International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.229-240
http://dx.doi.org/10.14257/ijsia.2016.10.4.22

Anonymous Routing Protocols for Mobile Ad-Hoc Networks

Tianbo Lu, Hao Chen, Lingling Zhao, Yang Li

School of Software Engineering, Beijing University of Posts and Telecommunications, 100876, Beijing, China
lutb@bupt.edu.cn, 475227473@bupt.edu.cn

Abstract

Nowadays, with the development of mobile ad hoc networks (MANETs), it attracts more attention by researchers. MANETs not only can be used for military application, but also can be used for citizens. For military, MANETs works in hostile environments with lacking of infrastructure. And for civil application, MANETs show their power in many way like communication between cars or self-construct temporary network consist of laptops. Meanwhile, more research focus on the anonymity and security of MANETs. To meet those requirements, many routing protocols were proposed to ensure the goal of anonymity and security. This paper introduce several anonymous routing protocols for MANETs, and classify those protocols into two parts: On-Demand Anonymous routing protocols and None On-Demand Anonymous routing protocols. Besides, this paper compares the differences between those protocols.

Keywords*: MANETs, Anonymity, Security*

1. Introduction

Ad Hoc Network is evolved from Packet Radio Network. DARPA (Defense Advanced Research Project Agency) of America began the project of Packet Radio Network at 1972. In the year of 1983, SURAN (Survivable Adaptive Network) project was started to continue the research of Packet Radio Network. At 1991, IEEE 802.11 decided to use Ad Hoc Network to express this kind of network.

Mobile Ad Hoc Network, which called MANET, is the Ad Hoc network consisted by mobile devices. MANETs is a self-configuring and self-organized network without fixed infrastructure. Any node of MANETs can join the network any time and leave whenever they want. The information that one node sends only can be received by the neighbor nodes. It lead that nodes not only play as roles of user, but also play as roles of router [13]. In general, there is no center nodes in MANETs, so that MANETs have a good robustness.

MANETs have wide range of applications. For example, in battlefield, MANETs can be used to send message even in hostile environments. And after terrible disaster like earthquake and flood, MANETs do his job costing little time without preparation of infrastructure. For personal use, MANETs can link our devices like laptops, pads and smart phones. And for inter-vehicular communication, it is also widely used cause the feature of mobile.

Up to now, the major applications of MANETs on military work in hostile environments so the anonymity and security are firstly concerned. And even for personal use, users may not want others know what he did or who he is communicating with. All of those requirements encourage the research of anonymity in MANETs that many routing protocol proposed to achieve.

We will discuss protocols including ANODR, MASK, Discount-ANODR, HANOR, AO2P, AODPR, RAODR, SDAR, AR3P, ASR, ASRPAKE and ASC. In follow section, we will discuss the classification of those protocols.

ISSN: 1738-9976 IJSIA

2. Classification of Anonymous Routing Protocols

Until now, there is not a classification of anonymous routing protocols that widely accepted. To introduce those protocols that will be discussed in a logical order and show the features of them, we use two ways to classify them.

The first way to classify them is based on what they propose for. Most of them designed for flat network environments, except HANOR and RAODR. HANOR is proposed for hierarchical mobile ad hoc network environments. And RAODR is proposed for both flat and hierarchical environments.

