A Simplified Anonymous Dynamic Source Routing Protocol for Ad-Hoc Networks

Chunum Kong, Hyunseung Choo*, and Won Kim

School of Information and Communication Engineering
Sungkyunkwan University
440-746, Suwon, Korea
Tel.: +82-31-290-7145
{cukong,choo}@ece.skku.ac.kr, wonkim@skku.edu

Abstract. In hostile environments, the communication content and communication route need to be shielded from malicious attackers. The AnonDSR (Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks) protocol has been proposed to ensure security and anonymity in ad-hoc networks. The protocol transmits data after establishing an encryption key and communication route. One weakness of the AnonDSR is that it consists of 3 steps: security parameter establishment, route discovery, and data transmission. In this paper, we propose a variant of AnonDSR that reduces the 3 steps into 2 steps. Our protocol decreases the communication route setup time for each communication session by 31% in comparison with the AnonDSR.

Keywords: Anonymous routing and Onion.

1 Introduction

The nodes of a mobile ad-hoc network are vulnerable to malicious attacks in the form of message forgery and eavesdropping. For ad-hoc networks deployed in a hostile environment, such as a battlefield, the consequences of a successful attack can be significant. As a result, security and anonymity of ad-hoc networks have been recent topics of research.

The AnonDSR [7] is the best-known anonymous and secure routing protocol. It consists of 3 steps, and uses both the public key and symmetric keys. The first is the security parameter establishment step; it establishes the symmetric key to use the trapdoor. The second is the anonymous route discovery step; the source and destination nodes obtain the intermediate node's IDs (instead of their route pseudonyms) and symmetric keys. The third is the anonymous transmission step; it transmits data using symmetric keys obtained in the second step.

In this paper, we propose a variant of the AnonDSR protocol, which we will call S-AnonDSR (Simplified AnonDSR). It combines the first two steps of the AnonDSR, and make the combined process more efficient than the two steps together. Moreover, the anonymous data transmission step performs additional

* Corresponding author.

O. Gervasi and M. Gavrilova (Eds.): ICCSA 2007, LNCS 4706, Part II, pp. 1072–1084, 2007.

encryption using the symmetric key. The route setup time in each communication session, compared with the AnonDSR, decreases by 31%. This is a significant improvement in performance, achieved without sacrificing security and anonymity, since the route setup time is a big part of each communication session.

The rest of this paper is organized as follows. Section 2 reviews the AnonDSR ad-hoc routing protocol in order to provide a basis of comparison with our S-AnonDSR. In Section 3 we describe the S-AnonDSR. In Section 4, we discuss the results of simulation studies. Section 5 concludes this paper.

2 Review of AnonDSR

Fig. 1 illustrates the necessity of anonymous and secure routing in the battlefield. For example, commander Tom commands a soldier Nick to attack target T via wireless communication. The top portion of Fig. 1 shows that a spy can pick off the communication and change the attack area from T to X by forging or modulating the message of an intermediate node. Encrypting the command message and the communication route, shown in the lower part of Fig. 1, makes forgery or modulation difficult.

A few anonymous and secure routing protocols precede the AnonDSR, including ANODR(Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks) [5], SDAR(A Secure Distributed Anonymous Routing Protocol for Ad Hoc Wireless Networks) [6]. SDAR uses the public key, and ANODR uses the symmetric key. AnonDSR, which has been proposed to complement SDAR and ANODR, uses both the public key and the symmetric key.

