Comparison: ASR is a Variant of ANODR

Jiejun Kong[†], Xiaoyan Hong[*], Mario Gerla[†], M.Y. Sanadidi[†]

[†]Department of Computer Science
University of California
Los Angeles, CA 90095

[*]Department of Computer Science
University of Alabama
Tuscaloosa, AL 35487

jkong@cs.ucla.edu, hxy@cs.ua.edu, {gerla,medy}@cs.ucla.edu

Abstract

Recently, on-demand routing approach has been embraced by several anonymous routing schemes to protect mobile ad hoc networks (MANETs) from traffic analysts' attacks[1]. ANODR [2][3][4] is the first in literature an on-demand anonymous routing protocol proposed for MANETs, followed by SDAR [5], ASR [6] and MASK [7] which use the same on-demand approach. While SDAR and MASK are significantly different from ANODR, ASR is not. In this report, we compare ASR with ANODR and conclude that ASR is an enhanced variant of ANODR.

Keywords—Anonymous Routing, On Demand Routing, ANODR, ASR, Mobile Ad Hoc Networks

1 Introduction

A mobile ad hoc network (MANET) can establish an instant communication structure for many time-critical and mission-critical applications. Nevertheless, the intrinsic characteristics of MANET, such as node mobility and wireless transmissions, make it very vulnerable to security threats.

Recently, on-demand routing approach has been embraced by several anonymous routing schemes to protect MANETs from traffic analysts' attacks[1]. Amongst them, ANODR [2][3][4] is the first in literature an on-demand anonymous routing protocol proposed. Similar on-demand approaches have been presented in SDAR [5], ASR [6] and MASK [7] to protect anonymous communications in MANET. Nevertheless, while SDAR and MASK are significantly different from ANODR, ASR is not.

We have compared ASR with ANODR. Our comparisons show that ASR is an enhanced variant of ANODR. In this report, we present facts leading to the conclusion. The report is organized as follows. Section 2 presents the straight-forward mapping between ANODR and ASR. In Section 3, we correct the wrong comments made in the ASR paper about ANODR. We summarize our report in Section 4 by giving the timeline of all related publication events. It is clear that all ANODR work were published before the ASR paper.

2 Comparisons of ASR and ANODR

With a comparison study of ASR, we conclude that ASR can be translated into ANODR in a straightforward manner. To justify this point, we list in this section the textual changes and algorithm substitution from ANODR to ASR, but not vice versa due to the fact that all the literatures about ANODR [2][3][4] were published or made public prior to the earliest ASR paper [6] (timelines can be found in Section 4):

1. *Renaming*: A sub-field X in the packet format is renamed as Y, or is renamed as Y_1, Y_2. A node X is renamed as Y.

2. *Field reordering*: The order of the sub-fields in the packet format is permuted into another form.

3. *Field length varying*: The bit-length of some sub-fields in the packet format is changed. For example, one protocol uses a 128-bit field, and the other may change the length to be 176 bits.

4. *Cryptographic scheme substitution*: A cryptographic scheme X is replaced with another scheme Y. For example, in route request (RREQ) and reply (RREP) phases, ANODR uses AES [8] in boomerang onion encryption/decryption, while ASR replaces AES with Vernam cipher [9]. It is true that AES and Vernam cipher are different cryptographic schemes. But in regard to network security protocol design, this substitution affects processing performance but does not produce a new network security protocol. Otherwise, TLS [10] protocol using RC5 cipher and the same TLS [10] protocol using 3DES cipher will be two different protocols.

It is important to point out that these four types of changes do *not* give us a new protocol. No protocol design, including ANODR's design, is perfect at the very beginning. Improvements over the original protocol designs are common practices, for example, both AODV [11][12] and DSR [13][14] have produced several new versions since their first publications. The changes made from one version to another are classified as "optimizations", which include not only the types of changes listed above, but also some more complex optimization techniques such as adding sub-protocols for gratuitous route repair. As a result, we conclude that applying the above four types of changes on ANODR is merely a special case of doing protocol optimization. It will only give us version 1, version 2, version 3, ..., of the same ANODR. Therefore, ASR is not a new protocol. It is a variant of ANODR. More details are given below.