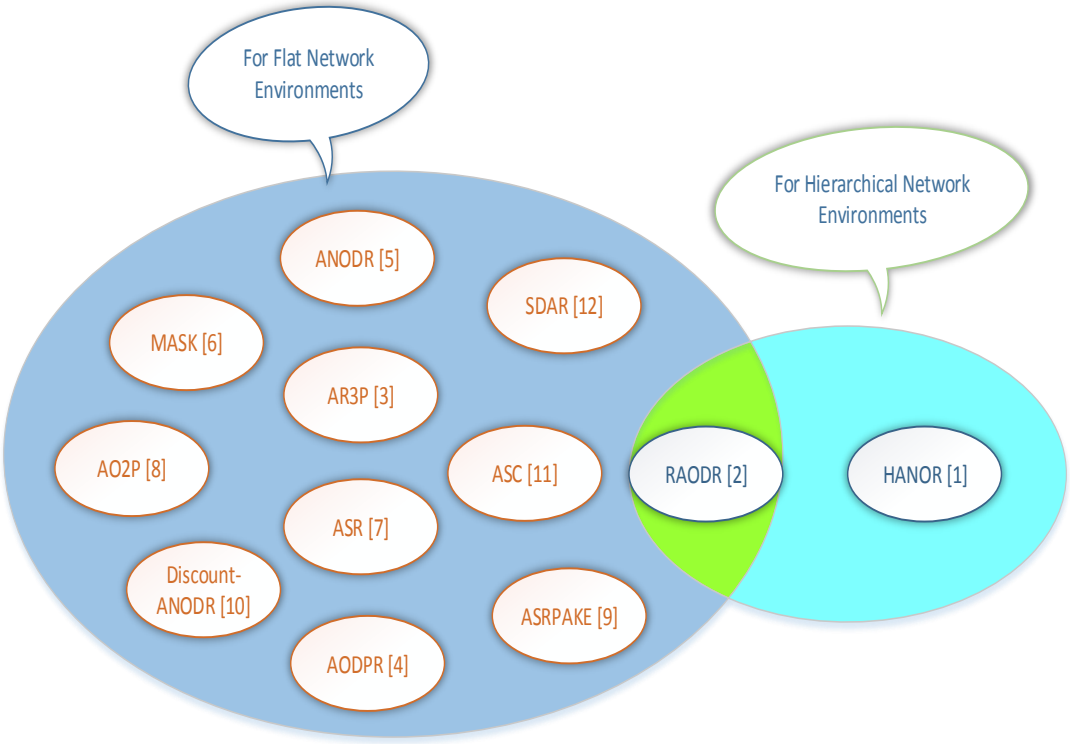

Figure 1. Classification by Flat or Hierarchical

Another way to classify protocols is by on-demand or none on-demand. The protocols that typical based on on-demand include ANODR, MASK, AO2P, HANOR, Discount-ANODR, AODPR, and RAODR. The rest of protocols include SDAR, ASR, ASC, ASRPAKE and A3RP, they are classified as none on-demand anonymous routing protocols. We use the figure as follows to show the relationship between them.

In this article, we use on-demand or none on-demand to classify those protocols. And follow sections introduce those protocols by this classification.

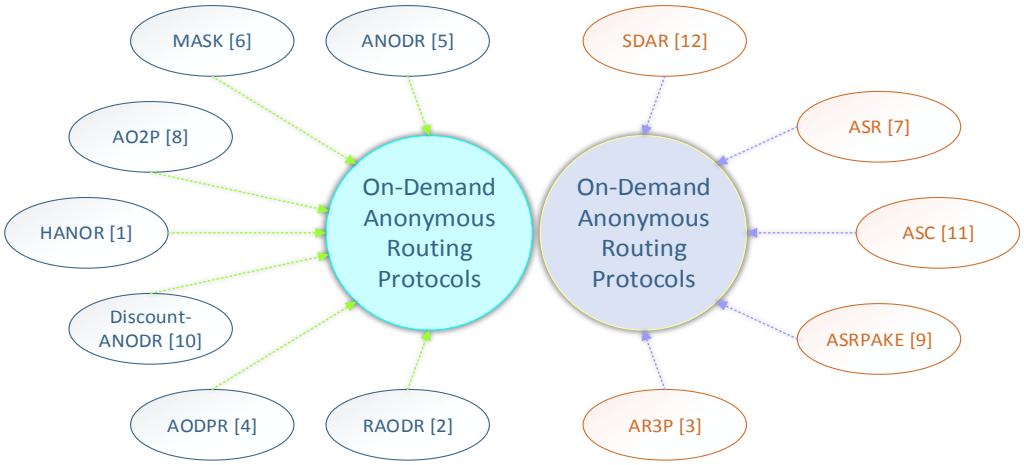

Figure 2. Classification by On-Demand or None On-Demand

3. On-Demand Anonymous Routing Protocols

Follow section we make a brief introduction of on-demand anonymous routing protocols. The follow figure shows all on-demand anonymous routing protocols we will mention. We order those protocols by the time they proposed. We also show the proposers and their universities or research institutions where they propose those protocols. As we can see, after ANODR which presented at 2003, researchers take more attentions on anonymous routing protocols.

