FASRP: A Fully Anonymous Security Routing Protocol in MANETs

Jun Pan(✉), Lin Ma, and Kai Yu

Broadband Wireless Communications Lab,
Shanghai Institute of Microsystem and Information Technology,
Chinese Academy of Sciences, Shanghai 200050, China
{jun.pan,lin.ma,kai.yu}@mail.sim.ac.cn

Abstract. The anonymous security in MANETs has drawn more attention in the military and commercial applications. Anonymous routing protocol is designed for avoiding node identity from being leaked by other nodes during communication and insuring the communication route not to be discovered. The anonymity goals of the protocol include identity anonymity, location anonymity and route anonymity. Although some anonymous routing protocols have been proposed, the requirement is not fully satisfied. In this paper, we propose a new anonymous routing protocol, i.e., fully anonymous security routing protocol (FASRP), to satisfy the requirement and defend against some potential attacks. We prove that it is an anonymous, effective and secure routing protocol. Through the simulation in NS-2, we demonstrate that FASRP has comparable network performance with the AODV and DSR routing protocols in some applications.

Keywords: Manets · Anonymity · Security · Onion routing · IBE

1 Introduction

DSR [7] and AODV [6] are two principal on-demand routing protocols in MANETs. However, they do not provide any security and anonymity protection, which make them vulnerable to a variety of security attacks. It is difficult to provide trusted and secure communications in adversarial environments, such as battlefields. Secure routing in MANETs has been studied extensively. All secure routing protocols focus on securing route discovery, route maintenance and defending against modification and fabrication of routing information. Anonymous communications are important for MANETs in adversarial environments, in which the node identities cannot be revealed to other nodes and the routes and traffic flows between the source and destination nodes cannot be recognized for protection purposed.

In the past decade many anonymous routing protocols are proposed to implement the anonymous communications in MANETs, which can be mainly classified into two categories: topology-based [1–5] and location-based routing protocol [11–14]. We focus on topology-based on-demand anonymous routing protocols, which are general for MANETs in adversarial environments. After examining these protocols, we find that the three goals of anonymity, including identity anonymity, location anonymity, and route anonymity are not fully satisfied.

G. Wang et al. (Eds.): SpaCCS 2016, LNCS 10066, pp. 292–304, 2016.
DOI: 10.1007/978-3-319-49148-6_25

Some common security mechanisms are widely used in anonymous secure routing. The trapdoor, which is initiated by ANDOR [1] and adopted by later anonymous routing protocols such as AnonDSR [4], ASR [2] and SDDR [5], is used to hide the destination true ID. To avoid the public key time-cost and energy-cost operation in the trapdoor, they advise the correspondence nodes negotiate the symmetric key in the first route discovery by public key cryptosystem, and then the source node use the symmetric key to construct the trapdoor effectively in later route discovery phase for the same destination node. However, the traditional public key cryptosystem use certificate to distribute the public key and authenticate the public key. And the authentication through traditional CA will cost more network limited resources and may disclose either nodal ID or their party membership information. The MASK [3] introduce IBE cryptosystem which can avoid the public key directory maintenance and certificate exchange in traditional CA service. However, it is a contradiction that the correspondents' ID must be kept anonymously while IBE cryptosystem should use the ID as public key. The MASK use the pseudo ID to replace the correspondents true ID to promise the anonymous security. The private key generator (PKG) should furnish each node with a large set of pseudo ID and corresponding secret point set in advance. The first limitation is that it will cost more TA resources to generate collision-resistant sufficient pseudo ID in advance and require more memory to store the pseudo ID in the each node. The second is the node has to repeat the pseudo ID when it is used up, which will influence the node anonymity.

In this paper, we devise a fully anonymous security routing protocol (FASRP) for MANETs in adversarial environments. We propose a novel method based on IBE cryptosystem to negotiate the symmetric key, and construct the trapdoor using bilinear map to hide the destination ID, thus avoiding the complex public key management in the traditional CA. The nodes can generate the pseudo public key and corresponding pseudo private key by itself. We use onion routing [8] to protect the data and routing information during the after route discovery phase and data forwarding phase.

