Computing and Informatics, Vol. 24, 2005, 149–165

DESIGN QUALITY OF SECURITY SERVICE NEGOTIATION PROTOCOL

Z n Yo Xia n Wang

Departments of Computer Science
Nanjing University of Aeronautics and Astronautics
Nanjing 210016, P. R. China
e-mail: zhengyou_xia@yahoo.com

Y C n Jiang

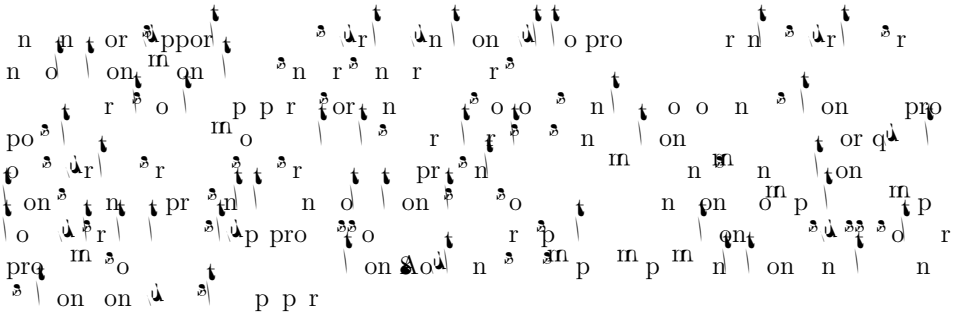
Departments of Computing and Information Technology
Fudan University, Shanghai 20043, China

Manuscript received 16 August 2004; revised 14 February 2005
Communicated by Ladislav Hluchý

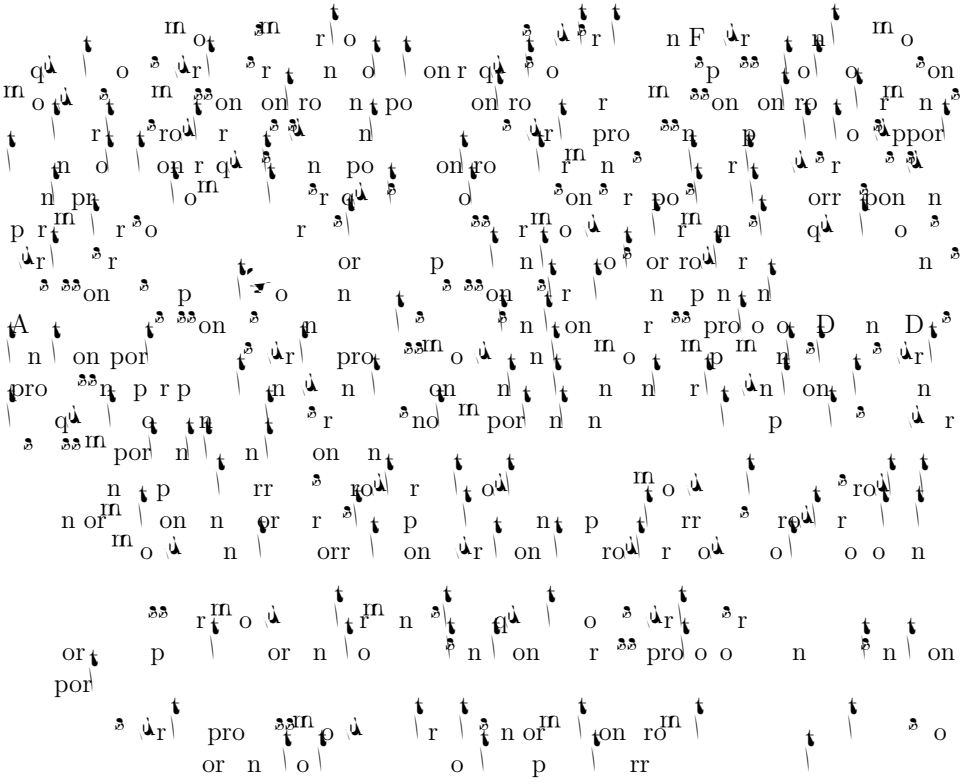
Abstract. With future network equipment the security service becomes a critical and serious problem. Especially in the network, users do not want to expose their message to others or to be forged by others. They make extensive use of cryptography and integrity algorithms to achieve security. The sender can achieve the high quality of security service ulnd securita(r)-5.15831(e-0.308961(v)5.15831(a)-1.80272())-387.