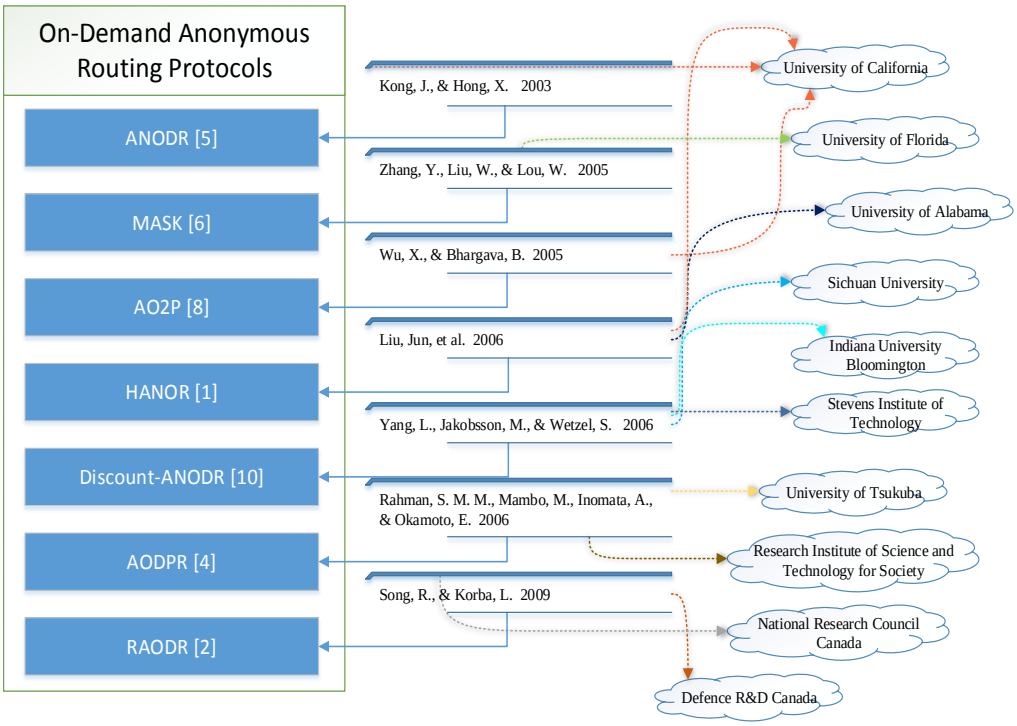

Figure 3. On-Demand Anonymous Routing Protocols

3.1 ANODR

ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks, is developed by Jiejun Kong, Xiaoyan Hong in Computer Science Department of University

of California. The main purpose of ANODR is to be used in the situation that the security and anonymity are taken seriously consideration. ANODR focus on untraceable routes. It means ANODR try to limit the track of the packet flow back to the source node when anonymity is considered. For secure consideration, ANODR hides the relationship between the transmitter and the true identity of it [5].

The routing process is divided into two parts by ANODR. The first part is anonymous route discovery and second part is anonymous route maintenance.

In the part of anonymous route discovery, source node generate RDRQ (Route Discovery Request Packet) and the then broadcast this packet over the network. The RREQ packet include the parameters include globally unique sequence number, cryptographic trapdoor, cryptographic onion and so on. The designer use three variants to explain the design. The best variant is ANODR-TBO which uses trapdoor boomerang onions (TBO) [5]. This protocol is described as flow steps.

First, any intermediate node will embeds a random nonce NX to the boomerang onion and encrypts the result with a random symmetric key Kx. The trapdoor information is only known by X. After destination node turns back boomerang onion by RREP (Route Discovery Reply Packet), only the corresponded next hop known the trapdoor. And the node decrypt the RREP so that the next hop can continue to deliver the RREP. For anonymous data forwarding, any node who send the packet, it use outgoing route pseudonym in its forwarding table and broadcast the packet. Node throw away the packet if the pseudonym of destination isn't in its forwarding table or changes the route pseudonym to the matched outgoing pseudonym if it find.

