11-2004

Anonymous Secure Routing in Mobile Ad-Hoc Networks

Bo ZHU

Zhiguo WAN

Mohan S. Kankanhalli

Feng BAO
Singapore Management University, fbao@smu.edu.sg

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

DOI: https://doi.org/10.1109/LCN.2004.21

Citation

ZHU, Bo; WAN, Zhiguo; Kankanhalli, Mohan S.; BAO, Feng; and DENG, Robert H.. Anonymous Secure Routing in Mobile Ad-Hoc Networks. (2004). *LCN 2004: 29th Annual IEEE International Conference on Local Computer Networks: Proceedings: Tampa, Florida, November 16-18, 2004*. 102-108. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/516

Anonymous Secure Routing in Mobile Ad-Hoc Networks

Bo Zhu[*†], Zhiguo Wan[*†], Mohan S. Kankanhalli[*], Feng Bao[†], Robert H. Deng[†]

[*]School of Computing
National University of Singapore
Singapore 117543
{zhubo, wanzhigu, mohan}@comp.nus.edu.sg
[†]Institute for Infocomm Research
21 Heng Mui Keng Terrace
Singapore 119613
{zhubo, zhiguo, baofeng, deng}@i2r.a-star.edu.sg

Abstract

Although there are a large number of papers on secure routing in mobile ad-hoc networks, only a few consider the anonymity issue. In this paper, we define more strict requirements on the anonymity and security properties of the routing protocol, and notice that previous research works only provide Weak Location Privacy *and* Route Anonymity*, and are vulnerable to specific attacks. Therefore, we propose the Anonymous Secure Routing (ASR) protocol that can provide additional properties on anonymity, i.e.* Identity Anonymity *and* Strong Location Privacy*, and at the same time ensure the security of discovered routes against various passive and active attacks. Detailed analysis shows that, ASR can achieve both anonymity and security properties, as defined in the requirements, of the routing protocol in mobile ad-hoc networks.*

I. Introduction

Compared to the wired networks, mobile ad-hoc networks are much more vulnerable to security attacks. This is mainly due to its features of open medium, dynamic topology, cooperative algorithms, lack of centralized monitoring and management point. Current research works on securing mobile ad-hoc networks mainly focus on confidentiality, integrity, authentication, availability, and fairness, and there are only a few papers [9], [3] considering the anonymity issue. However, anonymity should be one important part of the overall solution for truly secure mobile ad-hoc networks, especially in certain privacy-vital environments. For example, in a battle field, we not only want to ensure that adversaries cannot disclose the content of our communications (i.e., confidentiality) or disable the communications (i.e., availability and integrity), but also expect that the identities and location information of parties in communications are anonymous to adversaries. Otherwise, adversaries may deduce important information about the location or mobility model of communication parties, which can be used to locate the target of their physical attacks at a later time.

In previous works [9], [3], the definition of anonymity is somehow loose. In other words, anonymity achieved in [9], [3] is insufficient. In [9], the identity of the destination is disclosed to nodes en route. In contrast, in [3], the identities of the source and destination nodes are anonymous to other nodes, but the identities of nodes en route are open to the destination node. Therefore, two cooperative adversaries can easily collect identities of other nodes, and even know the relative locations of these nodes. It is certainly undesirable in the real world. In addition, in both [9] and [3], nodes en route have the knowledge about how far, i.e. the number of hops, they are from the source. In particular, when adversaries know that the source is just one hop away, they can locate the source node using directed antenna.

On the other hand, to be usable, the anonymous routing protocol to be designed should be robust under various attacks from adversaries. However, we notice that previous works [9], [3] are vulnerable to specific attacks. In addition, due to some inherent limitations resulting from anonymity-related requirements, we argue that solutions in current secure routing protocols [18], [21], [11], [5], [4] cannot be employed directly in anonymous routing protocols. That is to say, while designing anonymous routing protocols, we should keep both the anonymity and security requirements in mind at the same time, instead of patching security-related solutions at a later time.

In this paper, we first define more strict requirements on the anonymity and security properties of the routing protocol in mobile ad-hoc networks. Following that, we propose the Anonymous Secure Routing (ASR) protocol that can not only protect the privacy of nodes and routes, but also ensure the security of discovered routes. Afterwards, detailed analysis is given to show that ASR can ensure anonymity and security of the routing protocol against known passive and active attacks.

