Volume: 9 Issue: III Month of publication: March 2021

DOI: https://doi.org/10.22214/ijraset.2021.33137

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue III Mar 2021- Available at www.ijraset.com

An Object for Finding an Effective and Source Authentication Mechanism for Multicast Communication in the Hash Tree: Survey Paper

Poonam[1], Sarvpal Singh[2]
[1, 2]Information Technology, Department, MMMUT, Gorakhpur, India

Abstract: The Internet is the basis of all kinds of transmission, namely unicast, multicast, streaming. Multicast communication is very well; multicast communication provides more desirable communication than unicast and streams to context for bandwidth usage. Multicast communication is very famous in audio broadcasting, video broadcasting, and data distribution. Different mechanisms such as hashing process, hashing based on tree, and signing process on the hash tree. These programs are many issues such as communication costs and hash computation process. This communication works in the survey paper to calculate this idea's progress and measure performance with the existing mechanism. The source authentication suggests the flexibility process to the multicast system. A new approach is the source name of the Edward curve digital signature (EdDSA). It has fewer communication costs compared to secure hash standard (SHS), the hash mechanism for source authentication (HMSA), source authentication of Elliptic curve cryptography (ECCSA).

Keywords: Security Goals, cost of Communication, Multicast Communication, Edwards curve digital signature.

I. INTRODUCTION

The Internet is an essential digital communication backbone. There is a lot of new networking, like unicast, broadcast, and multicast. This unique communication community is known as multicast. The use of multicast interaction is improving every day. Multicast and broadcast communication systems provide less communication overhead than unicast communication systems, like unicast communication systems provide more overhead. A unicast address is known as the IP address of classes A, B, C. Often recognized as a multicast address is Class D's IP address; security is a significant objection in transmission because class D's IP address is public. To create a secure communication between source and destination, there is a need to enhance protection. The authority may not belong to this group in the multicast communication mechanism, so this community also collects information from every legitimate person. Hashing is a critical process for integrity achieved. Multicast communication has many difficulties. Congestion may occur when the number of users in the group is more; if the data has not been encrypting with the correct method, then the security threats are high. Source confirmation (authentication) is a possible method to verify that the source is an unauthenticated user. Source verification is our primary objective. "Here [1-8], use the source verification algorithm. Authors used the RSA algorithm to achieve authenticity, then communication costs and response time are high." Advanced authentication techniques used to solve these issues these techniques are Elliptic Curve Cryptography Digital Signature Algorithm (ECDSA) [14] and ECC-based source authentication (ECCSA) [2] used for multicast communication.

II. RELATED WORK

A literature review has many ways to achieve source authenticity. Different writers complete source verification. In the multicast communication system, security is another primary challenge. In this phase, security challenges and authentication have described. The current authentication method is the Simple Hash Chaining Scheme (SHS), which has tied to tree chains, is a sufficient multi-chain-bound signature for broadcast, and multicast source Hybrid authentication was used.

"The message (M) has separated by blocks (M1, M2, M3, etc.) in this hash chaining method [8], and then calculates the hash value of one block and signs it in, and sends the signed package to the official/authentic user."

"The chain binding method or tree chaining method [9-13], all packets must contain details about authenticity, and that's all packets can be independently satisfied or go through. If there are n packets and n − 1 package are lost, it is possible to verify the validity of one package received and compute each block's signature."

"Hamid Eltaief and Habib Youssef [10] efficient multicasting stream Signature (EMSS) - In this technique, even if 50 percent of pockets are lost, the remaining packets found have been verifying if the hash-link is maintained. Targeted packages have been randomly selecting from the EMSS system."

“Jin-Xn has developed the hybrid model known as Hybrid Multicast Source Authentication (HMSA) and Zhi-Guo Zhou et al. [9], where there uses a hash tree and digest chaining method, different types are to choose. The authors, however, do not have such a model that will fill everything verification requirements. In the next section, the new concept that authenticity by non-disclosure has suggested.”
“Cryptography-based source authentication (ECCSA) in the elliptic curve [2] - Adaptive hash tree and elliptic curve cryptography digital signature algorithm (ECDSA) have been using for authentication in this form.” Different authors implement so many models, and then no model completed all the requirements for authentication.

