# MAC based Multicast Source Authentication: A Survey

Ramanpreet Kaur
Department of Computer Science & Engineering
NIT,Jalandhar.

Amrit Lal Sangal
Department of Computer Science & Engineering
NIT,Jalandhar.

Krishan Kumar
Department of Computer Science & Engineering
SBSCET, Ferozpur

## ABSTRACT
Due to increased use of internet for novel types of group communication and bandwidth constraints an urgent need of simultaneous transmission of digital data arises. The applications of multicasting involve TV over internet, video-conferencing, news feeds, stock quotes, online video games and software updates. Some of these applications follow one to many models while others use many to many communications. But success of these applications depends on the factor that how secure they are. Each application has its own security requirements. Many applications require authenticating the source of received traffic to verify that it is originated from the valid member. Till date a large number of protocols have been proposed to support source authentication in multicasting. But each protocol has its advantages and disadvantages. Existing literature classify these protocols into two categories: MAC based approaches and Hash based approaches. This paper give a brief review of MAC based protocols to verify the authenticity of the sender along with their performance comparison based on security level, vulnerability to collusion,Laency at the source and receiver end ,tolerance to packet loss ,Time synchronization requirement and computation overhead parameters.

## Keywords
MAC, Multicast Source Authentication, Group communication security.

## 1. INTRODUCTION
Due to increased use of internet for novel types of group communication and bandwidth constraints an urgent need of simultaneous transmission of digital data, multicasting arises. The applications of multicasting involve TV over internet, video-conferencing, news feeds, stock quotes, online video games and software updates. Each application has its own security requirements. Some of these applications distribute private and sensitive data therefore security becomes prime concern. The basic concerns of securing multicast data is confidentiality, integrity, authenticity and non repudiation of data origin.

Actually the security requirements of a multicast protocol vary from one application to another. Some applications need confidentiality (such as pay per view), some needs source authentication (such as broadcasting stock quotes) while others need both confidentiality and source authentication (such as video conferencing).However in the present model of multicasting "anyone can send, anyone can receive" authenticating the source of multicasting becomes the chief security concern. To fulfill this requirement researchers provide a large number of multicast source authentication protocols. Basically a multicast source authentication protocol should provide the following security services:

***Data integrity:*** The protocol populates each receiver with the ability to verify that packets have not been modified during transmission.

**D*ata origin authentication*:** The protocol populates each receiver with the ability to verify that each received packet comes from the real sender as it claims.

***Non-repudiation:*** The protocol should ensure that the sender of a packet should not be able to deny sending the packet to receivers.

All the three services can be supported by an asymmetric key technique called signature. In one to one communication scenario, 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. However this is very time consuming and computationally expensive process, because communication and computational overhead is large. Thus for applications which do not require non-repudiation of origin a low cost solution MAC based approaches are used which has less communication and computational overhead.

To allow authentication of packets, the source must add authentication information to the distributed content. This authentication information is used by receivers to verify the origin of the transmitted content. This authentication information is computed based on the content to be transmitted. The content can be of two types: Real time content and Pre-recorded Content. The authentication information for the pre-recorded content can be computed in advance whereas real time content requires authentication information computation in real time thus limits the efficiency of the authentication algorithm. However existing literature validates the fact that real time data has stronger need of authentication .For example stock quote distribution where a malicious entity could produce disastrous results.

Over the years various solutions have been proposed by researchers but none of them appears to be a silver bullet. Existing literature differentiate these techniques based on the concept that whether they will provide non-repudiable proof of origin or not. Thus differentiation is based on the fact that technique satisfies source authentication only or source authentication along with non-repudiation of origin.

***Source Authentication*:** Provides the receiver with the ability to verify the authenticity of packet or we can say that receiver can validate the fact that packet is originated from the claimed sender.

***Non-repudiation (of origin):*** Ensures that sender cannot deny sending the data. For this purpose the data should be signed.

This paper will include only symmetric cryptography based approaches more specifically MAC based schemes for multicast source authentication. It will unfold as follows: Section II, give an overview of the common goals of source authentication approaches. Section III discusses the performance criteria's for the evaluation of multicast protocols. Section IV summarizes the proposed approaches. And section V is the conclusion of this literature survey.

## 2. DESIGN CHALLENGES

In unicast settings authentication is simple (MAC computation with secret shared key) but problem becomes much more complex in multicast environments and untrusted receivers along with lossy transmission medium make the problem more severe. Multicast source authentication problem exhibit the following challenges:

- **Receiver Diversity:** Multicast group includes more than two members, each one having different computational powers and storage requirements.
- **Group Dynamics:** Multicast group members can join or leave the group dynamically. Thus any multicast authentication scheme should take dynamism of group members into account.
- **Lossy Transmission Medium:** A large number of existing multicast source authentication schemes do not take into account the lossy nature of transmission medium. Thus fails in case some packet loss occurs.
- **Vulnerability to attacks:** It is possible that attackers exploit the vulnerabilities of multicast source authentication protocols to perform an attack. for example an attacker can perform Denial of Service (DoS) attacks by injecting bogus data packets to exhaust computational or storage capacities of the receivers.
- **Real time content:** For most of the real time applications efficiency is the biggest concern. Due to real time data, authentication information has to be generated in the real time and moreover these applications requires instant authentication at the receiver end.