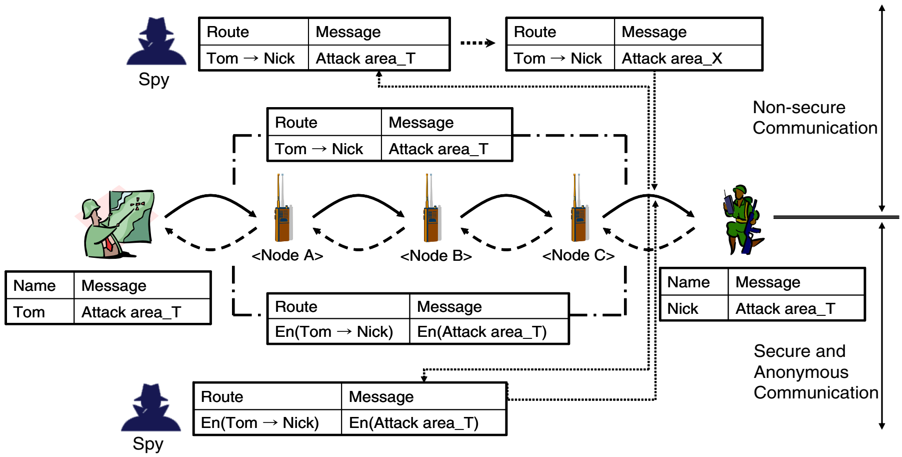


Fig. 1. Necessity of anonymous and secure routing

2.1 AnonDSR

Routing protocols for ad-hoc networks exchange messages using the RREQ (Route REQuest) and RREP (Route REPly) formats. Table 1 summarizes these formats and their components, which include the message and its description, route pseudonym, trapdoor, and encryption mechanism. The route pseudonym is used to identify a node with a random number instead of its network ID, and thus guarantee anonymity. Trapdoor is a technique that guarantees that only the destination node can decrypt a message encrypted at the source node. It encrypts a message using a secret key which is only shared by the source and destination nodes. A commonly used encryption mechanism is Onion [11], in which the message is encrypted successively with the secret key of each node.

Table 1. RREQ and RREP format of anonymous routing schemes

	Step	Message type	Security level	Temporal public key	Route pseudonym	Unique sequence num	Real ID	Routing pass	Trapdoor	Route encryption format
AnonDSR	1	RREQ	SecType	–	–	Seqnum	ID_{src}, ID_{dest}	RRec	SecPara	–
		RREP	SecType	–	–	Seqnum	ID_{src}, ID_{dest}	RRec	SecPara	–
	2	ANON-RREQ	–	PK_{temp}	–	–	–	–	tr_{dest}	onion
		ANON-RREP	–	–	N_{next}	–	–	–	–	onion
	3	ANON-DATA	–	–	N_{src}	–	–	–	–	onion

Before we describe the AnonDSR protocol, we summarize in Table 2 the notations and terminology we will use throughout this paper.

Table 2. Notations and terminology

ID_A	Identity for node A	K_X	A random symmetric key
N_X	A random nonce(number)	K_A	Symmetric key for node A
N_A	A random nonce for node A	K_S	Symmetric key to be shared between the source and destination nodes
N_S	A random nonce to be shared between the source and destination nodes	H()	A one way hash function
PK_{temp}	Temporary public key	PK_A	Public key for node A
SK_A	Private key for node A	P	Padding
PL	Padding length	$Sign_A$	Signature for node A
$E_K(M)$	A message M encrypted with a symmetric key K	$E_{PK}(M)$	A message M encrypted with a public key PK

There are three steps in the AnonDSR. The first is the security parameter establishment step. In this step, the symmetric key to be shared between the source and destination nodes is established. The security type is also selected among ‘non-secure’, ‘secure’, and ‘anonymous’.

In the RREQ phase of this step, the source node broadcasts an RREQ message to all nodes in order to reach the destination node. The following should be noted about this phase and some of the parameters of the message:

1. The SecPara in the RREQ message denotes the security parameter given by the source node. It is used by the trapdoor technique; for example, SecPara = $E_{PK_{dest}}(N_T,\, K_T,\, \text{Para})$ message, where PK_{dest} is the public key of the destination node and Para is a set of cryptographic parameters such as the encryption algorithm and the version used in the anonymous route discovery step or the anonymous data transmission step.
2. Only the destination node can confirm, using its own private key (SK_{dest}), the route pseudonym (N_T) and the symmetric key (K_T) after decrypting PK_{dest}.

In the RREP phase, the destination node changes the public key in SecPara to PK_{src}, which is public key of source node, and broadcasts a RREP message to its neighbor nodes.

The second step is the anonymous route discovery step. In this step, the source and destination nodes obtain the public keys and route pseudonyms of all nodes along the path for use in guaranteeing anonymous communication.

The following should be noted about the RREQ phase of this step, and some of the parameters of the message :

1. tr_{dest} is a trapdoor technique that uses the symmetric key (K_T). For example, $tr_{dest} = N_T,\, E_{K_T}(ID_{dest},\, SK_{temp})$, where K_T is a symmetric key which is decrypted only at the destination node.
2. The Onion encrypts the route pseudonym and symmetric key, which is generated at each intermediate node in every communication session. The resulting sequence of encrypted route pseudonyms and symmetric keys is called the path discovery Onion (PDO).

Fig. 2 shows the PDO and PRO.