For the part of anonymous route maintenance, it describes a situation that one or more hop had been broken. A node look up for other route pseudonym N which is associated with the broken hop. If a node find the N node, it should continue to find the matched N' and follow the same step.

ANODR have the advantage to against adversaries and such as omnipresent eavesdroppers. So it is useful in hostile environments. Furthermore, ANODR combine the broadcast of the network security and trapdoor information of the information security.

3.2 MASK

MASK is an anonymous on-demand routing protocol. It is developed by Yanchao Zhang, Wei Liu and Wenjing Lout from department of Electrical and Computer Engineering of University of Florida. MASK aim to operate against traffic analysis attacks.

MASK use pairing-based cryptography as the cryptographic foundation. The anonymity of MASK consist of two parts. One part of it is anonymous MAC-Layer communications while the other part is anonymous network-layer communications [15].

The anonymous MAC-layer communications discuss how to achieve anonymous single-hop MAC-layer communications through an anonymous neighborhood authentication protocol [6]. It is basic according to anonymous neighborhood authentication and anonymous MAC frame exchange.

In the part of anonymous network-layer communications, there are two subdivision including anonymous route discovery and anonymous packet forwarding. Anonymous route discovery may be same with other on-demand protocol. For anonymous packet forwarding, by looking up in the forwarding route table, the source picks a random LinkID from the next-LinkID-list field in the entry for the destination [6]. Packet then will send to the neighbor node witch shares the chosen LinkID.

MASK provide strong sender and receiver anonymity, the relationship anonymity between senders and receivers [6]. And MASK can thwart against traffic analysis attacks.

3.3 AO2P

Xiaoxin Wu and Bharat Bhargava propose Ad Hoc On-Demand Position-Based Private Routing Protocol (AO2P). AO2P is proposed for communication anonymity in ad hoc network. It works in the network with relatively high node densities [8].

The author of AO2P propose a virtual home region (VHR)-based [14] distributed secure position service, named DISPOSER. In this scheme, nodes gets their geographic position by GPS. DISPOSER guarantee security of position information of nodes. Furthermore, receiver classification scheme and receiver contention scheme are used to provide efficient route discovery. AO2P with reference point (R-AO2P) is also proposed to improve destination anonymity and privacy. In simulation of AO2P, the delay of searching for next hop takes little time.

The routing performance is compared between GPSR and AO2P. AO2P only add a few number of hops in the routing process while GPSR need significant much more information of position of nodes. And AO2P improve anonymity without much deterioration on performance.

3.4 HANOR

HANOR (Hierarchical Anonymous On-Demand Routing protocol) is based on a hierarchical MANETs architecture with multi-hop clustering [1]. HANOR was raised by Jun Liu, Xiaoyan Hong, Jiejun Kongt, Qunwei Zheng, Ning Hu, Phillip G. Bradford. They came from the Department of Computer Science of University of Alabama and University of California. HANOR is developed to solve problems in MANETs with some traditional routing protocol. The most serious problem is the deterioration of anonymity and privacy of the MANETs. The cause of this problem is the inherence of the flat anonymous routing protocols. With the nodes increasing, the communication between nodes deteriorated. HANOR aim to reduce this situation.

In HANOR, there are two logical tiers [1]. The floor tier is a network of multi-hop clustering. And the ceiling tier is consist of leader nodes. The architecture of the network can be configured previous or self-configured. If the network isn't pre-configured, they assume to use a algorithm to select the leader node.

Certificate authority (CA) infrastructures which are distributed among the networks decide the public key and private key of every node before nodes join the network. Each group will have a pair of asymmetric keys and the group ID is derived from this keys by the group leaders. A new node receive parameters include its ID, a pool of public/private key pairs PKTn/SKTn, PKCA, and the election algorithm with parameters if needed [1].

HANOR's anonymous routing is consisted by intra-group anonymous routing and inter-group anonymous routing. The first step of intra-group anonymous routing is that the source node try to find an anonymous route to the leader node of its group. And then route to the destination group while the leader of destination group building an anonymous route towards the destination node. Inter-group routing is established by the source group leader and destination group leader.

