Anonymous Proactive Routing for Wireless Infrastructure Mesh Networks

Alireza A. Nezhad, Ali Miri, Dimitris Makrakis

University of Ottawa
800 King Edward Ave., Ottawa, Ontario, Canada
{nezhad, samiri, dimitris}@site.uottawa.ca

Luis Orozco Barbosa

Instituto de Investigación en Informática
Universidad de Castilla-La Mancha. Campus Universitario
s/n 02071 Albacete, SPAIN
lorozco@dsi.uclm.es

Abstract. An overlay routing protocol for infrastructure mesh networks is proposed that preserves user location privacy, source anonymity, destination anonymity and communication anonymity against an omni-present eavesdropper, when the underlying routing protocol is based on a proactive approach. A client only trusts its immediate access router. In order to receive packets, a client establishes a secret hop-by-hop virtual circuit between an arbitrary router, called its *Rendezvous Point (RP)* and its own access router, ahead of time. Packets destined for that client would be sent to RP first. To thwart content analysis attacks, we have used per-hop encryption. Authenticity and confidentiality of exchanged messages are also ensured using a public key infrastructure (PKI).

Keywords: Location Privacy, Anonymity, Ad hoc Routing, Mesh Networks

1 Introduction

Recent advances in wireless communications have presented the research community with new challenges in regards with user security. Two important aspects of security in mobile wireless networks from the users' perspective are *location privacy* and *anonymity*. In this article, location privacy means unlinkability between the location and the identity of a user. Anonymity in communications can be categorized as sender, receiver and relationship anonymity [10]. Relationship anonymity, sometimes called *communication anonymity*, means that a third party cannot identify both the sender and the receiver of a message or both ends of a certain connection (data flow). If the communications activities of a mobile device can be monitored, then the identity and

the movement patterns of the user of that device can be revealed, which violates the anonymity and location privacy rights of that user.

Obviously, there are many ways in which the privacy rights of a user may be violated including unauthorized access to the databases of context-aware applications containing location samples, user identification and locating at the time of association with the network, location-dependent temporary IP addresses and RF fingerprinting, to name a few. However, in this paper we are concerned with preventing locations and identities of communicating devices from becoming known to unauthorized entities as a by-product of inherent functions of routing protocols in multihop ad hoc networks.

Wireless devices are usually limited in terms of radio coverage. In order to make communication between two distant nodes in a wireless networks possible, cooperation of other nodes is necessary. This gives rise to what is referred to as *multihop* wireless communications. As the name suggests, the path between two end-nodes may traverse multiple intermediary nodes. Finding and establishing such a path is the important task of routing protocols. In wireless networks, there are two main classes of wireless routing protocols, usually referred to as *proactive* and *reactive* routing protocols. Despite their long successful history in wired networks, proactive routing protocols (e.g. OSPF and RIP) proved at first to be inefficient in wireless networks. This was mostly due to their large control overhead generated by periodic routing updates needed to keep nodes' routing tables correct at all times, in the face of frequent changes in topologies of wireless (especially mobile) networks. In the frequently changing topologies of ad hoc networks, these updates have to be broadcasted more often, which means more consumption of power and bandwidth. Another problem with proactive routing protocols was their memory requirement in order to store routing tables on each node containing routes to every possible destination. Because of these reasons, the new reactive routing protocols designed for ad hoc networks (e.g. DSR [1] and AODV [2]) proved to be more efficient and scalable than their proactive counterparts (e.g. DSDV [3]). These protocols only create routes when they are needed and discard them when they are no longer used. However, this behavior results in the so-called "*slow start*" problem, which introduces a path setup delay.

Because of the success of reactive routing protocols in ad hoc networks, almost all of the efforts in the field of anonymous routing for this kind of network were also focused on this class of routing protocols. ANODR [6] and MASK [7] are examples of these protocols. However, due to advances in radio technology on one hand and the introduction of improved proactive routing protocols on the other, the outlook is gradually changing. Bandwidths upwards of 100 Mbps are now available in wireless networks, which means larger amounts of routing updates can be accommodated. Also, mobile devices are nowadays equipped with much more memory. Several new proactive routing protocols for ad hoc networks (mostly based on link state routing) have been designed that reduce the amount of routing overhead significantly, via efficient dissemination techniques. Among these protocols, OLSR [4] and TBRPF [5] are now two of the three MANET RFCs in the area of routing. In this paper, we propose an anonymous routing protocol based on a proactive approach.

