A Survey on Anonymous Routing Protocols in MANET

SHINO SARA VARGHESE, J. IMMANUEL JOHN RAJA
Department of Computer Science and Engineering
Karunya University
Karunya Nagar, Coimbatore, Tamil Nadu-641 114
INDIA
shinosaravargheese@karunya.edu.in    http://www.karunya.edu

Abstract: - The main characteristic and advantage of a mobile ad-hoc network is its infrastructure-less, highly dynamic topology, which is prone to malicious traffic analysis. Malicious intermediate nodes in wireless mobile ad-hoc networks are a threat to network security. A passive attacker can perform traffic analysis against interceptable routing information embedded in routing messages and data packets. Adversaries, if allowed to trace network routes and infer motion patterns of nodes, may affect covert operations. To overcome the issues related to passive attack, we need to propose a better routing scheme which hides the essential details but at the same time satisfies the requirements of a routing protocol.

Key-Words: - Anonymity, mobile ad-hoc network, security, on-demand routing, communications and data security, passive attacks, anonymous on-demand routing.

1 Introduction
Rapid deployment of independent mobile users will be the need of the next generation wireless communication systems. A mobile ad-hoc network is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Network scenarios which include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. Network topology changes rapidly and unpredictably over time due to the mobility of the nodes. There arises the need of incorporating the routing functionality into nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

MANET is very useful for many time-critical and mission-critical applications-military and civilian operations. The shared wireless medium of MANETs facilitates passive, adversarial eavesdropping on data communications whereby adversaries can launch various devastating attacks on the target network. On-Demand (or reactive) routing protocols are prevalent in MANETs in which a node attempts to discover a route to some destination only when it has a packet to send to that destination. So far, researchers have generally studied the routing problem in a non-adversarial network setting, assuming a trusted environment. To protect wireless communication, many security protocol suites have been designed and deployed. But, they do not give significance to anonymity protection and leave mobile nodes to be traceable by wireless traffic analysts.

First, we need to identify the new anonymity requirements for mobile wireless networks. Existing anonymity research has to make new underlying assumptions when it considers the case of mobile nodes. Thus, those meant for fixed networks do not support mobile environment. Therefore, design principles of new countermeasures have to be studied. A hybrid approach of identity-free routing and on-demand routing can meet the requisites of a wireless network. This hybrid routing scheme is called ANonymous On Demand Routing (ANODR) [1]. There are various other anonymous routing protocols being used to attain anonymity. Anonymous routing is becoming relevant in the present scenario of networks as there is an increased use of wireless networks.
2 Necessity of Anonymity in a MANET

Concept of anonymity [7] has recently attracted attention in mobile wireless security research. Proactive routing and global-knowledge-based routing schemes are the ones used in infrastructure networks to provide anonymity protection. These are not applicable in the case of mobile ad hoc networks. Mobile nodes are traceable by methods which were infeasible in infrastructure networks.

In hostile environments, the adversary can launch traffic analysis against interceptable routing information in routing messages and data packets. This should be prevented to make sure that active attacks do not take place. Route anonymity and location privacy are the two addressed issues to be handled by the anonymous routing protocol.

2.1 Anonymity

Anonymity is an important issue in electronic payments and electronic voting, electronic auctions, email and web browsing. The distinction between data anonymity and connection anonymity is as follows: data anonymity is filtering any identifying information out of the data that is exchanged in a particular application; connection anonymity is hiding the identities of source and destination during the actual data transfer. Here, we give emphasis on connection anonymity. Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. A sender is identifiable when we get information that can be linked to him.

Untraceability and intrusion tolerance should be achieved for the existing network scenario. The problem is very different from other related routing security problems such as resistance to route disruption or prevention of “denial-of-service” attacks. The enemy will avoid aggressive schemes, in the attempt to be as “invisible” as possible, until it traces, finds, and then physically destroys the assets.