In order to meet these challenges multicast authentication scheme should include the following:

- **Authenticity:** This property ensures that receiver is able to verify that packet is generated from the valid sender. There are two types of authentication in group communication:
  - **Group Authentication:** This type of authentication is to verify that the data is from a valid group member. It can be achieved by applying a MAC to the message with the help of a shared group key, because only valid group members are supposed to know this key. But this too requires frequent key change due to dynamic nature of the group.
  - **Source Authentication:** This type of authentication is to verify that a packet is originated from the claimed sender. It is complicated to achieve because it requires asymmetry of information in the sense that other group members can verify the authenticity but cannot generate it.
- **Integrity:** This property ensures that receiver should be able to verify that the received data is not modified during the transmission.
- **Non-Repudiation:** This property ensures that receiver is able to verify that a particular sender has sent the message along with proof so that a sender cannot later deny the transmission of that message.
- **Efficiency:** The efficiency of the solution is based on communication, storage and computation overhead at the source and receivers.
- ***Collusion resistance:*** The scheme should provide protection against collusion that is multicast authentication scheme should be resistant to collaboration of receivers for fraudulent purposes.
- ***Minimal latency*:** The scheme should introduce minimum delay for generating authentication information as well as for their verification.

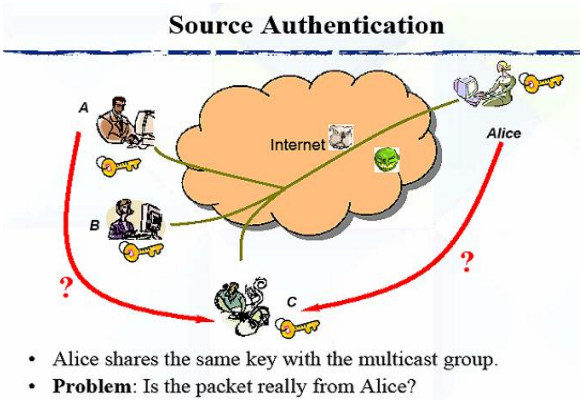


**Figure 1: Problem: Source Authentication**

- ***Robustness against packet loss:*** As we all know internet is an unreliable medium for communication so authentication scheme should take into account its unreliability. That is it should be tolerant to packet loss.
- ***Scalability:*** Scalability is the biggest concern for multicast applications. Because multicasting is a model of one to many communication thus multicast source authentication scheme should be scalable to a large number of receivers.

## 3. PERFORMANCE MEASURES

The parameters to measure the quality of multicast source authentication protocols are:

•***Robustness:*** The ability to verify the authenticity of received data even for unreliable transmission medium.

• ***Buffering:*** Buffering depends on the storage capacity of the sender's and receivers. It can be of two types:

- **Sender side buffering:** The maximum number of packets that need to be stored on the server to compute robust authentication information.
- **Receiver side buffering:** The maximum number of packets that need to be stored on the receiver side before a packet can be authenticated.

•***Computational Cost:*** The computational cost of the scheme. That is computation required to generate valid authenticators and then their verification.

•***Communication Overhead:*** The number of bytes per packets or you can say the size of authentication information that will be applied to the message for verification at receiver end.