1 INTRODUCTION

Definition 1



2 SSRSVP MODEL



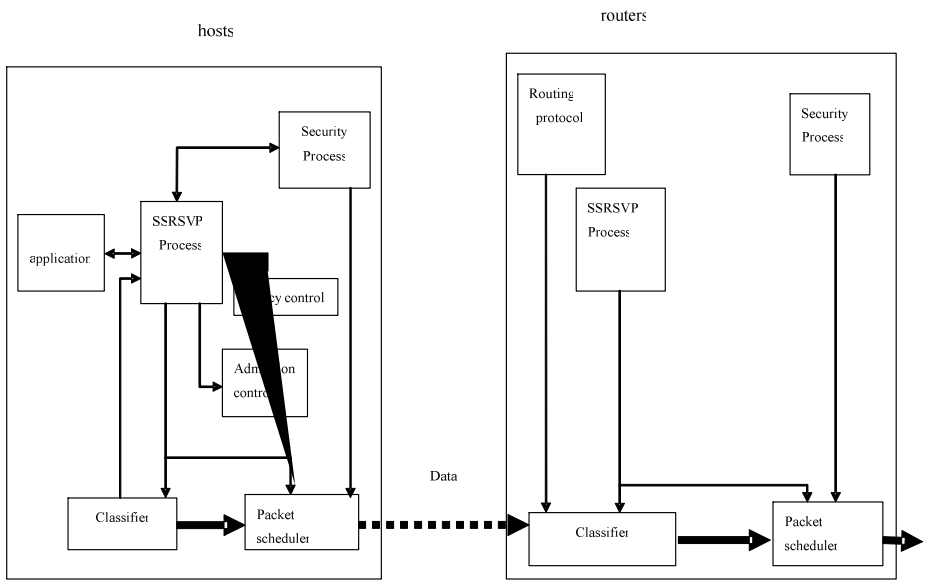
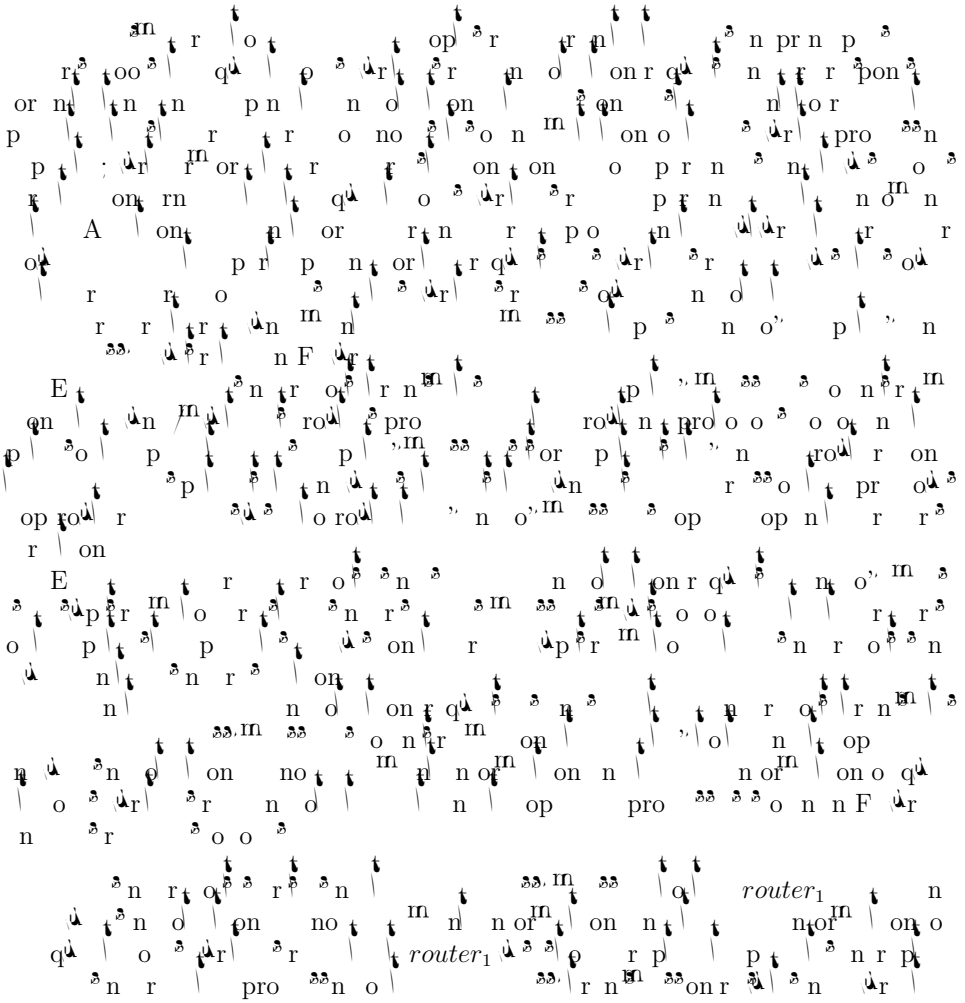


