymity. To analyze such impact, the notion of *intersection attack* has to be introduced.

An intersection attack occurs when an attacker knows its Entity of Interest (EOI) is in more than one anonymity set. In this case, it concludes that the

EOI must be in the intersected set among all these anonymity sets. As the intersected set is smaller than any of the original set, the anonymity level for the EOI decreases.

Node mobility helps attackers to conduct intersection attacks and therefore to degrade node anonymity. This is especially the case when the communication between the source and the destination lasts for a long time. Fig. 3 shows an example. Suppose that two packets arrive at the D-AZ at times t_1 and t_2, respectively. At time t_1, a set_1 of nodes is located in the D-AZ and at time t_2, a set_2 of nodes is located in the D-AZ. The sets set_1 and set_2 are not equal because some nodes may have moved out or into the D-AZ between the two transmissions. To an attacker, the anonymity set for the destination includes only the nodes that are in the D-AZ at both t_1 and t_2, that is, the intersection of the anonymity sets at the times t_1 and t_2. In this example, it is easy for the attacker to infer that the destination node is either e or f. The size of the anonymity set is reduced to 2, instead of 6 for set_1 or 5 for set_2.

If a session lasts long, the number of nodes remaining in the anonymity zone can be small. The destination anonymity thus can be very low. Note that the nodes that are originally out of an AZ move in the AZ during the communication do not contribute to anonymity, because the attacker knows these nodes cannot be the destination anyway.

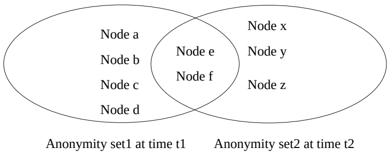


Fig. 3. Example of intersection attack.

Mitigating Techniques against Intersection Attack Different approaches can be adopted to mitigate the impact of node mobility and to reduce the anonymity degradation. One approach is to divide a long-duration session into a number of short subsessions that use different D-AZs. For each subsession, a D-AZ and the corresponding symmetric key are generated. As a subsession does not last a long time, the destination anonymity may only decrease moderately because of mobility. The challenge is how to make these subsessions un-linkable. A straightforward solution is to increase the inter-subsession duration, which improves anonymity at the cost of the communication delay.

Tradeoff between Privacy and Network Performance ZAP achieves privacy at the cost of network performance. The inaccurate routing information in PD-ZAP results in a decreased data delivery ratio in MANETs. In approaches that mitigate intersection attacks resulting from node mobility, additional signaling and increased redundant transmissions are required. In general, a better performance implies a sustained communication duration that is long enough to complete a session. A longer communication, on the other hand, may decrease node anonymity because it gives a tracer more opportunities to conduct an intersection attack. In a later section, we present an analysis on the flooding overhead with respect to the initial D-AZ size. An extensive analysis on the mutual impact between network performance and privacy will be carried out as part of our future work.

2.4 ZAP with Route Redundancy: Advanced Approach

As PD-ZAP has a relatively small anonymity set, we propose to use a route with redundant hops to increase the D-AZ; we call such an approach ZAP with route redundancy (RR-ZAP) (refer to Fig. 4.). RR-ZAP can be used in a network where the position of servers (that is, sources) are well known. Like PD-ZAP, in RR-ZAP, a client (destination) creates a pseudo destination, denoted by P in the figure, for building a private route. Unlike PD-ZAP, in RR-ZAP, P is not close to the real destination, but can be a few hops away. P is selected so that the real destination is close to the direct connection between the source and the pseudo destination, which is line SP in the figure. If the network nodal density is not too low, the routing path may not deviate too far away from SP. The real destination then is close to the path, and can *intercept* the data delivered to the pseudo destination. In Fig. 4, the real destination can receive the packet, probably, from node 3.

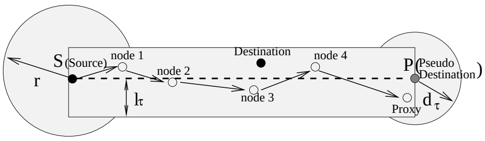


Fig. 4. The RR-ZAP approach.

The distance between the real destination and SP should not be higher than a threshold value l_τ. l_τ determines the anonymity set and successful delivery ratio. It depends on node density and distribution. To an attacker, as the destination can be any node that is no more than l_τ away from the SP, the anonymity zone for the destination then includes the shaded rectangular area in the figure. Other than that, the real destination can also be located at the circular shaded areas at the two ends of the path, which are respectively the coverage of the source and the anonymity zone for PD-ZAP.

When an immediate acknowledgment from the real destination to the source is required, all the nodes in the path will collect ACKs from their neighbors and send back the lists to the source. The source then knows whether the real destination has received the packet.

3 Simulation Study

We further evaluate the destination anonymity and the network performance of the proposed protocols through simulation. The evaluation metrics include: *(i) the size of the anonymity set*: the number of nodes that remain in the anonymous zone when a session ends compared to those at the beginning of the session; *(ii) packet delivery ratio*: the ratio between the number of data packets received and those originated by the sources; *(iii) normalized packet forwarding overhead*: the number of packets transmitted by ZAPs normalized to those transmitted by GPSR under the same condition. *(vi) average end-to-end packet latency*: the average time from when the source generates the data packet to when the destination receives it.