Regardless of being reactive or proactive, all of the early ad hoc routing protocols were designed without security in mind. One of the aspects of security that has been neglected in these routing protocols is *user location privacy*. Mobile users are not sta-

tionary and tracking of their movements through monitoring of their communications is a real concern. Another security-related shortcoming of regular ad hoc routing protocols is their lack of *communication anonymity*. Normally, the identities (IDs) of the source and the destination are contained in every data packet and hence known at the same time. Also, in reactive routing protocols, these IDs are present in route discovery messages.

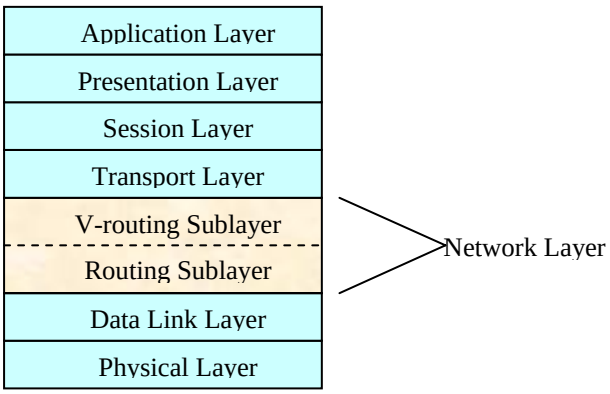

Fig. 1. V-routing protocol in the OSI reference model

Our *V-Routing* routing scheme is an overlay protocol that provides location privacy and communication anonymity to the end nodes of a data flow. As shown in Fig.1, it is an overlay protocol in the sense that it uses the services of an underlying proactive routing protocol in order to actually deliver packets. It allows the destination to establish a secret virtual circuit on top of the actual route in a way that its location is hidden even though it remains reachable.

In the next section, we provide a brief review of some related works. In section 3, we explain our network model. In Section 4, we outline our privacy objectives. In Section 5, our threat model is described. In Section 6, we provide a description of our proposed routing protocol. Finally, we conclude the paper with a summary.

2 Related Work

Recently, several protocols have been designed that add security including user anonymity and location privacy to regular ad hoc routing protocols. Furthermore, several new protocols have been introduced for this purpose that have been designed from scratch. However, in regards with location privacy and communication anonymity, virtually all of the efforts have been directed towards reactive routing protocols.

Kong and Hong presented ANODR [6], an identity-free anonymous routing protocol that uses route pseudonyms for each hop on the source-destination path, instead of node identities, in order to construct an end-to-end path. To reduce the cost and la-

tency of its cryptographic onion approach, ANODR uses a novel technique called Trapdoor Boomerang Onion in the route discovery process that makes sure no local or global eavesdropper can learn the complete path. However, ANODR has several practical issues including its reliance on the existence of a global trapdoor that implies the source and destination have a pre-established shared secret, extra path setup delays at the intermediary nodes due to various symmetric and asymmetric cryptographic operations as well as a slow and overhead-expensive route repair mechanism.

MASK [7] is another identity-free anonymous routing protocol very similar to ANODR, except that it takes a different approach to generating route pseudonyms. In addition, it has high processing and memory requirements for intermediary nodes. AO2P [8] is a position-based on-demand routing protocol that offers communication anonymity. It delivers packets to a geographical location where destination has been reported to reside lately. Several problems can be seen with this protocol. For example, the premise of this protocol is that only one node exists at any particular position at any time. Nodes must be equipped with GPS, several special position servers are needed and the position management system produces additional overhead in the network. Besides, the source can legitimately learn the exact location of the destination node, eavesdroppers can trace the RREQ (Route REQuest) packet to the destination using an un-mutable field in it called "authentication code" and they can trace the RREP (Route REPly) packet back to the source by correlating the RREQ and RREP packets.

AnonDSR [9], which is an anonymous routing protocol based on DSR prevents a data packet from being traced back to the sender or receiver, but this protection is limited to the data transmission phase. In the route acquisition phase, similar to regular DSR, the identities of the two end nodes and all the intermediary nodes are transmitted as clear text. Moreover, the RREQ packet carries a temporary public key that is fixed across all the hops between the source and the destination. An omni-present adversary (a global adversary who can monitor all transmissions) can use this field to trace the packet back to the source and the destination.

