National Journal of Advanced Research
Online ISSN: 2455-216X; Impact Factor: RJIF 3.42
www.allnationaljournal.com
Volume 2; Issue 2; March 2016; Page No. 47-50

Implementation of secure communication and authentication in multicast environment

Harshita

Asst. Professor, Department of CSE, ITM University, Gwalior, Madhya Pradesh, India

Abstract
Multicast establishes a group communication, where one sender can transmit the same message to multiple receivers. Multicasting makes this transmission efficient by making the client to send just one copy. But secure transmission in the multicast environment is a major issue it should maintain the authentication, non-repudiation and integrity of messages. For this we have created a multicast environment which ensures all these properties by applying digital signature for authentication by signing the messages by private key of sender and using more secure hash algorithm SHA-192 for improving integrity of messages.

Keywords: SHA-192, multicast, authentication, integrity, non-repudiation

1. Introduction

Multicast is an efficient technique to transfer multimedia contents like video, real time quotes from a sender to number of receivers. Multicast provides efficient transport mechanism to communicate between one-to-many and many-to-many communications [4]. In the network, multicast is the transfer of a message or information to destination computers concurrently in a single transmission from the source. Basically applications of multicast are video conferences, live video broadcast, video on demand, interactive games etc. In multicasting authentication is also a major security issue which should be kept in mind. By using authentication in multicast the receiver will be able to authenticate the sender of the message. Authentication in multicasting will also have the following properties:-

1. **Data integrity:** In this, receiver should be able to determine whether the receive content is modified or not during transmission.
2. **Data origin authentication:** In this each receiver should be capable to declare that each received packet arrives from the actual sender. In secure multicast group members must be able to verify that the data received is indeed sent by an authorized sender.
3. **Non-repudiation:** In this the sender of a packet should not be capable to reject sending the packet to receivers in case there is a disagreement among the sender and receivers.

All the three services can be supported by an asymmetric key technique called Digital Signature. The sender generates a signature for each packet with its private key, which is called signing, and each receiver checks the validity of the signature with the sender's public key, which is called verifying. If the verification succeeds, the receiver knows the packet is authentic.

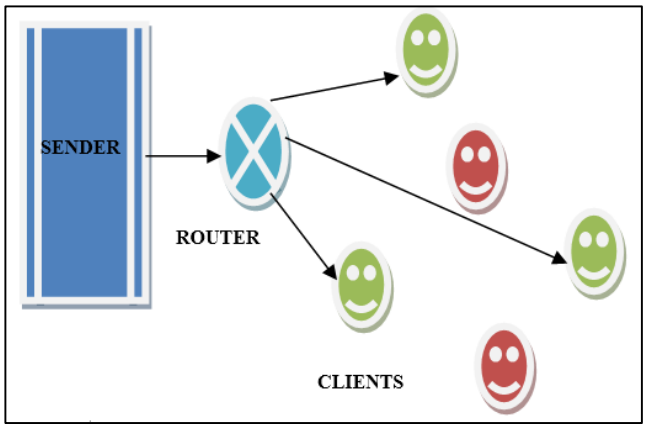

Fig 1: Example of Multicasting

In fig.1, it shows that sender sends just one copy to the router, and then the router creates multiple copies and sends them to connected clients.

2 Implementation

Our system ensures the authentication, integrity and non-repudiation principle of security. For authentication purpose we used harn's DSA, where sender signs the message with its private key and the receiver can verify this using the public key of sender. In harn's DSA p and q are large prime numbers and y is the public key, known by the clients. X is the secret key of sender. To provide more security and integrity to the

packets we have used a modified SHA-192 algorithm results the hash of 192 bits. Because SHA-192 is time efficient when it compared with SHA256 and more secure than SHA160 in terms of bit difference [1].

The multicast environment can be explained into below steps of implementation:

2.1 Sender creates the socket, and waits for router to connect.

2.2 As soon as the router is activated it connects to the sender on the same socket and start waiting for clients too. This establishes the connection between sender and router.