The untraceable routing problem is addressed by a route pseudonymity [2] approach. In a computer network, entities are identified by unique IDs. Network transmissions are considered as the items of interest (IOIs). Pseudonym is an identifier of subjects to be protected. It could be associated with a sender, a recipient, or any protégé demanding protection. The concept of pseudonymity is defined as the use of pseudonyms as IDs. The concept of anonymity is defined in terms of either unlinkability or unobservability. The difference between unlinkability and unobservability is whether security protection covers IOIs or not.

Anonymity in terms of unlinkability is defined as unlinkability of an IOI and a pseudonym. An anonymous IOI is not linkable to any pseudonym, and an anonymous pseudonym is not linkable to any IOI. More specifically, sender anonymity means that a particular transmission is not linkable to any sender’s pseudonym, and any transmission is not linkable to a particular sender’s pseudonym. Recipient anonymity is similarly defined. A property weaker than these two cases is relationship anonymity where two or more pseudonyms are unlinkable. In particular for senders and recipients, it is not possible to trace who communicates with whom, though it may be possible to trace who is the sender, or who is the recipient. In other words, sender’s pseudonym and recipient’s pseudonym (or recipients’ pseudonyms in case of multicast) are unlinkable.

Unobservability also protects IOIs from being exposed. That is, the message transmission is not discernible from random noise. More specifically, sender unobservability means that a could-be sender’s transmission is not noticeable. Recipient unobservability means that a could-be recipient’s transmission is not noticeable. Relationship observability means that it is not noticeable whether anything is sent from a set of could-be senders to a set of could-be recipients. Anonymity in terms of unlinkability is given priority here. Thus, the term “anonymity” is used instead of “anonymity in terms of unlinkability”.

2.2 Attackers

Passive eavesdroppers may be omnipresent in a hostile environment. However, an adversary with unbounded computing and active interference capability is capable of overwhelming any practically implemented security protocol. Thus, the routing schemes are so designed so as to be secure against a powerful adversary with unbounded eavesdropping capability but bounded computing and node intrusion capability.

An adversary at the level of link intrusions is an external adversary that poses threat to wireless link only. The adversary knows and actualizes all network protocols and functions. It can eavesdrop, record, inject, re-order, and re-send (altered) wireless packets. (i) The adversary can access its computational resources via a fast network with negligible delay (e.g., using directional antenna). This implies that collaborative adversaries can also contact each other in short latency. (ii) However, their computational resources may be abundant, but not unbounded. Network members can employ public key cryptosystems (e.g., RSA) and symmetric key cryptosystems (e.g., AES) to protect critical messages. They can also employ efficient message authentication protocols to get rid of unauthenticated and out-of-date packets injected by the adversary.

An adversary at the level of node intrusions is an internal adversary that also poses threat to network members. (i) After the adversary compromises a victim node, it can see the victim’s currently stored records including the private route caches. (ii) The adversary
may move from one node to another over time. However, its capability to intrude legitimate members is not unbounded. During a time window $T_{win}$ it cannot successfully compromise more than $K$ members. (iii) Intrusion detection is not perfect. A passive internal adversary exhibiting no malicious behaviour will stay in the system and intercept all routing messages. This means encrypting routing messages cannot stop a passive internal adversary.

![Underlying graph $G = <V,E>$ (Traffic analysts are depicted as solid black nodes. A sender in cell L1 is communicating with a recipient in L2. Identified active routing cells are depicted in shade). Adapted from [2].](image)

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

### 3 Anonymous Protocols

The global routing approach and the proactive routing approach were the dominant choices in anonymous routing design. But these became impractical in wireless environment. Then came proposals like Anonymous On Demand Routing (ANODR) [1], Anonymous Dynamic Source Routing (AnonDSR) [5], MASK [4], Secure Distributed Anonymous Routing Protocol (SDAR) to perform the anonymous routing.

ANODR uses pseudonyms instead of real identities in the route discovery protocol to hide the identities of the intermediate nodes in the route. This scheme makes use of Onion in the route discovery protocol, as applied in the Internet for anonymous data transmission, to establish an anonymous route.