In the RREP phase, note the following :

1. The destination node broadcasts the RREP message to each neighbor node.
2. N_{next} is the route pseudonym of the next node on the path back to the source node. It is changed at each successive next node.

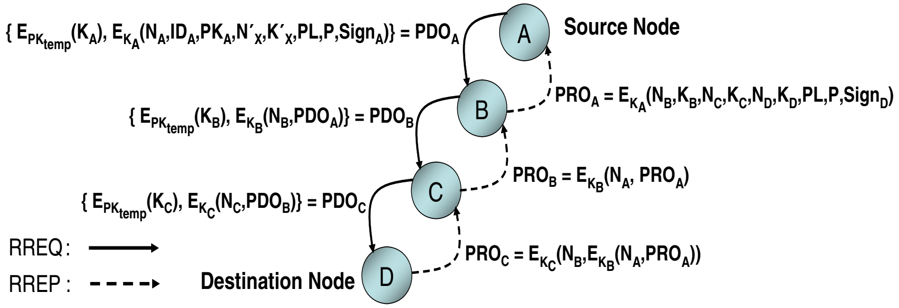

{ $E_{PK_{temp}}(K_A)$, $E_{K_A}(N_A, ID_A, PK_A, N'_X, K'_X, PL, P, Sign_A)$} = PDO_A
A
Source Node
$PRO_A = E_{K_A}(N_B, K_B, N_C, K_C, N_D, K_D, PL, P, Sign_D)$
{ $E_{PK_{temp}}(K_B)$, $E_{K_B}(N_B, PDO_A)$} = PDO_B
B
$PRO_B = E_{K_B}(N_A, PRO_A)$
{ $E_{PK_{temp}}(K_C)$, $E_{K_C}(N_C, PDO_B)$} = PDO_C
C
RREQ :
RREP :
Destination Node
D
$PRO_C = E_{K_C}(N_B, E_{K_B}(N_A, PRO_A))$

Fig. 2. The PDO and PRO

3. The Onion in this phase is called the path reverse Onion (PRO). It is the reverse of PDO.

The third step is the anonymous data transmission step. It performs the actual anonymous communication by encrypting data using Onion, which uses the symmetric key (K_X) of each node. The ANON-DATA format is shown in Table 2. The following should be noted about the anonymous data transmission step and some of the parameters of the transmission:

1. The source and destination nodes already have the route pseudonyms and symmetric keys of all intermediate nodes. Encryption is done using each node's symmetric key.
2. When N_{src} arrives at a node on the path, it is changed to the route pseudonym of the node.
3. The sending Onion is called the anonymous communication data Onion (ADO).
4. The receiving Onion is called the reverse anonymous communication data Onion (RDO).

Fig. 3 shows the ADO and RDO.

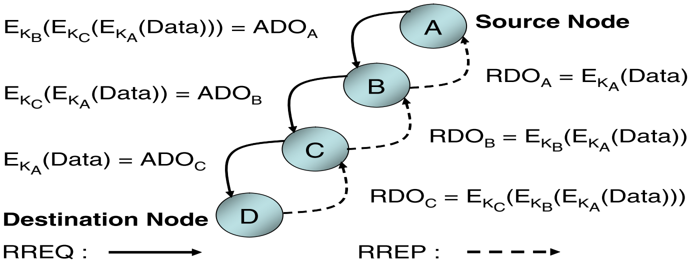

$E_{K_B}(E_{K_C}(E_{K_A}(Data))) = ADO_A$
A
Source Node
B
$RDO_A = E_{K_A}(Data)$
$E_{K_C}(E_{K_A}(Data)) = ADO_B$
C
$RDO_B = E_{K_B}(E_{K_A}(Data))$
$E_{K_A}(Data) = ADO_C$
D
$RDO_C = E_{K_C}(E_{K_B}(E_{K_A}(Data)))$
Destination Node
RREQ :
RREP :

Fig. 3. The ADO and RDO

A user can select the security and anonymity level that suit his needs. Data transmission that does not require security can be done without encryption.

3 The S-AnonDSR Protocol

In this section, we present our S-AnonDSR protocol. It may be viewed as a simplified variant of the AnonDSR. It collapses the 3 steps of the AnonDSR into two steps, while retaining the same level of security and anonymity that the AnonDSR offers, but improving performance significantly. We make the same assumptions that the AnonDSR makes; namely, that each node on the network already has the public keys of all other nodes, and each node generates a route pseudonym and symmetric key when it receives the RREQ message.