2.1 Depiction of routing

Both Figure 4 of the ANODR paper [2] and Figure 1 of the ASR paper [6] depict the routing process.

Figure 4 of the ANODR paper [2] clearly shows the difference of conventional routing based on node identity and ANODR's node identity-free routing.

Figure 1 of the ASR paper [6] shows a renaming change. Instead of calling nodes as A, B, C, D, E, the node names are changed to $S, X_1, ..., X_i, ..., X_n, D$. This helps to explain the protocol behavior, but does not change the protocol design itself.

2.2 RREQ packet

The full RREQ packet format of ANODR is specified in the paragraph ”Setting and opening global trapdoor” of Section 3.3 of the ANODR paper [2]. The RREQ packet of ASR is specified in Section IV.A of the ASR paper [6]. The following table shows a straight-forward mapping in notations:

ANODR	ASR
pk_{one}	PK_{i-1}
$K_T(dest, K_c)$	$K_T(dest, K_s, U_0)$
$K_c(dest)$	$K_s(seq, END)$
TBO	U_{i-1}

In ANODR, the one-time public key field pk_{one} in the RREQ packet is used by each RREQ forwarder to put its temporary public key there, and the RREQ downstream node sees the temporary public key before it overrides the field with its own temporary public key. Later the RREP upstream node at RREP phase, which was the RREQ downstream node at RREQ phase, uses the known public key to do a key exchange.

Therefore, ASR's PK_{i-1} is ANODR's pk_{one} after renaming. In addition, ANODR's TBO[1] is formed by layered encryption in a symmetric key cryptosystem like AES. ASR simply replaces AES with Vernam cipher, which is faster than AES. The encryption latency is reduced from micro-seconds to nano-seconds. But in ad hoc routing design, this does not significantly affect the routing performance.

Also for the global trapdoor proof verification in RREP packet forwarding, ANODR uses the predicate $K_c(dest)\overset{?}{=}K'_c(dest)$ where the expressions $K_c(dest)$ and $K'_c(dest)$ are literally replaced by $K_s(seq, END)$ and $K'_s(seq, END)$, respectively.

Clearly, the changes in notation, field length and cipher algorithm choice do not change ANODR into another protocol, but gives us a variant of ANODR.

2.3 RREP packet

The full RREP packet format of ANODR is specified in the paragraph ”Setting and opening global trapdoor” of Section 3.3 of the ANODR paper [2]. The RREP packet of ASR is specified in Section IV.B of the ASR paper [6]. The following table shows a straight-forward mapping in notations:

ANODR	ASR
K_{seed}	T_{i+1}
$K_{seed}(K'_c, TBO)$	$T_{i+1}(seq, K'_s)$

As we explained above, ANODR's pk_{one} is a per-hop temporary public key used in key exchange. An RREP upstream node at RREP phase (which was the RREQ downstream node at RREQ phase) chooses a random key K_{seed} and encrypts the random key with the temporary public key of its RREP downstream node (which was the RREQ upstream node at RREQ phase). Then the neighboring RREP forwarders share

[1] Jiejun Kong's Ph.D. thesis [4], which was published before the due date of the ASR paper's camera ready, specifies an improved ANODR, where the boomerang onion is strictly 128-bit long. Symmetric key encryption is applied on the 128-bit onion at each RREQ stop again and again. The right-shift p_x-bit operation in ASR design describes a padding process in boomerang onion formation. As padding is not needed in the improved ANODR [4], less communication overhead is incurred compared to the original ANODR [2] and the ASR variant [6].

a per-hop secret. This per-hop secret K_{seed} is used in pseudorandom number generation to generate route pseudonyms for data packet transmission at the hop (see the next "DATA packet" subsection for more details on ANODR data transmission design), and also functions as the (WEP/TKIP/CCMP) payload cipher key to decrypt/re-encrypt the data payloads at the hop.