Authors of this paper use a simulation to test the HANOR. Compare with ANODR, with the size of MANETs grow up, path length of ANODR grows accordingly. Meanwhile, the hop numbers of HANOR inside the group nearly remain the same. And the public key operations of HANOR is obviously less than ANODR. The cause is the less receivers of the RREP due to the use of group scheme. And the group member don't need to decrypt GRREP. As the paper says, the main advantage of HANOR is that it effectively controls computational overhead using the hierarchical routing scheme and preserves routing anonymity [1].

3.5 Discount-ANODR

Discount-ANODR is developed to reduce the computation and communication complexities in the ANODR by Liu Yang, Markus Jakobsson and Susanne Wetzel. The main purpose of Discount-ANODR is to make MANETs lighter and more anonymous [10].

Compared with ANODR, the main difference between Discount-ANODR and ANODR is the different type of key operations. Discount-ANODR only uses symmetric key operations. And every time a route is found, it will be saved into the route cache to reuse. The mainly Superiority of Discount-ANODR is that it is a lightweight protocol. Besides this, it remains anonymity and security.

3.6 AODPR

An anonymous on-demand position-based routing (AODPR) in mobile ad hoc networks is proposed by Sk. Md. Mizanur Rahman, Masahiro MAMBO, Eiji OKAMOTO from Graduate School of Systems and information Engineering of University of Tsukuba and Atsuo INOMATA Japan Science and Technology agency, Research Institute of Science and Technology for Society.

For AODPR routing algorithm, the most important parts are position management and control packets. Position management scheme, which called virtual home region-based DIstributed Secure POsition SERvice (DISPOSER), is used for AODPR [4]. In this scheme, nodes know their position via Global Positioning System (GPS) and report position information to the position servers which keep security of those information. Another significant part is control packets. Route Request Packet (RRQ), Route Reply Packet (RRP) and Fail Packet (Fail) are used for routing discovery of AODPR.

Compare to other protocol, ANOPR not only achieve identity privacy, location privacy, routing anonymity that other anonymous provided, but also defend from wormhole attacks and DoS. In conclusion, AODPR ensure security and anonymity and preventing the target-oriented attack [4].

3.7 RAODR

Ronggong Song from Defence R&D Canada and Larry Korba from National Research Council Canada propose RAODR (Robust Anonymous ad hoc On Demand Routing). It's a new routing protocol aim to providing better security and anonymity protection and working on both hierarchical and flat ad hoc network topologies [2].

RAODR can operate well even in hostile military environment, and solve problems including security, anonymity, scalability, route maintenance. It use an anonymous neighborhood trust model to guarantee security and anonymity [2]. In this model, nodes can authenticate their neighboring nodes without reveal their identities and organization information.

Compare to other anonymous routing protocol, RAODR has several advantages. Compare with ANODR, RAODR provide protection for the data transfer. Besides, compare with HANOR witch is a protocol only for hierarchical ad hoc network environments, RAODR is designed for hierarchical and flat network environments. In the aspect of intrude node detection, RAODR also have a well performance while MASK can't detect intrude nodes effective if nodes use multi- pseudonym.

4. None On-Demand Anonymous Routing Protocols

In this section, we will discuss none on-demand anonymous routing protocols. Those protocols include SDAR, ASR, ASC, ASRPAKE and A3RP. None on-demand means that they are not based on on-demand routing protocols. The follow

figure shows the order of those protocols by the time they proposed. Besides, universities and research institutions are also mentioned.