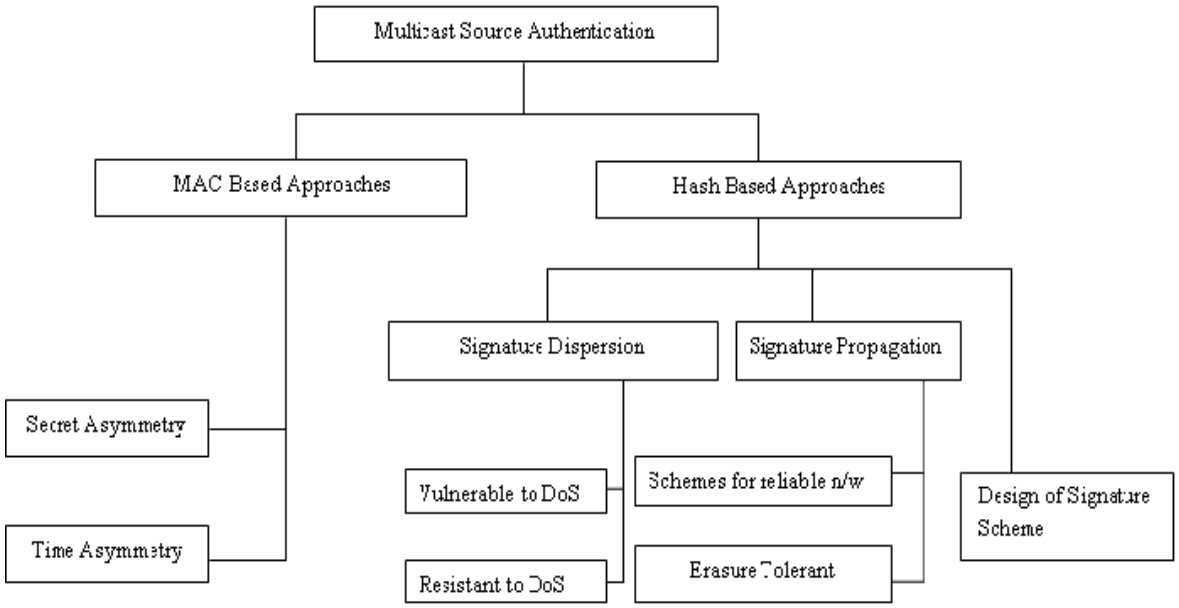


**Figure 2: Classification of Multicast Source Authentication schemes**

Here sender and receiver side buffering are used in the protocols where the authentication information of a packet is stored in one or several other packets. The ideal protocol is one which has perfect robustness, has no buffering or latency and has computational cost and communication overhead as low as possible.

# 4. REVIEW OF EXISTING SCHEMES

This section performs review of MAC based constructions providing data source authentication. To solve the problem of multicast source authentication researchers have proposed many schemes.

As already explained in Section 1 these schemes can be classified into two categories depending on whether they provide a non-repudiable proof of the stream origin or not, namely Protocols without Non-repudiation of Origin and Protocols with Non-repudiation of origin. Protocols without Non-repudiation of origin uses MAC based approaches and Protocol with Non-repudiation of origin uses computationally secure digital signatures.

Figure 2 describe the classification of existing solutions for Multicast source authentication .In a first level they are classified according to their security objective. Then MAC based multicast source authentication techniques can be further classified based on the technique used to introduce asymmetry. This paper illustrates only the schemes that are consistent with the left subtree of this classification tree that is protocols without non-repudiation of origin.

## 4.1 MAC based Protocols

In one to one communication scenario authentication problem is quite simple and can be easily solved by sharing a secret key between communication entities. Where a sender can use the secret key to generate an authenticator and append it to corresponding message whereas receiver will verify the sender's authentication using this secret key by computing the MAC of the received message and compare it with received MAC of the message. However this is not true for multicast communication system because if multiple receivers will have the secret key they can easily generate a valid authenticator and impersonate as another group member. Moreover multicast group is not static, here member's can join or leave the group frequently thus there is a strong need to change the key whenever a member leaves the group. Thus taking into consideration these problems researchers conclude that symmetric solution can only solve the problem of group authentication but fails to address source authentication issue. To address source authentication issue an asymmetric solution is required where receivers are only able to verify the authentication information but are not able to generate it.

To provide MAC based asymmetric solutions 2 approaches are used by researchers in the existing literature:

- **Secret Asymmetry based Solutions:** In these kinds of solutions a secret is shared between the sender and receiver in a way that sender knows the entire secret to generate valid authenticators while receivers only knows a part of the secret that is sufficient to verify the authenticity of received message. In other words a secret is shared in a partial way where senders are able to generate authenticators and receives are only able to verify them using that secret.
- **Time Asymmetry based Solutions:** These kinds of solutions introduce asymmetry in symmetric solutions by delayed disclosure of keys to the receiver. Once the key is disclosed it is no longer a valid key to generate authenticators thus only those messages are valid which are received before key disclosure. However this approach requires periodic key

change as well as buffering resources. Thus introduce the problem of denial of service attack.

## 4.2 Secret Asymmetry based Solutions

Secret asymmetry based approach solve the source authentication problem based on shared secret key mechanism where each member has different set of keys.

The most straightforward way is to use a shared key between sender and each receiver. Suppose a multicast group with n

members. In its most basic form secret asymmetry based solution a sender computes n MAC's and appends them to corresponding message. Each receiver can then verify the authenticity of the message using MAC calculated by the shared key between it and the sender. But this solution has higher communication and computational overhead and suffers from scalability problem.

These secret asymmetry based solutions can be divided into 2 major classes: Computationally secure authentication and unconditionally secure authentication schemes.

- **Unconditionally Secure Protocols**

Unconditionally secure protocols are used for the environments where adversary's resources are unknown in advance. These types of protocols are first suggested by Simmons [9] and later used for multicast environments by Desmedt et. al [18].Unconditionally secure protocols guarantee strong authentication but are not practical in the real world due to their unsubstantial resource needs.

## 4.3 Desmedt.et.al Protocol

Desmedt.et.al[18] suggested a polynomial based scheme which is similar to shamir's secret sharing scheme.In this scheme for every data packet D , the sender selects two polynomials $P_0(X)$ and $P_1(X)$ of degree t and a prime number p at least as large as number of possible data packets to be sent.Then it sends a private share $P_0(i)$ and $P_1(i)$ to each receiver.After that it multicast an authenticator polynomial $A_p(X) = P_0(X)+D.P_1(X)$. Upon reception of data packet D the receiver check the authenticity of data packet by testing if $A_p(i) = P_0(i)+D.P_1(i)$.

