Session Key Reuse Scheme to Improve Routing Efficiency in AnonDSR

Chunum Kong, Min Young Chung, and Hyunseung Choo*

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

Abstract. The importance of security in ad hoc network is increasing gradually to deliver information safely among nodes in hostile environment. The data is encrypted using various encryption techniques for the security reinforcement or for hiding the communication path. AnonDSR which offers anonymity to encrypt communication path, guarantees anonymity efficiently. The anonymity of source and destination nodes is guaranteed through 3 protocols. However, secret keys and route pseudonyms must be newly created for security, whenever an anonymous communication session occurs. It generates large overhead.Therefore, the proposed scheme reduces overhead of AnonDSR to reuse symmetric keys and route pseudonyms during a certain period which is defined by user. It is possible so that the data is encrypted by symmetric key which is shared between source and destination nodes, because intermediate nodes cannot decrypt the data. This scheme maintains security features of AnonDSR to perform anonymous communication, and only performs anonymous data transfer protocol when duplicate session is occurred. Then, the route setup time is improved a minimum of 47.1% due to the decrease of route setup procedure.

Keywords: Anonymous Ad Hoc Routing, Key Reuse, and Onion.

1 Introduction

When nodes achieve wireless communication in hostile environment, the nodes vulnerable to attack from malicious nodes can become the target of forgery or modification. Anonymous routing schemes which provide security for communication path are researched recently, and the necessity in several fields is increased for more secure communication.

There are representative schemes such as SDAR [2], ANODR [1], and Anon DSR [3]. These schemes maintain anonymity using the trapdoor technique [4]. This technique is method to distinguish destination node. The destination node is decided if a node can decrypt the encrypted message at source node, because this message is encrypted by secret key which is shared between source and

* Corresponding author.

Y. Shi et al. (Eds.): ICCS 2007, Part IV, LNCS 4490, pp. 303–311, 2007.

destination nodes. SDAR uses a public key in the trapdoor. The data are attached continuously after encryption by a temporary public key. ANODR uses a symmetric key in the trapdoor, and does not use secret key when this scheme encrypts data. And AnonDSR is used to mix a symmetric key and a public key. This encrypts the data using the onion technique [5].

AnonDSR solves the limitation of SDAR and ANODR. It consists of 3 protocols. First, the security parameter establishment protocol sets the symmetric key, shared only with source and destination nodes, for secure communication. Second, the anonymous route discovery protocol is that source and destination nodes have route pseudonyms and symmetric keys instead of intermediate nodes' identity for anonymous communication. Finally, the anonymous data transfer protocol enforces security of data using the onion technique which uses symmetric keys of each node. AnonDSR creates a new session to guarantee anonymity. This session must always update the symmetric key and route pseudonym. Otherwise, it causes the problem that the source node's identity is exposed from the attack of malicious nodes. Both create considerable overhead by regenerating the symmetric key and route pseudonym for anonymous communication.

Therefore, the proposed scheme reuses symmetric keys and route pseudonyms during a certain period which is defined by user, in spite of changing a session. Because it improves encryption of AnonDSR by adding a further encryption, which shares the symmetric key with source and destination nodes, and intermediate nodes cannot decrypt this symmetric key. As a result, the proposed scheme only executes anonymous data transfer protocol instead of 3 protocols when duplicate session occurs at anonymous communication. The route setup time is decreased as the number of occurrence at duplicate session and security is enhanced increasing the number of encryption at data transfer protocol. If duplicate session happens, performance of route setup time is improved by a minimum of 47.1%. At this time, as the used keys have a persistence of a certain period, it leads to confusion if session key terminology is used. Consequently, this is called a long term session key.

The rest of the paper is organized as follows. Section 2 describes anonymous ad hoc routing schemes. The proposed scheme is illustrated in Section 3. Section 4 analyzes security and anonymity of the proposed scheme compared to that of existing schemes. Section 5 concludes this paper.

2 Related Works

We review the comparison of ANODR and AnonDSR for anonymous ad hoc routing schemes and discuss their characteristics and deficiencies. Each scheme exchanges messages in RREQ and RREP, and is decided features according to encryption techniques. We use the notations and terminology shown in Table 1.

Table 2 shows RREQ and RREP format of anonymous routing schemes that include common message type, route pseudonym, trapdoor, and route encryption format. RREQ and RREP mean a message type. The route pseudonym identifies a node by random number, instead of ID, which guarantees anonymity.