2.3 Sender sends the message to router as:

2.3.1 Sender divides the message into packets.

2.3.2 To maintain the integrity of messages it calculates the hash of each packet. We calculated the hash by using SHA-192 because it is more secure than SHA-1 and takes less time to generate the hash than SHA-256[1]. h(m)=SHA-192(m)

2.3.3 For non-repudiation server sign the each packet by its own private key using digital signature algorithm and sends r, s and hash for verification at client side. Sender signs each packet individually.

$$r = (g^k \bmod p) \bmod q$$
$$s = ((r * k) - (h(m) * x)) \bmod q$$

Where k is a new random integer for each packet.

2.3.4 Sender attaches these r and s with the message and sends to the router

2.4 Router receives the packets and buffers them forward. When client connects it forward the packets to the client.

2.5 The client:

2.5.1 Receives the packets.

2.5.2 Calculate the hash of received message.

h(m)=SHA-192(m')

2.5.3 Verifies each packets, discard if nor verified; accept otherwise.

$$w = r'^{-1} \bmod q$$
$$u1 = (h(m') * w) \bmod q$$
$$u2 = (s' * w) \bmod q$$
$$r' = (g^{u2} y^{u1} \bmod p) \bmod q$$

3 Result and analysis

In our research work we have applied SHA-192 in multicast to obtain more data integrity on the messages which is to be multicast over the network. For multicasting there is one sender, a router and clients. We have implemented this in java by the help of socket programming and multithreading. The results are describes in following figure:

Step 1: Server waits for router to connect, when it gets connection with router, it asks for the message to enter, that the sender has to multicast.

Step 2: Router connects to the server.

Step 3: After connecting to the router the server sends the digitally sign message. Fig. 2 shows the packetizing of the message and sending the packets after computing the r, s and hash of message using digital signature algorithm over each packet.

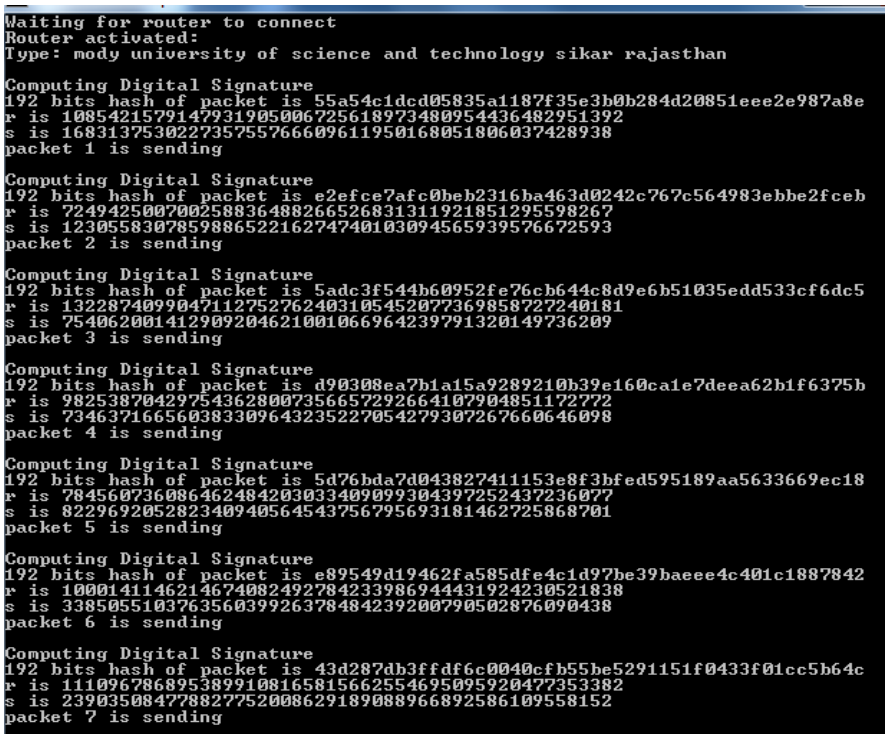

Fig 2: Sender connects to router and sends messages in form of packets to router after applying Digital signature algorithm to each packet and calculated the hash of each packet then sends hash, r and s.

Step 4: After sending the messages router receive the each packet and sends the various clients. Fig. 3 shows the number of packets gets from sender and no of clients which are connected.