### 4.3.1 Advantages:

1. Desmedt et. al protocol tolerates packet loss . Because each packet is used on its own to check its authenticity with the help of authenticator.So verification of each packet is independent from other. So it bears packet loss.
2. 2.This scheme proven to be secure against k receiver's impersonation or substitution attack with a probability greater than 1/ p ( p is chosen large enough so that it is hard for the attacker to make a good guess)
3. 3.S. Obana and K .Kurosawa [11] derived lower bounds on the cheating probabilities (substitution and impersonation) and the sizes of keys of k out of n multi-receiver authentication schemes and showed that the scheme proposed by Desmedt et al. meets all their bounds with equality, which means that this scheme is optimum.

### 4.3.2 Disadvantages:

1. 1.This construction can be used one time only as new polynomials $P_0(X)$ and $P_1(X)$ have to be computed (and new shares to be distributed) for each data packet P which limits the practicality of this solution for streaming.
2. 2.This scheme's security relies on the existence of a secure channel between the sender and each receiver. It is clear that this requirement limits the applications of those constructions as most multicast channels are not secure.

### 4.3.3 Extensions *:*

In [15,16] Naini & Wang generalized the above construction so that the same polynomial can be used to authenticate several packets. The first scheme is based on the notion of Cover free set systems that is for a given set of keys used by sender to authenticate messages,how can the subsets of these keys to the receiver be affected in such away that j(j<k) fraudulent receivers cannot collaborate using their subset of keys to cover the key's subset of a group member.In the same way fujji et al suggested a protocol which is a special case of Naini & Wang approach.

### 4.3.4 Computationally secure protocols:

These protocols give a practical solution with a security guarantee that they cannot be broken with the current computer technology within a period short enough to be practicable. As unconditionally secure protocols are expensive to implement thus researchers focus their attention towards computationally secure protocols.

## 4.4 k-MAC Authentication Scheme

Cannetti et al[14] presented a new approach that is based on the concept that a sender knows several secret MAC keys and these keys are shared with the recipients in such a way so as to maintain several properties of the subsets of keys held by the recipients. For example: one such property could be that no collection of w receivers should know all the keys known by any other receiver. The sender can authenticate a message by computing MACs using all its secret keys and appending all these MACs to the message. This collection of MACs is known as asymmetric MACs. Each recipient can verify the parts of asymmetric MAC for which it knows the secret keys and if all these MACs verify then the receiver accepts the message as genuine. In other words, the sender knows the entire secret required to authenticate messages, and receivers know only a partial view of the secret that allows them to verify received messages' authenticity so that they are not able to generate valid authenticators but can verify them. Note that a receiver, by itself cannot forge an asymmetric MAC since it does not know all the keys of a sender or even all the keys known to some other recipient.

### 4.4.1 Advantages:

1. 1.This scheme can employ well-studied and cryptographically secure MACing schemes and remain secure till the limit on the number of colluders is reached and also for small groups or groups with small number of expected colluders the scheme is very efficient in terms of CPU usage and size overhead.
2. This Scheme tolerates packet loss. Because each packet carries its own authentication information, So verification of each packet is independent from other. Thus it bears packet loss.

### 4.4.2 Disadvantages:

1. 1.From the property of the subsets , even w receivers cannot collude to forge an asymmetric MAC to fool some other recipient. However once there are more than w colluders the security of the scheme could break clown and once there are sufficient colluders to know all the sender keys then the scheme breaks down completely.
2. It does not work well in scenarios where the multicast group is very large and large collusions are likely to occur or difficult to detect.

## 4.5 Time Asymmetry

This approach achieves asymmetry by using delayed disclosure of secrets. In these solutions the sender keeps the key secret for some time interval. Till the key is secret the receivers buffer the packet because they do not have the key to authenticate packets. After some time sender discloses the key and receiver use that key to verify the authenticity of received packets.

However the use of delayed key disclosure introduces a new security threat as receiver must buffer received packets before it can authenticate them. Therefore, an opponent can easily exhaust the victim's resources by sending the illegitimate packets and results in drop of legitimate packets. Thus results in Denial of Service attack. Also a solution based on time asymmetry requires time synchronization between the sender and receivers.

Most of the MAC based approaches requires a secure channel between the sender and receiver in order to share a secret with each receiver. However this requirement cannot be fulfilled in the real world. Thus in the absence of secure channel any attacker can pretend to be valid sender and send a key to the multicast group. Therefore a secure way to send a secret to receiver is required.This requirement is fulfilled in time asymmetry based solutions using one way chains.For this purpose, a one way hash function is used to generate one way chain. For example: Pick a random number $r_N$ and a public one way function F. Here $r_i = F(r_{i+1})$.