AnonDSR employs anonymous onion routing between the source and destination, and each intermediate node owns a shared session key with the source and destination nodes when the protocol is completed. These routing schemes are sensitive to the node mobility because only one route is established in the route discovery. As nodes move, the path may be broken and has to be re-established.

MASK can establish multiple routes for data transmission by indicating the real identity of the destination node in the route request packet. With the knowledge of the destination identity in the route request, it can obtain multiple routes with the route information cached in other nodes, which cannot be achieved by any other anonymous protocol due to the hiding of the targeted destination node in the route request packet. Although observers cannot correlate a real identity with a particular node, it may detect the traffic pattern of the applications in the system, for example, if most of the data flows are destined to the same identity, attackers can conclude that the node with the identity may be a critical node in the network.

An ideal anonymous routing protocol for MANETs should have the following properties: (1) we should not assume the knowledge of topological information about the network as accessing the topological information renders the system vulnerable to attacks (2) the identities and locations of the nodes in the route, and in particular, those of the source and the destination, should be hidden and protected (3) multiple paths should be established to increase the difficulty of traffic analysis and avoid broken links due to node mobility.

#### 3.1 Anonymous On Demand Routing (ANODR)

ANODR [2] can be explained under three phases: anonymous route discovery, anonymous route maintenance and anonymous route forwarding. Anonymous route discovery establishes an on-demand route. A communication source initiates the route discovery procedure by assembling an RREQ (Route request) packet and locally broadcasting it. There are RREQ phase and RREP phase in the route discovery process. Except the first route discovery, ANODR is identity-free and incurs no public key encryption overhead in RREQ floods (though ANODR always incurs public key processing overhead in RREP unicasts by using one-time public keys on RREP forwarding nodes). The source puts a random nonce as the onion “core.” If each RREQ forwarder adds a layer of encryption during the RREQ phase, then only the node itself can peel off this layer during the RREP phase. The onion is formed during RREQ propagation and will be used to set up an anonymous virtual circuit when the RREPs come back. ANODR implements 1) symmetric
key agreement between two consecutive RREP forwarders and 2) enforces destination-initiated RREP procedure. The global trapdoor holds secret information for the intended destination and a public commitment for the same destination. RREP proof (or receipt) from the destination is obtained to prevent an adversarial network node to send back fake RREPs to disrupt ANODR.

For anonymous route maintenance, the routing table entries are recycled upon timeout $T_{win}$ similar to the same parameter used in DSR and AODV. When one or more hop is broken due to mobility or node failures, nodes cannot forward a packet via the broken hops. The one-hop sender can detect such anomalies when the retransmission count exceeds a predefined threshold. Upon anomaly detection, the node looks up the corresponding entry in its forwarding table, finds the other which is associated with the one of the broken hop, and assembles an anonymous route error report packet.

### 3.2 Anonymous Dynamic Source Routing (AnonDSR)

AnonDSR [5] routing consists of three protocols: security parameter establishment, anonymous route discovery, and anonymous data transfer.

The security parameter establishment protocol has two phases: $RREQ$ phase and $RREP$ phase. The anonymous route discovery protocol establishes an anonymous route between a pair of source and destination nodes that is resistant against traffic analysis attacks launched by any adversaries including the intermediate forwarding nodes. The protocol is used when the source and destination want to create an anonymous path for their communications and they already have a shared secret key and secret key index in their key ring (established by the security parameter establishment protocol). The protocol consists of two phases: $RREQ$ phase and $RREP$ phase. The anonymous data transfer protocol builds a cryptographic onion for anonymous communication data protection. The protocol is only used when an anonymous route discovery protocol is completed.