3 Network Model

One of our main assumptions in this paper is that at any given time there are a number of legitimate member nodes in the network, which do not require location privacy and anonymity. Therefore, these nodes participate fully in the routing process i.e. they identify themselves to their neighbors, collect and broadcast their neighborhood information (about neighbors that authorize it) to other nodes by way of routing updates and forward packets for other nodes according to their own routing tables. We refer to these nodes as *routers* or *access points.* On the other hand, some of the nodes in the network may like to hide their locations and their movements as much as possible. We refer to these nodes as *ordinary nodes* or *clients.* If a client does not need location privacy, it may broadcast its neighborhood information but it will still identify itself as a client meaning it would not act as a router[1]. This way, it can avoid the costs

[1] We will explain later that this design is tailored towards 1-hop clustered architectures, such as infrastructure mesh networks. Another version of our protocol, not described here, is appli-

associated with the location privacy protocol. In other words, our protocols give the client the option to dynamically decide whether it wants to remain hidden and pay the cost of privacy or prefers to bypass our security mechanisms and reveal its location. Every wireless device is identified by a unique location-independent network identifier (ID) such as its real permanent IP address. We call a neighboring router of a client with which the client associates an *Access Router* of that client. For simplicity, *i*n this paper, we consider only one access router per ordinary node. The access router of the source node (*S*) in a connection is denoted by *AS* and the access router of the destination (*D*) is denoted by *AD*. An access router does not advertise its membership information. A client connects to its access router on the link layer as in 802.11 without specifying its own MAC address. Instead, it uses the secret link layer key that it shares with its access router to hide its ID.

Clients who do wish to keep their locations hidden refrain from advertising their locations and neighborhood information. This network model is essentially a clustered architecture with access points as clusterheads, which are directly connected to their clients. An example, which is more akin to our assumed network structure, is an *infrastructure mesh* network in which clients do not participate in routing. At this time, we are not considering *client-mesh* networks where clients also help in routing packets. Mesh technology is becoming increasingly popular with applications in consumer, small business, metropolitan, and military situations, to name a few. A mesh network is typically a network of WLANs where only one or a few access points are directly connected to the wired world and act as gateways to the public networks. Other access points use multihop routing in order to access one of these gateways or any other access point, effectively forming a wireless virtual backbone. An example of this kind of network architecture is a public network of WLAN hotspots e.g. a Wireless Internet Service Provider (WISP). For instance, recently, Toronto Hydro Telecom Inc. in Canada turned the whole Toronto downtown into a large WiFi zone [11]. In this network, many access points are deployed throughout a very large area forming a backbone that uses multihop routing to connect mobile users to the wired Internet. Another example is known as Wireless Community Networks, a confederation of WLANs usually meant to provide free Internet access to users. A long list of such networks can be found in [12]. Mesh networks are being widely used to easily and cost-effectively help municipalities, counties and organizations like departments of transportation overcome the challenges of rolling out fixed and mobile wireless data networks. It enables vehicles, mobile devices and individuals to instantly and securely connect directly with each other and to the public telephone network, the Internet and private networks for access to voice, video and data services. In such an environment, it is reasonable to assume that users of the system would not be happy to know that the network operator and all other users can potentially take advantage of the weaknesses in the ad hoc routing protocol to track all their movements. The two main proposals for mesh networking namely SEEMesh and Wi-Mesh have been merged to form a starting point for the 802.11s [14] extension to WiFi standard.

---

cable to a general mesh network as well as 4G-model ad hoc networks in which user devices belong to multihop clusters and participate in packet forwarding within their cluster. An example of this kind of networks is a multihop WiFi hot-spot.

The mesh architecture is also being considered by the industry to be used with Wi-Max (IEEE 802.16) technology, instead of the traditional point-to-multipoint configuration [15], [16].

4 Privacy Objectives

The design of our protocol depends greatly on our trust model e.g. where the destination's trust lies. In this article, we assume that a client trusts at least one router in its neighborhood (its access router) with its location and identifies itself to it in order to be able to receive packets. This is in accordance with the community network model and an ad hoc kind of network. For example, in a community network consisting of houses, a client may fully trust its access router because he/she is either the owner or a guest in the house. On the other hand, in the WISP model, a client may only trust its home domain while roaming. Another version of V-routing, not discussed here, is designed for that scenario. There may be any number of reasons for lack of trust in other routers including their vulnerability to intrusion, the so-called "big brother" problem and opportunistic public network operators especially when the routes pass through foreign domains.