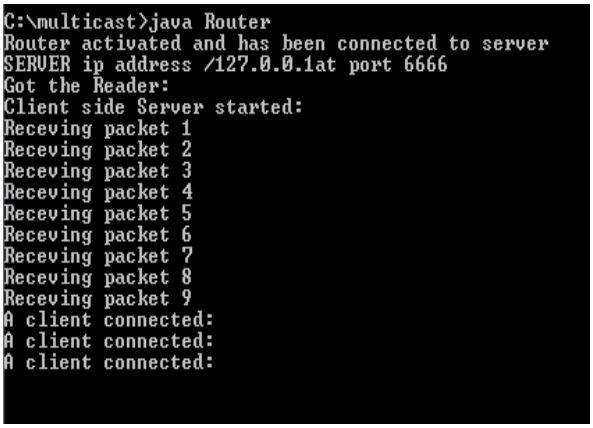

Fig 3: Router accepted packets and sends to connected clients

Step 5: Router sends the packets to the connected clients. Here there are 3 clients connected to router and they individually apply signature verification on each packet by comparing hash of actual message and received message. In fig. 4, 5 and 6 they shows the three clients are connected and gets the signed messages and accepts the packets after applying verification algorithm.

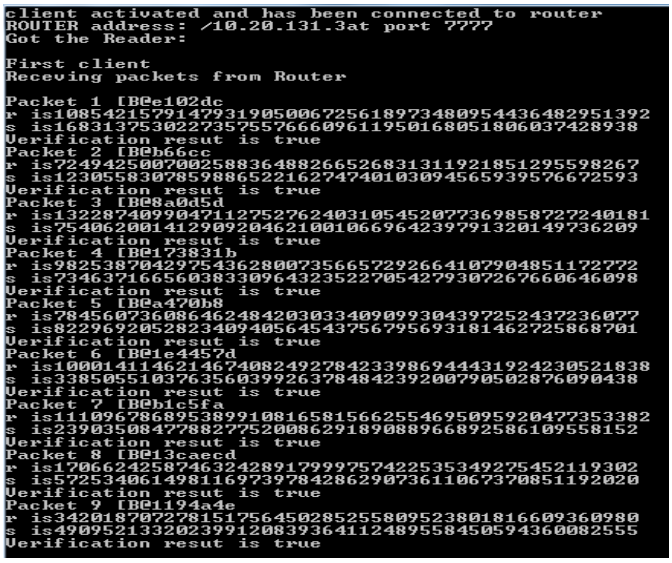

Fig 4: Client1 is connected and apply digital signature verification to each coming packet.

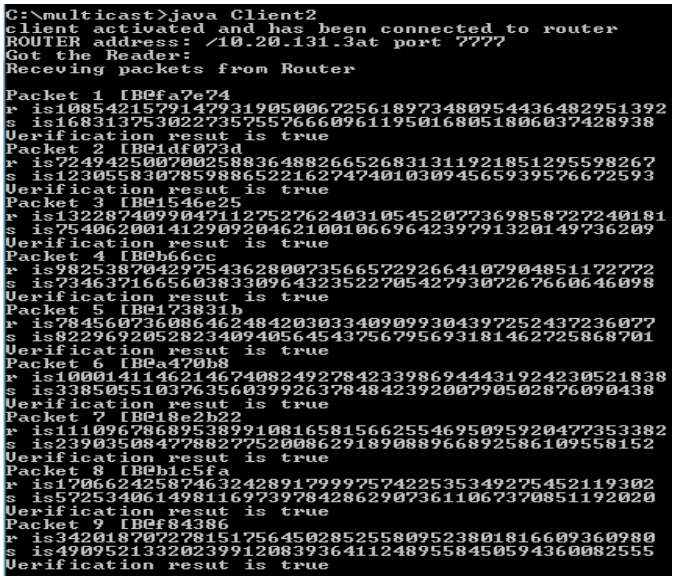

Fig 5: Client2 is connected and apply digital signature verification to each coming packet