Figure 1 SSRSVP model in hosts and nodes

- — p Err
- — n oErr
- — r
- — n o r
- — n oCon
- —
- —
- —

4 SSRSVP MECHANISMS



F ,, r rn o n r o r o o n op r on r p r or

router$_1$ n , n n or on n n or on o q o r r *router*$_2$ o r p p n r p *router*$_1$ *router* n r n o *router*$_1$ r ro n r pro *router*$_2$ r rn F , o *router*$_1$ n n *router*$_1$ r rn F , o n r o pro o o n op r on r p r or

router$_3$ n r n rn , o r r r r rn , o *router*$_3$ n *router*$_3$ r rn , o *router*$_2$ n o on n n n r f n , n r n n o r n r on p , o r r

o o pro o , r n on n p p r r n n o n n r o r n r on K'' n n r p E$_K$ n n r o p o *router*$_1$ o n r p on K'' n n r p E$_{router_1}$ K, E$_K$ A n r pr o n r p n p n r p , n on E$_{sender}$ *timestamp*, E$_{router_1}$ K, E$_K$ n or r o *router*$_1$ o op r on , n r n *router*$_1$ n o r p

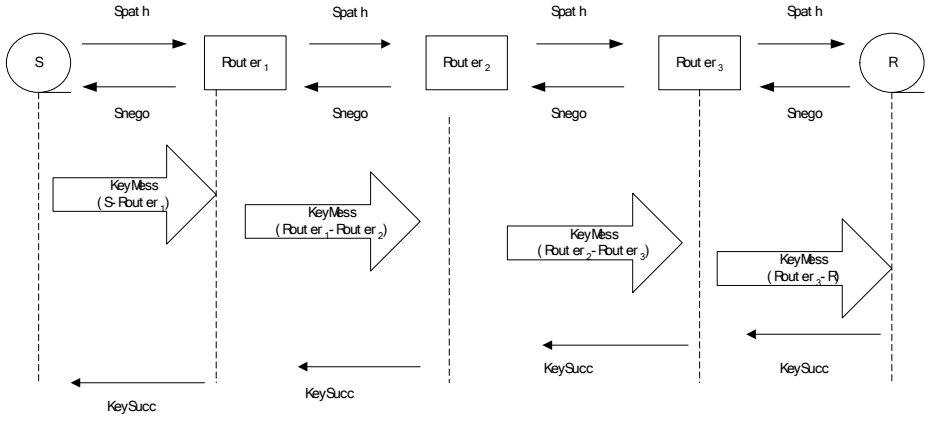
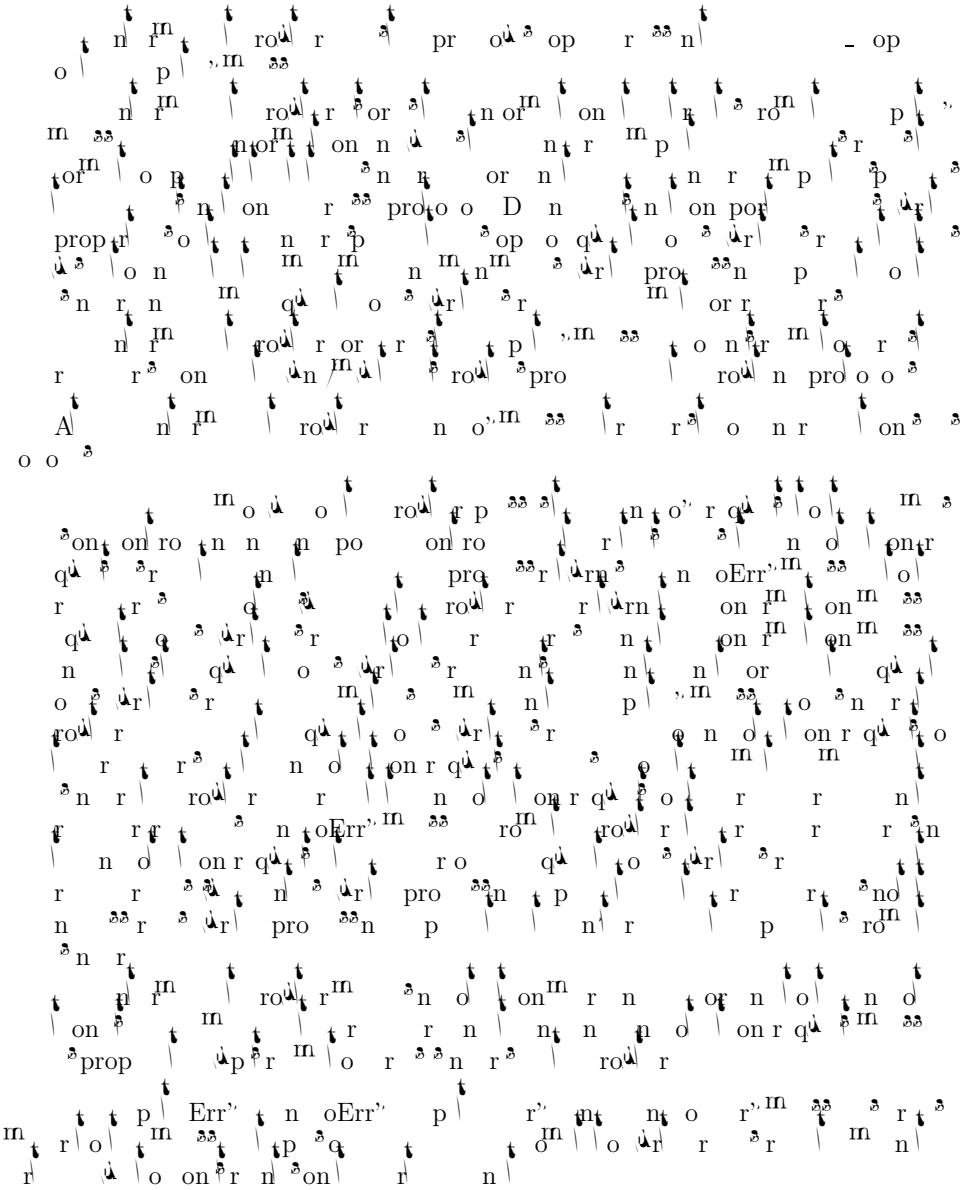


