A Survey of Source Authentication Schemes for Multicast transfer in Adhoc Network

Tibin Thomas[1] Jyothish K John[2]
[1]M. Tech [2]Assistant Professor
[1, 2] Department of Computer Science and Engineering
[1, 2] Federal Institute of Science and Technology (FISAT), Angamaly, India

Abstract—An adhoc network is a collection of autonomous nodes with dynamically changing infrastructure. Multicast is a good mechanism for group communication. It can be used in the group oriented applications like video/audio conference, interactive group games, video on demand etc. The security problems obstruct the large deployment of the multicast communication model. Multicast data origin authentication is the main component in the security architecture. The authentication schemes should scalable and efficient against packet loss. In this article we discuss varies authentication scheme for multicast data origin with their advantage and disadvantage

Keywords: Digital Signature, Elliptic curves, Hashes, Message Authentication code, UMAC function

I. INTRODUCTION

An adhoc network is a collection of autonomous nodes with dynamically changing infrastructure. Nodes in the network can communicate each other either directly or by using multi-hop communication. One of the main advantages in adhoc network is multicast communication. Multicast communication provides large scale content distribution through many-to-many or one-to-many data transferring schemes

A. Multicast Communication

Multicast is the best communication mechanism for team oriented application like conferences, video games, video on demand etc. For sending the data in multicast communication uses a multicast tree that covers all the nodes in the network, and thus saves the bandwidth.
The three main properties of multicast communication are:

Open group communication: It allows the group membership is transparent to the source.
All members in the group have same multicast address: This provides the data sent to a multicast address will delivers to all members in that group.
Open access to send packet to the group: Any host in the group can send multicast data, and the data will delivered to all members in the group.
One of the main challenges in multicast data transfer is source authentication. Source authentication enables receiver to verify the authenticity of received packet. Other issues in multicast communication are nonrepudiation, data integrity and data confidentiality. Non-repudiation allows the receiver to prove which host send a particular message. Data integrity makes the receiver to check whether the data has not been modified Data confidentiality allows the information is not made disclosed to the unauthenticated receivers.

B. Authentication in group communication

Authentication in group communication remains a challenging problem in the terms of efficiency, scalability and performance. Even though there are technologies like hashes [16-18], MACs [19], and digital signature [20, 21] provides integrity, authentication and non-repudiation for data, they are designed for point-to-point communication. This problem is mainly due to the presence of multiple members in the group. There are two types of authentication in group communication

1) Group communication: For assuring that received multicast data is from a valid group member.
2) Data origin authentication: For assuring that received multicast data from group members originate from a source having valid identity.

To provide the group authentication, the members in the group use a shared key. By creating a MAC with this group key assures that source (group member) of the data is valid, since only valid group member have the shared key. Using a single shared key is not a secure solution for the data origin authentication in multicast communication because this key is known to all group members cannot be used to identify a specific members. Below we are describes the various data origin authentication schemes. The schemes can be classified into two levels. In the first level includes the data origin authentication schemes having nonrepudiation. The second level includes s data origin authentication schemes without nonrepudiation

The remaining of this paper is organized as follows. In section 2 describes multicast data origin authentication with non-repudiation schemes are discussed with their advantage and disadvantage. In section 3 describes multicast data origin authentication without non- repudiation schemes are discussed with their advantage and disadvantage. Section 4 compares different authentication schemes. We also propose a modified scheme in section 5.

II. MULTICAST DATA ORIGIN AUTHENTICATION WITH NON-REPUDIATION

To assure authentication and non-repudiation the sender has to sign the message. For signing the sender has to use a private key. Hence, a possible solution to guarantee non repudiation would be to sign each multicast message and

then send the signature along with the message. Upon receiving the data, the receiver can verify the signature using the public key of the sender. The figure 1 shows a general procedure of creating and verifying a signature