Table 1. Notations and terminology

ID_A	Identity for node A	K_X	A random symmetric key
N_X	A random nonce	K_A	Symmetric key for node A
N_A	A random nonce for node A	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 K

Table 2. RREQ and RREP format of anonymous routing schemes

	Phase	Message type	Security level	Temporal public key	Route pseudonym	Unique sequence num	Real ID	Routing pass	Trapdoor	Route encryption format
ANODR	–	RREQ	–	–	–	Seqnum	–	–	tr_{dest}	onion
	–	RREP	–	–	N_{dest}	–	–	–	pr_{dest}	onion
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

The trapdoor represents a technique where only the destination node can check the message received from the source node. Generally, this is encrypted data using the shared secret key between source and destination nodes. The route encryption format represents a method of encrypting data. The onion technique repeatedly encrypts data its own secret key at a node.

3 Proposed Scheme

This scheme consists of 3 protocols: Security Parameter Establishment Protocol (SPEP), Anonymous Route Discovery Protocol (ARDP), and Anonymous Data Transfer Protocol (ADTP). SPEP and ARDP consist of RREQ and RREP, ADTP exchanges data.

We assume that firstly, like AnonDSR, the public key of each node is distributed to all the nodes in a network by Certificate Authority (CA), and secondly, the proposed scheme does not use the general concept of session key, and it defines a long term session key in order to use secret key and route pseudonym continuously even if a session is changed. Also, the route pseudonym created between nodes uses the original node continuously and is available to control the terms of validity by the user.

3.1 Security Parameter Establishment Protocol

To ensure secure communication, the SPEP exchanges a secret key between source and destination nodes. The secret key is shared and managed by only

the source and destination nodes. Route pseudonym (N_T) and symmetric key (K_T) are created at the source node. N_T and K_T mean secret index and shared secret key, respectively. The source node should maintain the N_T and K_T as a table. It is possible to check the previous communication session by this table. If there is the same secret key in the table, only anonymous data transmission is performed. 3 protocols are performed sequentially when the same secret key does not exist in the table. Route pseudonym (N_T) and symmetric key (K_T) are used as the concept of long term session key.

In the RREQ, the source node broadcasts RREQ messages and uses the trapdoor technique, which encrypts the public key of the destination node. The RREQ is composed as follows:

<RREQ, SecType, seqnum, ID_{src}, ID_{dest}, RRec, SecPara>

Where RREQ is the type of message; SecType chooses the degree of security in RREQ; seqnum is a unique sequence number; ID_{src} and ID_{dest} are the identity of source node and destination node, respectively; RRec is the source route record [3]; and SecPara is the security factor provided by the source node. When security and anonymity are required, SecPara is used by the trapdoor technique keeping $E_{PK\_dest}(N_T, K_T, \text{Para})$, $Sign_{src}$ where PK_{dest} is a public key of the destination node. $Sign_{src}$ is a signature that encrypts basic elements of the source node using a hash function. Only the destination node has a private key (SK_{dest}) and can confirm a route pseudonym (N_T) and symmetric key (K_T) decrypting PK_{dest}.

The RREP broadcasts the RREP message from the destination node to neighborhood nodes. RREP is composed as follows:

<RREP, SecType, seqnum, ID_{src}, ID_{dest}, RRec, SecPara>

RREP is the type of message. It is identical with RREQ process except that the public key in SecPara is only replaced with PK_{src}, the public key of the source node.

3.2 Anonymous Route Discovery Protocol

The source and destination nodes can have the entire route using the trapdoor and onion mechanism. The non secure and secure communication methods of AnonDSR are not changed and the process of anonymous communication method is modified.

The RREQ improves the encryption process of the onion, which is the Path Discovery Onion (PDO). It is encrypted data at the source node using the symmetric key (K_T), shared only with source and destination nodes of the SPEP, by use of a long term session key. The RREQ is composed as follows:

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

Where ANON-RREQ is the type of RREQ message that requires anonymous communication; PK_{temp} is a temporary public key created at the source node,

and is used to encrypt the data of intermediate nodes; tr_{dest} is a trapdoor technique and only the destination node can decrypt it by encrypting a symmetric key. For example, $tr_{dest} = N_T$, $E_{K\text{-}T}(ID_{dest}, SK_{temp})$; the onion, route encryption format, is used to encrypt a symmetric key (K_X) and route pseudonym (N_X) which each session is created newly at intermediate nodes. The onion, route encryption format, process is called the Path Reverse Onion (PRO) and it is created via PDO in reverse order. Fig. 1 shows the PDO and PRO processes.