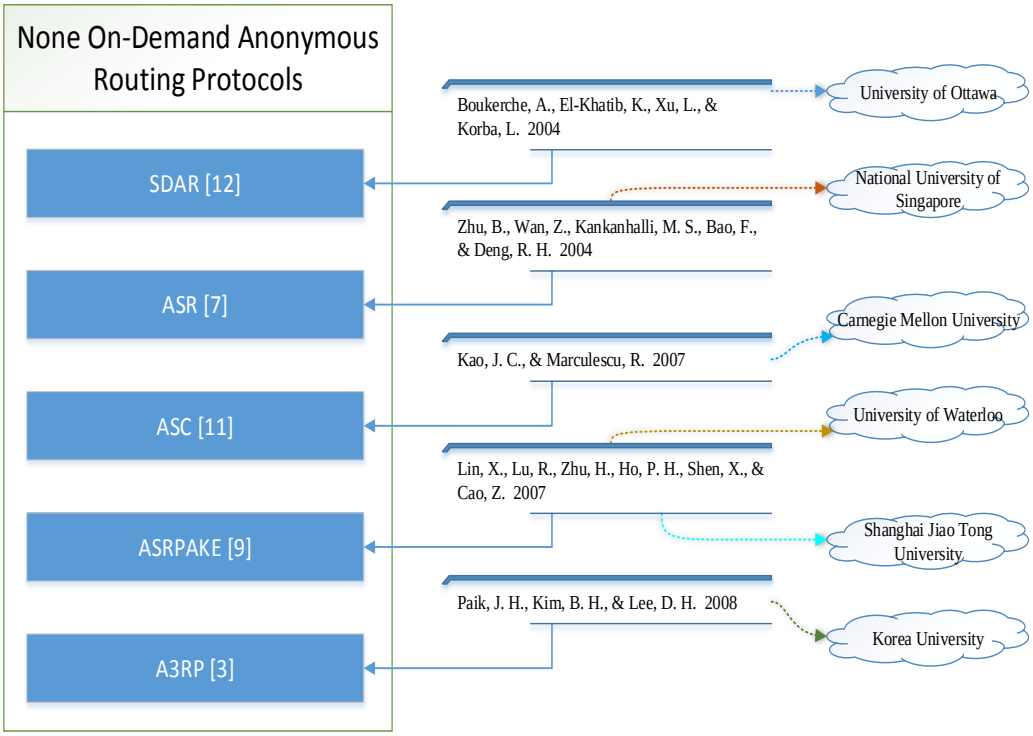

Figure 4. None On-Demand Anonymous Routing Protocols

4.1 SDAR

SDAR (Secure Distributed Anonymous Routing Protocol) is designed by Azzedine Boukerche, Khalil El-Khatib, Li Xu and Larry Korba from University of Ottawa. SDAR is protocols that ensure security, privacy and the safety while work in a hostile environments [12].

SDAR have three main feather including Non-Source-Based Routing, No Source Control over Route Length and Resilience against Path Hijacking [12].

For Non-Source-Based Routing, that means in SDAR, nodes don't need to know the topology and state of the network before send message. SDAR rely on path discovery and path reverse messages to deliver the message. No Source Control over Route Length maybe the bad dimension. It can't control the number of nodes in the path. At last, SDAR use a smart way to against path hijacking. The protocol wouldn't stop till a path reverse message sent by an intended receiver. So malicious nodes can't sent forward message to another malicious nodes.

SDAR deliver messages by selected trust neighbors. It first proposes the definition of trust node.

4.2 ASR

Anonymous Secure Routing (ASR) protocol is proposed by Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng from School of Computing National University of Singapore. ASR aim to provide more security and anonymity compared to other protocol [7].

The author of ASR notice that many protocol concern about security while anonymity seems not that important. So they define more strict requirements on the anonymity and security properties of the routing protocol in mobile ad-hoc networks in the paper about

ASR. To ensure security, ASR provides identity privacy, location privacy and route anonymity [7]. The identity privacy ensure that no nodes know the identity of sender and receiver except themselves and even the sender and receiver don't know the identity of intermediate nodes. Location privacy means that nodes not only don't know the identity of other nodes like above, but also don't know the location, the distance between nodes and other information about position. Route anonymity guarantee that no one can track a packet flow to find the source or destination. Besides, ASR defends from several attacks, for example, attacks on Route Maintenance, to ensure security.

Compare to ANODR and SDDR, ASR provides identity anonymity and gives strong location privacy. And ASR combined both protection and anonymity while other anonymous protocols not have e well behavior. The most important point is that ASR meet all the strict requirements of security and anonymity.