III. PROPOSED METHOD

The proposed method has selected a flexible hash tree. Different writers have used the hash tree to calculate root hash and applied it to all hash nodes, so the hash’s enumeration cost is higher. This mechanism has been using a flexible hash tree that can count on the root hash; the proposed system have given below. “Here data (D) has a partition in equivalent block sizes (M11, M12, M13, M14, M15, M16, M17, and M18). The block size can take 2, 4, 8, 16, 32, 64, 128, and 256 (packets).” The hash tree has generated the root hash has given in Fig 3.1.

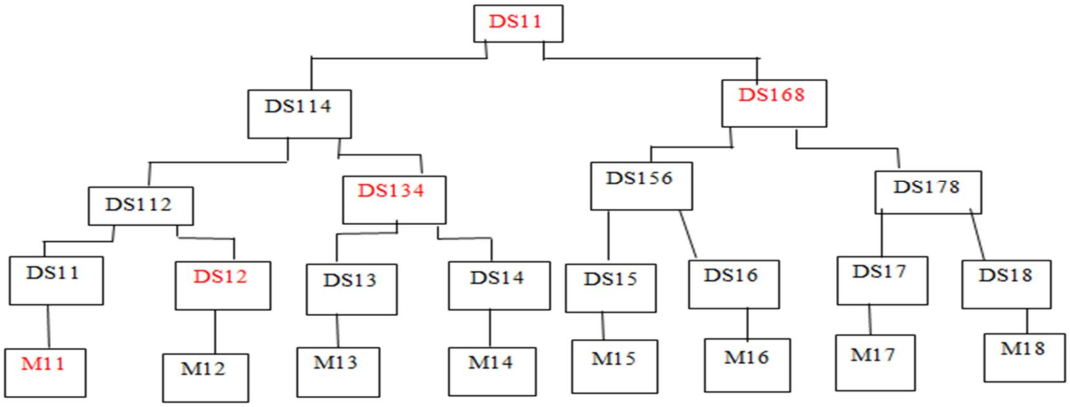

Fig-1: Process of hash tree generation

A. Process of Hash Generation in Sender Side

1) Calculate hash value DSxy (x=1 and y= 1 to 8) of the first block. In the end, calculate root hash [DS118] by using packet hashes DS11, DS12, DS13, DS14, DS15, DS16, DS17, DS18, and the hash value of intermediate nodes. Similarly, calculate the hash value of other blocks using this method.
2) In the next step, sign in the first block’s root hash value.
3) The signed hash packet has been transferring to all legal users.
4) The first packet has been sending to (M11) with packet ID, sibling hashes (DS12, DS134, and DS158) to root (DS118).
5) The second packet has sent using the first packet hash value DS11. It has used to calculate the root hash (DS118) of the value DS11.
6) Send the packet (M13) with hash vale (DS14) and hash value (DS12) and use the store values to compute the root of the 1st block.
7) Send the packet (M14) with only the hash value (DS13).
8) Similarly, other packets have been sending (M15, M16, M17, M18) using these four steps in sequences.
9) The same method has been applying to other blocks.

B. Key Generation processes for EdDSA

“Public key S, private key r.
Select a random a-bit string as r.
Calculate DS(r) = (ds0, ds1... ds2a−1).
Calculate x = 2 a−2 +∑3≤i≤a−3 2 ihi.
Compute S = xC.”

C. Signature Generation processes for EdDSA

“Message A, private key r, and DS(r) = (ds0, ds1... ds2a−1).
EdDSA signature (R, 0, S) on A.
Calculate l = DS (da... d2a−1, A).
Compute R = lB ∈ E. – R 0 = (the sign bit of the x-coordinate of R) || (the y-coordinate of R).
Compute S = l +DS(R, 0, C, A) x (mod l).”

D. Signature Verification processes for EdDSA

“Message A, public key S, and signature (R, 0, S).
True or false. – Calculate DS (R, 0, C, A).
Calculate R from R 0 (using a square-root computation as described in the text).
Take the signature if and only if the equation SB = R+DS(R, 0, C, A) C holds.”

