ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (68-71), Month: July - September 2016, Available at: www.researchpublish.com

Multicast Authentication-A Comparative Study

Rini S

M Tech in Computer and Information Science, TKM Institute Of Technology, Kollam, Kerala

Abstract: **This article gives you a basic idea on what multicast authentication means. We can provide many methods for authentication like digital signature, batch wise authentication, encryption and decryption using L-A-R algorithms or simply simple encryption and decryption techniques. The primitive packet sending techniques are not attack resistant, we need a good protocol that will perform authentication in real time, so that we can resist packet loss and pollution attacks. Multicasting is one of the techniques for sending confidential data to multiple users in a secure way if encryption is done in a good way. Here we will be discussing about batch signature its drawbacks and L-A-R protocol, also some simple cryptographic techniques.**

Keywords: **Batch Signature, cryptography, L-A-R protocol, Digital Signature.**

I. INTRODUCTION

Multicast scheme is implemented in Internet Protocol on the basis of multicast theory; this usually takes place in routing level. The different types of media used in multicast applications are text, audio, video etc.We derive the memory and bandwidth requirements for each type before transmitting them. **Multicast** (one-to-many or many-to-many distribution) is a type of group communication where data are addressed to a group simultaneously. Authentication [1] is one of the key ideas in securing multicast. Basically, multicast authentication provides the following security services:

1. Data integrity: Here each receiver should be able to assure that the packets received are not modified during data transmissions and also the data received is valid.

2. Data origin authentication: In this each receiver should be able to identify that each received packet arrives from the original sender as it claims and not masked

3. Non-repudiation: Here the sender of the packet should not be capable to stop sending the packet to receivers in case there is a dispute among the sender and receivers.

Other than Multicasting there are various other techniques in message sending this include Anycast, multicast, Broadcast, Geocast and Unicast

UNICAST:

Unicast is the term used to describe communication where a piece of information or data is sent from one person to another. Here there is only one sender, and one receiver. Unicast transmission where a packet is sent from a single source to a specified receiver, is still the conventional form of transmission on LANs and within the Internet. All LANs and Internet Protocols in networks support the unicast transfer mode which is simple and error prone to a limit, and most of the users are familiar with several unicast applications (e.g. http, smtp, ftp and telnet) .

BROADCAST:

Broadcast is a type of communication where there are multiple receivers. Here case there is just one sender, but the information is sent to multiple receivers. Broadcast transmission is supported on most Local area networks and can be used to send the same information to all computers on the LAN.Broadcasting has been mainly used in communication .considering broadcasting the numbers of receivers are more compared to other routing schemes.

MULTICAST:

Multicast is used to describe communications where a piece of information is sent from one or more sender to multiple receivers in different locations. Here there is may be one or more senders, and the information is evenly distributed to a set of receivers. Fine example of application which uses multicast is a video server sending out networked TV channels to multiple receivers. Simultaneous delivery of better quality video to each of a large number of delivery platforms will reduce the capability of even a high bandwidth network with a good video clip server. One simple way to ease scaling to larger groups of clients is to introduce multicast networking.

Multicasting is a unique technique of delivering the same packet simultaneously to a group of clients/receivers. The IP multicasting provides dynamic many-to-many communication between a set of senders (at least 1) and to a group of receivers. The format of IP multicast packets are almost same to that of unicast packets and are identified only by the use of a special class of destination address which identifies a specific multicast group. Since Transmission Control Protocol supports mainly the unicast mode, multicast applications must use the UDP transport protocol. Unlike the broadcast transmission (used in some local area networks), multicast clients receive a stream of packets only if they have previously advised to do so. Membership of a group is dynamic and anonymously controlled by the receivers which in turn informed by the local client applications. The routers which are the backbone in multicast network checks which sub-networks have active receivers for each multicast group and attempt to minimize the transmission of packets to those parts of the network for which there are no active clients.

The multicast communication is useful if a group of receivers requires a common set of data simultaneously, or when the receivers are able to receive and store (cache) sent data until needed. Where there is a common need for the same data required by a group of receivers, multicast transmission will provide significant bandwidth savings (up to 1/N of the bandwidth compared to N separate unicast clients)which are reliable. The majority of LANs are able to support the multicast transmission mode. Shared LANs which is using hubs/repeaters support multicast, since all packets will reach all network interface cards connected to the LAN. In older times the LAN network interface cards had no specific support for multicast and introduced performance degradation by forcing the adaptor to receive all packets (promiscuous mode) and perform software screening to remove all unwanted packets which was time consuming.