3.1 Anonymous Route Assurance Step

The first of the two steps of our S-AnonDSR is the anonymous route assurance step. Conceptually, it combines the security parameter establishment step and the anonymous route discovery step of the AnonDSR into a single step, and further makes the resulting single step efficient.

In anonymous communication, the source and destination nodes collect route pseudonyms (N_X) and symmetric keys (K_X) of the intermediate nodes rather than their IDs. The route pseudonym (N_T) and symmetric key (K_T), which is only shared between source and destination nodes, are generated at the source node; they are in addition to the route pseudonym (N_X) and symmetric key (K_X) generated at the source node for the source node.

The following should be noted about this phase and some of the parameters of the message :

1. The message is encrypted by trapdoor for broadcasting.

$$<\text{ANON-RREQ}, PK_{temp}, tr_{dest}, \text{onion}>$$

2. ANON-RREQ will indicate anonymous communication.
3. PK_{temp} is a temporal public key, which is generated by the source node and is used by the intermediate nodes to encrypt their route pseudonyms and symmetric keys.
4. tr_{dest} is a trapdoor technique that encrypts the route pseudonym and symmetric key by using the destination node's public key (PK_{dest}). The private key of the destination node (SK_{dest}) is used to decrypt it. For instance, the trapdoor is $tr_{dest} = E_{PK_{dest}}(N_T, K_T, ID_{dest}, SK_{temp})$.
5. As a result, the destination node checks N_T, K_T and the actual destination node ID. In addition, it has a temporal public key (PK_{temp}) and a temporal private key (SK_{temp}).
6. Similar to AnonDSR, Onion is used to encrypt the route pseudonyms (N_X) and symmetric keys (K_X), which are generated by each intermediate node in every communication session. This is also called the path discovery Onion (PDO). For efficient encryption, the route pseudonym and symmetric key at each node are encrypted using the symmetric key and then the temporal public key.
7. Reverse anonymous communication data Onion (RDO) is also similar to the RDO of AnonDSR.

At the source node, the PDO is formed as follows.

$$PDO_A = E_{PK_{temp}}(K_A), E_{K_A}(N_A, ID_A, PK_A, N'_X, K'_X, \text{PL}, \text{P}, Sign_A)$$

The source node (A) encrypts data using its own symmetric key (K_A). The K_A is encrypted by PK_{temp} and the next node (B) encrypts the previous PDO using its own symmetric key (K_B). This is done repeatedly until the PDO reaches the destination node. When the PDO arrives at the destination node, the destination node can obtain SK_{temp} from tr_{dest}. It already has the symmetric keys of all

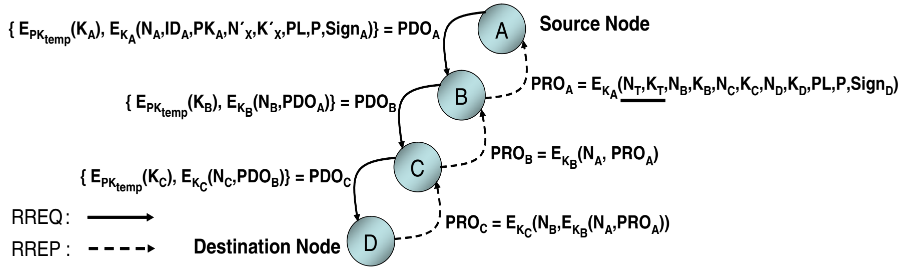

$\{E_{PK_{temp}}(K_A), E_{K_A}(N_A, ID_A, PK_A, N'_X, K'_X, PL, P, Sign_A)\} = PDO_A$
A
Source Node
$PRO_A = E_{K_A}(\underline{N_T, K_T}, N_B, K_B, N_C, K_C, N_D, K_D, PL, P, Sign_D)$
$\{E_{PK_{temp}}(K_B), E_{K_B}(N_B, PDO_A)\} = PDO_B$
B
$PRO_B = E_{K_B}(N_A, PRO_A)$
$\{E_{PK_{temp}}(K_C), E_{K_C}(N_C, PDO_B)\} = PDO_C$
C
$PRO_C = E_{K_C}(N_B, E_{K_B}(N_A, PRO_A))$
RREQ :
RREP :
Destination Node
D

Fig. 4. The PDO and PRO in S-AnonDSR

intermediate nodes. Thus it can decrypt all Onions. Then the destination node obtains the route pseudonyms of all nodes on the route. $Sign_A$ is the signature of node A, which includes the source node's ID, N_A, and K_A encrypting SK_A. The route pseudonym (N'_X) and symmetric key (K'_X) are used in the next communication session to avoid using duplicate route pseudonym and symmetric key. Fig. 4 shows the PDO and PDO in S-AnonDSR.