The rest of the paper is organized as follows. Section 2 presents the protocol preliminaries. In Sect. 3 FASRP protocol is described, which consists of symmetric key anonymous negotiation phase, anonymous route discovery phase and anonymous data forwarding phase. In Sect. 4 anonymity achievements and security analysis are given. In Sect. 5 performances is analyzed. Finally in Sect. 6 conclusion and future works are described.

2 Preliminaries

2.1 The Generation of Pseudo ID Public Key in IBE

In our protocol, the PKG should also generate the private key corresponding to each node real ID in advance. But the PKG needn't generate the large set of pseudo ID for each node. The pseudo ID public key of each node can be generated by each node randomly in secret. The method not only reduces the PKG computational overhead, but also prevents the PKG to overhear the communication between nodes in MANETs to some extent. The principle basis of the method is described as follows.

We assume the PKG master key $s \in Z_q^*$ and the system parameter $\{\hat{e}, G_1, G_2, q, P, P_{pub}, H_1, H_2\}$. When node i joins the MANETs, it will get the private key SK_{IDi} from the PKG, where $SK_{IDi} = sPK_{IDi} = sH_1(ID_i)$. Now the node i can generate its pseudo public key and corresponding pseudo private key by itself to protect its anonymous security. It selects a random $r \in Z_q^*$ and generates the temporal pseudonym public key $PK_{PIDi} = rPK_{IDi} = rH_1(ID_i)$. As a result, the corresponding private key is $SK_{PIDi} = rSK_{IDi}$. The derivation process is described as following equation: $SK_{PID_i} = sPK_{PID_i} = srH_1(ID_i) = rsH_1(ID_i) = rSK_{IDi}$.

Therefore each node can randomly generate its pseudo public key and corresponding pseudo private key by itself in secret.

2.2 Network Assumption and Attack Model

- We assume that all nodes are wishing to forward the packets according to the protocol and have enough computational ability to process the algorithms in our protocol.
- We assume that the adversaries have unbounded eavesdropping capability to overwhelm any practical security protocol but bounded computing and node intrusion capabilities.
- We assume that passive adversaries can communicate with each other through private and fast communication methods, either wireless or wired. They can collaborate with each other to monitor every radio transmission on every communication link. In addition, they may compromise any node in the target network to become an internal adversary.

3 Anonymous Route Protocol

3.1 Symmetric Key Anonymous Negotiation Phase

The IBE cryptography, in which the nodes ID can be used as public key, is more effective than RSA decryption algorithm due to admissible bilinear map based on elliptic curves. We introduce the pairing [10] to construct trapdoor in the protocol. In symmetric key anonymous negotiation phase, the communication sequence number and the corresponding symmetric key, which is used to construct the trapdoor in the later route discovery phase, are exchanged anonymously. It is mentioned that we use the broadcast mode in the whole phase to protect the anonymous security.

The follows depict how the source node Alice and destination node Bob negotiate the symmetric secret key. We denote their ID as ID_A and ID_B respectively. ID_A selects the random $r \in Z_q^*$ and generates the temporal pseudo public key and pseudo private key (PK_{PIDA}, SK_{PIDA}) (refer to Sect. 2.1. The source node broadcasts symmetric key anonymous negotiation packet (SKN_{AB}) described as follows:

$$< SKN,\ TR_{AB},\ PK_{PIDA},\ S\_INFO >$$

Where the detail parts is as follows:

$$\begin{aligned} PK_{IDB} &= H_1(ID_B), \\ f_{AB} &= \widehat{e}(SK_{PIDA}, PK_{IDB}), \\ TR_{AB} &= H_2(f_{AB}), \\ K_{AB} &= H_3(f_{AB}), \end{aligned}$$

$$\begin{aligned} S\_INFO = E_{K_{AB}}(&REQ, SOURCE\_ID, DEST\_ID, EXP\_TIME, \\ &Sequence\_number, Shared\_symmetric\_key) \end{aligned}$$