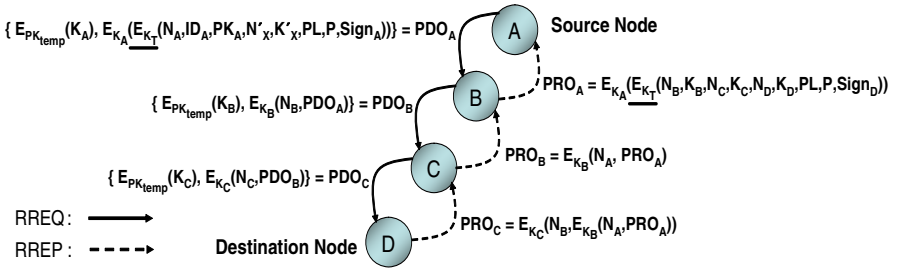

Fig. 1. PDO and PRO processes

Prior to encryption, it is appended the process of data encryption by symmetric key (K_T) generated in the SPEP. PDO at the source node is composed as follows:

$$PDO_A = E_{PK\text{-}temp}(K_A),\ E_{K\text{-}A}(E_{K\text{-}T}(N_A,ID_A,PK_A,N'_X,K'_X,\text{PL,P},Sign_A))$$

Where a route pseudonym (N_X) and symmetric key (K_X) are the long term session key to create each node independently; $Sign_A$ is the signature of ID, N_X, and K_X which are encrypted the private key (SK_A) of the source node (A); N'_X, K'_X means the used secret key and route pseudonym when the next Session has another route. The source node encrypts its own information using its own symmetric key (K_A) and the sharing symmetric key (K_T). This symmetric key (K_A) is encrypted by the temporary public key (PK_{temp}) created at the source node, and this process repeats whenever a node moves. If the destination node is reached, tr_{dest} as the trapdoor technique is decrypted by symmetric key (K_T). Then, the destination node can decrypt the symmetric keys of each node after it obtains the temporary private key (SK_{temp}), and decrypts the data of PDO encrypted by the temporary public key (PK_{temp}).

The RREP improves the encryption process of onion. The PRO adds the encrypting process by symmetric key (K_T), the long term session key, prior to encrypting the symmetric key of each node. RREQ is composed as follows:

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

Where ANON-RREP is the type of RREP message that requires anonymous communication; N_{next} is updated whenever a node moves, because this means the next route pseudonym. PRO, route encryption format, represents the onion technique and is created in PDO reverses order; PRO at the source node is composed as follows:

$$PRO_A = E_{K\_A}(E_{K\_T}(N_B,K_B,N_C,K_C,N_D,K_D,\mathrm{PL},\mathrm{P},Sign_D))$$

This encrypts the symmetric key of each node by the onion method in reverse route to inform total route pseudonyms and symmetric keys on route to the source node (A). The PRO is encrypted by the shared symmetric key (K_T) at first.

3.3 Anonymous Data Transfer Protocol

The source and destination nodes already have all symmetric key and route pseudonym on the routing route. These are used to encrypt data. Only each node on the routing route is encrypted a part of data by the onion mechanism. Prior to encryption, security is augmented by appending the data encryption process with the symmetric key (K_T) generated in the SPEP. If the intermediate node that has all symmetric keys (K_X) on the route does not contain the sharing symmetric key (K_T), security is enhanced as the encrypted data cannot be decrypt. The anonymous data transfer message is composed as follows:

$$<\text{ANON-DATA}, N_{src}, \text{onion}>$$

Where ANON-DATA is a message that informs a data transmission; N_{src} represents a route pseudonym of a starting node initially and is shifted by the route pseudonym of the next node whenever arriving at a node on the path; Onion, route encryption format, encrypts the data with symmetric keys which are collected at the previous two protocols. When transmitting, it is called Anonymous communication Data Onion (ADO) and when receiving, it is called Reverse anonymous communication Data Onion (RDO). Fig. 2 shows ADO and RDO processes.

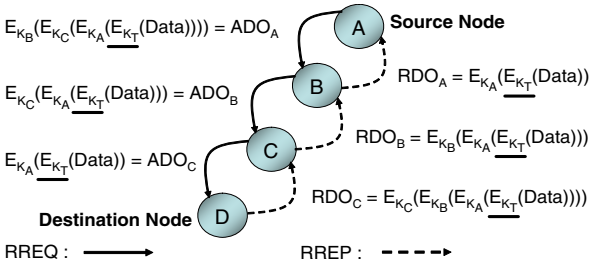

Fig. 2. ADO and RDO processes

4 Performance Evaluation

4.1 Analysis of Security, Anonymity, and Scalability

The simulation is performed on an Intel Pentium 4 Processor with 2.60GHz clock generator and, 768MB RAM. The network consists of 500 nodes and each node has 4 neighbors. It is implemented in C. The processing overhead of each encryption technique [1,3] is given Table 3.