The rest of the paper is organized as follows. In Section II and Section III, we define the goals and assumptions of our works. The details of our protocol are presented in Section IV. Following that, in Section V, we classify attacks towards anonymous routing protocols, and analyze the anonymity and security properties achieved in ASR. In Section VI, we present the related work. Finally, in Section VII, we draw the conclusion.

II. Design Goals

We intend to design a routing protocol which can protect the privacy of nodes and routes, and at the same time ensure the security of discovered routes. We define the expected goals or properties that we want to achieve in ASR as follows:

A. Ensure Privacy

1) Identity Privacy: Identity Privacy consists of the following requirements: (a) no one knows the real identities of the source and the destination, except themselves; (b) the source and the destination have no information about the real identities of intermediate nodes en route.

2) Location Privacy: Location Privacy consists of the following requirements: (a) no one knows the exact location of the source or the destination, except themselves; (b) other nodes, typically intermediate nodes en route, have no information about their distance, i.e. the number of hops, from either the source or the destination. This requirement is optional, but it is desirable in keeping both identity and location anonymity of the source or the destination, especially when the distance is just one hop.

For a protocol satisfying (a), we say that such protocol provides *Weak Location Privacy*; for a protocol satisfying both (a) and (b), we say that such protocol provides *Strong Location Privacy*.

3) Route Anonymity: Route Anonymity consists of the following requirements: (a) adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination; (b) for adversaries not in the route, they have no information on any part of the route; (c) it is difficult for adversaries to infer the transmission pattern and motion pattern of the source or the destination;

B. Ensure Security

The protocol can protect the necessary functionalities, such as discover and maintain the route, from various types of attacks.

III. Assumptions

In this paper, we assume that (1) there is a shared secret between the source and destination; (2) wireless links are symmetric. Namely, if node A is in transmission range of some node B , then B is in transmission range of A as well; (3) adversaries have unbounded eavesdropping capability but bounded computing and node intrusion capabilities.

IV. Anonymous Secure Routing Protocol

In this section, we present the details of ASR. The whole protocol consists of the following parts: *Route Request, Route Response, Anonymous Data Transmission, and Route Maintenance*.

As showed in Figure 1, we denote the source node, nodes en route, and the destination node as S, X_i ($i = 1, 2, \ldots, n$), and D, respectively. n denotes the number of nodes between the source and the destination.

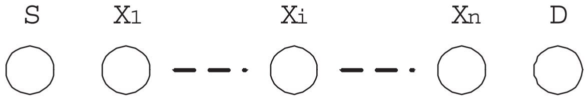

Fig. 1. The Route from Source S to Destination D

A. Route Request

During the route request process, each node en route denoted as X_i ($i = 1, 2, \ldots, n$) receives a route request with the following format:

$$\left[\begin{array}{c} RREQ,\ seq,\ K_T(dest, K_s, U_0),\ K_s(seq, END), \\ PK_{i-1},\ U_{i-1} \end{array} \right],$$

where

seq — the sequence number of the current session
K_T — the secret shared between the source and destination
dest — the identity of the destination D
K_s — the session key of the current session
END — a sign that the destination has received the route request
PK_{i-1} — the public key of the one-time key pair generated by the previous node X_{i-1}. PK_0 is the one-time public key chosen by the source S.
U_0 — a random number chosen by the source S
U_{i-1} — a number computed by X_{i-1}.

For U_i $(i = 1, 2, \cdots, n)$ in RREQ, X_i computes it according to Equation (1):

$$U_i = f(U_{i-1}, S_i) = (U_{i-1} \oplus S_i) \gg p_x, \qquad (1)$$

for $i = 1, 2, \ldots, n$, where S_i is a random number chosen by X_i with size p_x. U_0 is a random number chosen by the source S with size p_s. Note that, in Equation (1), $\oplus$ means the operation that S_i, the length of which is p_x, XORs with the least p_x bits of U_{i-1}. Thus, the computation denoted by Equation (1) includes two steps. The output of the first step is a number with size p_s. The least p_x bits of the output is the result that S_i XORs with the least p_x bits of U_{i-1}, while the higher bits are the same as the corresponding bits of U_{i-1}. The next step is to right shift the result of the first step for p_x bits.