Each intermediate forwarding node checks whether the pseudonym of the data packet belongs to it and decrypts one layer of the data onion using its session key if it is on the anonymous route. It then changes the route pseudonym by its forwarding routing table, uses the decrypted onion instead of the received onion, and broadcasts the new packet locally. It discards the packet if it is not on the anonymous route. The procedure is repeated until the data packet arrives at the destination. A reverse anonymous communication data transfer from the destination to the source uses the reverse data onion (RDO).

### 3.3 MASK

MASK [4] is designed to meet the following objectives:

- Sender-, receiver-, and relationship anonymity.
- Untraceability and unlocatability.
- Anonymous yet secure neighbourhood authentication.
- Low cryptographic overhead and high routing efficiency.
- Resistance to a wide range of adversarial attacks.

MASK relies on a proactive neighbour detection protocol to constantly see the snapshot of its one-hop mobile neighbourhood. However, the MASK’s neighbour detection protocol is identity-free. Each MASK node only knows the physical presence of neighbouring ad hoc nodes. This is achieved by a pairing-based anonymous handshake between any pair of neighbouring nodes. MASK uses a three-stage handshake for key exchanges among a node and its new neighbouring 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. MASK does not use a global trapdoor. In the MASK’s $RREQ$ packet, source $S$ explicitly puts in the destination node $D$’s network ID. This saves the processing overhead to open the global trapdoor, thus sparing the need of end-to-end key agreement and results in a more efficient $RREQ$ procedure. However, the security trade-off is that recipient anonymity is compromised by every $RREQ$ receiver.

### 3.4 Comparison of Anonymous Protocols

The first three aspects have significant performance impacts on mobile ad hoc routing: 1) Proactive neighbor detection incurs periodic communication and computational overhead on every mobile node. 2) Because public key cryptography requires longer keys and more CPU cycles, using expensive public key cryptography (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 $l$ real-time encryption delay on the source node and then a single real-time decryption delay on every data packet forwarding node. The next two aspects affect anonymity protection: 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 the mobile wireless adversary, which can quickly scan the entire network at once and obtain an estimation of the entire network topology. 5) Ensuring recipient anonymity (of the destination’s network ID) is a critical security concern. Otherwise, every $RREQ$ receiver can see how busy a destination node is. This traffic analysis can be used by the adversary to define the priority in node tracing attacks.
Table 1. Protocol Comparison

<table>
<thead>
<tr>
<th></th>
<th>ANODR</th>
<th>AnonDSR</th>
<th>MASK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purely On demand?</td>
<td>Purely on demand</td>
<td>Purely on demand</td>
<td>Proactive neighbour detect</td>
</tr>
<tr>
<td>PKC in RREQ flood</td>
<td>First contact</td>
<td>All the time</td>
<td>No</td>
</tr>
<tr>
<td>Data delivery</td>
<td>Virtual circuit</td>
<td>MIX-net onion</td>
<td>Virtual circuit</td>
</tr>
<tr>
<td>Neighbour exposure</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Recipient anonymity</td>
<td>Crypto-protected for destination</td>
<td>Crypto-protected for destination</td>
<td>Broken by any RREQ receiver</td>
</tr>
</tbody>
</table>

3.5 Enhancement of ANODR
ANODR is the first anonymous protocol that came into existence. It tries to satisfy almost all the requirements of an anonymous protocol. But its computational overhead is high and it has to be reduced to increase its efficiency. Usage of public key cryptography is another issue. It increases cost in effect. Onions are encrypted on the way out.

To increase the efficiency of ANODR, computational overhead should be decreased. Onion encryption should be used in the way back.

4 Conclusion
ANODR which is compliant with its design principles-identity-free routing and on-demand routing is compared with the AnonDSR and MASK. Each of them has got its own merits and demerits due to the different techniques being used to achieve their goals. We give priority to ANODR due to its inherent characteristics of providing anonymity to the network. Improving and making it more efficient will help in creating a new anonymous protocol meeting all the requirements of an anonymous protocol.

Here we analyzed the other protocols that are related to ANODR. We prefer to improve ANODR rather than creating a new protocol.

References: