Various Signature Techniques for Multicast Authentication: a Review

Rahul Chourasia1, Dr. Samidha D. Sharma2

Abstract—Here in this paper a complete survey of all the techniques related to the authentication using signatures and multicasting is introduced. Although there are various security protocols implemented which provides security from various attacks such as DOS attack, DDOS attack, Confidentiality, Unforgeability, but there all the authentication techniques can’t prevents from all types of attack, hence a survey is done here to check and compare the security analysis of various protocols so on the basis of their strengths and weakness a strong and efficient technique is implemented.

Index Terms—Multicast, Authentication, Geocast, unicast, Batch Signature, Anycast, Broadcast.

I. INTRODUCTION

In computer networking, multicast is the delivery of a message or information to a group of destination computers simultaneously in a single transmission from the source. Copies are automatically created in other network elements, such as routers, but only when the topology of the network requires it. Multicast is most commonly implemented in IP multicast, which is often employed in Internet Protocol (IP) applications of streaming media and Internet television. In IP multicast the implementation of the multicast concept occurs at the IP routing level, where routers create optimal distribution paths for datagrams sent to a multicast destination address. At the Data Link Layer, multicast describes one-to-many distribution such as Ethernet multicast addressing, Asynchronous Transfer Mode (ATM) point-to-multipoint virtual circuits (P2MP) or Infiniband multicast.

In this paper we are going to present a review on multicast authentication with different signature techniques. This paper is organized as various routing schemes in section 2, related work in section 3 followed by conclusion in section 4.

II. DIFFERENT ROUTING SCHEMES

2.1 Anycast

Anycast is a network addressing and routing methodology in which datagrams from a single sender are routed to the topologically nearest node in a group of potential receivers all identified by the same destination address.

2.2 Broadcast

Broadcasting is the distribution of audio and video content to a dispersed audience via any audio or visual mass communications medium, but usually one using electromagnetic radiation (radio waves). The receiving parties may include the general public or a relatively large subset thereof. Broadcasting has been used for purposes of private recreation, non-commercial exchange of messages, experimentation, self-training, and emergency communication such as amateur (ham) radio and amateur television (ATV) in addition to commercial purposes like popular radio or TV stations with advertisements.

2.3 Multicast

Multicast is most commonly implemented in IP multicast, which is often employed in Internet Protocol (IP) applications of streaming media and Internet television. In IP multicast the implementation of the multicast concept occurs at the IP routing level, where routers create optimal distribution paths for datagrams sent to a multicast destination address.

2.4 Geocast

Geocast refers to the delivery of information to a group of destinations in a network identified by their geographical locations. It is a specialized form of multicast addressing used by some routing protocols for mobile ad hoc networks.
2.5 UNICAST

In computer networking, unicast transmission is the sending of messages to a single network destination identified by a unique address.

2.6 Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication [1] is one of the critical topics in securing multicast.

Basically, multicast authentication may provide the following security services:

1. Data integrity: Each receiver should be able to assure that received packets have not been modified during transmissions.
2. Data origin authentication: Each receiver should be able to assure that each received packet comes from the real sender as it claims.
3. Nonrepudiation: The sender of a packet should not be able to deny sending the packet to receivers in case there is a dispute between the sender and receivers.

2.7 Batch Signature

The [1] three services of security like Data integrity, Data origin authentication, Nonrepudiation can be supported by an asymmetric key technique called signature. In an ideal case, 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.

III. RELATED WORK

In 2010 Yun Zhou, Xiaoyan Zhu, and Yuguan Fang [1] proposed a multicast Authentication protocol MABS. This protocol has two schemes. The first scheme is (MABS-B) which eliminates the correlation among packets and provides the perfect resilience to packet loss; it is efficient in terms of latency, computation, and communication overhead. Its efficient cryptography batch signature supports the authentication of any number of packets simultaneously. The second scheme is enhanced scheme MABS-E, which the combination of the basic scheme and packet filtering mechanism [1].

In 2011 J.Sridevi and R.Mangaiyarkarasi proposed a conventional scheme that uses efficient signature algorithms which reduce computation overhead and are vulnerable to packet injection by malicious. MABS achieves perfect resilience to packet loss in lossy channels.

Basic scheme MABS-B is efficient in terms of latency, computation and communication overhead. An enhanced scheme called MABS-E combines the basic scheme MABS-B and a packet filtering mechanism to tolerate packet injection [2]. In Hilda C.P, Mr. Liaqat Ali khan, M.Grace Venncie, P.V.Shalini invented a multicast authentication protocol called MABS (Multicast Authentication Based on Batch Signature) by including two specified schemes MABS-B and MABS-E [3].

In 2005 Seonho Choi proposed a multicast authentication scheme for real-time streaming Applications. It is resistant to denial-of-service attacks and consumes less resources like CPU and buffer. This scheme uses prediction hashing (PH) and oneway key chain (OKC) techniques which is based on erasure codes and distillation codes and gives less CPU overhead and buffer requirements compared to other block-based solution approaches [4]. In 2011 Riham Abdellatif, Heba K. Aslan, and Salwa H. Elramly introduced a protocol which uses erasure code functions over the sig-nature to resists packet loss and uses symmetric encryption of the erasure code out- Put which resist pollution attacks. It also resists replay attack. The proposed protocol called Latif-Aslan-Ramly1 (LAR1) is analyzed using Burrows, Abadi and Needham (BAN) logic. It achieves the authentication goals without bugs or redundancies [5].

In 2001 Adrian Perrig, Ran Canetti, Dawn Songy J. D. Tygar introduced a protocol which uses the concept of TESLA and improves it. It allows receivers to authenticate most packets as soon as they arrive and also improves the scalability of the scheme, reduce the space overhead for multiple instances, increase its resistance to denial-of-service attacks, and more [6]. In 2002 Shouhua Xu and Ravi Sandhu proposed two Internet Protocol which uses multicast tree as an essential authentication mechanism. This technique is efficient and immune to multicast denial-of-service attack. This allows the receivers to immediately authenticate the packets without taking care of the packet loss characteristics of the underlying network [7].

In 2012 Vinoth George C proposed a Tree Hash algorithm traversal of Merkle trees. It generates a sequence of leaves with their associated authentication paths. This technique gives improvement in space and time complexity over any previously published algorithm [8]. In 2010 Chris Szilagyi and Philip Koopman proposed a new scheme which uses unanimous voting on message value and validity amongst a group of nodes thus improve overall bandwidth efficiency and reduce authentication latency by using. It uses one extra bit per additional voter and decreases the probability of successful per-packet forgery.
For multicast flows, and to eliminate the co-channel problem which minimise the signing cost under a certain verification cost, and propose a heuristic solution to solve it [10].

In 2009 Qiyan Wang, Himanshu Khurana, Ying Huang, Klara Nahrstedt proposed a new signature model TV-OTS which gives one-time signatures in constructing multicast authentication schemes. TV-OTS uses much smaller signature size. It supports time-critical multicast authentication scheme TV-HORS in combination of hash chains with TV-OTS that can authenticate streaming packets. It gives short end-to-end computational latency, perfect tolerance to packet loss, and strong resistance against malicious attacks [11]. In 2012 Shilpa S. Harnale and Gouri Patil proposed MABS-B can achieve perfect resilience to packet loss in lossy channels in the sense that no matter how many packets are lost, the already received packets can still be authenticated by receivers. MABS-B reduces the packet loss by eliminating the co-relation between packets, and due to its efficient cryptographic primitive called the batch signature, it provides efficient latency, computation and communication overhead [12].

In 2008 Thomas C. Schmidt, Matthias Wahlisch, Olaf Christ, and Gabriel Hege introduced a new protocol for the authentication of mobile multicast senders. It uses in the network infrastructure and receivers. The strong graphically and oneway signaling scheme gives two advantages first is to conforms multicast mobility management schemes and second is to allows for a uniform signalling of the mobile source [13]. In 2007 Yacine Challal, Abdelmadjid Bouabdallah proposed a new and efficient source authentication protocol which guarantees non-repudiation for multicast flows, and tolerates packet loss. It is simulation of protocol NS-2 and results is the protocol allows achieving improvements over protocols fitting into the same category [14].

In 2012 Ghada F. ElKabbany1 and Heba K. Aslan introduced an efficient design for the implementation of Wong and Lam multi-cas authentication protocol.

It uses two-levels of parallelism to solve the computation overhead problem and uses Universal Message Authentication Codes (UMAC) instead of hash function which reduces the communication overhead. The design is analyzed for both NTRU and elliptic curve cryptography algorithms. This design decreases the execution time of Wong-Lam protocol [15].

IV. Conclusion

Here in this paper a survey of all the authentication techniques implemented for using multicasting is given and also the brief overview of all the technique and their security features. Here the concept of Batch signatures is given in details and various authentication techniques and their brief overview.

REFERENCES

AUTHOR’S PROFILE

- Rahul Chourasia is currently pursuing masters degree program in Information Technology in NIIST Bhopal, RGPV University, India, PH:+919926786502.
  E-mail:kanhaiya.chourasia@gmail.com

- Dr. Samidha D. Sharma is a HOD of IT Department in NIIST Bhopal, RGPV University, India, PH:+918989154878.
  E-mail:samidhad2000@gmail.com