We evaluate protocols PD-ZAP and RR-ZAP. For RR-ZAP, the simulation area limits the number of hops we can choose for redundancy. Thus in our implementation, a pseudo destination is positioned at the intersection of the boundary and it is chosen to ensure that l_τ equals to the half of the transmission range. We present GPSR for reference when appropriate.

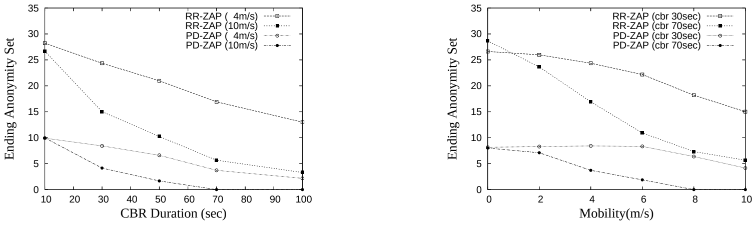
We use QualNet [15], a detailed packet-level network simulator, in investigating the impact from the protocol specific parameters and varying network conditions on the aforementioned metrics. The simulated ad hoc network has 180 nodes initially uniformly distributed in a $2000m \times 2000m$ area. The nodes move according to Random Waypoint Model [5], with a pause time of zero and the minimum and the maximum speeds set to the same (note that this configuration avoids the problem pointed out in [16]). The average density is around 20 neighbors per node. Simulations use renewal CBR application so to constantly maintain five CBR sessions. Each source generates data packets of 256 bytes at a rate of 4 packets per second. The source-destination pairs are chosen randomly from all the nodes(but we exclude the pairs that are located close to the edge of the network to be destinations). The session duration is a variable. We use IEEE 802.11b DCF at MAC layer and two-ray ground propagation model at physical layer. Network devices have link bandwidth at 2Mbps and 370m power range. The results are averaged over several simulation runs with various random seeds.

3.1 Anonymity

The destination anonymity is measured by the size of the anonymity set ($Size_{AS}$) that consists of the nodes remained in the D-AZ through out the session. We investigate how it is affected by session time, mobility, and the sizes of the anonymous zone. The default AZ sizes are 250m.

Figure 5(a) reports the change of $Size_{AS}$ as a function of the session duration. The figure illustrates several interesting facts. First, when session duration increases, all curves show a decreasing trend in anonymity set. Second, when mobility is high, the anonymity set size decreases faster because more nodes move out of the initial anonymous zone during the session. Third, in general, the anonymity set of RR-ZAP is larger than that of PD-ZAP because the entire route becomes the anonymous region, which, in most cases is larger than a destination-based D-AZ.

Figure 5(b) shows the change of $Size_{AS}$ of ZAPs as a function of mobility for long and short sessions. The trends are similar to the previous figure. RR-ZAP has larger AS size. But the set size decreases when mobility increases, especially when sessions last longer the decreasing is quicker. This is because RR-ZAP's anonymous zone is generally long and narrow. It is more sensitive to mobility. Yet PD-ZAP can tolerate higher mobility when session is short (30sec). Up to mobility equals to 6m/s, the sizes of the AS are mostly not affected by mobility, due to the fact that few nodes can move out of the original AS region in a short



(a) AS vs. CBR Duration

(b) AS vs. Mobility

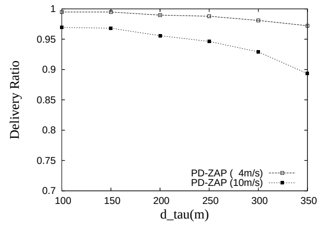
Fig. 5. Payoffs with perfect information

period of time. When session is long (70Sec), all the ZAPs start degradation at low mobility.

3.2 Routing Performance

We investigate how the packet delivery performance of the ZAP protocols are affected by session time, mobility, and the sizes of D-AZs. While we try to stress one condition, we keep other parameters moderate.

Figure 6 investigates how the zones affect PD-ZAP on the delivery ratio. Sessions are kept short in 30 seconds. It shows that PD-ZAP maintains high delivery ratio when mobility is low (4m/s) no matter how d_τ increases. This is because the distance a node can move in the short session time does not cause many nodes to move out of its D-AZ, which is a little smaller than a node's transmission range. But delivery ratio degrades quickly in high mobility (10m/s) as expected.

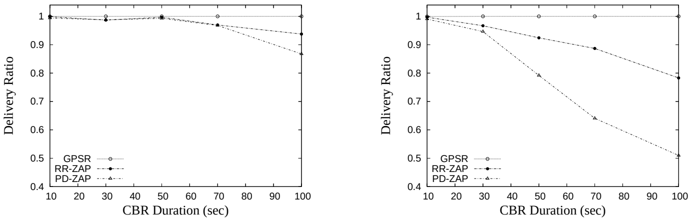


PD-ZAP

Fig. 6. D-AZ Impact on Delivery Ratio

Figure 7 reports the impact from session duration, where d_τ is 250m. The figure shows that GPSR has the nearly perfect data delivery ratio over all the session length. All ZAPs suffer from delivery ratio degradation when sessions are long. High mobility has large impact even when sessions are short. Impact from session duration and mobility is caused by the fact that destination nodes move away from the anonymous region.