IV. SURVEY RESULT AND ANALYSIS

A. Parameters used for EdDSA

EdDSA has 11 parameters:

1) Assume that odd prime power is p. “An elliptical curve over the finite field GF (p) is used by EdDSA.”
2) A number b with 2^ (b-1) > p. Especially, EdDSA public keys have b bits, and EdDSA signatures have 2*b bits. Often B is recommended to be a multiple of 8, so the calculation unit of a public key and signature lengths integral differs of octets.
3) A (b-1) bit is encoding of GF finite field (p).
4) Generation of 2*b-bit output with a cryptographic hash function H. Square measure proposed conservative hash functions (i.e., hash functions where collisions cannot make), which do not have a great deal of effect on the entire value of EdDSA.
5) A number and c = 2 or 3, Hidden EdDSA scalars are square measure multiples of 2^c. The number c is that the base-2 index of the logarithm of the so-called cofactor.
6) An integer of n and c <= n < b. Hidden EdDSA scalars have strong n + 1 bits, always set the highest bit, and always clear the bottom c bits.
7) A non-square element of GF is d (p). The same old advice requires it because there is a right curve given by the value closest to zero.
8) A square non-zero part of GF a (p). A = -1 if p mod 4 = 1, and a = 1 if p mod 4 = 3 might be the same old recommendation for best results.
9) A B-component! = (0, 1) of the set E = {(x, y) GF (p) x GF (p) may be a member defining * x^2 + y^2 = 1 + d * x^2 * y^2}.
10) [L] B = 0 and 2^c * L = #E. An odd prime L is defined. The number #E (the number of curve points) is part of the standard data supplied for the elliptical curve E or computed as the order of the cofactor *.
11) “A “pre-hash” PH function. Pure EdDSA suggests EdDSA wherever PH is the function of identity, i.e., PH(M)= M. Wherever PH is the identity function. Hash EdDSA implies that EdDSA, regardless of how long the message is, wherever PH generates a brief output; as an example, PH(M)= SHA-512 (M).

There are the following parameters used for the survey in given table 1.

Table-1: Survey parameters

Parameters used in the survey	Assumed Values
Size of block	2, 4, 8, 16, 32, 64 (Number of packets)
Packets	64, 128, 256, 512 (Bits)
SHA-1	32 Byte
EdD Signature	64 Bits
Buffer size	2 Block
Simulation time	59 sec

B. Topology used in the Survey Paper

In this topology, here is one source and eight destinations. The source forwards the packet to the implemented network. Many routers have presented multicast communication, and these routers make a duplicate of the package, and these packages are delivering to its neighboring routers. Eventually, whole receivers receive the packet sent by the source.

The general and complete multicast state begins when the host/administrator holds to combine the multicast site through the Internet Group Management Protocol (IGMP), which includes a 30-member process, and this process is called a group member. The host is eligible to send or receive messages to or from other team members based on active membership.

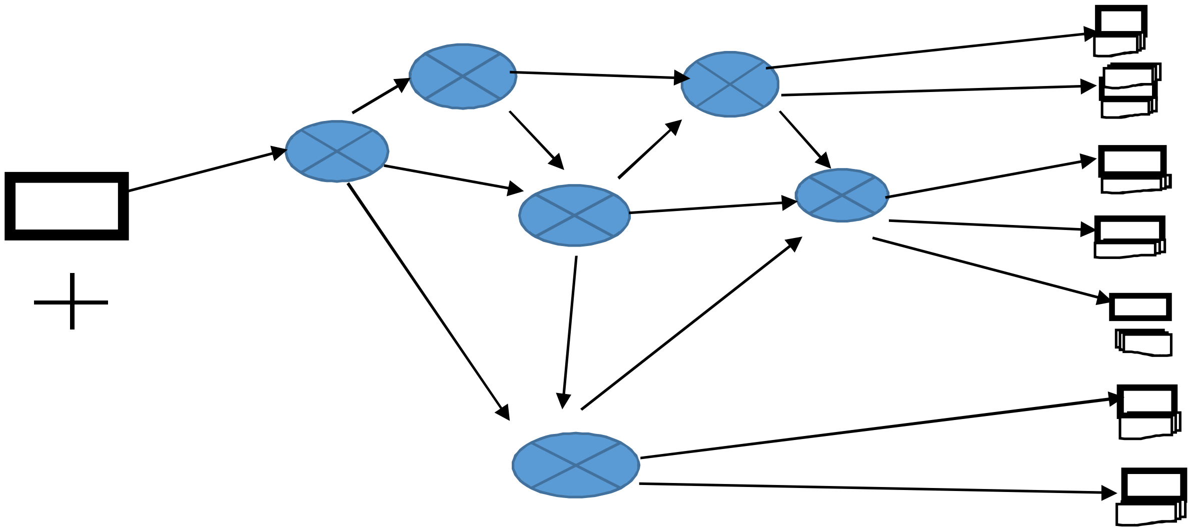

Fig. 4: Experimental base Topology

C. Survey Result Analysis

In this literature survey, all of these approaches have been using for source authentication in the RSA algorithm. Using EdDSA25519 with crucial size 128 bits, we achieved 64 bits security, 128 bits security using ECDSA with the necessary size 256, while the RSA algorithm requires 3072 bits to obtain the same level of protection. This approach thus reduces the cost of measurement and the cost of communication of the proposed methodology.

