### C. *The EPJRSA protocol can resist packet-injection*

The adversary end sets the rate of packet-loss zero-percent, and the rate of packet-injection forty-percent. Choose the EPJRSA protocol at the server and the client.

The result will be success, and the video can be played as **Figure 8**:


Figure 8. Packet-injection test on EPJRSA model

### D. *The EPJRSA protocol cannot resist packet-loss*

The adversary end sets the rate of packet-loss forty-percent, and the rate of packet-injection zero-percent. Choose the EPJRSA protocol at the server and the client.

The result will be failed, and the video can be played as **Figure 9**:


Figure 9. Packet-loss test on EPJRSA model

### E. *The Advanced EPJRSA protocol can resist packet-loss and packet-injection at the same time*

The adversary end sets the rate of packet-loss forty-percent, and the rate of packet-injection forty-percent. Choose the advanced EPJRSA protocol at the server and the client.

The result will be success, and the video can be played as **Figure 10**:


Figure 10. Packet loss and injection test on advanced EPJRSA model

## V. CONCLUSIONS

We use the advanced EPJRSA protocol to build up a video broadcast system. This system is made up of server, adversary end and client. The adversary end can stimulate the packet- loss and illegal attack while transferring. Comparing the advanced EPJRSA protocol with EPJRSA protocol, the result states that the system can resist the adversary's attack, do the real-time authentication of broadcast data source, and play the legal video. This also guarantees the correctness of video source and information and protect the benefit of both video servers and users.

## REFERENCES


[1] V Lehtovirta, F Lindholm, Security Key Management In IMS-Based Multimedia Broadcast And Multicast Services (MBMS) US Patent 20,120,027,211, 2012

[2] D Phan, D Pointchecal, M Strefler, Security notions for broadcast encryption, Ctyptography and Network Security, 2011-Springer

[3] Park Y, Cho Y. The eSAIDA stream authentication scheme[A]. Proceedings of ICCSA 2004[C]. Assisi, Italy, 2004. 799-807.

[4] Tang H, Zhu L H, Li J, Cao R Q, Efficient packet-injection resistant data source authentication protocol for group communication[J].Journal on Communications, Vol.29 No.11A, November 2008. Pp.96-100.

[5] Park J M, Chong E K P, Siegel H J. Efficient Multicast Packet Authentication Using Signature Amortization[A]. Proceedings of 23rd IEEE Symposium on Security and Privacy[C]. Oakland, California, USA, 2002. 227-240.

[6] Perrig A, Ganetti R, Tygar J, et al. Efficient authentication and signing of multicast streams over lossy channel[A]. Proceeding of 21st IEEE Symposium on Security and Privacy[C]. Berkeley, California, USA, 2000. 56-73.

[7] Wang C K, Chen A. Immediate data authentication for multicast resource constrained networks[A]. Proceedings of ACISP 2005[C]. Brisbane, Australia, 2005. 133-121.

[8] Liu D, Ning P. Broadcast authentication for distributed sensor networks[J]. ACM Transactions in Embedded Computing System, 2004. 3(4):800-836.

[9] Miner S, Staddon J. Graph-based authentication of digital streams[A]. Proceedings of 22nd IEEE Symposium on Security and Privacy[C]. Oakland, California, USA, 2001. 233-246.

[10] Challal Y, Bouabdallah A, Bettahar H. H2A: hybrid hash-chaining scheme for adaptive multicast source authentication of media-streaming[J]. Computer & Security, 2005. 24(1):57-68.

[11] Lysyanskaya A, Tamassia R, Triandopoulos N. Multicast authentication in fully adversary networks[A]. Proceedings of 24th IEEE Symposium on Security and Privacy[C]. Berkeley, CA, USA, 2003. 241-253.

[12] Bi H J, Wang J. New generation video compassion standard——H.264/AVG(The second edition) [M]. Beijing: The People's Posts and Telecommunications Press,2009.