The route setup time of each scheme can be calculated using the actual encrypting and decrypting time of encryption schemes in Table 3, and the encrypting and decrypting number in Table 4. The route setup time of the proposed scheme and AnonDSR are almost identical. However, overhead is decreased and security is enhanced to increase the encrypting number of data if duplicate session is occurred. Therefore, the proposed scheme is more efficient than AnonDSR.

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

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

Contents		Protocols	SDAR	ANODR	AnonDSR	Proposed Scheme
RREQ	Intermediate Nodes	Symmetric Key (Encrypting/Decrypting)	N	2n	2n	2n
		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	4
		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+3
		Public Key (Encrypting)	0	0	1	1
		Private Key (Decrypting)	0	0	1	1
Summation		Symmetric Key (Encrypting/Decrypting)	2n+L+2	3n+4	3n+L+4	3n+L+7
		Public Key (Encrypting)	n+L	0	n+3	n+3
		Private Key (Decrypting)	n+L	0	L+2	L+2

The total number of encryption and decryption concerned with symmetric keys and public keys in anonymous routing schemes are compared Table 4 to analyze the scalability of computing. AnonDSR and the proposed scheme consider the SPEP and the ARDP since SDAR and ANODR do not have the ADTP.

In Table 4, n means the number of different RREQ and RREP messages on an ad hoc network and L means the number of hop of a RREQ and RREP message from source node to destination node. Total route setup time and scalability are identical almost, because the total number of decryption concerned with public key in the proposed scheme are identical with AnonDSR in each anonymous scheme.

4.2 Performance Comparison of Proposed Scheme and AnonDSR

The proposed scheme is more secure than AnonDSR as the proposed scheme has a higher encrypting number of ADTP. In case of the same communications session, the encrypting and decrypting number of the entire process must be known including the ADTP. Therefore, it can calculate the route setup time using the encrypting and decrypting time of encryption schemes in Table 3.

The proposed scheme and AnonDSR are calculated using the encrypting and decrypting number and the processing time of the encryption scheme. If the same session occurs, the overhead of the proposed scheme is reduced, as shown in Fig. 3, when the duplicate session occurs initially. The efficiency improves 63.3% $\sim$ 64.5% when the same session occurs twice.

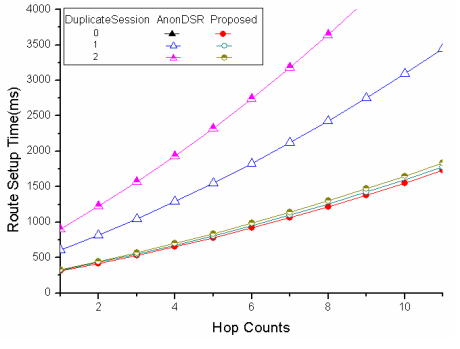

Fig. 3. Route setup time of duplicate session.

5 Conclusion

In this paper, we research a better anonymous routing scheme to solve the problems of AnonDSR, which uses the trapdoor and onion method effectively. The proposed scheme improves the encryption techniques of AnonDSR using a long term session key which is kept for a certain period of time. The proposed scheme can use the symmetric key and route pseudonym continuously, despite a changing session. Because it improves encryption of AnonDSR by adding an additional encryption procedure, which shares the symmetric key only with source and

destination nodes. As a result, We know that the route setup time is improved a minimum of 47.1%, and the efficiency of route setup time is improved increasing the occurrence of duplicate session.

Acknowledgments. This research was supported by MIC, Korea under ITRC IITA-2006-(C1090-0603-0046).

References

1. Kong, J., Hong, X.: ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks. ACM Symposium (2003) 291-302
2. 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)
3. Song, R., Korba, L., Yee, G.: AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks. SASN (2005) 32-42
4. Yao, A.: Theory and Applications of Trapdoor Functions (Extended Abstract). Symposium on Foundations of Computer Science (1982) 80-91
5. Goldschlag, D., Reed, M., Syverson, P.: Onion Routing for Anonymous and Private Internet Connections. Communication of the ACM (1999) 39-41