SKN denotes that it is a symmetric key negotiation packet. The source node calculates the bilinear map f_{AB} by its own temporal private key SK_{PIDA} and the destination node's public key PK_{IDB}. Then they can calculate the trapdoor TR_{AB} by hash function H_2 and the temporal symmetric key K_{AB} by hash function H_3 which is used to encrypt the *S_INFO* symmetrically. There are six parts in the *S_INFO*, which is explained in the following Table 1:

Table 1. S_INFO parameters

Parameters	Description
REQ	It indicates the packet is request packet for symmetric secret key negotiation
SOURCE_ID	Source node identity
DEST_ID	Destination node identity
EXP_TIME	It is timeout value for symmetric key and sequence_number valid period.
Sequence_number	The communication sequence number, which is used for later route discovery phase and can be generated by hashing the source address and destination address through a collision resistant one-way function [9]. It should be global unique in the MANETs. The size of it is 128 bits. It is suggested that the sequence_number should be updated synchronously by hash function between the source node and destination node in the same manner.
Shared_symmetric_key	The shared symmetric key is corresponding to sequence_number one-to-one

When nodes receive the *SKN* packet, process as follows:

(a) Check if the packet has been received by comparing with PK_{PIDA}. If yes, discard it silently.

(b) If no, then calculate bilinear map by using its own private key and the source node temporal pseudo public key PK_{PIDA} and get the trapdoor TR_{iA} by hash function

H_2. We can determine the node is destination node if the trapdoor TR_{iA} is equal to TR_{AB}. The reason is showed as follows:

$$\begin{aligned} f_{BA} &= \hat{e}(SK_{IDB}, PK_{PIDA}) = \hat{e}(sPK_{IDB}, PK_{PIDA}) = \hat{e}(PK_{IDB}, PK_{PIDA})^s \\ &= \hat{e}(PK_{IDB}, sPK_{PIDA}) = \hat{e}(PK_{IDB}, SK_{PIDA}) = f_{AB} \end{aligned}$$

$$TR_{BA} = H_2(f_{BA}) = H_2(f_{AB}) = TR_{AB}$$

When ID_B assures itself as destination node, it can calculate the K_{BA} by hash function H_3. And then it decrypts the *S_INFO* by K_{BA} and get the communication sequence number and the corresponding shared symmetric key. After checking the packet is integrity and non-repudiation by the *S_INFO* content, the destination node should reply the acknowledge packet to the source node. The packet format is depicted as follows:

$$\begin{aligned} &< SKN\_ACK,\ Sequence\_number,\ SIGN_{AB} > \\ &SIGN_{AB} = E_{K_{AB}}(ACK, SOURCE\_ID, DEST\_ID, Sequence\_number, \\ &Shared\_symmetric\_key) \end{aligned}$$

When source node receives the *SKN_ACK* packet by checking the *Sequence_number* in the packet, it will decrypt the $SIGN_{AB}$ by secret key K_{AB} and confirm the destination node has agreed on the sequence number and shared symmetric key. To reduce the forwarding delay due to the bilinear map calculation processed by each intermediate node, we suggest the nodes broadcast the *SKN* packet firstly and then calculate the trapdoor. It is also helpful to hide the destination node into the intermediate nodes and protect the destination ID. Although it also incurs packet flood in the MANETs, we think it doesn't matter due to the only one-time occurrence in the communication.

Through symmetric key anonymous negotiation phase, the correspondents will negotiate the communication sequence number and the corresponding shared symmetric key which are stored into the shared symmetric key table as follows. The timer column is used to store the timer threshold value they have negotiated in *EXP_TIME* which is existed in *S_INFO*. When the timer timeout the node could delete the corresponding row entry (Table 2).