The following should be noted about the RREP phase and some of the parameters of the message:

1. The destination node sends a cryptogram, which includes the route pseudonyms and symmetric keys of all intermediate nodes, for the source node to share.
2. Additionally, the destination node encrypts N_T and K_T for acknowledgment of receipt of the message from the source node.

$$\text{<ANON-RREP, } N_{next}\text{, PRO>}$$

3. ANON-RREP will indicate anonymous communication.
4. N_{next} in the RREP message is the route pseudonym of the next node on the path back to the source node, and is changed whenever the message passes to a next node.
5. The Onion in this phase is called the path reverse Onion (PRO). It is the reverse of the PDO. When the RREP message arrives at the source node (A), the format of the PRO is as follows.

$$PDO_A = E_{K_A}(N_T, K_T, N_B, K_B, N_C, K_C, N_D, K_D, \text{PL}, \text{P}, Sign_D)$$

Each node from the destination (D) to the source node (A) can find the routing path back to the source node by using the route pseudonyms, and decrypt the PRO with the node's symmetric key. When the message arrives at the source node, the source node can decrypt PRO_A and thus receive the route pseudonyms and symmetric keys of all intermediate nodes. $Sign_D$ is a signature that contains the destination ID, route pseudonym (N_D), and symmetric key (K_D). It is used to encrypt the destination node's private key (SK_D).

3.2 Anonymous Data Transmission Step

The second step of the S-AnonDSR protocol is anonymous data transmission. The source and destination nodes already have the symmetric keys (K_X) and route pseudonyms (N_X) of all intermediate nodes, and can therefore create the Onions using the symmetric key (K_X) of each intermediate node. This step reinforces security by including data encryption using the symmetric key (K_T) of the destination node. Although each intermediate node has the symmetric keys (K_X) of all intermediate nodes, it cannot decrypt the cryptogram, because it does not have the symmetric key (K_T). The following summarizes this second step.

The anonymous data transmission message consists of

1. <ANON-DATA, N_{src}, onion>
   Where ANON-DATA is the message to be transmitted, and N_{src} is the source node's route pseudonym. This term is changed to the next node's route pseudonym when the message reaches that node.
2. The Onion is generated at the source and destination nodes using a symmetric key and further encrypts data by using the symmetric key (K_T). When transmitting a message, it is called the anonymous communication data Onion (ADO). When receiving, it is called the reverse anonymous communication data Onion (RDO).

Fig. 5 shows the ADO and RDO.

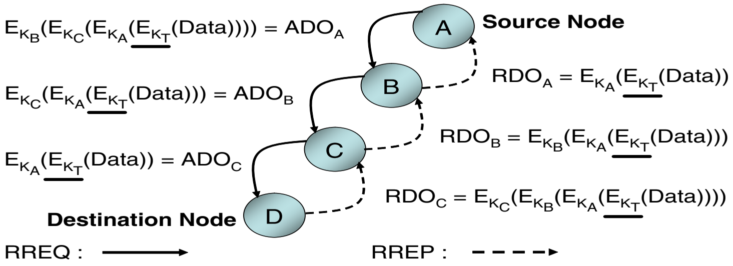

$E_{K_B}(E_{K_C}(E_{K_A}(\underline{E_{K_T}}(Data)))) = ADO_A$
A
Source Node
B
$RDO_A = E_{K_A}(\underline{E_{K_T}}(Data))$
$E_{K_C}(E_{K_A}(\underline{E_{K_T}}(Data))) = ADO_B$
C
$RDO_B = E_{K_B}(E_{K_A}(\underline{E_{K_T}}(Data)))$
$E_{K_A}(\underline{E_{K_T}}(Data)) = ADO_C$
D
$RDO_C = E_{K_C}(E_{K_B}(E_{K_A}(\underline{E_{K_T}}(Data))))$
Destination Node
RREQ :
RREP :

Fig. 5. The ADO and RDO in S-AnonDSR

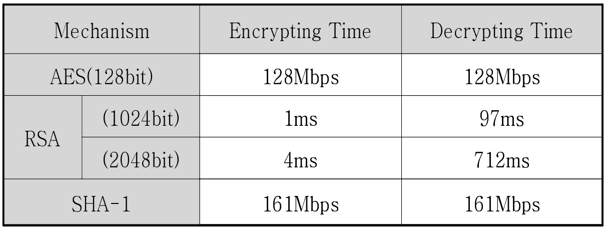
4 Performance Evaluation

In this section, we describe our simulation studies and analyze the results to report the scalability, security and performance characteristics of our S-AnonDSR protocol in comparison with the AnonDSR and a few proposals that preceded the AnonDSR.