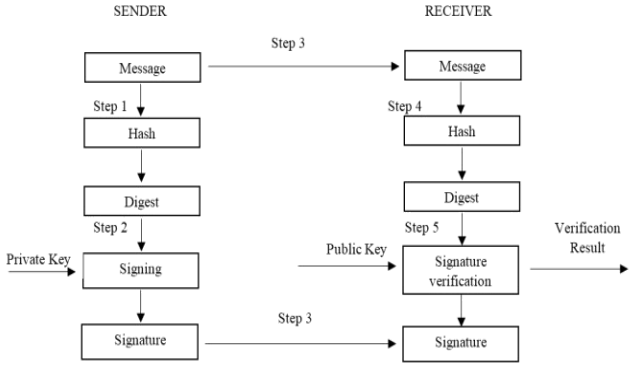

Fig. 1: A general method of assuring non-repudiation using digital signature

A. *Latif-Aslan-Ramly Multi-cast Authentication Protocol*

The authentication protocol described in [6] uses both public key signature and UMAC function. It uses eraser code function to resist the packet loss and a counter value to resist reply attack. The use symmetric encryption system like AES provides confidentiality. At last sender sends the data packet with counter, the UMAC output, and output of the encryption algorithm. The protocols have lowest computation and communication and the protocol doesn't require time synchronization, and have more resistance against the packet loss.

B. *MABS*

This Zhou *et al.* [7] protocol named MABS which uses batch signature to authenticate an arbitrary number of data packets simultaneously. The basic scheme called MABS- B provides batch signatures. The author's propose two batch scheme based on BLS and DSA signature scheme. The author's also extends the MABS-B with packet filtering named as MABS-E, which can alleviate the DOS impact. The scheme eliminates correlation among the packets and also has small latency and communication overhead .The main advantage of the scheme is, even if attacker forged some packet we can verify the received packet. This advantage is actually cause problem, because it gives provision for the sender to deny the ownership of sent packet.

C. *Amortized scheme*

Abuein *et al* [8] propose a multicast stream authentication scheme which amortizes a single signature over a group of packets. The scheme uses a multiple connected chain model, in which each chain connects some packets together. In this the message is first divided into many blocks, where each block contain many packets. For strong loss resistance hash of each packet is append to other packets. For a specific number of packets, source finds the hash Then appends all the hash and sign them using the key Then sends this signature packet at the end of the block to achieve non-repudiation. By increasing the numbers of appended hashes to other packet the scheme achieve higher authentication probability and strong loss resistance against burst packet loss. Since signature packet is sending at end of the block, no immediate authentication is possible

D. *Hybrid scheme*

Aslan proposed [9] a hybrid scheme for authentication over lossy networks. The method can be used for authenticating real time data applications. The scheme is based on the work done by Gennaro and Rohatgi [10] with an enhancement using the Golle and Modadugo [11] method. In this the stream is divided into *m* packets. Then hash of each packet is appended into preceding packet and to another place in the stream. At last the first packet is signed. The scheme requires only less buffer space and low delay at the sender and receiver side. It can resist packet loss and the packets are joinable at any time

E. *Tree chaining*

Wong and Lam [12] proposed tree chaining, a technique that partitions the stream of data packets into blocks and forms a tree structure to perform authentication. In the proposed method a single signature can be used to authenticate each block of n messages. Each leaf node is a Message digest of a data packet. Then the parent nodes are the message digest of two children. At last the root node become the message digest of the entire block, which is signed and send with message. The receiver recomputes digest and compared it to the signed received digest. The scheme improved the signing and verification rates. Packet signature is small and they are individually verifiable. The data packets are associated between each other, so they are sensitive to packet loss.

F. *ECDSA*

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a mathematically derived form of Digital Signature Algorithm (DSA). It has been accepted by ANSI, ISO and IEEE. Johnson et al. gave a complete account of ECDSA in [13]. It uses a public key and a private key. The public key is a random multiple of the base point, while the private key is the integer used to generate the multiple. The key pair is associated with a particular set of Elliptic Curve domain parameters. Since we are using the elliptic curve, the strength per bit is high. After the authentication of information this scheme provides fast and secure distribution of information. Even after providing high security level, this scheme is vulnerable to the attack on Elliptic Curve Discrete Logarithmic Problem and Attacks on the hash function.

III. MULTICAST DATA ORIGIN AUTHENTICATION WITHOUT NON-REPUDIATION

The best solution to make multicast data origin authentication is to make the parties in the group to use a shared key. For sending a message sender finds the MAC of the message using the shared key and send the MAC along with the message. On receiving the message with the MAC, the receiver verify the authentication by verifying the received MAC. Figure 2 shows a general

The above solution creates security problems in multicast communication, since all the members are using same shared key. So the chance of impersonation as the valid

user becomes high. This problem can be solved by making authentication information as asymmetric. Asymmetric means, receivers can only verify the authentication information but cannot forge an authentication information.

There are three major approaches to introduce asymmetry in authentication data.

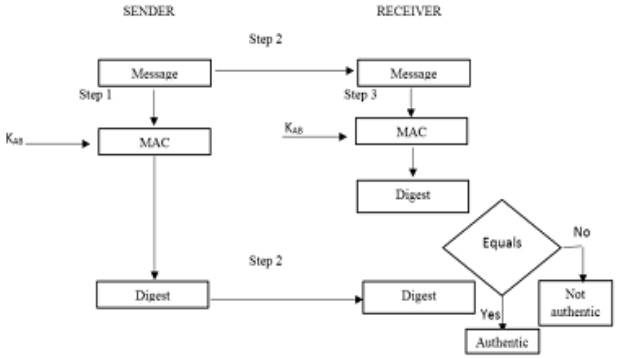

Fig 2: A general method for assuring data origin Authentication using MACs

Secret Information Asymmetry: Here each sender have a set of secret keys. Each receiver have a share of these keys. In this strategy for creating an authentication information requires the knowledge of all keys. So the receivers cannot forge an authentication information.

1) *Time asymmetry:* In this scheme the time asymmetry is achieved by changing the shared key periodically. Also sender guarantees that, the message will be delivered to all members before disclosing the key that is used in the corresponding interval. This prevents the attacker for forging the message using that key.
2) *Hybrid asymmetry:* This is the combination of both time and secret information asymmetry. It avoided the disadvantage of both approaches. In the following subsections we describe the each categories with their advantage and drawbacks.

A. SECRET INFORMATION ASYMMETRY

1) Canetti et al. Protocol

The Canetti et al. protocol [1] assures the authentication by appending MACs to the message. Sender calculates the MACs using k different keys. Each receiver holds a share of secret keys among k keys and verifies the authenticity of the received massage using that shared keys. For an attacker to create a message requires k keys from a coalition of m receivers. The main challenge of this solution is that, sender must share the keys such that no coalition of m bad creates all the holds by a good member. Since this scheme depends on the MACs, which is very efficient to generate and verify this proposed scheme allows an efficient generation and verification of authentication data. Since each packet contain the authentication data, each packets are individually verifiable at any time and also tolerant to packet loss. The main disadvantage of this scheme is that, it cannot overcome the vulnerability that caused by collusion of bad members.

2) Desmedt et al. Protocol

Desmedt et al. Protocol [2] is a polynomial based scheme.This scheme can assure a k out of n multicast authentication. In this scheme each sender creates a polynomial of degree l using the message that is to be send. Then the sender sends a share of the polynomial to each receiver. The source sends the share in such a way that, at least l share of polynomial is required to forge an authenticator. Since the scheme allows a maximum of l-1 members to collude, the security of the system holds. The main advantage of this method is the authenticator of each packet is small in size. This scheme is also tolerant to packet loss, since all packet contain the authentication information. Thus each packet can be verified independently from other packet at any time. The main drawback is that, this method is not practical for most of the steaming application, because the source needs to generate the polynomial and shares them to each receiver for each message.

B. TIME ASYMMETRY

1) TESLA

The TESLA (Timed Efficient Stream Loss-tolerant Authentication) protocol proposed by Perrig et al.[3] uses one way key chain to create the MAC for a message. The sender first generate one way key chain to use as the MAC keys. From that a secret MAC key used to generate the MAC for a particular message in a time interval. Then the message with the corresponding MAC is send to the receiver. The key that is used to authenticate the message is kept secret for a time interval, and discloses the key to the receiver after the interval. This prevent the attacker to receive the key before the message. Upon receiving the key the receiver can verify the authenticity of the previously received packet. For each time interval, this scheme used new MAC key from the one way key chain. Each key is valid only for a time interval. The message that contain the MAC with expired key will be discarded. The main advantage is the reduced size of the authentication information. The generation and verification are efficient and the packets are tolerant against the packet loss. The requirement of time synchronization is the main overhead of this scheme. This scheme is also vulnerable to memory based DoS attack

2) µTESLA

Perrig et.al proposed a modification [4] for removing some disadvantage of the TESLA protocol. By modifying authentication information, the receiver can immediately authenticate the received packet. This scheme also improve the scalability properties of TESLA protocol. µTESLA is more useful in adhoc network with resource constrained environment.

C. HYBRID SCHEME

1) BiBA

Perrig [5] proposed a hybrid asymmetric authentication scheme called BiBa which provides one time signature and broadcast authentication protocol. The BiBa signature exploits the birthday paradox of a hash function on some pseudo random number called SEALS to achieve efficiency and security. SEAL values are the values which

can be verified by the public key of the sender. Sender sends the message with the signature which consist of the subset of SEALS that shows birthday paradox and can be verified at receiver side. This way it achieve the secret information asymmetry. Signing the consecutive messages of the stream, receiver would know all SEALS held by the sender. To avoid this problem BiBa use time asymmetric approach by using different set of SEAL values after a time period. Since BiBa append the signature with each packet, the scheme is tolerant to packet loss. Biba is not vulnerable to collusion of bad receivers because of the time asymmetry feature. The disadvantages of the system are 1) public key size is larger and 2) the sender and receiver must be time synchronized so that receiver know which SEALs to be used for verifying the signature.

D. TAM

Althouse et al. proposed a hybrid two tiered scheme that exploits network clustering to reduce overhead and increase scalability. In this method, the entire adhoc network is divided as clusters, where the inter cluster authentication is done using time asymmetric approach while the intra cluster authentication is done using TESLA protocol (discussed in the previous section). Cluster head is created for each cluster for communicating in inter cluster multicasting. Less communication overhead and scalability are the main advantages. The main disadvantage of this scheme is memory DoS attack. Delayed authentication and time synchronization are the other challenges of this method.

IV. COMPARISON OF DIFFERENT AUTHENTICATION

Latency: Due to the delay in creation/verification of signature latency may occur at sender/receiver sideTime synchronization: Since keys for time asymmetry schemes are valid only for a period, time synchronization may be required. Resist the packet loss: A good authentication scheme must handle the authentication of packets even if some packet lost.

SCHEMES

PAPER	APPROACH	LATENCY	TOLERATE PACKET LOSS	SYNCHRONIZATION REQUIRED	ADVANTAGES
Efficient authentication and signing of multicast streams over lossy channels	EMSS: attaching hash of previous packet, and signing.	At the receiver side	The authentication probability of a packet is at least 90 percent	Yes	With nonrepudiation.
Multicast security: a taxonomy and efficient constructions	MAC based secret information asymmetric scheme.	At the source side	Yes	No	Dynamic addition of sources. Saved the time needed to generate the signature.
The BiBa one-time signature and broadcast authentication protocol	Utilizes birthday paradox scheme. Generate one way SEAL chain for broadcast authentication protocol	At the source side	Yes	Yes	Smaller signature, so verification is fast. With non-repudiation
Multi-receiver/Multisender Network Security: Efficient Authenticated Multicast/Feedback	Polynomial based secret information asymmetry	At the source side	Yes	No	Each packet is small in size.
A Graph-based new amortization scheme for multicast streams authentication	Amortize a single signature over a group of packet. Multiple Connected Chain Model scheme is used.	Not at source or receiver side	Yes	No	Higher authentication probability.
New Real Time Multicast Authentication Protocol	Latif-Aslan-Ramly Multicast Authentication Protocol using public key signature & UMAC	At source and receiver side	No	No	Resist pollution attack Resist replay attack .
MAIS: Multicast Authentication Based on Batch Signature	Use batch signature scheme with packet filtering.	Not at source or receiver side	Yes	Yes	No correlation among packet. Verification possible even if some packet attacked.
Digital Signatures for Flows and Multicasts	Tree chaining technique. Feige-Fiat-Shamir digital signature scheme was extended.	At source and receiver side	Yes	No	Improve signing and verification rates. Packets in a flow are individually verifiable
The Elliptic Curve Digital Signature Algorithm (ECDSA)	Mathematical form of DSA. Uses asymmetric key pair	At source side	No	No	Strength per key bit is high. Secure and faster dissemination of information.
A hybrid scheme for multicast authentication over lossy networks	Combines Gennaro & Rabatgi and Golle & Modadugo scheme	Not at source or receiver side	Yes	Yes	Authentication can be performed at real time Resist the packet loss & possible at real time
TAM: A Tiered Authentication of Multicast Protocol for Ad-Hoc Networks	Network is clustered for authentication, Both time and secret information asymmetry is used.	Not at source or receiver side	Yes	Yes	Less Communication overhead Scalable

The authentication schemes can be analysed mainly based on some features like latency of sending or receiving the data, need of time synchronization, the ability to resist the packet loss etc.