Table 2. Shared symmetric key table

Target_node	*Sequence_number*	*Shared_symmetric_key*	Timer
Node A	SEQNUM_A	SSK_A	Timer_A
Node B	SEQNUM _B	SSK_B	Timer_B
…	…	…	…

3.2 Anonymous Route Discovery Phase

The route discovery phase consists two phases: the ARREQ phase (anonymous route request phase) and the ARREP phase (anonymous route reply phase).

ARREQ Phase. During the ARREQ phase, the source node broadcasts the ARREQ packet to the destination node. The ARREQ packet contains five parts as follows:

$$< ARREQ,\ SEQNUM_{tagt},\ PK_{temp},\ TR_{tagt},\ PDO >$$

ARREQ denotes the packet is anonymous route request packet. $SEQNUM_{tagt}$ is the global unique sequence number negotiated between source and destination node in the symmetric key anonymous negotiation phase. PK_{temp} is a temporally public key, and its corresponding private key SK_{temp} is stored in the trapdoor TR_{tagt}. Only the destination node can decrypt the trapdoor and get SK_{temp}. TR_{tagt} is the trapdoor encrypted by the symmetric key which is the shared symmetric key SSK_{tagt}. It is composed of the trapdoor sign, source ID, destination ID, and the temporal private key SK_{temp}.

$$TR_{tagt} = E_{SSK_{tagt}}\left(PDO\_SIGN, ID_{tagt}, ID_{src}, SK_{temp}\right)$$

PDO is similar to the route table in the RREQ of DSR protocol. It requires that any intermediate node forwarding the ARREQ should generate the temporal pseudo ID N_i and temporal symmetric session key K_i in advance. (N_i,K_i) should be a global unique pair in the whole MANETs. And then the intermediate nodes can asymmetrically encrypt the temporal session key K_i using the temporal public key PK_{temp}. At the same time, they also symmetrically encrypt the other information such as N_i, PDO_{i-1} and dummy pad by the temporal session key K_i. The ARREQ route is showed as follows. We assume the node A is source node and node E is destination node. The following figure depicts the route flow.

The *PDO* means it is a path discovery onion, and the *PRO* means a path reverse onion. The details of *PDO* is described as follows:

$$\begin{aligned}
PDO_A &= \{E_{PK_{temp}}(K_A), E_{K_A}(N_A, ID_A, PK_A, PAD)\} \\
PDO_B &= \{E_{PK_{temp}}(K_B), E_{K_B}(N_B, PDO_A, PAD)\} \\
PDO_C &= \{E_{PK_{temp}}(K_C), E_{K_C}(N_C, PDO_B, PAD)\} \\
PDO_D &= \{E_{PK_{temp}}(K_D), E_{K_D}(N_D, PDO_C, PAD)\}
\end{aligned}$$

When node i receives the ARREQ packet, it processes as following steps:

(1) It checks whether the $SEQNUM_{tagt}$ is the first time to be received. It will drop the packet if it has received previously.
(2) It checks whether the $SEQNUM_{tagt}$ is stored in its shared_symmetric_key table. If yes the node is the destination node and will use SSK_{tagt} to decrypt the trapdoor TR_{tagt}.
(3) If the node is not intended destination node, then:

(a) Generates the randomly nonce and the session key (N_i and K_i) which can also be generated in advance;
(b) Encrypts the K_i using the temporal public key PK_{temp} and generates the new PDO_i by encrypting the N_i and PDO_{i-1} using K_i. To defend against the packet trace attack, it can pad the dummy message to the PDO_i;
(c) Broadcasts the new ARREQ packet to the neighbor nodes;
(d) Adds N_i and K_i to the route table which is described in following Table 3. The TIMER entry is used as overtime timer and will increase when the route entry is not used for a pre-defined period. When the timer expires, it will delete the corresponding row entry.