D. Impact of Packet Size on cost of Transmission

A simple hash chaining system has very high communication costs, and a hybrid multicast system provides better results than the proposed method (EdDSA). It also provides much better results than another proposed system. The computing costs in the event of SHS are high, and the computing costs of the EdDSA scheme are low compared to other systems.

V. CONCLUSION

This proposed method is also known as EdDSA. EdDSA method has introduced two algorithms, the first is the hash tree method, but another algorithm has used for authentication. This method is useful to decrease the computation cost as well as the cost of communication.

REFERENCES

[1] K. Balasubramanian and R. Roopa, HTSS: Hash Tree Signature Scheme for Multicast Authentication, IJCA Proceedings on International Conference in Recent trends Computational Methods, Communication and Controls (ICON3C), No. 6, pp. 28- 32, April 2012.

[2] Vicky Vikrant, Hariom Tyagi, A Source Authentication Mechanism for Multicast Communication System Using Adaptive Hash Tree, International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), ISBN: 978-1-7281-4826-7/19/$31.00 ©2019 IEEE, 2019

[3] Diana Berbecaru, Luca Albertalli, and Antonio Lioy, The ForwardDiffSigScheme for Multicast Authentication, IEEE/ACM transaction on networking, Vol 18, No.6, pp. 1855 – 1868, December 2010.

[4] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar, Efficient and secure source authentication for multicast, Proceedings of Network and Distributed System Security Symposium (NDSS-2001), Vol. 1, pp. 35–46, 2001.

[5] Jung Min Park, Edwin K. P. Chong, and Howard jay Siegel, Efficient multicast packet authentication using signature amortization, Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 227– 240, 2002

[6] Iuon-Chang Lin and Chia-Chang Sung, An Efficient Source Authentication for Multicast based on Merkle Hash Tree, Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP-2010), pp. 5 – 8, October 2010.

[7] Adrian Perrig, J.D. Tygar, Dawn Song and Ran Canetti, Efficient Authentication and Signing of Multicast Streams over Lossy Channels, IEEE Symposium on Security and Privacy, pp. 56–73, 2000.

[8] Adrian Perrig, Ran Canetti, Dawn Song and J. D. Tygar et.al, Efficient and Secure Source Authentication for Multicast, Internet Society Network and Distributed System Security, pp. 35-46, 2001.

[9] HE Jin-Xin and ZHOU Zhi-Guo, FU Xiao-Dong, XU Gao-Chao, A Hybrid and Efficient Scheme of Multicast Source Authentication, Eighth ACIS International Conference on Software Engineering, Artificial Intelligence Networking and Parallel/Distributed Computing,2007 vol. 2, pp.123-125.

[10] Hamdi Eltaief and Habib Youssef, RMLCC: Recovery-Based Multi-Layer Connected Chain Mechanism for Multicast Source Authentication, 35th Annual IEEE Conference on Local Computer Networks, Colorado 2010.

[11] Rosario Gennaro and Pankaj Rohatgi, How to Sign Digital Streams, Information and Computation 2001.

[12] Jung Min Park, Hdwin K. P. Chong, Howard Jay Siegel, Efficient Multicast Packet Authentication Using Signature Amortization, IEEE Symposium on Security and Privacy, 2002.

[13] Aldar C-F. Chan, A graph-theoretical analysis of multicast authentication, 23rd Int. Conf. on Distributed Computing Systems, 2003.

[14] Ghada F. ElKabbany and Heba K. Aslan, Efficient Design for the Implementation of Wong-Lam Multicast Authentication Protocol Using Two-Levels of Parallelism, International Journal of Computer Science Issues. All Rights Reserved, 2012.

[15] Shivkumar and S. & G. Umamaheswari, Certificate Authority Schemes Using Elliptic Curve Cryptography, RsaAnd Their Variants-simulation Using Ns2, American Research on Design Principles of Elliptic Curve Public Key Cryptography and Its Implementation" International Conference on Computer Science and Service System 2012.