4.3 ASC

Anonymous Symmetrically Cryptographic (ASC) routing protocol is proposed by Jung-Chun Kao and Radu Marculescu from Carnegie Mellon University. ASC is based-on symmetric cryptosystem to improve performance compare to protocols that use asymmetric cryptography [11].

Asymmetric cryptography is good enough but still have several problems and the most important one is the consumption on computation. ASC uses typically symmetric cryptosystem and brings a 4 order of magnitude speed up. ASC use adaptive transmission power scheme for security. Besides, path encryption witch based-on symmetric cryptosystem gives anonymity for message transmission. Each intermediate node shuffles the payload and the header of a packet by using link encryption and virtual circuit identifiers and those behavior don't cost too much resource [11]. The above measures ensure anonymity and help defense from attackers. Benefit from the using of symmetric cryptosystem, those measures need little computation.

Compare with ANODR, ASC have a low delay of average end-to-end packet transmission. And with the increase of nodes in the MANETs, the speed of data delivering of ASC decrease slowly. Compare with AO2P, when total traffic injection at a high rate, ASC's performance is better than AO2P that ASC is more likely to send message successfully.

4.4 ASRPAKE

Xiaodong Lin, Haojin Zhu, Pin-Han Ho, Xuemin (Sherman) Shen from Department of Electrical and Computer Engineering of University of Waterloo and Rongxing Lu, Zhenfu Cao from Department of Computer Science and Engineering of Shanghai Jiao Tong University propose an Anonymous Secure Routing Protocol with Authenticated Key Exchange (ASRPAKE) for mobile ad hoc networks [9].

ASRPAKE provides anonymity for the node on routing path and use authenticated key exchange mechanisms. To complete authenticated key exchange, an efficient ring signature scheme based on Elliptic Curve Cryptosystem (ECC) is applied witch provide anonymity to all group members. ASRPAKE consist by five phrase including key pre-distribution phase, the neighborhood discovery phase, the route discovery phase, the route reverse phase, and the data forwarding phase [9]. And a DECOY mechanism is prepared for snare attacks to protect very important node (VIN) from lure of adversaries.

ASRPAKE can maintain end-to-end anonymity and ensure the security of session key. Besides, DECOY mechanism is a useful way to protect VIN from snare attacks.

4.5 A3RP

Anonymous and Authenticated Ad Hoc Routing Protocol (AR3P) is proposed by Jung Ha Paik, Bum Han Kim, Dong Hoon Lee from Graduate School of Information

Management and Security Korea University. The author think that the anonymity ad hoc protocol provided including entity anonymity, route anonymity, location/topology anonymity. Although many protocols provide those anonymity, not many of them do job for authentication. AR3P provides not only anonymity but also authentication in ad hoc routing [3].

Authentication is important for ad hoc network. Without authentication, adversaries can send illegal information or do things without enough limitation such as exhausting network resource by overload on the network broadcasts route request packets. The authentication is based-on group signature scheme witch consist by three parts including group public key, group secret key and group master key in AR3P.

Compare to ANODR, ASRP and ODAR, AR3P provide authentication that none of above protocol have. And AR3P resist DoS attack effectively. Besides, this protocol establishes the secret session key between the source and destination after path discovery [3].

5. Conclusion

	Entity&Aoute Anonymity	Location/ Topology Anonymity	Symmetric	Asymmetric	DoS	Traffic Analysis
ANODR [5]	○	x	○	○	x	○
MASK [6]	○	x	○	x	x	○
AO2P [8]	○	○	○	○	x	x
HANOR [1]	○	x	○	○	x	x
Discount-ANODR [10]	○	○	○	x	x	x
AODPR [4]	○	○	○	x	○	○
RAODR [2]	○	○	○	x	○	○
SDAR [12]	○	x	○	○	x	○
ASR [7]	○	x	○	○	○	○
ASC [11]	○	x	○	x	x	○
ASRPAKE [9]	○	x	○	x	x	x
AR3P [3]	○	○	○	x	○	x

Figure 5. Comparison between Anonymous Routing Protocols

The above of this article introduce 12 protocols including 7 on-demand anonymous routing protocols and 5 none on-demand routing protocols. With the research of anonymous routing protocols, researcher try to improve performance of protocols for anonymity, security, attack defense and efficiency.