The keys $K_n$ are derived from $s_n$ using a publicly available one-way function F', while the $s_n$ are related to each other via a reverse-time chain of one-way functions. To create the chain of key-seeds, the sender chooses a terminal seed $s_l$, and generates $s_{l-1}$ using a one-way function F. The remaining seeds $\{s_0, s_1, \cdots, s_l\}$ are derived via $s_l \rightarrow s_{l-1} \rightarrow s_{l-2} \rightarrow \ldots \rightarrow s_1 \rightarrow s_0$. The sender uses the seed-chain in the opposite direction (starting with seed $s_0$) to derive the keys by applying the one-way function F via $s_n \rightarrow K_n$. These one way hash chains are used to certify a single secret and this secret is used to generate a chain of secrets.

## 4.6 Chained Stream Authentication

Bergadano et al.[8] suggested a new protocol that is based on the concept of one way hash chains.Thus each packet of data is authenticated with a MAC that is computed using key that is generated by one way key chain.The recursive relation between the keys facilitates recovery of lost keys as well as to check the validity of received key that is sent by the key sender. In the proposed scheme, the sender sends data and authentication information in separate streams (Data Sender and Key Sender Process).Receivers also consume data and verify authentication in two step process (Receiver and Authenticator).

***Sender Process:*** First of all the sender announces the session including some essential security information such as session number , starting time, random secret $r_N$, and synchronization information signed by the sender. Then the data sender stream multicast MAC of the packet computed using $r_{N-1}$ along with the message for time period T.Then sender will wait for the delay time and then multicast $r_{N-1}$.Here delay is needed so that the receiver receives all the packets before the corresponding key will be released.

***Receiver Process:***

*Receiver:* Receives X where X can be a MAC, a data block or a key. And then authenticator performs 3 tasks:

1. Receives session announcement and verify signature.
2. Verify the corresponding interval key by computing hash.
3. Check whether the packet is within time bound or late. Here late means packet is receiver after the corresponding key was released. If the packet is not late and interval key is valid then the packet is marked as authentic.

This scheme is based on the concept of delaying just secrets, not information. When secrets are late, viewing is ahead of authentication, and we call this an authentication delay. The delay would be small and roughly equivalent to three times the network latency. The reason is that a MAC must be sent, then the authenticated acknowledgement is returned, and finally the MAC key is sent. Only then can the corresponding block be authenticated by the receiver.

### 4.6.1 Advantages:

1. It is important to note that, for every block, the only authentication information that is multicast is one MAC (sent by the data sender) and one hash value (sent by the key sender). This does not grow with N.
2. This scheme is robust to packet loss. Because losing a packet do not obstruct the authentication of subsequent packets.

### 4.6.2 Drawback:

1. The length of the one-way key chain is limited, and hence to use this solution with infinite streams, the sender would commit to a new one-way keychain and announce it periodically. This periodic announcement induces a new overhead that consists of a digital signature over the first MAC key of the announced chain.

## 4.7 TESLA (Timed Efficient Stream Loss Tolerant Authentication)

Perrig et al.[3,4] introduced a new protocol called TESLA, short for Timed Efficient Stream Loss-tolerant Authentication. Initially, the sender uses a regular signature scheme to sign the initial commitment. All subsequent packets are authenticated through one way hash chaining.

TESLA's working starts by attaching MAC to each packet at sender side with the help of a secret key known only to sender and send these packets to receivers. Receivers in turn store these packets without being able to authenticate them. After some time the sender discloses the key and make the receiver capable to authenticate stored packets. However the receivers discard the packet if they are received too late. However for the proper working of TESLA receiver should synchronize its clock with sender ahead of time. The detailed working of TESLA is explained below:

1. The sender splits up the time into time intervals of uniform duration. Next, the sender forms a one-way chain of self-authenticating values, and assigns the values sequentially to the time intervals (one key per time interval). The one-way chain is used in the reverse order of generation, so any value of a time interval can be used to derive values of previous time intervals. The sender define a disclosure time for one-way chain values, usually on the order of a few time intervals. The sender publishes the value after the disclosure time.
2. The sender attaches a MAC to each packet. The MAC is computed over the contents of the packet. For each packet, the sender determines the time interval and uses the corresponding value from the one-way chain as a cryptographic key to compute the MAC. Along with the packet, the sender also sends the most recent one-way chain value that it can disclose.
3. Each receiver that receives the packet performs the following operation. It knows the schedule for disclosing keys and, since the clocks are loosely synchronized, can check that the key used to compute the MAC is still secret by determining that the sender could not have yet reached the time interval for disclosing it. If the MAC key is still secret, then the receiver buffers the packet.
4. Each receiver also checks that the disclosed key is correct (using self-authentication and previously released keys) and then checks the correctness of the MAC of buffered packets that were sent in the time interval of the disclosed key. If the MAC is correct, the receiver accepts the packet.