The location of a client is considered to be known if its access router is known. The locations of the source and the destination must only be known to their own respective access routers. Communication anonymity has to be supported with regards to peers as well as the network. In other words, only the source and the destination must know that they are communicating. We provide this feature by ensuring sender anonymity. Only the destination of a packet can know who is the original sender of the packet. Receiver anonymity is provided with regards to all third parties except one router on the source-destination path, called a rendezvous point for that connection, as will be explained later.

5 Adversary Model

We assume the existence of an omni-present adversary sometimes called a *global adversary* that can monitor all transmissions throughout the network. The adversary is assumed to be very strong in terms of processing power and storage capacity but it cannot break the cryptographic measures used by legitimate nodes in bounded time. It launches only passive attacks (eavesdropping) not active attacks such as DoS (Denial of Service), impersonation, message modification, man-in-the-middle, etc. These attacks can be discovered and the culprit can be identified using intrusion detection techniques. The kind of adversary that we have assumed wishes to remain undetected until it gathers its desired information.

We assume that the adversary is capable of performing traffic analysis. Attackers use traffic analysis techniques including content analysis and timing analysis to gain meaningful knowledge about the data flows, even though the data itself may be encrypted. They can exploit things such as packet length, packet headers, timing of transmissions on successive links, traffic patterns and so on to infer valuable conclu-

sions about communications in the network. While we do not concern ourselves with traffic analysis too much, we do address one aspect of *content analysis* that is related to routing. A global adversary can match certain fields in packets (that either do not change or change in a predictable fashion) across successive links in order to trace them back to the source and/or the destination. For example, an RREQ packet in AODV can be traced using its sequence number. To resist this kind of threat, all packets must look completely independent of each other on different links, a notion sometimes referred to as one-time packets. Two methods are in common use for achieving this effect; one is to use onion routing where a new layer of encryption is applied to the packet every time it is relayed, thus changing how it looks on consecutive links. Usually, the source node encrypts data with the key that it shares with the destination or with the destination's public key. The next hop forwarder, encrypts the received packet again for the destination, so on and so forth. The destination, applies sequential decryption in the reverse order until it recovers the original data. This method requires either a PKI infrastructure or pre-established shared keys between the destination and all the intermediary nodes. The second method is per-hop encryption/decryption (re-encryption) between neighboring nodes. For example, in IEEE 802.11, the WEP (Wired Equivalent Privacy) key option allows neighboring nodes to share a link layer secret key. In our protocol, we have used the second method to prevent content analysis attacks.

6 Proposed Routing Protocol

In the spirit of taking the proactive approach to routing, in order to avoid the path setup latency of reactive protocols, the V-Routing protocol works in a proactive manner as well. It consists of two parts; *path establishment* and *data transmission*. Before a client can receive data packets, it has to go through the path establishment phase and set up at least one secret route towards itself, starting at an arbitrary router. In other words, the main part of routing is in the control of the destination and that is the secret behind destination location privacy in V-routing.

Suppose that a source node S wishes to establish a connection to a destination node D. If D is a router, its location in the network is known because it broadcasts routing advertisements. However, if it is an ordinary node, our underlying table-driven routing protocols cannot find a path to reach it because it hides its location by refraining from broadcasting routing information. S too, may be a router or an ordinary node. If it is an ordinary node, the V-routing protocol allows it to hide its location as well.

6.1 Path Establishment Phase

When an ordinary node D joins the network, it looks at the current network topology obtained from periodic routing update messages broadcasted by routers. From this information, it chooses one of the reachable routers anywhere in the network, to be its *Rendezvous Point* (RP). This router will be used as a transient destination for any packet destined for D. Therefore, any future source node S trying to send a data

packet to D will send that packet to RP first, creating a triangular path, as shown in Fig.2. We denote the first leg of this triangular path with S-RP and the second leg with RP-D. Having a global view of the network topology, D is able to calculate a secret route from RP to itself according to a policy of its choice such as the shortest path[2]. However, for security reasons this path must be as unpredictable as possible. In fact, this information may be readily available to D from the routing updates of RP. In other words, depending on the routing protocol, these updates may specify the path from RP to AD.