Table 3. Anonymous route table in the intermediate node

Communication sequence number	Temporal nonce	Temporal key	Timer
$SEQNUM_{tagt}$	N_i	K_i	$timer_i$
…	…	…	…

(4) If the node is the destination node, it will decrypt the trapdoor TR_{tagt} using symmetric key SSK_{tagt}, and extract ID_{tagt} and SK_{temp}. The ID_{tagt} is used to check the destination ID again. Then the receiver decrypts the PDO_i by private key SK_{temp} and gets the (K_i,N_i) information of all nodes en route which construct the complete anonymous route from source to destination. The whole route information is defined as PR_{route} which is $\{N_A, K_A, N_B, K_B, N_C, K_C, N_D, K_D\}$.

It is noted that there may exist multiple paths from source to destination node and the destination node can select the shortest path. The multi-path is also useful for anonymous security (Table 3).

ARREP Phase. The destination node will return the ARREP (anonymous route reply) packet after receiving the ARREQ. It sends ARREP packet on unicast mode which is different from the ARREQ broadcast mode. The destination node uses the whole route (K_i,N_i) to encrypt the PR_{route} information layer by layer as an onion, which is defined as PRO_i(path reverse onion). To prevent the adversary from detecting the route by tracing ARREP identifier, we use the same identifier as data payload to mix the ARREP packet into the data packet. To distinguish the ARREP from the true ADATA packet, we add RREP identifier in the each layer encryption.

The PRO_i flow is depicted as Fig. 1. The ARREP detail format is showed as follows:

$$
\begin{aligned}
&< ADATA,\ N_D,\ PRO_D,\ PAD > \\
PRO_D =& E_{K_D}(RREP,\ N_C,\ E_{K_B}(RREP,\ N_B,\ E_{K_B}(RREP,\ N_A,\ E_{K_A}(END,\ PRroute)))) \\
PRroute =& \{N_A, K_A, N_B, K_B, N_C, K_C, N_D, K_D\}
\end{aligned}
$$

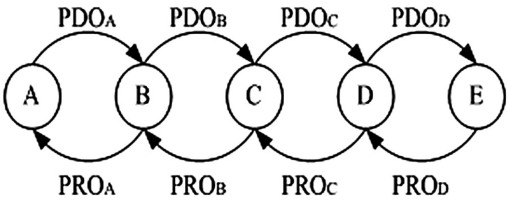

Fig. 1. Path discovery onion

PRO_D is the onion constructed by the destination node and encrypted symmetrically layered by the session key K_i corresponding to nodes en route. In the PRO_D, the RREP identifier represents the ARREP packet. When node D receives the ARREP packet, it checks whether N_D is exist in the anonymous route table. If yes it can peel off one layer by decrypting the PRO_D and get the next hop node's pseudo ID N_C. The *PAD* is dummy message which is used to prevent against the traffic analysis attack. Node D can also add new *PAD* to the new ARREP. The detail content is as follows:

$$<ADATA,\ N_C,\ PRO_C,\ PAD>$$
$$PRO_c = E_{k_c}(RREP, N_B, E_{k_B}(RREP, N_A, E_{k_B}(END, PRroute)))$$

The ARREP packet sent by node C is as follows:

$$<ADATA,\ N_B,\ PRO_B,\ PAD>$$
$$PRO_B = E_{K_B}(RREP, N_A, E_{K_A}(END, PRroute))$$

The ARREP packet sent by node B is as follows:

$$<ADATA,\ N_A,\ PRO_A,\ PAD>$$
$$PRO_A = E_{K_A}(END, PRroute)$$

At last the node A will get the ARREP packet according to N_A and decrypt the PRO_A. When it find the *END* identifier, it will know it is the destination of the packet and get the whole route information.