Fig. 3. SSRSVP mechanism

A n r m r o r p , r r r n r on o o o N o p , m p n on n po on ro o ro r



5 NEGOTIATION STYLE OF SSRSVP

r n on op n n or n r o m n on op n r n rr n
p r r q p r r no o
m n r r or n r n or r r o
p q o r r o n o on r q o m m
n r o r n r q

Des n ua ty of ecur ty erv ce Ne ot at on Protoco

cryptography and integrity algorithms	DES and MD5	3DES and MD5	1024 bits RSA and MD5	1024 bits RSA and SHA	2048 bits RSA and SHA
Quality of security service level	1S				

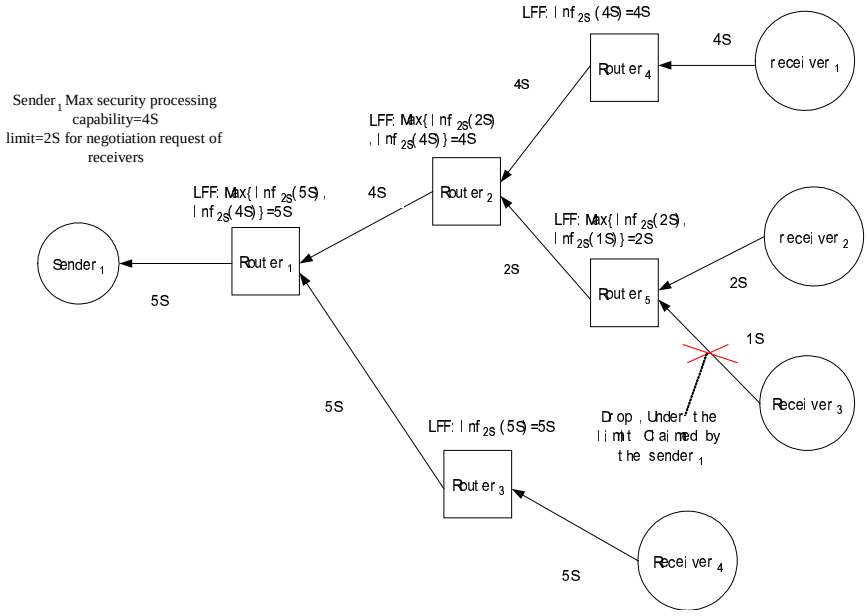


Fig. 6. One complete SSRSVP negotiation request example from one source node to the four different receiver nodes using LFF style