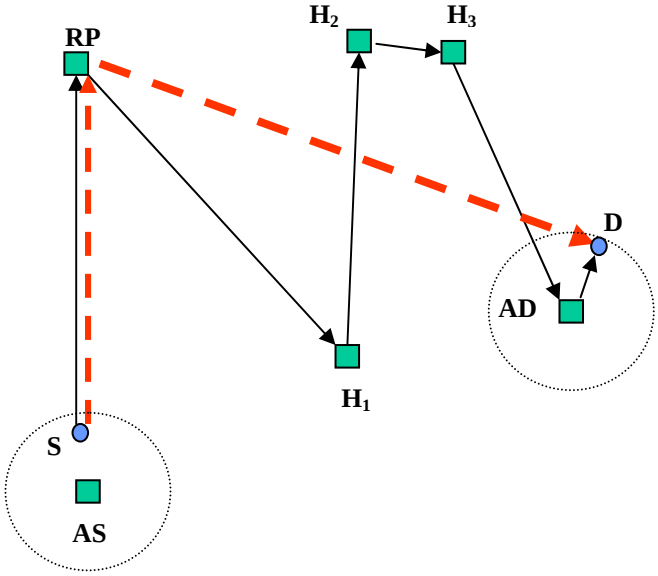

Fig. 2. Triangular Path in V-routing

D follows its own local policies to select RP. Reachability, distance and trust may be some of the criteria. Specifically, one factor that affects this decision is whether D can securely communicate with this router. D must either be able to obtain a signed public key for its RP (if public key infrastructure is used) or it should share a secret key with it (if symmetric cryptography is used). D uses unicast *forward_req* (forwarding request) messages in order to set up its second leg path. It secretly sends several such messages to a few selected routers of its choice, located along the RP-D leg, beginning with RP and ending with AD, in effect establishing a virtual circuit. We call these nodes *Virtual Hop Routers (VHR)* because each consecutive pair of them may or may not be physically one hop apart but will be able to reach each other,

[2] If D is not computationally powerful enough, AD may perform the path establishment on D's behalf but it should not identify itself in forwarding request messages.

using the underlying routing protocol. The format of a forward_req message is shown below. In this paper, $E_x(M)$ denotes an encryption of a message M for an entity x.

$$<forward\_req, RP\_elect, E_{VHR}(2^{nd}\text{-}leg\text{-}id, first\_VHR, D, next\_VHR)>$$

This message is delivered by the underlying routing protocol to the recipient VHR. *next_VHR* is the ID of the VHR downstream (towards D) from the recipient VHR. In order to prevent content analysis attacks, this message is re-encrypted at each hop. The boolean value *RP_elect* indicates to the recipient router whether or not it has been selected as a rendezvous point by D. 2^{nd}-leg-id is a global identifier chosen by D that uniquely determines this 2^{nd}-leg path and has the same format as IDs[3]. The Boolean field *first_VHR* will be explained later. D may obtain the authentic public keys of VHRs from a certificate authority or they may advertise their signed public keys in their routing update messages. Alternatively, if D shares a secret key with the VHR, they can use symmetric cryptography instead of PKI to communicate.

D sends its first *forward_req* message to RP asking it to forward any packets destined for D to a next_VHR, which we denote by H_1. If RP is willing to act as a rendezvous point for D, it broadcasts this decision in the network using an *I_AM_RP* packet. This packet is not encrypted and is readable by every one. Therefore, any node wishing to communicate with D will know it must send its packets to RP first. The I_AM_RP packet is shown below:

$$<I\_AM\_RP, RP, D, next\_VHR\_OK>$$

Due to the dynamic nature of ad hoc networks, there is a chance that the routing tables of D and RP may not match. Therefore, RP may not actually be able to reach H_1 even though it may be willing to act as D's rendezvous point. In the event of that happening, RP will set the Boolean field *next_VHR_OK* in I_AM_RP to FALSE and proceed to advertising its current routing information. After acquiring the correct routing information regarding RP, D chooses another router as H_1 and sends a new forward_req message to RP. If RP can reach the new H_1, it will set *next_VHR_OK* in I_AM_RP to TRUE.