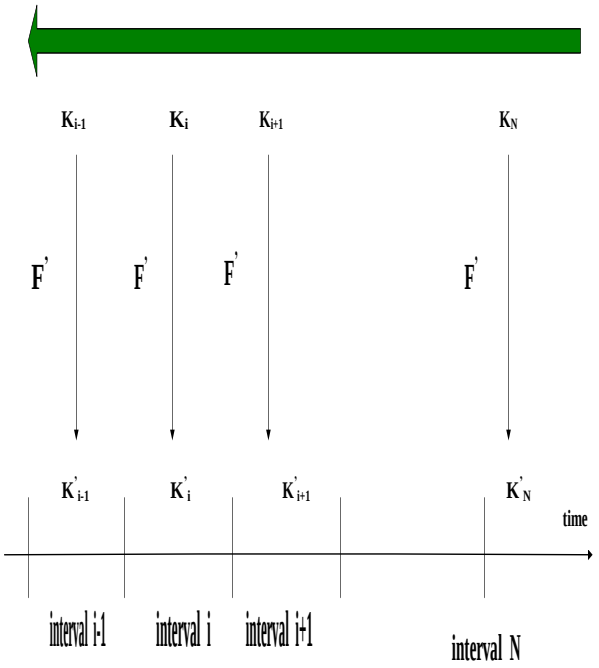


**FIGURE 3: KEY GENERATION**

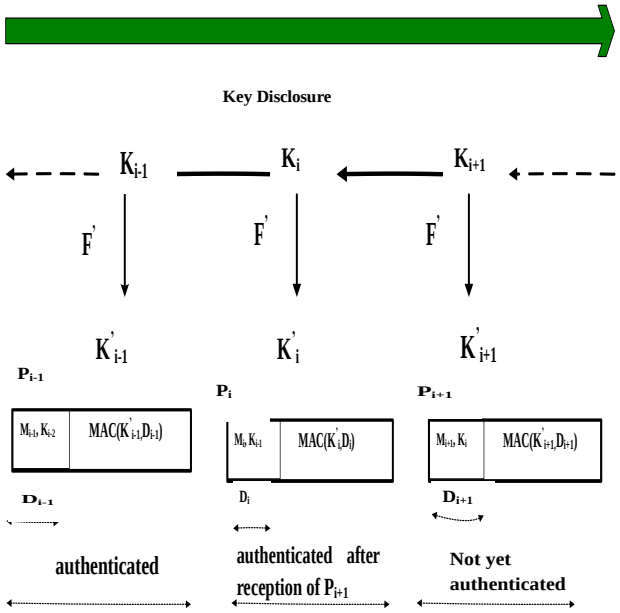


**FIGURE 4:KEY DISCLOSURE**

It differs from the Chained Stream authentication in the sense that it requires initial time synchronization. Whereas in Chained Stream Authentication a confirmation is required (i.e. a challenge-response mechanism) for each received packet and this confirmation value is also a value from a one-way chain - a new key is released only when the arrival of the previous key is confirmed.

**4.7.1 Advantages:**

1. One-way chains have the property that if intermediate values of the one-way chain are lost, they can be recomputed using later values. So, even if some disclosed keys are lost, a receiver can recover the key chain and check the correctness of packets.
2. It has low computation and communication overhead. Since the authentication information size is only one MAC.

**4.7.2 Drawback:**

1. 1.In TESLA the sender needs to perform authenticated time synchronization individually with each receiver. This may not scale well, especially in cases where many receivers wish to join the multicast group and synchronize with the sender at the same time.
2. 2.In TESLA the receiver has to buffer packets, until the sender discloses the corresponding key, and until the receiver authenticates the packets. This may delay delivering the information to the application, may cause storage problems, and also generates vulnerability to denial-of-service (DoS) attacks on the receiver (by flooding it with bogus packets).
3. 3.TESLA assumes that all members have joined the group and have synchronized with the sender before any transmission starts. In reality, receivers may wish to join after the transmission has started.

## 4.8 Improvements to TESLA

1. ***Immediate Authentication:*** The original TESLA protocol is vulnerable to Denial of Service attack due to the requirement of buffering of packets at receiver's end before authenticate them. To overcome this drawback researchers propose a new method to support immediate authentication that is packets will be authenticated as soon as receiver receives them. Basically this method replace receiver buffering with sender buffering. The sender will buffer packets for one disclosure delay, and store the hash value of the data of a later packet in an earlier packet. Thus if earlier packet is authenticated, the data in the later packet will be authenticated through the hash value.
2. ***Concurrent TESLA instances:*** Choosing the disclosure delay is very critical problem. Because if a very short disclosure delay is chosen for receivers with long network delay by the researchers then most of the packets will violate the security condition and get dropped whereas a longer disclosure delay for short network delay receivers causes unnecessarily long authentication delay. Thus a balance between these two must exist, which is quite difficult to achieve. Thus researchers propose a new solution which uses multiple instances of TESLA with different disclosure delay simultaneously. So that each receiver can decide which disclosure delay and hence which instance to use.
3. ***Time Synchronization Issues:*** An important component of TESLA is loose time synchronization between the sender and receiver. However there are many sophisticated time synchronization protocols exist but they have high complexity and considerable management overhead. Thus are not suitable for TESLA protocol. That's why researchers propose a new simple and secure time synchronization protocol that satisfies the requirements of TESLA protocol