3.3 Anonymous Data Forwarding Phase

When source node, we assume node A, get the whole route, it can send data payload by using multi-layer encryption like TOR. To distinguish from the ARREP packet, we also introduce the PL identifier in the onion data (OD). The data packet format is described as follows:

$$<ADATA,\ N_i,\ OD_i>$$

It is mentioned that whether in the forward direction (from source to destination) or in the reverse direction (from destination to source) the sender should multi-layer encrypt the OD in advance. It is different from the TOR and AnonDSR method because they needn't multi-layer encryption in the reverse direction in advance. We describe the data flow from node A to node E as following Fig. 2:

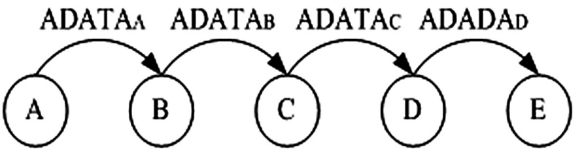

Fig. 2. Anonymous data forwarding

The data format in the different node is showed as follows:

$$ADATA_A = \{ADATA, N_B, OD_B = E_{K_B}(PL\_SIGN, N_C, OD_C), PAD\}$$
$$ADATA_B = \{ADATA, N_C, OD_C = E_{K_C}(PL\_SIGN, N_D, OD_D), PAD\}$$
$$ADATA_C = \{ADATA, N_D, OD_D = E_{K_D}(PL\_SIGN, N_E, OD_E), PAD\}$$
$$ADATA_D = \{ADATA, N_E, OD_E = E_{K_E}(PL\_END, data), PAD\}$$

The source node A firstly constructs the encrypted onion data as above and broadcasts the *ADATA* packets. The intermediate nodes check whether the N_i existed in its route table. If it is yes, it will decrypt the OD_i using the corresponding key in the route table. When the node see the *PL_SIGN* identifier, it will replace the N_i and OD_i with N_{i+1} and OD_{i+1} which are both extracted from the OD_i and construct the new $ADATA_{i+1}$. The process is repeated until the destination node receives the *PL_END* identifier.

4 Anonymity Achievement and Security Analysis

4.1 Identity Anonymity

During the symmetric key anonymous negotiation phase, we construct the trapdoor by using bilinear map and hash function. The adversary can't disclose the destination node ID with non-negligible probability. Meanwhile, the source node ID is replaced by the randomly pseudo public key and is also anonymous security.

During the anonymous route discovery phase, there are no node identity, including the source and the destination, exposed to the adversary due to the trapdoor information in ARREQ. The intermediate nodes identity is also protected by the onion encryption.

During the ARREP phase and the anonymous data forwarding phase, only the intermediate nodes' pseudo ID are exposed and ADATA packet is protected by the cryptographic onion method. So the identity anonymity is promised.

4.2 Location Anonymity

During the symmetric key anonymous negotiation phase, all packets are transferred on broadcast mode and the adversary can't locate the destination node and the source node by tracing the packet flow.

In the anonymous route discovery phase, the ARREQ is broadcast packet and the ARREP is hided in the ADATA flow. So the destination and source node are difficult to be located by tracing the ARREQ and ARREP packets.

The adversary may eavesdrop on ARREQ and ARREP packets and then deduce the distance from the source or the destination by checking the length of those packets. The method to address the problem is all packets can be padded to the same size.

4.3 Route Anonymity

During the route discovery phase, the packets are onion encrypted and their true IDs are replaced by the pseudo IDs. In addition, the discovery phase duration is not long. So it is difficult for adversary to find the route. We think the attack on the route anonymity always happen in the data forwarding phase. Of course, the adversary can't disclose the route from the packet content because the payload is onion encrypted by temporal public key.

However, the traffic analysis is a passive attack and hard to defend. One kind of traffic analysis is time analysis by monitoring the time of incoming packet and outgoing packet through some node. Refer to [9], we can buffer the incoming packet and send the buffered packet out of order. Moreover FASRP use CSMA/CD as MAC mechanism and the node may delay their packet transmission due to MAC channel collision. It also influences the time relationship between the incoming packets and outgoing packets. As a result, the adversary is difficult to find the route by timing analysis attack. The other kind of traffic analysis is packet length analysis which the adversary can trace the packet flow upon measuring the nodes input and output packet length. We introduce to pad dummy message to ADATA packet to change the packet length, and so the length information don't leak any information about packet flow.