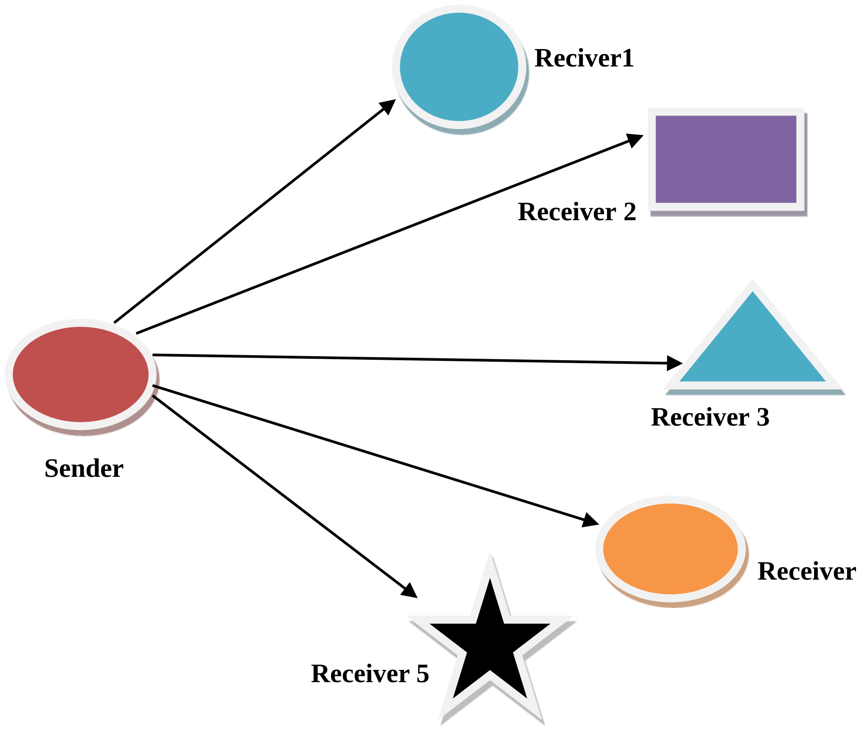


Fig.1: Multicasting

II. AUTHENTICATION TECHNIQUES

A. Batch Signature:

In the Batch signature [1] authentication there are mainly three security services namely Non-repudiation (don't transmit data in the unauthentic case), Data Integrity (received data is authentic) and Data origin authentication (data from authentic sender) which can be maintained by an asymmetric key collectively known as signature [1]. The sender creates a signature for each packet to be sent with sender's private key that is called signing. Signing will help to identify the authentication of the sender. Then each receiver can confirm the authenticity of the sender's signature with the help of sender's public key which is shared. This process is known as verifying. If the verification is confirmed, the receiver knows the packet is authenticated. MABS stand for Multicast Authentication Based on Batch Signature. In 2010 Yun Zhou et al [1] put forward a multicast Authentication protocol called MABS. This protocol has mainly two schemes. The first scheme will (MABS-B) eliminate the correlation among sent packets and provides the perfect resilience to packet loss; it is efficient while considering in terms of computation, latency, and communication overhead. Its efficient cryptographic batch signature supports the authentication of multiple numbers of packets simultaneously. The second scheme is enhanced scheme which is MABS-E, which the combination of the basic scheme and packet filtering techniques .Our target is to authenticate multicast streams from sender to multiple recivers.Inorder to fulfil the requirement the basic scheme MABS –B uses an efficient signature that is batch signature where multiple packets are verified not in a group but individually. Batch signature scheme is based on BLS and DSA which is more efficient than RSA scheme.

A.1 ADVANTAGES AND DISADVANTAGES OF MABS:

Advantages:

- Correlation among packet is eliminated
- Attack due to DOS is reduced
- Secure transmission
- Forward and Backward secrecy is maintained.

Disadvantages:

- Signature for every packet has large communication and computation overhead.
- Large number of recipients must verify the data sender
- No authentication in real time
- No measures are taken for packet loss, pollution attacks and reply attacks.