Let H_{max} denote the maximum number of hops that S wish the route to be. Then, we have:

$$p_s = (H_{max} + 1) \cdot p_x \qquad (2)$$

For instance, given that the length of the random number chosen by X_i, i.e. S_i, is 16, the source wants to discover a route between the destination and itself, and expects the length of the route is no more than 10 hops (i.e. $H_{max} = 10$). According to Equation (2), we know that $p_x = 176$, and thus generate a random number U_0 with 176 bits during the generation of the route request message.

Once receiving the RREQ packet, each forwarding node denoted as X_i first checks whether seq has been recorded in its route table. If yes, it simply discards the packet without decrypting the third element of the RREQ packet. Otherwise, X_i tries to decrypt $K_T(dest, K_s, U_0)$. If fails, X_i records the seq, PK_{i-1}, and $K_s(seq, END)$ into the local route table, generates U_i as shown in Equation (1), and then replaces PK_{i-1} and U_{i-1} with PK_i and U_i, respectively. Finally, X_i broadcasts the modified packet locally.

If succeeds, it means that X_i is the destination node of this packet, since only the destination can successfully decrypt the packet. Afterwards, D compares U_0, which is recovered from the third element of the RREQ packet, with U_n to recover the length of the route, if the length is equal to or less than H_{max}. The destination discards those packets whose U_n has been modified by more than H_{max} nodes (i.e., the discovered route is longer than H_{max} hops). Thereafter, D generates and broadcasts a RREP packet for each route with less than H_{max} hops.

At the end of the route request process, each node en route has the public key of the previous node, and the destination has knowledge about the length of each route found between S and D, whose length is equal to or less than H_{max}.

B. Route Response

During the route response process, each node en route denoted as X_i $(i = 1, 2, \ldots, n)$ receives a route response with the following format:

$$[\ RREP,\ \{T_{i+1}\}_{PK_i},\ T_{i+1}(seq, K'_s)\ ]$$

where

K'_s — the proof that the destination has recovered the secret from the third element of the RREQ packet

T_{i+1} — a random number chosen by X_{i+1}, which is used as the shared secret between X_i and X_{i+1} after the routing discovery process.

Once receiving the RREP packet, each forwarding node denoted as X_i first tries to decrypt $\{T_{i+1}\}_{PK_i}$, and recovers the last element of the RREP packet. Since the second element is encrypted by PK_i, only X_i can decrypt it. Then X_i extracts seq from the recovered information, and checks whether seq has been recorded in its route table. If no, it simply discards the packet without any furtherer checking. Otherwise, X_i extracts K'_s from the recovered information. Thereafter, X_i also needs to make sure that the RREP packet is from the destination. It can be verified by Equation (3), because only the destination D can recover K_s from the RREQ packet. If Equation (3) is not satified, X_i simply discards this RREP packet.

$$K'_s(seq, END) \stackrel{?}{=} K_s(seq, END), \qquad (3)$$

After successfully verifying the validity of the RREP packet, X_i chooses a random number T_i, and adds T_i and T_{i+1} into the record with the corresponding *seq*. Then computes $\{T_i\}_{PK_{i-1}}$ and $T_i(seq, K'_s)$, which are used to replace the last two elements of the RREP packet. Finally, X_i broadcasts the modified RREP packet locally.

At the end of the route response process, each forwarding node has established shared secrets with the previous and next nodes. The format of a record in the route table of X_i is shown as follows:

seq	PK_{i-1}	T_i	T_{i+1}
160 bits	160 bits	128 bits	128 bits

C. Anonymous Data Transmission

To realize anonymous data transmission, we need to make sure that adversaries are not able to read or deduce information about the source and destination from data packets, and such information is only open to entities holding corresponding secrets. It is definitely not a good idea to encrypt the whole data packet using the shared secrets, although this solution is workable in theory; otherwise, each node has to try to decrypt the whole content of every packet received before decides to accept or discard it. Consequently, this method results in a great amount of computational costs.