4.1 Simulation Setup and Assumptions

We have performed simulation studies on an Intel Pentium 4 2.60GHz, 768MB RAM computer. We modeled a network with 500 nodes, and each node with

Table 3. Processing overhead of encryption schemes



Mechanism		Encrypting Time	Decrypting Time
AES(128bit)		128Mbps	128Mbps
RSA	(1024bit)	1ms	97ms
	(2048bit)	4ms	712ms
SHA-1		161Mbps	161Mbps

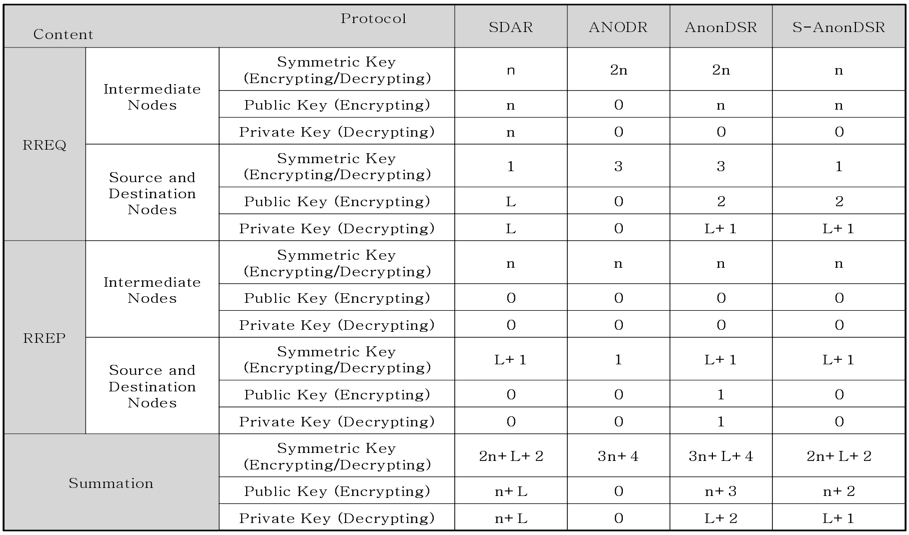
4 neighbors. We use the same values for all environment variables, except for the symmetric keys and public keys, as those used by previous proposals [5,6,7]. We use the processing overhead for each encryption technique reported in the literature [5,7], as shown in Table 3.

4.2 Scalability of the S-AnonDSR vs. Other Protocols

Table 4 compares the number of encryptions and decryptions. The purpose of this comparison is to analyze the scalability characteristics of the protocols. Only the security parameter establishment and anonymous route discovery steps are considered, as the SDAR and ANODR protocols only support these two steps.

The computation time for encryption and decryption using a public key is longer than that using a symmetric key. When using a public key, the time for decryption is longer than the time for encryption. Further, the decryption

Table 4. The number of encryptions/decryptions in anonymous routing protocols



Content		Protocol	SDAR	ANODR	AnonDSR	S-AnonDSR
RREQ	Intermediate Nodes	Symmetric Key (Encrypting/Decrypting)	n	2n	2n	n
		Public Key (Encrypting)	n	0	n	n
		Private Key (Decrypting)	n	0	0	0
	Source and Destination Nodes	Symmetric Key (Encrypting/Decrypting)	1	3	3	1
		Public Key (Encrypting)	L	0	2	2
		Private Key (Decrypting)	L	0	L+ 1	L+ 1
RREP	Intermediate Nodes	Symmetric Key (Encrypting/Decrypting)	n	n	n	n
		Public Key (Encrypting)	0	0	0	0
		Private Key (Decrypting)	0	0	0	0
	Source and Destination Nodes	Symmetric Key (Encrypting/Decrypting)	L+ 1	1	L+ 1	L+ 1
		Public Key (Encrypting)	0	0	1	0
		Private Key (Decrypting)	0	0	1	0
Summation		Symmetric Key (Encrypting/Decrypting)	2n+ L+ 2	3n+ 4	3n+ L+ 4	2n+ L+ 2
		Public Key (Encrypting)	n+ L	0	n+ 3	n+ 2
		Private Key (Decrypting)	n+ L	0	L+ 2	L+ 1

count at the source and destination nodes is much more significant than that at the intermediate nodes. In Table 4, n means the number of RREQ or RREP messages at the intermediate nodes, and L means the hop count from the source node and the destination node. The decryption count for the public key for the S-AnonDSR is smaller than that for the AnonDSR. Thus the computation time for the S-AnonDSR is smaller than that for the AnonDSR.