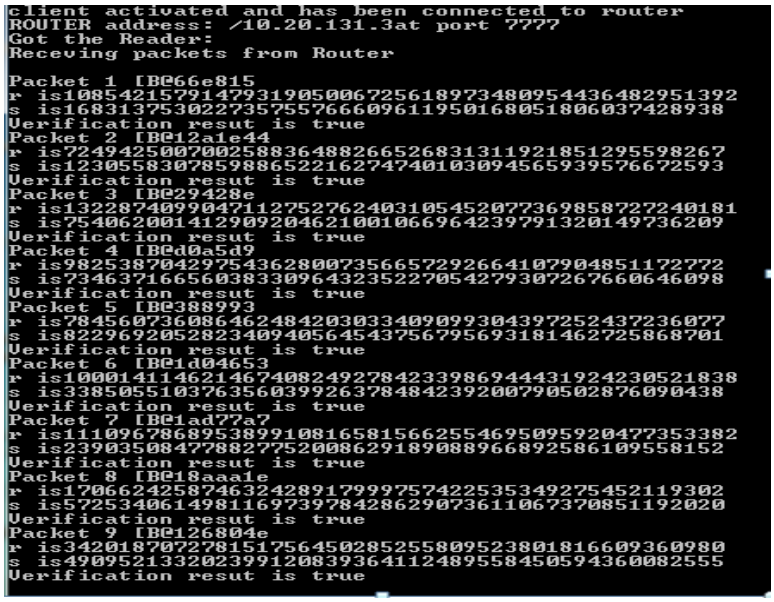

Fig 6: Client3 is connected and apply digital signature verification to each coming packet

4 Conclusion

In this paper, we have applied authentication, data integrity and non-repudiation to the packets which are multicast over the network so that there will be secure communication and no third party will be able to modify the messages during transmission. In our future work we will apply batch verification over the packets instead of applying individual verification on individual packets.

References

1. Harshita, Tanwar S. Implementation and performance analysis of Enhanced SHA-192. *International conference on recent cognizance in wireless communication and image processing in association with Springer*, Poornima university jaipur, 2015; 16-17.
2. Rahul Chourasia, Dr. Samidha Dwivedi Sharma. A Survey of Multicast Authentication with Different Signature Techniques. *International Journal of Emerging Technology and Advanced Engineering*. 2014; 4.
3. Rajarajan K, Thiyagu TM, Chandrasekar S. Multicast Authentication Based on Batch Sinature. *International Journal of Engineering Research & Technology (IJERT).* 2013; 2(4): 2278-0181.
4. Abirami N, Sasikala K, Reka R. Multicast Authentication using Batch Signature [MABS] in Mobile Ad Hoc Networks. *International Journal of Advanced Research Computer Science and Software Engineering*. 2013; 3(8).
5. Wen Tao Zhu. A Comment on MABS: Multicast Authentication Based on Batch Signature, *IEEE Transactions*, 2012; 11(11).
6. Kannan Balasubramanian, Roopa Anbu Malar R. HTSS: Hash Tree Signature Scheme for Multicast Authentication, *International Conference on Recent Trends in Computer Methods, Communication and Controls. published in Internations Journal of Computer Applications*, 2012.
7. Sridevi J, Mangaiyarkarasi R. Efficient Multicast Packet Authenticatio using Digital Signature *International Conference on Emerging Technology Trends (ICETT)*, 2011.
8. Zhou Yun, Xiaoyan Zhu, Yuguang Fang. MABS: Multicast Authentication based on Batch Signature. *Mobile Computing, IEEE Transactions* 2010; 9(7):982-993.
9. Min-Shiang Hwang, Cheng-Chi Lee. Research Issues and Challenges for Multiple Digital Signatures. *International Journal of Network Security*. 2005; 1:1-7.
10. Hilda CP, Mr. Liaqat Ali Khan, Grace Vennice M, Shalini PV, Basic Model of Multicast Authentication based on Batch Signature-MABS. *Internation Journal of Computer Science & Information.* 2, 1-2.
11. Srikant Bethu K, Kanti Kumar, Asrar Ahmed MD, Soujanya S. Comparison Analysis in Multicast Authentication based on batch Signature in Network Security, 2013.
12. Khaldun Ibraheem Arif. An Efficient DSA Approach for batch Verification.