In ASR, we provide a solution by making use of the shared secrets between any two consecutive nodes (i.e. T_i). Our idea is to construct some small-size information which is sent together with the data packet so that a forwarding node only needs to verify a small size information instead of the whole packet. It is similar to the construction of *route pseudonym* in [9], but is more simple and efficient. The small size information denoted as TAG is constructed as follows.

Given that, node X_i and node X_{i+1} shares a secret denoted as T_{i+1}. Let $H_K()$ be a keyed fast one-way function, which use K as the key. The format of TAG on the packet from X_i to X_{i+1}, denoted as TAG_i, is calculated as $[N,\ H_{T_{i+1}}(N)]$, where N is a non-decrease number chosen by X_i and is increased per packet received or sent in this route.

The data transmission process is similar to the route discovery process. Any forwarding node broadcasts the data packet to its neighbors, and then neighbors verify the validity of TAG. If the packet passes the verification, the forwarding node re-calculates and replaces TAG. In addition, before broadcasting the packet to its neighbors, the content of data packets should shuffled by an efficient encryption so that the adversaries cannot match payload contents to trace data forwarding. If the packet fails to pass the verification, it is discarded. Such process is repeated until the packet reaches the destination.

D. Route Maintenance

We assume that, nodes can detect route failures when re-transmission count exceeds a predefined number. Upon detection, a node looks up the corresponding entry in its forwarding table, finds the TAG information that it shares with the previous node, and assembles a route error packet of the format: $[RERR,\ TAG]$.

V. Anonymity & Security Analysis

Firstly, we need to make clear that the *Security* term discussed in this section does not include issues about security of the content of data packets being transmitted. It is easy to see that security of the content of data packets is orthogonal to anonymity and security of the route protocol.

A. Passive Attacks & Active Attacks

Attacks against anonymous and secure routing in ad hoc networks can be classified into two types:

- *Passive Attacks* typically involve unauthorized "listening" to the routing packets or silently refusing to execute the function requested. The former type of attacks might be an attempt to gain routing information from which the attacker could extrapolate data about the positions of each node in relation to the others. Such an attack is usually impossible to detect, since the attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routed traffic.
- *Active Attacks* are meant to degrade or prevent message flow between the nodes. They can cause a degradation or complete halt in communications between nodes. Normally, such an attack involves actions performed by adversaries, for instance, the replication, modification, and deletion of exchanged data.

Typically, adversaries may launch both passive and active attacks at the same time, and the information obtained from the former can be used to enhance the effectiveness of the latter. For example, adversaries may sniff broadcast data and record specific signs that are used to identify the route, and then launch *Denial of Service* (**DOS**) or *Distributed Denial of Service* (**DDOS**) attacks by sending or broadcasting fake data using recorded signs.

For the anonymity and security analysis in this section, we consider attacks from both internal nodes (i.e. in the route) and external nodes (i.e. out of the route).

B. Anonymity Analysis

Here, we want to check whether ASR has achieved anonymity-related goals defined in Section II, namely *Identity Privacy*, *Location Privacy*, and *Route Anonymity*. In the context of anonymity analysis, we assume that all the nodes including nodes on the discovered route are potential adversaries and are interested in the privacy information about the two communication parties and discovered routes.

1) Identity Privacy: In ASR, there is no node identity involved except the destination's identity, namely $dest$, in the RREQ packet. Fortunately, $dest$ is encrypted by the shared secret between the source and the destination, and thus it is known only to the two communication parties. Therefore, ASR can ensure *Identity Privacy* in mobile ad-hoc networks.

2) Location Privacy: The idea of current attacks on *Location Privacy* is to overhear the route request and route response packets and then deduce the distance from the source or the destination by checking the length of those packets. In [3], each forwarding node appends fixed-length information, including the id of the node and a session key (shared encryption key generated by the node), etc., to the route request packet. Therefore, every node receiving the route request packet can deduce the distance between the source and itself. In [9], authors propose to add random padding to the packets to prevent such attack. This method works well, when adversaries are not in the route. However, in order to calculate and replace the onion[1] in the route request and route response packets, internal nodes (nodes en route) need to have full knowledge about the actual size of the onion received. Consequently, their work is still vulnerable to internal nodes. In ASR, the length of the meaningful content of the route request and route response does not increase along the route. As a result of it, both external and internal nodes cannot deduce how far they are from the source or the destination.