The processing time for each protocol can be calculated using the actual times for encryption and decryption shown in Table 3, and the sum of the encryption and decryption counts in Table 4. Fig. 6 compares scalability of the S-AnonDSR against previous proposals. The route setup time of the S-AnonDSR is longer than that for the ANODR; however, it is shorter than that for the other two protocols.

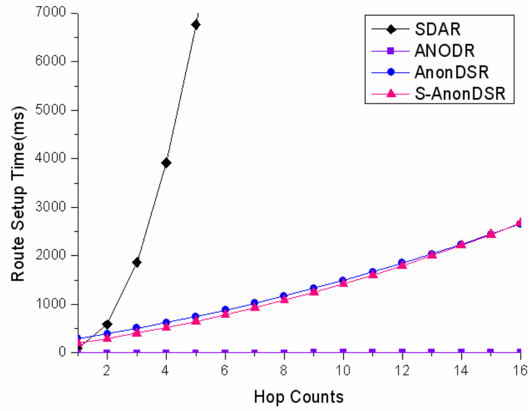


Fig. 6. Route setup time of anonymous routing protocols

4.3 S-AnonDSR vs. AnonDSR

Since the S-AnonDSR performs anonymous data transmission using the Onion technique, security is stronger than that of the AnonDSR, because it has an additional process of encrypting the symmetric key, which is only shared by the source and destination nodes.

The AnonDSR and S-AnonDSR protocols support security parameter establishment, anonymous route discovery, and anonymous data transmission. Table 5 summarizes the scalability characteristics of the two protocols. It shows that the S-AnonDSR requires higher encryption and decryption counts than the AnonDSR. However, we can calculate the total route setup time on the basis of the data in Table 3 and Table 5. Fig. 7 shows that the total route setup time of the S-AnonDSR is lower than the AnonDSR within 16 hop counts, because the S-AnonDSR is simpler than the AnonDSR.

Fig. 7 shows that the route setup time of the S-AnonDSR is up to 31% lower than that of the AnonDSR. This is a significant improvement in performance, since route setup takes place for each and every communication session. When

Table 5. Scalability of S-AnonDSR and AnonDSR

Content		Protocol	Security Parameter Establishment Step		Anonymous Route Assurance Step		Anonymous Data Transmission Step	
			AnonDSR	S-AnonDSR	AnonDSR	S-AnonDSR	AnonDSR	S-AnonDSR
RREQ	Intermediate Nodes	Symmetric Key (Encrypting/Decrypting)	0	0	2n	n	n	n
		Public Key (Encrypting)	0	0	n	n	0	0
		Private Key (Decrypting)	0	0	0	0	0	0
	Source and Destination Nodes	Symmetric Key (Encrypting/Decrypting)	0	0	3	1	L+ 1	L+ 3
		Public Key (Encrypting)	1	0	1	2	0	0
		Private Key (Decrypting)	1	0	L	L+ 1	0	0
RREP	Intermediate Nodes	Symmetric Key (Encrypting/Decrypting)	0	0	n	n	n	n
		Public Key (Encrypting)	0	0	0	0	0	0
		Private Key (Decrypting)	0	0	0	0	0	0
	Source and Destination Nodes	Symmetric Key (Encrypting/Decrypting)	0	0	L+ 1	L+ 1	L+ 1	L+ 3
		Public Key (Encrypting)	1	0	0	0	0	0
		Private Key (Decrypting)	1	0	0	0	0	0
Summation		Symmetric Key (Encrypting/Decrypting)	0	0	3n+ L+ 4	2n+ L+ 2	2n+ 2L+ 2	2n+ 2L+ 6
		Public Key (Encrypting)	2	0	n+ 1	n+ 2	0	0
		Private Key (Decrypting)	2	0	L	L+ 1	0	0