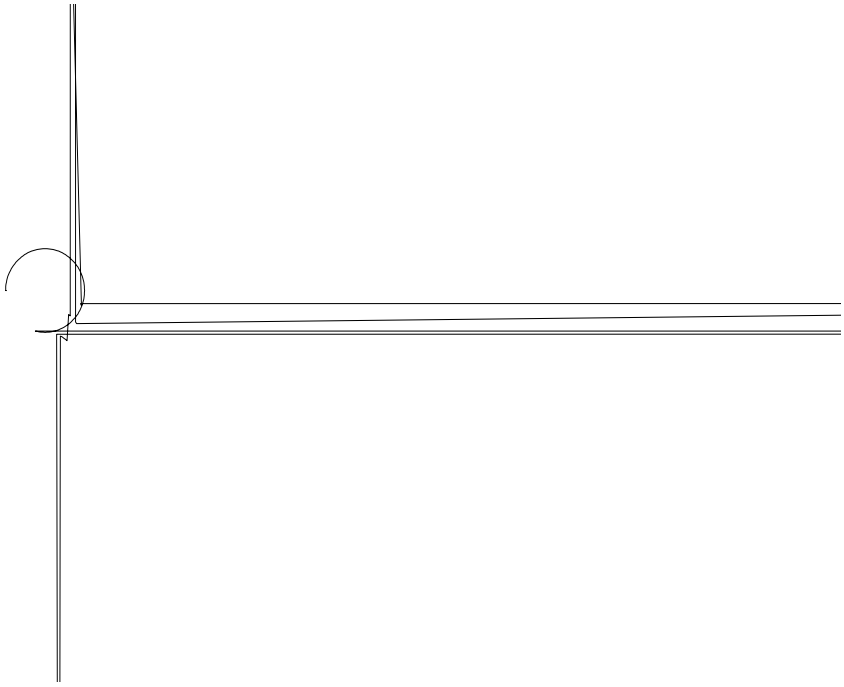
on o q o r r *router*1 o r p p n r p n r n o r r ro *sender*1 *router*1 n n o on no n or on n n or on o q o r *router*2 n *router*3 o r p p n r p *router*1 r p n o r r no r p m r r n F r n F r n FF n FF r p

7 DISCUSSION ABOUT SSRSVP

7.1 Tear, Error Message and Policy Control

r o n m r m o p or n o on mm r r o p o r o n p r n n o r A p r m r r r o r r o n r m ro po n o n on n p p n n o on on A n o r m n o on n r o r n r p r m ro po n o n on m r r r o rror m p Err n n oErr p Err m n p r m o n r r rror n o no n p n ro r o p


Sender$_1$



8 SIMPLE IMPLEMENTATION

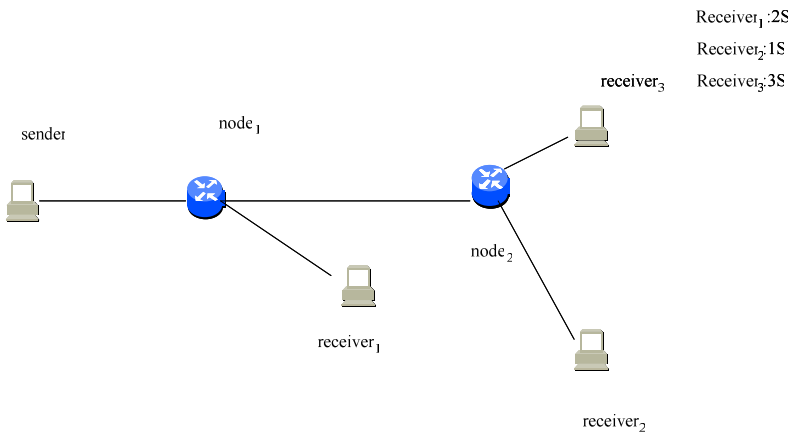


Fig. 9. Experiment paradigm

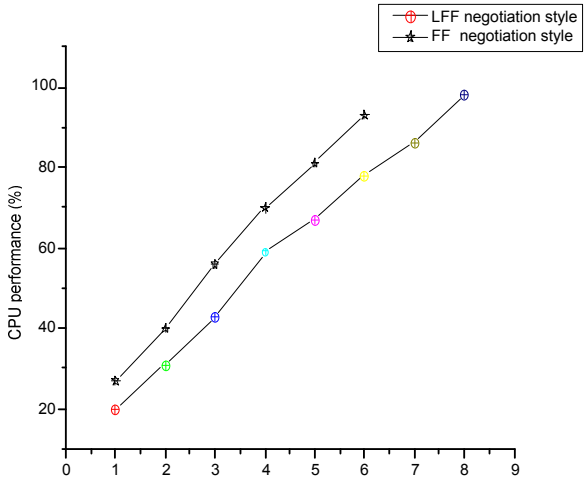


Fig. 10. Throughput out $node_2$ (M bytes/s)