4.4 Security Analysis

During the symmetric key anonymous negotiation phase, the trapdoor is based on bilinear map and the source node pseudo ID public key is generated in secret. So none adversary can decrypt the trapdoor and the source pseudo ID public key in polynomial time. In addition, the destination node can find whether the packet is modified by decrypting and checking the content.

S_INFO can also be helpful to resist the man-in-the-middle (MITM) attack. Although the attack can replace the pseudo public key of source ID and TR_{AB} in *SKN* packet by its own, the destination node can distinguish the forged packet by checking whether the *S_INFO* can be decrypted successfully because K_{AB} can't be forged.

During the route discovery phase, the communication sequence number and the shared symmetric key are only shared between the source and the node. And they are

also updated periodically, so it is difficult for adversary to decrypt the packet and can thwart against the replay attack. In the route discovery and data forwarding phase, the intermediate nodes only use their temporal nonce and the payload are onion encrypted in advance, the adversary can't intercept the true content including route information in the packets and change the packet content.

5 Performance Evaluation

In this section, we evaluate FASRP and compare its network performance with MANET routing protocols (AODV, DSR) through the simulation. The cryptographic processing overhead evaluated in simulation is based on the [4, 9] testing results. In our simulation, we use RSA-2048 as the public key cryptosystem, AES/Rijndael (128 bit key) as the symmetric key cryptosystem, and SHA-1(160 bit) as the hash function.

The simulation is conducted within NS-2. 50 mobile nodes are randomly distributed with 1000 m-by-500 m. CBR sessions are used to generate network data traffic. For each session, data packets of 512 bytes are generated in a rate of 2 packets per second. The nodes maxim moving speed is 20 m/s. The ticks on x-axis represent the node pause time. The simulation lasts 100 s (Figs. 3, 4 and 5).

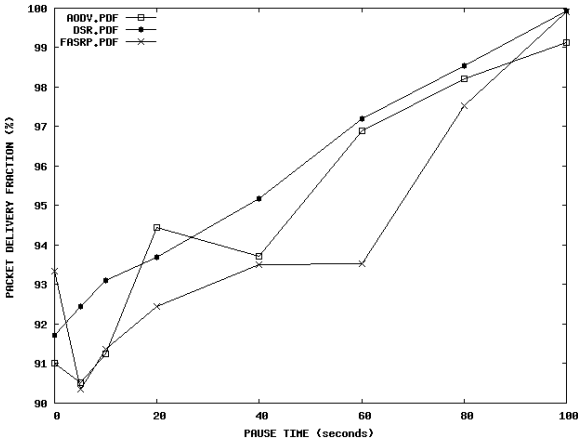

Fig. 3. Packet average delivery fraction (MAX CBR pair = 5)

The simulation results show that it is a trade-off between routing performance and anonymous security. To ensure the anonymous security, FASRP must introduce the excessive cryptographic process and lack all kinds of optimized process, which the DSR has, such as route cache, route packet snoop and Automatic Route Shortening.

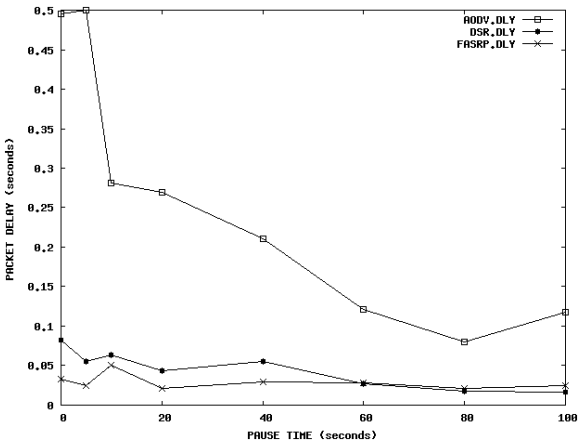

Fig. 4. Average end-to-end delay (MAX CBR pair = 5)