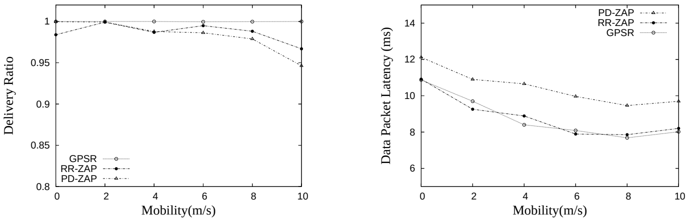
Figure 8 gives mobility impact on the performance of protocols. The configuration is: CBR sessions are 30 seconds long), d_τ is the same as in previous figure. Figure 8(a) shows the mobility impact on delivery ratio. GPSR is not affected by mobility since it can always find a closer forwarder in the current node density (nodes update location database once per second). Both RR-ZAP and PD-ZAP are not significantly affected as well because the CBR session time is relatively



(a) Low Mobility (b) High Mobility

Fig. 7. Session Duration Impact on Delivery Ratio.

short. Figure 8(b) shows the latency over mobility. Again, it is expected to see that mobility has little impact on each individual protocol.



(a) Delivery Ratio (b) Packet Latency

Fig. 8. Mobility Impact on Routing Performance

In summary, our simulations show that for destination anonymity protection, RR-ZAP has successfully increased the AS size. But RR-ZAP is more sensitive to mobility and communication duration than PD-ZAP.

4 Conclusion

In this paper we proposed ZAP, an anonymous routing protocol that adopts the group-based anonymity idea in MANET. An anonymity zone is defined, and the nodes residing in the anonymity zone form the anonymity set. Because nodes are mobile, the anonymity set in our work is dynamic, which is different from that in wired networks. We use both analysis and simulation to study the protocol performance such as node anonymity and packet delivery percentage. We have found that if the anonymity requirement is not high, PD-ZAP can be used because it achieves efficient node anonymity and a good routing performance (e.g., a low probability of a delivery failure). We then propose RR-ZAP, which uses redundant route to further improve anonymity. RR-ZAP is more sensitive to mobility, but it is worthy to trade-off for anonymity compared to PD-ZAP.

References

1. M. K. Reiter and A. D. Rubin, *Crowds: Anonymity ForWeb Transactions*, ACM Transactions on Information and System Security, 1(1):6–92, 1998.
2. R. Sherwood, B. Bhattacharjee, and A. Srinivasan, *p5: A Protocol for Scalable Anonymous Communication*, IEEE Symposium on Security and Privacy, pages 53–65, Oakland, CA, May 2002.
3. V. Scarlata, B. Levine, and C. Shields, *Responder Anonymity and Anonymous Peer-to-Peer File Sharing*, IEEE International Conference on Network Protocols (ICNP), Riverside, CA, 2001.
4. C.E. Perkins and E.M. Royer, *Ad-hoc On-Demand Distance Vector Routing*, in proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90–100, 1999.
5. D. Johnson and D. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*, in proceedings of ACM SIGCOMM-Computer Communications Review, 1996.
6. I. Stojmenovic, *Position based routing in ad hoc networks*, in IEEE Commmunications Magazine, 40(7):128-134, July 2002.
7. B. Karp and H. T. Kung, *GPSR: Greedy Perimeters Stateless Routing for Wireless Network*, in proceedings of MOBICOM'00, 2000.
8. X. Wu and B. Bhargava, *AO2P: Ad Hoc On-Demand Position-Based Private Routing*, Accepted for publication in IEEE Transaction on Mobile Computing.
9. B. Gedic and L. Liu, *Location Privacy in Mobile System: A Personalized Anonymization Model* in Proceedings of ICDCS, 2005.
10. R. Cheng, D. V. Kalashnikov and S. Prabhakar, *Querying Imprecise Data in Moving Object Environments*, in IEEE Transactions on Knowledge and Data Engineering (IEEE TKDE), Vol. 16, No. 9, pp. 1112-1127, Sep 2004.
11. National Institute for Standards and Technology (NIST). *The Keyed-Hash Message Authentication Code*, FIPS 198, 2002.
12. D. L. Chaum, *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*, Communications of the ACM, 24(2):84–88, 1981.
13. M. Reed, P. Syverson, and D. Goldschlag, *Anonymous Connections and Onion Routing*, IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection, 16(4):482–494, 1998.
14. J. Kong and X. Hong, *ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks*, 4th ACM international symposium on Mobile ad hoc networking and computing, Annapolis, MD, June 2003.
15. *QualNet*, Scalable Network Technologies (SNT), http://www.qualnet.com/.
16. J. Yoon, M. Liu, and B. Noble, *Random Waypoint Considered Harmful*, in Proceedings of IEEE INFOCOM, 2003.