Clearly, changing the notation and varying field lengths in RREP packet format do not change ANODR into another protocol, but gives us a variant of ANODR.

2.4 DATA packet

In Section VI.C of the ASR paper [6], the authors claim that ASR's route pseudonym design is more simple and efficient. But the design is same as what the ANODR paper [2] specified in Section 3.3[2].

Moreover, ANODR studied how route pseudonym can be updated in a unreliable wireless channel, but ASR does not. We believe that the extra study on wireless channel error is indispensable. The overhead caused by wireless channel error should not be classified as less simple and efficient, because the reliable channel assumed in the ASR paper [6] does not exist in the real wireless world. In related papers like [4][16], this important problem is also considered and similar solutions to ANODR's are proposed.

2.5 RERR packet

The route maintenance design of ASR is same as ANODR, except the route pseudonym notion N is replaced by TAG. Both N and TAG denote the shared route pseudonym on the corresponding hop. This route pseudonym is generated by the self-synchronized pseudorandom generators on the two ends of the hop.

3 Incorrect claims in the ASR paper

The ASR paper [6] presents a comparison of ASR with other protocols in its **TABLE I**. However, the difference between ANODR and ASR listed in the **TABLE I** is incorrect. In fact, ASR does not provide more security protections to the network than what ANODR provides.

For example, ANODR is identity-free, which means any mobile node keeps its own identity to itself and never reveals its identity to other nodes. It is impossible to compromise identity privacy[3] of the source/destination unless the adversary intrudes the source/destination. The corresponding claim made in the ANODR column of the **Table I** is technically wrong.

In addition, ANODR ensures "strong location privacy" (defined as not knowing the distance, i.e., the number of hops, towards the source and the destination according to Section II.A of the ASR paper). Actually, the notion of "strong location privacy" proposed by Kong in [4], includes both what the ASR paper defines and more, for example, one-time packet contents:

[2] Jiejun Kong's Ph.D. thesis [4], which was published before the due date of the ASR paper's camera ready, discussed various choices in generating pseudorandom sequences for route pseudonyms. In practice, we can either use the repetitive re-encryption used in the original ANODR paper [2] and the ASR paper [6], or use standard fast pseudorandom generators like the one used in X9.17 [15].

[3] ANODR calls it "identity anonymity".

- We require that all RREQ (or RREP or RERR) packets in ANODR are in uniform length and hold one-time packet contents. For example, for two different RREQ floods, the two RREQ packets only has the same type (which is RREQ), but the contents are one-time only, that is, the global trapdoor is one-time per flood and the boomerang onion is one-time per hop. For two different RREP or RERR unicast packets, only the type (which is RREP or RERR) is the same, but the contents are one-time per-hop.

- ANODR's DATA packet is also one-time. For two different DATA packets, only the type (which is DATA) is the same, but the contents are one-time only. However, due to performance concerns, ANODR doesn't require DATA packets to be of a uniform length. Each data forwarder adds its own random padding and the next forwarder strips it off to add its own. Obviously, if ANODR ignores performance concerns, it is trivial to implement DATA packets with one-time contents and uniform length.

Intuitively, the term "one-time" means "computationally one-time", which in turn means "indistinguishable from truly random bits by the (PPT) adversary". This is because truly random bit-strings are effectively one-time in the sense that independent bit-strings are enumerated again and again. In cryptography, cryptographically strong pseudorandom bit-strings (generated from the same seed shared by two neighboring nodes) are indistinguishable from truly random bit-strings if neither of the seed owners is compromised. Therefore, in ANODR the adversary does not know the number of hops from itself to the source/destination, unless it compromises[4] all nodes all the way to the source/destination and count the hops. Hence ANODR ensures the "strong location privacy" defined in the ASR paper.