Once RP is established, D sends unicast forward_req messages to H_1 and the other VHRs on the RP-D path. In each of these messages, D specifies the next virtual hop router for the recipient and sets the parameter RP_elect to FALSE. Of course, AD knows that it must forward packets destined for D directly to it on the link layer. This way, each VHR knows only its next VHR in order to reach D. Other nodes and eavesdroppers only know that D is using RP as its rendezvous point. Only D knows the entire RP-D leg. D can omit its ID from these messages, which enhances receiver anonymity.

If RP is not willing to act as the rendezvous point for D, it will refrain from broadcasting an I_AM_RP packet. Therefore, D can interpret the receipt of such a packet as an ACK (acknowledgement) from RP and its absence as RP's unwillingness or a NACK (negative acknowledgement), in which case it may try RP again (in case the previous message was lost.) or choose another router and repeat the same process.

[3] Hash functions can be used to generate identifiers that are globally unique. IETF RFC 4122 defines a namespace for globally unique identifiers.

Making RP, instead of D itself, responsible for disseminating this information in the network has two benefits. First, it prevents a nearby eavesdropper from locating D. Note that D's ID is not encrypted in the I_AM_RP packet because we want every node (potential source nodes for D in future) to learn the fact that D is using RP as its rendezvous point. Secondly, it reduces the overhead of the protocol because it lets RP to implicitly send an ACK to D (piggybacking). Thirdly, RP is able to take advantage of advanced flooding techniques already in use by the underlying routing protocol such as the "multipoint relay" method of OLSR to further reduce the overhead. D (or AD) needs to ensure that its 2^{nd}-leg path(s) is always connected. Therefore, it must receive a notification from the underlying routing protocol when a change in the network topology is detected.

6.1.1 Acknowledging forward_req Messages

As was explained, RP acknowledges a forward_req message with an I_AM_RP packet. Other VHRs use a different mechanism for this purpose that carries a cumulative ACK message from all VHRs back to D. To enable this mechanism, we have to include a Boolean field *first_VHR* in the forward_req message, which is only set to TRUE for H_1. After receiving a forward_req message, H_1 assembles an ACK packet, which contains a long fixed length randomly filled data structure called *magazine*. We have chosen this name for this field because of its similarity to the magazine of a machine gun where the bullets are pushed in on top of each other and are later released in the reverse order. Another analogy for this field is a First In last Out memory stack. The format of this ACK message is shown below:

$$<ACK, E_{next\_VHR}(2^{nd}\text{-}leg\text{-}id), magazine>$$

H_1 pushes its ID (encrypted for D) at one end of the magazine and sends the message to H_2. H_2 and every other VHR on the path down to and including AD do the same. If VHRs use D's public key, each of them must first append a nonce (a one-time random number) to its own ID. Otherwise, a compromised intermediate router could systematically try each ID in the network encrypted with all the available public keys to eventually uncover each address in the magazine. A compromised VHR would be in a better position to mount this attack because it knows it only needs to try the public key of D. When a nonce is used, only D, using its private key, can uncover each filed in the magazine. Delivering an ACK packet from one VHR to the next one is the responsibility of the underlying routing protocol. Each VHR determines its next VHR based on 2^{nd}-leg-id. Every VHR decrypts this field and then re-encrypts it with the public key of its next VHR. Per-hop re-encryption at the link layer is applied to the whole packet in order to prevent content analysis resulting in uncovering D's location.

If the ACK message traverses every VHR and successfully arrives at AD and is then forwarded to D, D will know that the second leg is complete. However, if some H_i is unable to reach H_{i+1} it will broadcast the so far accumulated ACK message. H_i encrypts the 2^{nd}-leg-id for D. On the other hand, after waiting for a specified amount of time, H_{i+1} issues an ACK message if it does not receive one from a previous VHR. At the end, D may end up with a few contiguous segments with gaps between each two. At that point, for every *hanging* H_i (a VHR unable to reach its next VHR) D se-

lects a new H_{i+1} (reachable by H_i and able to reach the old H_{i+1}) and sends a new forward_req message to H_i. D also sends a forward_req message to the new H_{i+1} specifying the old H_{i+1} as its next virtual hop router. By setting the *fisrt_VHR* to TRUE, D instructs the first hanging VHR in the chain to originate an ACK message and the process continues like the first time.