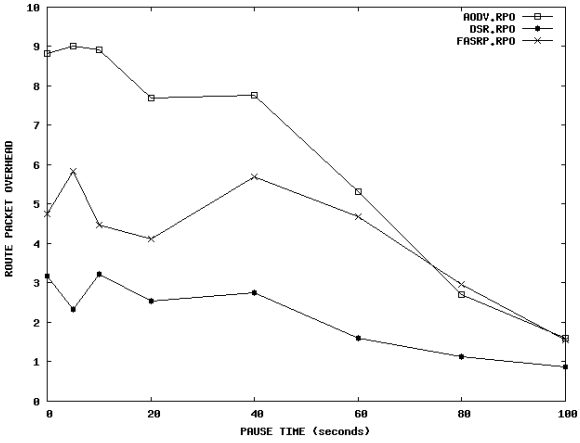

Fig. 5. Route pakcket overhead (MAX CBR pair = 5)

6 Conclusions

In order to provide an efficient, secure, and anonymous routing for MANETs in adversarial environments, we propose a novel protocol FASRP. It addresses the problems existing in other related anonymous routing protocols. Also we clarified the achievement of anonymity and security. FASRP ensures identity anonymity, location anonymity and route anonymity and strong against most known attacks. Meantime, FASRP can support multipath routing and unidirectional channel. This characteristic can strengthen the anonymous security and make FASRP more suitable for severe environment.

Acknowledgments. This research was supported in part by the National High Technology Research and Development Program of China (863 Program), SS2015AA011306.

References

1. Kong, J., Hong, X.: ANODR: anonymous on-demand routing with untraceable routes for mobile ad-hoc networks. In: Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003), pp. 291–302 (2003)
2. Zhu, B., Wan, Z., Kankanhalli, M.S., Bao, F., Deng, R.H.: Anonymous secure routing in mobile ad-hoc networks. In: Proceedings of the 29th IEEE International Conference on Local Computer Networks (LCN 2004), Tampa, USA, pp. 102–108, November 2004
3. Zhang, Y., Liu, W., Lou, W.: Anonymous communications in mobile ad hoc networks. In: Proceedings of the 24th International Conference of the IEEE Communications Society (INFOCOM 2005). IEEE (2005)
4. Song, R., Korba, L., Yee, G.: AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks. In: ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN) (2005)
5. El-Khatib, K., Korba, L., Song, R., Yee, G.: Secure dynamic distributed routing algorithm for ad hoc wireless networks. In: Proceedings of ICPP Workshops, Kaohsiung, Taiwan, October 2003
6. Perkins, C., Belding-Royer, E., Das, S.: Ad hoc on-demand distance vector (AODV) routing, RFC 3561, July 2003
7. Johnson, D.B., Maltz, D.A., Hu, Y.: The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), April 2003. http://draft-ietf-manet-dsr-09.txt
8. Dingledine, R., Mathewson, N., Syverson, P.: Tor: the second-generation onion router. In Proceedings of the 13th USENIX Security Symposium, August 2004
9. Jiejun, K., Xiaoyan, H., Gerla, M.: An identity-free and on-demand routing scheme against anonymity threats in mobile ad hoc networks. IEEE Trans. Mob. Comput. **6**(8), 888–902 (2007)
10. D. Boneh and M. Franklin. Identify-based Encryption from The Weil Pairing. In: Proceedings of CRYPTO 2001, Springer-Verlag (2001)
11. Wu, X., Bhargava, B.: AO2P: ad hoc on-demand position-based private routing protocol. IEEE Trans. Mobile Comput. **4**(4), 335–348 (2005)
12. Defrawy, K.E., Tsudik, G.: Privacy-preserving location-based on demand routing in MANETs. IEEE J. Sel. Areas Commun. **29**(10), 1926–1934 (2011)
13. Shen, H., Zhao, L.: ALERT: an anonymous location-based efficient routing protocol in MANETs. IEEE Trans. Mob. Comput. **12**(6), 1079–1093 (2013)
14. Liu, W., Yu, M.: AASR: authenticated anonymous secure routing for MANETs in adversarial environments. IEEE Trans. Vehicular Tech. **63**(9), 4585–4593 (2014)