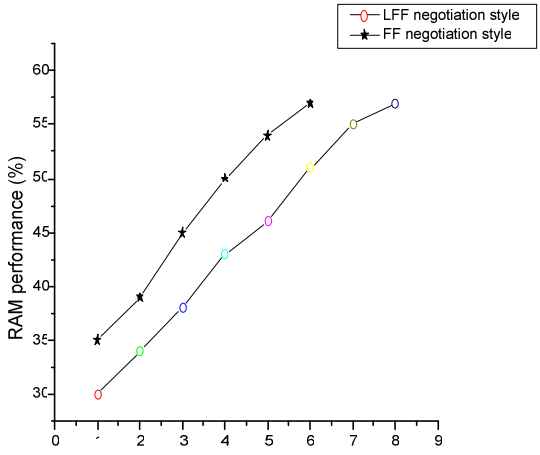


Fig. 11. Throughput out $node_2$ (M bytes/s)

9 SUMMARY

Acknowledgments

REFERENCES

[1] Zhang, L. et al.: RSVP: A New Resource Reservation Protocol. IEEE Network, Sept. 1993, pp. 8–18.

[2] Braden, R. et al.: Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification. RFC 2205, Sept. 1997.

[3] Braden, R.—Clark, D.–Shenker, S.: Integrated Services in the Internet Architecture: An Overview. RFC 1633, June 1994.

[4] Irvine, C.—Levin, T.: Quality of Security Service. Proc. of New security Paradigms workshop 2000, Cork, Irelanbd, September 2000.

[5] ANSI X3.106, American National Standard for Information Systems – Data Link Encryption. American National Standard Institute, 1983.

[6] Rivest, R. L.: The MD5 Message Digest Algorithm, RFC1321, Apr. 1992.

[7] Kenneth Castelino 3DES and Encryption, http://kingkong.me.berkeley.edu/~kenneth/courses/sims_,*0/des.html.

[8] Rivest, R. L. et al.: Amethod for Obtaining Digital Signatures and Public-Key Cryptosystems. Communication of the ACM, v21, n.2, Feb. 1978, pp. 120–126.

[9] Peterson, J.: Neustar, RFC 3323 – A Privacy Mechanism for the Session Initiation Protocol.

[10] Handley, M.—Jacobson, V.: SDP: Session Description Protocol. RFC 2327, April 1998.

[11] Cherkasova, L.—Phaal, P.: Session Based Admission Control: A Mechanism for Improving Performance of Commercial Web Service, http://citeseer.ist.psu.edu/cherkasova session.html.

[12] Arkko J.—Torvinen, V.—Niemi, A.—Haukka, T.: Security Mechanism Agreement for the Session Initiation Protocol. RFC 3329.

[13] RFC 2408, ISAKMP.

[14] Mittra, S.: A Framework for Scalable Secure Multicasting. ACM SIGCOMM '97, pp. 227–288, 1997.

[15] RFC 2747 – RSVP Cryptographic Authentication.

[16] RFC3097 RSVP Cryptographic Authentication – Updated Message Type Value.

[17] RFC 2207 – RSVP Extensions for IPSEC Data Flows.

ZhengYou Xia (born in 1974) is Associate Professor at Nanjing University of Aeronautics and Astronautics. He received Ph. D. degree in computer science of the Department of Computing and Information Technology, Fudan University, China. His research interests include mobile agent system, and network security.

Yichuan Jiang was born in 1975. He received his M.S. degree in computer science from Northern Jiaotong University, China in 2002. He is currently a Ph. D. candidate in computer science of the Department of Computing and Information Technology, Fudan University, China. His research interests include mobile agent system, artificial intelligence and network security.

Wang Jian, Associate Profesor, Ph. D., received the Ph. D. Eng. degree in October 1998 from the Department of Computer Science and Technology, Nanjing University. His present research interests include multicast security, key management, broadcast encryption, and sensor network.