3) Route Anonymity: Current attacks on *Route Anonymity* are based on *Traffic Analysis* [15]. The theory behind all these attacks is to detect common information among sniffed packets, and assume that any two packets are transferred along the same route, if they have information in common. The "common information" could be either identical content (e.g., the same sequence number) in sniffed packets, or identical time consumed by handling sniffed packets, or certain pattern of variations (e.g., the increase of the length of the packets). In ASR, hop-by-hop payload shuffle is employed to prevent adversaries from matching the content of packets. The second case is also referred as *Time Analysis*. In timing analysis, the adversary can use temporal dependency between transmissions to trace a victim message's forwarding path. One usual method to thwart timing analysis is to use mixing technique [14], [8], [2]. More specifically, we can use a buffer to store and reshuffle the sequence of received data packets, and at the same time inject dummy packets into the buffer if necessary. As to the third case, we ensure that the length of packets does not change during the transmission, since the increase of the packet length could be one signal for route tracing.

Table I shows the comparison of the anonymity-related properties achieved in known anonymous routing protocols in mobile ad-hoc networks. In the table, $SDDR$ and $ANODR$ stand for the anonymous routing protocols proposed in [3] and [9], respectively.

C. Security Analysis

1) Passive Attacks: The most simple attack on the route protocol is that adversaries or selfish nodes silently refuse to perform functions requested in the protocol. In normal routing protocols, the watchdog model [10] can be employed to detect such actions. However, in anonymous routing, the route response is modified hop-by-hop and is supposed to be undistinguishable from other route responses. Therefore, by nature, we can not figure out which route a given sniffed route response belongs to, since it is a trade-off between anonymity and security. The only usable solution is to discover and maintain a few routes at the stage of route discovery.

	SDDR	ANODR	ASR
Identity Privacy of The Source and The Destination	√	X	√
Identity Privacy of Forwarding Nodes en Route	X	√	√
Weak Location Privacy	√	√	√
Strong Location Privacy (external nodes)	X	√	√
Strong Location Privacy (internal nodes)	X	X	√
Route Anonymity	X	√	√

TABLE I

COMPARISON OF THE ANONYMITY PROPERTY OF ROUTING PROTOCOLS

2) DoS Attacks: According to the target of the attack, DoS attacks in the context of anonymous routing can be classified into two types: *Multiple-to-One* attacks and *One-to-Multiple* attacks. In the former attacks, multiple adversaries (or one adversary with strong power) may cooperate to exhaust the resource of a given target. The first step of such attacks is to identify the target. Our protocol is immune to this type of attacks, since *Identity Privacy* is ensured in ASR. As to the latter attacks, one adversary can send fake route request or route response packets which exhaust the computation resources of all consequent nodes along the route, since those nodes would perform the cryptographic computation as requested in the protocol. In ASR, such attacks are prevented by (a) little computation, i.e., a symmetric key decryption to check whether the node is the expected destination, is involved in handling the RREQ packet; (b) employ hop-by-hop authentication on the RREP packet. In [3], the computation involved in handling the route request is much higher than that of [9], which is slightly higher than the computation taken in ASR due to the calculation of the onion.

3) Attacks on Route Maintenance: One possible attack is that adversaries send fake route error packet to fool the source to choose another route or even re-launch the route discovery process. It makes no sense when adversaries en route launch such an attack. Therefore, in the context of attacks on route maintenance, we only consider adversaries which are not in the route. In [3], there is no shared secret between consecutive nodes en route, and thus a node detecting route failures has difficulties in informing the source such failures. In ASR, no adversary out of the route can construct fake route error packets, because it does not hold any secret with any node en route, which is necessary to generate TAG in the RERR packet.

4) Wormhole Attacks: In *Wormhole Attacks* [6], an attacker records packets received at one location in the network, tunnels them to another location, and retransmits them into the network. Hu, Perrig, and Johnson propose an approach to detect wormhole attacks based

[1] Onion is a cryptographic data structure which is firstly proposed in [16].