## 4.9 Staggered TESLA

Li et al. [13] describes a scheme known as Staggered TESLA, which is built upon the TESLA scheme, but uses multiple staggered authentication keys that are used in computing MACs for authenticating a packet. Thus in staggered TESLA receiver could partially authenticate a packet by using those authentication keys it has prior to the arrival of new key seeds. Because in TESLA, a MAC computed by the authentication key corresponding to that particular interval is attached whereas in staggered TESLA additional MACs are also attached. Actually these additional MACs provides partial source authentication.

In staggered TESLA receiver side buffers packets in the form of a sequence of queues. When a receiver receives packet it put the packet in the top level of the queue and gradually moves the packet to lower levels as additional key seeds arrive at the receiver and corresponding MACs are verified. This process repeats until the final key is disclosed and complete authentication is performed. If any verification fails the packet is immediately dropped. Thus staggered TESLA is based on the concept that if a packet is forged by an opponent, MACs computed by earlier keys are likely to be wrong, with the help of which receiver will be able to detect the presence of bogus packets before the actual key is disclosed. In this way staggered TESLA is resistant to DoS attack as compared to conventional TESLA.

**4.9.1 Advantages:**

1. The property of staggered TESLA to drop bogus packets before the actual key is disclosed makes it resistant to DoS attack as compared to conventional TESLA. Because now adversary has to perform DoS attack at higher rates so that they will occupy receivers resources before victim can actually identify that they are forged.
2. The use of partial authentication concept provides intermediate security levels between two extremes that are not-authenticated and fully-authenticated. Thus new security policies can be developed.
3. Staggered TESLA improves the buffer utilization of receivers. Because bogus packets are dropped faster in staggered TESLA than in conventional TESLA.

***4.9.2 Drawbacks:***

1. The idea of using multiple MAC results in shift attack. In the shift attack, the adversary may take advantage of the fact that there is more than one MAC attached to each packet, and make use of the MACs from previous packets and shift them to forge later packets.
2. Staggered TESLA requires extra computation and communication to verify and transmit the extra MACs compared to conventional TESLA.

# 5. PERFORMANCE

This section summarizes the performance of the above protocols in the tabular form with respect to their performance evaluation criteria. Their performance is summarized in table

# 6. CONCLUSION

This paper discusses Multicast Source authentication problem particularly MAC based approaches along with design goals and performance evaluation criteria's for them. It reviewed Asymmetric solutions based on symmetric key cryptography where asymmetry means that receiver can verify authentication information but cannot generate it by placing them into 2 main classes: Protocols based on secret asymmetry and Protocols based on time asymmetry. Protocols based on secret asymmetry tolerates packet loss and no sender or receiver side buffering is required however they have high computation and communication overhead and does not scale well in case of large number of recipients. Also the problem of collusion is there, whereas in case of time asymmetry there is low computation and communication overhead but they have a buffering and time synchronization requirement that minimizes its efficiency. The schemes for multicast authentication reviewed in this paper suffer from one of these drawbacks:

1. Most of the key asymmetry based techniques are prone to collusion attacks. That is receivers can collaborate to form collusion and share keys. Thus we can say that key asymmetry based techniques cannot be applied in scenario where receivers are untrusted.
2. Most of time asymmetry based solutions require time synchronization between the sender and the receivers. With the receivers located at different locations for applications such as online stock quotes, pay-per-view TV, etc. it becomes difficult to maintain time synchronization between the sender and the receivers.
3. They have sender or receiver side buffering requirements. This may delay delivering the information to the application, may cause storage problems, and also generates vulnerability to denial-of-service (DoS) attacks.
4. Moreover secret asymmetry based solutions assume the presence of secure channel to share secrets. Which is not true in the real world.

This paper also concludes that current research work in the field of Multicast source authentication focuses on Hash based approaches because several techniques have been proposed which reduces the signature overhead by using signature propagation and signature dispersion techniques. And thus the communication and computation overhead of digital signature based schemes becomes comparable to that of MAC based approaches. However these MAC based schemes still act as a basis for the environment where sender and receivers have limited resources such as wireless sensor networks scenarios. Thus for wireless sensor networks modified MAC based approaches such as µTESLA, SPINS etc.

In the end we can say that there is no solution which can satisfy all the requirements .Hence the best solution for one application may not be best for another. Therefore it is important to understand fully the requirements of the application such as buffer space at sender and receiver side, tolerance to packet losses and nature of application before selecting a solution.