As we can see in the table, not any protocols is perfect. The improvement of anonymity and security will cost much computation resource and that lead to a decrease of efficiency. Besides, different cryptosystems also cause the difference of efficiency between protocols. Symmetric cryptosystems needs less computation for encryption or decryption compare to asymmetric cryptosystems. But what paid is the security and anonymity. Not all of the protocols use asymmetric cryptosystems. And attacks defense is

linked with anonymity and security. Protecting protocol from adversaries eventually result in a better anonymity and security.

And we think that anonymity have a more important status compare with efficiency. For further study, more research will focus on better anonymity while less reduction on efficiency.

Acknowledgements

This work is supported by the following programs: the National Natural Science Found ation of China under Grant No.61170273; 2010 Information Security Program of China N ational Development and Reform Commission with the title “Testing Usability and Securi ty of Network Service Software”.

References

[1] L Jun, *et al*. "A hierarchical anonymous routing scheme for mobile ad-hoc networks." Military Communications Conference, 2006. MILCOM 2006. IEEE. IEEE, **(2006)**.
[2] S Ronggong, and L Korba. "A robust anonymous ad hoc on-demand routing." Military Communications Conference, 2009. MILCOM 2009. IEEE. IEEE, **(2009)**.
[3] P Jung Ha, Bum Han Kim, and Dong Hoon Lee. "A3RP: anonymous and authenticated ad hoc routing protocol." Information Security and Assurance, 2008. ISA 2008. International Conference on. IEEE, **(2008)**.
[4] R Sk Md Mizanur, *et al.* "An anonymous on-demand position-based routing in mobile ad hoc networks." Applications and the Internet, 2006. SAINT 2006. International Symposium on. IEEE, **(2006)**.
[5] K Jiejun, and Xiaoyan Hong. "ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks." Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing. ACM, **(2003)**.
[6] Z Yanchao, W Liu, and Wenjing Lou. "Anonymous communications in mobile ad hoc networks." INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. Vol. 3. IEEE, **(2005)**.
[7] Z, Bo, *et al*. "Anonymous secure routing in mobile ad-hoc networks." Local Computer Networks, 2004. 29th Annual IEEE International Conference on. IEEE, **(2004)**.
[8] W Xiaoxin and Bharat Bhargava. "Ao2p: Ad hoc on-demand position-based private routing protocol." Mobile Computing, IEEE Transactions on 4.4, **(2005)**,pp. 335-348.
[9] L Xiaodong, *et al*. "ASRPAKE: An anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks." Communications, 2007. ICC'07. IEEE International Conference on. IEEE, **(2007)**.
[10] Y Liu, Markus Jakobsson, and Susanne Wetzel. "Discount anonymous on demand routing for mobile ad hoc networks." Securecomm and Workshops, 2006. IEEE, 2006.
[11] K Jung-Chun and R Marculescu. "Real-time anonymous routing for mobile ad hoc networks." Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE. IEEE,**(2007).**
[12] B, Azzedine, *et al.* "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks." Local Computer Networks, 2004. 29th Annual IEEE International Conference on. IEEE, **(2004)**.
[13] K Thomas and S Büettrich. "Wireless mesh networking." posted at Wireless DevCenter on Jan 22 **(2004)**, pp. 1-9.
[14] W Xiaoxin. "VPDS: Virtual home region based distributed position service in mobile ad hoc networks." Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on. IEEE, **(2005)**.
[15] Z Yanchao, W Liu, and WLou. "Anonymous communications in mobile ad hoc networks." INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. Vol. 3. IEEE, **(2005)**.

Authors

Tian-Bo Lu was born in Guizhou Province, China, 1977. He is an Associate professor in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information security and computer network.

Hao Chen was born in Anhui Province, China, 1993. He is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information and network security, anonymous communication.

Ling-Ling Zhao is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. Her technical interests include Cyber-Physical System and P2P network.

Yang Li was born in Hunan Province, China, 1978. He is a PhD and his technical interests include information security, distributed computing and P2P network.