V. PROPOSED SYSTEM

The above discussed hybrid scheme TAM uses the protocol TESLA. The main disadvantage of TESLA protocol is memory DoS attack. Perrig et al. [15]describes about this problem in detail and provides the solution. He proposes a modification to TESLA protocol and create a new protocol called TESLA++. In this protocol the MAC of packet send to the destination with the index of the key before sending the data. The MAC is stored in a compressed form to reduce the memory requirement at the receiver side. Then sends the message and the key. Only message having a corresponding MAC, already received will be accepted, otherwise rejected. This way flooding of invalid message can be reduced and thus receiver can gain memory. So to avoid the shortcoming of TAM, we propose to use TESLA++ instead of TESLA.

VI. CONCLUSION

In this article we first show the problems that are related to the data source authentication. Then we presented protocols that falls in different classes. This survey gives us many conclusions regarding the authentication. First, the

data source authentication is an important part ingroup communication. However many problems like, the number of members in the group and volume of data used by the multicast application need scalability. Since the receivers may have less amount of resources the schemes that we discussed cannot assume high availability of resources. So these type of problems must be solved to allow a larger deployment of multicast applications.

REFERENCES

[1] R. Canetti et al., "Multicast security: a taxonomy and efficient constructions," in Proc. 1999 IEEE INFOCOM
[2] Y. Desmedt, Y. Frankel, and M. Yung, "Multi-receiver/Multisender Network Security: Efficient authenticated Multicast/Feedback," IEEE INFOCOM'92, 1992, pp. 2045–54
[3] A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient authentication and signing of multicast streams over lossy channels," in Proc. 2000 IEEE Symposium Security Privacy.
[4] A. Perrig et al., "Efficient and Secure Source Authentication for Multicast," 8th Annual Internet Society Symp. Network and Distributed System Security, 2001.
[5] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," in Proc. 2001 ACM Conf. Computer Commun. Security.
[6] R.Abdellatif, H.K. Aslan, and S.H.Elramly "New Real Time Multicast Authentication Protocol", International Journal of Network ecurity, Vol.12, No.1, PP.13-20, Jan. 2011.
[7] Y.Zhou, X. Zhu, and Y.Fang"MABS: Multicast Authentication Based on Batch Signature" IEEE Trans. On Mobile Computing, vol. 9, no. 7, pp. 982-993 July 2010.
[8] Q. Abuein and S. Shibusawa, "A Graph-based new amortization scheme for multicast streams authentication", Journal of Advanced Modelling and Optimization, Vol. 7, No. 2, pp.238-261, 2005.
[9] H. K. Aslan "A hybrid scheme for multicast authentication over lossy networks" Elsevier, Computer & security, Vol. 23 pp 705 -713, 2004.
[10] Gennaro R, Rohatgi P. How to sign digital streams. In: Proceedings of CRYPTO'97. California, USA; August 1997. p. 180e97.
[11] Golle P, Modadugo N. Streamed authentication in the presence of random packet loss. In: Proceedings of the ISOC network and distributed system security symposium. California, USA; February 2001. p. 13e22.
[12] C. Wong and S. Lam, "Digital Signatures for Flows and Multicasts," IEEE/ACM Trans. On Networking , vol. 7, Aug ,2004.
[13] Don Johnson, Alfred Menezes and Scott Vanstone. "The Elliptic Curve Digital Signature Algorithm (ECDSA)". Published in International Journal of Information Security, Vol. 1 (2001) pp. 36-63
[14] Mohamed Younis, Osama Farrag, and Bryan Althouse."TAM: A Tiered Authentication ofMulticast Protocol for Ad-Hoc Networks" IEEE Trans. On Network and Service management, vol 9, March 2012
[15] A. Studer, F. Bai, B. Bellur & A. Perrig "Flexible, Extensible, and Efficient VANET Authentication" IEEE Journal of Communications and Networks , vol. 11, no. 6, Dec. 2009
[16] D. Eastlake and P. Jones, US Secure Hash Algorithm 1 (SHA1), Sept. 2001, RFC 3174.
[17] B. Kaliski, "The MD2 Message-Digest Algorithm," Apr. 1992,RFC 1319.
[18] R. Rivest, "The MD5 Message-Digest Algorithm," Apr. 1992,RFC 1321.
[19] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," Feb. 1997, RFC 2104.
[20] Federal Information Processing Standards Publication, Digital Signature Standard (DSS), May 1994, FIPS PUB 186.
[21] R. L. Rivest, A. Shamir, and L. M. Adelman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Commun. ACM, vol. 21, no. 2, 1978, pp. 120–26.