	SDDR	ANODR	ASR
Passive Attacks	√	√	√
Multiple-to-One DoS Attacks	X	X	√
One-to-Multiple DoS Attacks	X	√	√
Attacks on Route Maintenance	X	√	√
Wormhole Attacks	√	√	√

TABLE II
COMPARISON OF THE SECURITY PROPERTY OF ROUTING PROTOCOLS

on packet leashes [6]. The key intuition is that by authenticating either an extremely precise timestamp (i.e., *temporal leashes*) or location information combined with a loose timestamp (i.e., *geographical leashes*), a receiver can determine if the packet has traversed a distance that is unrealistic for the specific network technology used. Both of the solutions can be easily integrated into ASR without any conflict. In fact, ASR can provide a simple method to detect wormhole attacks. As mentioned in Section IV, in ASR, the destination knows the length of each route, as long as the length does not exceed H_{max}. Therefore, a verification mechanism can be employed to detect anomalies when comparing the metric (e.g. numbers of hops).

Table II shows the comparison of the security-related properties achieved in known anonymous routing protocols in mobile ad-hoc networks. In the table, $SDDR$ and $ANODR$ stand for the anonymous routing protocols proposed in [3] and [9], respectively.

VI. RELATED WORK

A. Privacy and Anonymity on the Internet

Previous research works on privacy and anonymity on the Internet concentrate on two issues: user anonymity and anonymous communication. User anonymity aims at providing the users anonymity while they are using the network by letting them hide their identity from the communicating peers. Research on anonymous communication focuses on providing a communication channel that is immune to traffic analysis so that the communicating parties can be anonymous against the eavesdroppers.

Anonymizer [1] is a user anonymity solution, which prevents online tracking by blocking the real IP address. Users can enjoy anonymity by rerouting their HTTP packets through the Anonymizer, which replaces the information in the packet headers so that the websites cannot infer the users' identities. This approach has the problem of a centralized trusted entity. The Anonymizer site can track all the anonymous user activities and is also a single point of failure. In [17], Reiter and Rubin introduce a system called *Crowds* for protecting users' anonymity on the Internet. It is based on the idea of "blending into a crowd," i.e., hiding one's actions within the actions of many others. Upon receiving one request, each member of *Crowds* can either submit the request directly to the end server or forward it to another random chosen member. When the request is eventually submitted, it is submitted by a random member, thus preventing the end server from identifying its true initiator.

One of the approaches on anonymous communication is Onion Routing [16]. Such approach requires a set of onion routers, and anonymous connections through the network are multiplexed over longstanding socket connections among onion routers. One advantage of this approach is that, each onion router can only identify the previous and next hop along a route, and data cannot be tracked en route. However, the sequence of onion routers in a route is strictly defined at connection setup. An onion proxy takes charge of the task of defining the route. Therefore, if the onion proxy is compromised, the anonymous property of routes is compromised at the same time. Besides that, the assumption of the existence of such an onion proxy is unsuitable for purely ad-hoc networks.

In [19], [20], Shields and Levine present a protocol, *Hordes*, for providing anonymous communication on the Internet. Hordes employs multiple proxies similar to those used in Crowds [17] to anonymously route a packet towards the responder, but then uses multicast services to anonymously route the reply to the initiator.

B. Anonymous Routing Protocols for Ad Hoc Networks

In [3], authors proposed a secure dynamic distributed routing algorithm (denoted as SDDR in this paper) for ad hoc wireless networks, which is based on the onion routing protocol [16]. The anonymity-related properties achieved in this algorithm include *Weak Location Privacy* and *Route Anonymity*. However, it ignores one important part of privacy in mobile ad-hoc networks, namely, *Identity Anonymity*, and cannot provide *Strong Location Privacy*.

In [9], Kong et al. design ANonymous On Demand Routing (ANODR). Similar to Hordes, ANODR [9] also explores multicast/broadcast to improve recipient anonymity. However, ANODR is an on-demand protocol, and it extensively explores trapdoor information in broadcast. These features are not discussed in Hordes' multicast mechanisms. Compared to [3], Kong et al. give a more comprehensive analysis on the anonymity and security properties achieved, and provide detailed simulation results on the efficiency of ANODR. In addition, ANODR is more efficient than SDDR at the data transmission stage. Similar to [3], *Identity Anonymity* and *Strong Location Privacy* are not provided in ANODR.