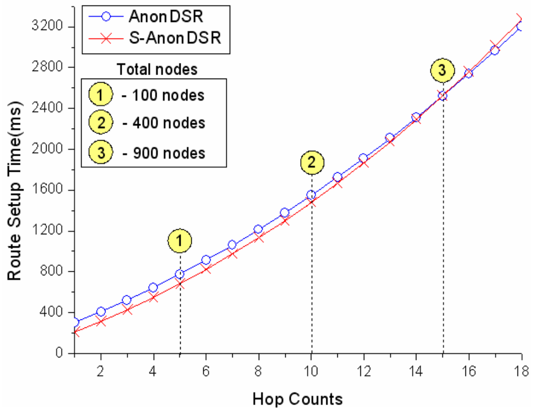


Fig. 7. Route setup times of S-AnonDSR and AnonDSR

the hop count is more than 16, the execution time of the AnonDSR becomes lower than that of the S-AnonDSR. This case is not general in mobile ad-hoc networks, because there must be over 900 nodes in order for the hop counts between the source node and the destination node to be greater than 16. Therefore, the S-AnonDSR is better than the AnonDSR in general ad-hoc network environments.

5 Conclusion

In this paper, we proposed a simplified variant of the AnonDSR anonymous routing protocol, by combining the security parameter establishment and anonymous route discovery steps of the AnonDSR into a single efficient step by modifying the trapdoor technique. It also reinforces security by performing additional encryption during the anonymous data transmission step by using the symmetric key shared by the source and destination nodes. Through simulation studies, we have verified that the route setup time of the S-AnonDSR is 31% lower than that for the AnonDSR. The S-AnonDSR is particularly well-suited when the source and destination nodes are in close proximity.

Acknowledgments. This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment), IITA-2006-(C1090-0603-0046). We thank Jun-Hee Lee for his help with the performance evaluation part of our research.

References

1. Johnson, D., Maltz, D., Broch, J.: DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. Ad Hoc Networking 5, 139–172 (2001)
2. Kargl, F., Geis, A., Schlott, S., Weber, M.: Secure Dynamic Source Routing. In: The 38th Hawaii International Conference on System Sciences (2005)
3. Perkins, C.E., Royer, E.B.: Ad-Hoc On-Demand Distance Vector Routing, RFC 3561 (July 2003)
4. Yao, A.: Theory and Applications of Trapdoor Functions (Extended Abstract). In: Symposium on Foundations of Computer Science, pp. 80–91 (1982)
5. Kong, J., Hong, X.: ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks. In: The 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 291–302 (2003)
6. Boukerche, A., El-Khatib, K., Korba, L., Xu, L.: A Secure Distributed Anonymous Routing Protocol for Ad Hoc Wireless Networks. Journal of Computer Communications (2004)
7. Song, R., Korba, L., Yee, G.: AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks. In: The 12th ACM Conference on Computer & Communications Security, pp. 32–42 (November 2005)
8. Zhang, Y., Liu, W., Lou, W., Fang, Y.: MASK: anonymous on-demand routing in mobile ad hoc networks. IEEE Transactions on Wireless Communications 5(9), 2376–2385 (2006)
9. Seys, S., Preneel, B.: ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks. In: The 20th International Conference on Advanced Information Networking and Applications, vol. 2, pp. 133–137 (2006)
10. El-Khatib, K., Korba, L., Song, R., Yee, G.: Secure Dynamic Distributed Routing Algorithm for Ad Hoc Wireless Networks. In: The ICPP 2003 First International Workshop on Wireless Security and Privacy (October 2003)
11. Goldschlag, D., Reed, M., Syverson, P.: Onion Routing for Anonymous and Private Internet Connections. Communication of the ACM 42, 39–41 (1999)

12. Boukerche, A., El-Khatib, K., Xu, L., Korba, L.: A Novel Solution for Achieving Anonymity in Wireless Ad Hoc Routing Protocol. In: Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks (October 2004)
13. Hu, Y.C., Perrig, A., Johnson, D.B.: Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In: International Conference on Mobile Computing and Networking (MobiCom) (September 2002)
14. Papadimitratos, P., Haas, Z.J.: Secure Routing for Mobile Ad Hoc Networks. In: Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS) (January 2002)
15. Zhu, B., Wan, Z.: Anonymous Secure Routing in Mobile Ad-Hoc Networks. In: The 29th Annual IEEE International Conference on Local Computer Networks, pp. 102–108 (2004)