After all, the corrected **TABLE I** is shown below:

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

4 Summary

We summarize our report by giving the timeline of all related publication events below:

1. The camera ready version of ACM MobiHOC'03 [2] was due on April 7, 2003. At this moment we filed UCLA CSD technical report [3] to present technical details that cannot be included in [2] due to page limit. Our MobiHOC shepherd, Professor Jean-Pierre Hubaux of EPFL (`http://people.epfl.ch/jean-pierre.hubaux`), was given the technical report during the shepherding process.

[4] Similarly, if the adversary is a timing analyst in control of all links between itself and the source/destination, it can know the number of hops if traffic mixing is not implemented. Nevertheless, traffic mixing is not studied in the ASR paper [6].

2. The first author's Ph.D. thesis [4] was filed and online on July 4, 2004. ANODR was described in details in [4]. In addition to ANODR, the notions of "strong/weak location privacy" were used in [4] to denote new mobile anonymity demands. These notions cover the same notions proposed in [6].

3. The camera ready version of LCN'04 where ASR [6] is published was due on August 25, 2004.

4. The ASR paper [6] was published in LCN'04 proceedings on November 17, 2004.

Clearly, all ANODR works listed in this report were published before the earliest ASR paper. This fact strongly supports our claim that ASR is an enhanced variant of ANODR.

References

[1] Jiejun Kong, Xiaoyan Hong, and Mario Gerla. A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks. In *IEEE MILCOM*, 2003.

[2] Jiejun Kong and Xiaoyan Hong. ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks. In *ACM MOBIHOC'03*, pages 291–302, 2003.

[3] Jiejun Kong, Xiaoyan Hong, and Mario Gerla. An Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks. Technical Report CSD-TR030020, Dept. of Computer Science, UCLA, 2003.

[4] Jiejun Kong. *Anonymous and Untraceable Communications in Mobile Wireless Networks*. PhD thesis, University of California, Los Angeles, July 2004.

[5] Azzedine Boukerche, Khalil El-Khatib, Li Xu, and Larry Korba. SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks. In *29th IEEE International Conference on Local Computer Networks (LCN'04)*, pages 618–624, Nov. 2004.

[6] Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, and Robert H. Deng. Anonymous Secure Routing in Mobile Ad-Hoc Networks. In *29th IEEE International Conference on Local Computer Networks (LCN'04)*, pages 102–108, Nov. 2004.

[7] Yanchao Zhang, Wei Liu, and Wenjing Lou. Anonymous Communications in Mobile Ad Hoc Networks. In *IEEE INFOCOM*, 2005.

[8] National Institute of Standards and Technology. Advanced Encryption Standard. `http://csrc.nist.gov/encryption/aes/`, 2001.

[9] G. S. Vernam. Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications. *Journal American Institute of Electrical Engineers*, XLV:109–115, 1926.

[10] T. Dierks and C. Allen. The TLS Protocol, version 1.0. `http://www.ietf.org/rfc/rfc2246.txt`, 1999.

[11] Charles E. Perkins and Elizabeth M. Royer. Ad-Hoc On-Demand Distance Vector Routing. In *IEEE WMCSA'99*, pages 90–100, 1999.

[12] Charles E. Perkins, Elizabeth M. Royer, and S. Das. Ad-hoc On Demand Distance Vector (AODV) Routing. `http://www.ietf.org/rfc/rfc3561.txt`, July 2003.

[13] David B Johnson and David A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In Tomasz Imielinski and Hank Korth, editors, *Mobile Computing*, volume 353, pages 153–181. Kluwer Academic Publishers, 1996.

[14] David B. Johnson and David A. Maltz. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), April 2003.

[15] American National Standards Institute. American National Standard X9.17: Financial Institution Key Management (Wholesale), 1985.

[16] Jiejun Kong, Shirshanka Das, Edward Tsai, and Mario Gerla. ESCORT: A Decentralized and Localized Access Control System for Mobile Wireless Access to Secured Domains. In *ACM WiSe'03 in conjunction with MOBICOM'03*, pages 51–60, 2003.