**Table 1: Performance Summary**

| Scheme | Security Level | Vulnerability to Collusion | Latency at Source | Latency at Receiver | Tolerance to packet Loss | Synchronization Required | Communication Overhead |
|---|---|---|---|---|---|---|---|
| Desmedt et.al | Uncondionally | Yes | No | No | Yes | No | $(t+1)[\log_2 p]$ |
| K-MAC | Conditionally | Yes | No | No | Yes | No | l bits, where l depends on the size of the largest fraudulent receivers coalition |
| CSA | Conditionally | No | No | Yes | Yes | Yes | \|MAC\|+MAC key |
| TESLA | Conditionally | No | No | Yes | Yes | Yes | \|MAC\|+MAC key |
| Stagg.TESLA | Conditionally | No | No | Yes | Yes | Yes | d\|MAC\|+seed |

## 7. REFERENCES

[1] Adi Shamir," How to share a secret," Communication of the ACM, 22(11):612 – 613, November 1979.

[2] Adrain Perrig, Ran Canetti, Dawn Song, and J. D.Tygar," Efficient and secure source authentication for multicast," In NDSS 2001, pages 35 – 46, San Diego, USA, February 2001. Internet Society.

[3] Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Song," Efficient authentication and signing of multicast streams over lossy channels," In IEEE Symposium on Security and Privacy, pages 56 – 73, Oakland, USA, May 2000. IEEE Press.

[4] Adrian Perrig et al., "The TESLA Broadcast Authentication Protocol," RSA CryptoBytes, vol. 5, Summer 2002.

[5] Alain Pannetrat,Refik Molva ," Efficient Multicast Packet Authentication," In Proceedings of the Symposium on Network and Distributed System Security Symposium (NDSS 2003). Internet Society, Feb. 2003.

[6] Christophe Tartary," Authentication for Multicast Communication," PhD thesis, Macquarie University, October 2007.

[7] D.Boneh,G.Durfee, and M. Franklin,"Lower Bounds for Multicast Message Authentication,"Eurocrypt '01, LNCSvol.,no. 2045, 2001, pp. 437-52.

[8] Francesco Bergadano, Davide Cavagnino, and Bruno Crispo. Individual single source authentication on the MBONE. In ICME 2000, volume 1, pages 541 – 544,New York, USA, July 2000. IEEE Signal Processing Society.

[9] Gustavus J. Simmons," A survey of information authentication,"Proceedings of the IEEE,76(5):603 – 620, May 1988.

[10] H. Fujii, W. Kachen, and K. Kurosawa ,"Combinatorial Bounds and Design of Broadcast Authentication," IEICE Trans., E79-Avol., no. 4, 1996, pp. 502-06.

[11] K. Kurosawa and S. Obana,"Characterization of (k,n)Multireceiver Authentication," Information Security and Privacy, ACISP'97, LNCS, vol., no. 1270, 1997, pp. 204-15.

[12] Paul Judge and Mostafa Ammar ,"Security Issues and Solutions in Multicast Content Distribution:A Survey",IEEE Network,Jan/Feb. 2003,pp.30-36.

[13] Qing Li and Wade Trappe ,” Staggered TESLA:A Multicast Authentication Scheme Resistant to Dos Attacks “,In IEEE Global Telecommunication Conference (Globecom’05) Volume 3 ,November 2005.

[14] Ran Canetti, Juan Garay, Gene Itkis, Daniele Micciancio, Moni Naor, and Benny Pinkas,” Multicast security: A taxonomy and efficient constructions,” In IEEE Conference on Computer Communications, volume 1, pages 708–716, New York, USA, March 1999. IEEE Press.

[15] Rei Safavi-Naini and Huaxiong Wang,” New results on multi-receiver authentication code,” In Advances in Cryptology - Eurocrypt’98, volume 1403 of Lecture Notes in Computer Science,pages 527 – 541, Espoo, Finland, June 1998. Springer - Verlag.

[16] Rei Safavi-Naini and Huaxiong Wang,” Multireceiver authentication codes: Models, bounds, constructions, and extensions,”Information and Computation, 151(1-2):148 172, May 1999.

[17] S. Obana and K. Kurosawa, “Bounds and Combinatorial Structure of (k, n) Multi-receiver A codes,” Designs, Codes and Cryptography, vol. 22, no. 1, 2001, pp. 47-63.

[18] Yvo Desmedt, Yair Frankel, and Moti Yung,”Multireceiver/multi-sender network security:Efficient authenticated multicast/feedback,” In IEEE INFOCOM1992, volume 3, pages 2045 –2054, Florence, Italy,May 1992. IEEE Press.

[19] Y. Challal, H. Bettahar, and A. Bouabdallah, “A taxonomy of mukticast Data Origin Authentication:Issues and Solutions,”IEEE Communication Surveys ,Third Quarter 2004.

[20] Y. Challal, H. Bettahar, and A. Bouabdallah, “A2Cast: An Adaptive Source Authentication Protocol for MultiCast Streams,” IEEE- ISCC’2004, June 2004