C. Secure Routing Protocols for Ad Hoc Networks

One hot area of securing mobile ad-hoc networks is secure routing. Many solutions, such as ARAN [18], AODV-S [21], SRP [11], Ariadne [5], SEAD [4], have been proposed for protecting popular routing protocols, such as AODV [13], DSR [7], and DSDV [12], from various passive and active attacks. However, due to some inherent limitations resulting from anonymity-related requirements, those solutions cannot be employed directly in anonymous routing protocols. For example, in [18], forwarding nodes need to verify route request and route response packets with the source's and the destination's certificates. This conflicts with the goal of protecting the anonymity of the two communication parties in anonymous routing protocols.

VII. Conclusion

Anonymity is a very important part of the overall solution for securing mobile ad-hoc networks. In this paper, we first gave a comprehensive definition on the goals that should be supported in anonymous routing protocols. To achieve them, we proposed the Anonymous Routing Protocol, which ensure both the anonymity and security of the routing protocol. We also gave a detailed analysis on how anonymity and security is achieved in our protocol, and at the same time showed advantages of our protocol, compared to previous works. Our future work will aim at improving the efficiency of ASR in the terms of route changes. One possible extension is to provide the functionality of repairing broken routes locally without compromising anonymity and security.

References

[1] Anonymizer. http://www.anonymizer.com.

[2] O. Berthold, H. Federrath, and M. Kohntopp. Project anonymity and unobservability in the internet. In *Computers Freedom and Privacy Conference 2000 (CFP 2000), Workshop on Freedom and Privacy by Design*, 2000.

[3] K. El-Khatib, L. Korba, R. Song, and G. Yee. Secure dynamic distributed routing algorithm for ad hoc wireless networks. In *International Conference on Parallel Processing Workshops (ICPPW'03)*, 2003.

[4] Y.-C. Hu, D. B. Johnson, and A. Perrig. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. In *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002)*, pages 3–13, June 2002.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, pages 12–23, 2002.

[6] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, 2003.

[7] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. *Mobile Computing*, 353, 1996.

[8] D. Kesdogan, J. Egner, and R. Bschkes. Stop-and-go-MIXes providing probabilistic anonymity in an open system. In *Second International Workshop on Information Hiding, Lecture Notes in Computer Science 1525*, pages 83–98, 1998.

[9] J. Kong and X. Hong. ANODR: ANonymous on demand routing with untraceable routes for mobile ad-hoc networks. In *Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'03)*, pages 291–302, 2003.

[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Mobile Computing and Networking*, 2000.

[11] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, January 2002.

[12] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector (DSDV) routing for mobile computers. In *Proceedings of ACM SIGCOMM'94*, Aug. 1994.

[13] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *WMCSA'99*, 1999.

[14] A. Pfitzmann, B. Pfitzmann, and M. Waidner. ISDN-MIXes: Untraceable communication with very small bandwidth overhead. In *Proc. GI/ITG-Conference "Kommunikation in Verteilten Systemen" (Communication in Distributed Systems)*, pages 451–463, 1991.

[15] J.-F. Raymond. Traffic analysis: Protocols, attacks, design issues, and open problems. In *DIAU00, Lecture Notes in Computer Science 2009*, pages 10–29, 2000.

[16] M. G. Reed, P. F. Syverson, and D. M. Goldschlag. Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications, Special Issue on Copyright and Privacy Protection*, 16(4):482–494, 1998.

[17] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security (TISSEC)*, 1(1):66–92, 1998.

[18] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer. A secure routing protocol for ad hoc networks. In *Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP)*, 2002.

[19] C. Shields. *Secure Hierarchical Multicast Routing and Multicast Internet Anonymity*. PhD thesis, Computer Engineering, University of California, Santa Cruz, 1999.

[20] C. Shields and B. N. Levine. A protocol for anonymous communication over the internet. In *ACM Conference on Computer and Communications Security (CCS 2000)*, pages 33–42, 2000.

[21] H. Yang, X. Meng, and S. Lu. Self-organized network-layer security in mobile ad hoc network. In *Proceedings of the ACM Workshop on Wireless Security*, pages 11–20, 2002.