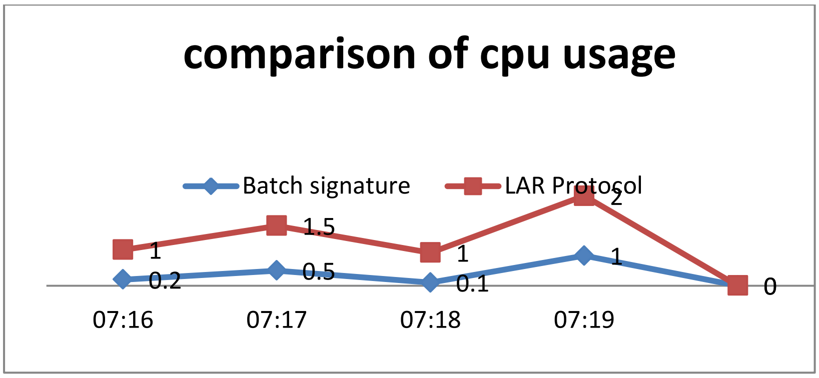
TABLE.I: Communication overhead and signature scheme

SCHEMES	LENGTH(bits)
MD5	128
SHA-1	160
RSA	1024
BLS	171
DSA	320

B. LAR PROTOCOL:

LAR is an efficient protocol for multicast authentication; it uses both public key signature and symmetric key encryption. This protocol has low computation and communication overheads. It resist packet loss, pollution and replay attacks. In 2011 Riham Abdellatif, Heba K. Aslan, and Salwa H. Elramly[5] introduced a protocol which uses erasure code functions over the generated signature to resists packet loss and uses symmetric encryption of the erasure code output which resist pollution attacks. It also fights replay attack. The proposed protocol called Latif-Aslan-Ramly1 (LAR1) is verified using Burrows, Abadi and Needham (BAN) logic. The proposed protocol achieves the authentication goals without bugs or redundancies.

Here the stream is divided into blocks of packets then applies the digital signature and erasure code function on the signature we also add a counter to the packet resist reply attacks. Then the sender calculates the UMAC finally the sender output will be the data packet appended with its counter, the UMAC output and the output of the encryption algorithm. Scientifically calculated communication overhead for LAR is 27.4 which is much less compared to all other like WONG-LAM, TESLA, BATCH SIGNATURE etc.



III. CONCLUSION

The research topics in the field of multicast authentication has many alternatives and challenges. Here we have done a brief study of multicast authentication based on batch signature and LAR protocol .we can conclude that LAR has more advantages than Batch signature. The verification shows that LAR achieves its goal free of redundancy and bugs. We can also generate OTP to secure transmission. Today multicast is still evolving, new multicast routing protocols are being developed and application of multicasting is also growing to higher levels.

REFERENCES

[1] Yun Zhou, Xiaoyan Zhu, and Yuguang Fang "MABS: Multicast Authentication Based on Batch Signature" 2010 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010.

[2] J.Sridevi and R.Mangaiyarkarasi "Efficient Multicast Packet Authentication using Digital Signature" 2011 Proceedings of International Journal of Computer Applications (IJCA) 2011.

[3] Hilda C.P, Mr. Liaqat Ali khan , M.Grace Vennice , P.V.Shalini "Basic Model of Multicast Authentication Based On Batch Signature-MABS"

[4] Seonho Choi "Denial-of-Service Resistant Multicast Authentication Protocol with Prediction Hashing and One-way Key Chain" 2005 Seventh IEEE International Symposium on Multimedia (ISM'05), PP: 12-14 Dec. 2005.

[5] Riham Abdellatif, Heba K. Aslan, and Salwa H. Elramly "New Real Time Multicast Authentication Protocol" 2011 International Journal of Network Security, ISSN No. 1816353X, Pages: 13-20, 2011.

[6] Adrian Perrigy_ Ran Canettiz Dawn Songy J. D. Tygar "Efficient and Secure Source Authentication for Multicast" 2001 In Network and Distributed System Security Symposium(NDSS '01), 2001.

[7] Shouhuai Xu and Ravi SandhuIn "Authenticated Multicast Immune to Denial-of-Service Attack" 2002 Proceedings of the 2002 ACM symposium on Applied computing (SAC '02), pp. 196-200, 2002.

[8] Vinoth George C "Efficient and Secure Multicast Authentication Based on Batch Signatures Using Fractal Merkle Tree" 2012 International Journal of Computer Science and Management Research, ISSN. 2278-733X, Vol 1, Issue 4, November 2012.

[9] Chris Szilagyi and Philip Koopman "Low Cost Multicast Authentication via Validity Voting in Time-Triggered Embedded Control Networks" 2010 Proceedings of the 5th Workshop on Embedded Systems Security (WESS-10), 2010, 2010.

[10] Qinghua Li, Guohong Cao "Multicast Authentication in Smart Grid With One-Time Signature" 2011 IEEE Transactions on Smart Grid, pp. 686 – 696, Dec. 2011.