6.1.2 Data Transmission Phase

When a source node S wishes to send a packet to D, it sends it to RP as D's rendezvous point. This data packet is formed as:

$$<RP, E_D(S, nonce), E_{RP}(D, nonce), payload>$$

The main purpose of nonce is similar to what was explained in the path establishment phase. RP understands that it must forward the packet to D, the final destination. It replaces D's ID in the packet with the appropriate 2^{nd}-leg-id encrypted for H_1 and forwards the packet to it. This field is re-encrypted at each VHR for the next VHR. In order to prevent content analysis using the un-mutating fields of source ID and payload, they are also re-encrypted at every VHR. S is also encrypted for the destination thus the communication is anonymous to all other nodes even the two access routers AS and AD. A data packet forwarded from H_{i-1} ($i > 0$ to include RP as well) to H_i looks like:

$$<H_i , E_{Hi}(E_D(S, nonce)), E_{Hi}(2^{nd}\text{-}leg\text{-}id), E_{Hi}(payload) >$$

Every VHR determines its next VHR based on the 2^{nd}-leg-id and modifies the packet accordingly. At the last hop, the payload and $E_D(S)$ are forwarded by AD to D on the link layer using their shared secret key. These indirect packets are transported using regular IP protocols, e.g. according to the IP encapsulation specifications of the IETF RFC 2003 [13].

Summary

In this paper, we proposed a protocol for supporting user location privacy, user anonymity and communication anonymity in wireless infrastructure mesh ad hoc networks, where a client trusts its access router. We applied our general concept of *destination-controlled routing* to design one version of our V-routing protocol for this kind of network. To the best of our knowledge, V-routing is the only anonymous ad hoc routing protocol based on a proactive approach. Nevertheless, in our protocol, a user node does not advertise its neighborhood information and its location. Instead, it secretly and in advance, establishes a path towards itself starting at a transient destination (its rendezvous point), which receives packets destined for that user and then forwards them to it along the secret path. Source location privacy, source anonymity and communication anonymity are ensured by disclosing the identity of the source only to the destination. The identity of the destination of a packet is revealed only to its rendezvous point.

References

1. David B. Johnson, David A. Maltz, and Josh Broch: DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, in Ad Hoc Networking, Chapter 5, pp.139-172, Addison-Wesley, 2001.
2. Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das, Ad Hoc On Demand Distance Vector (AODV) Routing., IETF RFC 3561.
3. Perkins and P. Bhagwat, Routing over Multihop Wireless Network of Mobile Computers, in Mobile Computing, edited by Tomasz Imielinski and Henry F. Korth, Chapter 6, pp. 183-206, Kluwer Adademic Publishers, 1996.
4. T. Clausen, P. Jacquet, A. Laoiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, Optimized Link State Routing Protocol, IETF RFC 3626, October 2003.
5. R. Ogier, F. Templin, M. Lewis, Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), IETF RFC 3684, February 2004.
6. J. Kong, Anonymous and Untraceable Communications in Mobile Wireless Networks, PhD thesis, University of California, Los Angeles, June 2004.
7. Y. Zhang, W. Liu, and W. Lou, Anonymous Communications in Mobile Ad Hoc Networks, IEEE INFOCOM, Miami, FL, March 2005.
8. Xiaoxin Wu and Bharat Bhargava, AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol, IEEE Transactions on Mobile Computing, vol.4, no.4, July/August 2005.
9. Ronggong Song, Larry Korba, George Yee, *AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks*, SASN'05, November 7, 2005, Alexandria, Virginia, USA.
10. A. Pfitzmann and M. Kohntopp. Anonymity, Unobservability and Pseudonymity -- A Proposal for Terminology, in Hannes Federath(Ed), Designing Privacy Enhancing Technologies, Lecture Notes in Computer Science, LNCS 2009, pp.1-9, Springer-Verlag, 2001.
11. http://michaelocc.com/2006/09/downtown-toronto-hydro-wifi-grid.html
12. http://en.wikipedia.org/wiki/List_of_wireless_community_networks_by_region
13. C. Perkins, IP Encapsulation within IP, October 1996, http://www.ietf.org/rfc/rfc2003.txt
14. http://www.ieee802.org/11/PARs/11-04-0054-02-0mes-par-ieee-802-11-ess-mesh.doc
15. http://www.wi-fiplanet.com/news/article.php/3549846
16. http://www.wi-fiplanet.com/news/article.php/3553326