Framework for Anonymity in IP-Multicast Environments

Christian Grosch
University of Hagen, Department of Communication Systems
Feithstr. 142/TGZ, D-58084 Hagen, Germany
Email: christian.grosch@fernuni-hagen.de

Abstract— **The importance of the global internet for conferencing and entertainment increases with the expanding availability of multicast capable networks. As with other applications and services, security concerns in multicast environments become a major topic for the research community. While there are a lot of publications available analysing the problems of group authentication and privacy, the aspect of anonymity in multicast environments has seldom been considered yet. This paper focuses on a fundamental overview of this topic, introduces a concept for providing anonymity for both senders and receivers in a multicast scenario and presents a optimisation concept for the system.**

I. Introduction and Motivation

The attractiveness of applications for multipoint communication increases with the expanding availability of conference partners in the Internet. To manage the transmission of high bandwidth multimedia streams, produced by special tools for video and audio conferencing or shared editing, new protocol elements for better scaling, more efficient usage of network resources and improved security services are being developed and integrated in the IP architecture.

The use of the multicast capable Internet backbone, the MBone, for business conferencing, entertainment, education, gaming and private conversation rises the need for security considerations. The global Internet as a public switched network offers a number of weaknesses to an attacker, who could easily gain access to the packets traversing public links and routers. Therefore multicast security has been established as an important research area quite recently. The first attempts to improve the security of group communication have been published in 1994 [4], followed by a number of further papers [6], [9], [5]. These papers mainly concentrate on the efficient distribution of symmetric session keys to all legal group members and the reliable exclusion of former members, leaving the group.

While these works cover the security services of authentication and privacy, the research results presented in this paper deal with the aspect of anonymity in multicast environments, a security element which has not been regarded yet in the context of group communication, but which is quite apparent in the context of point-to-point communication in the WorldWideWeb. The idea was to develop mechanisms and protocol extensions for providing receiver and sender anonymity, reflecting the following main design goals:

- *Compatibility with current protocols.*
The solution should work without changing elements of the existing multicast protocol framework.
- *Minimisation of protocol overhead.*
The advantages of efficient media distribution via multicast should remain.
- *Scalability of the system.*
The concept has to be expandable, depending on the degree of the desired security measures and the number of hosts participating in specific multicast sessions.

To fulfill this set of requirements, a number of models have been developed. These are the *Dedicated* and *Shared Multicast Anonymiser* for receiver anonymity and the *Shared Sender Anonymiser* for sender anonymity.

II. Group Communication and Anonymity

Although anonymity has seldom been regarded in the context of multicast until now, a lot of work has been done for anonymising traditional point-to-point communication in the Internet and the WorldWideWeb. The Internet user becomes more and more aware of the fact, that he produces data traces in the network by simply using a web browser. By contacting a web server, personal information like operating system type and version, language, IP address, the most recently connected web server address and sometimes even the email address could be transmitted. Internet shopping makes the situation even worse, because data like name, address, bank account information and credit card numbers are often transmitted without any safeguarding. The potential danger of the availability of these information reaches from customer profiling for advertising to massive credit card misuse.

In his paper [1], David Chaum presented a general concept for providing anonymity, called *Mix*. This fundamental idea is the basis for several emerging services for web anonymity. Projects like *Onion-Routing* [3], *The Anonymizer*[1] or *Janus/Rewebber* [8] are available via a web browser and provide a kind of proxy service. They contact web servers and get information requested by a client, so that a server could only identify the anonymiser as the demanding host, not the client himself. Another approach, differing from Chaums Mix concept is named *Crowds* [7]. The main idea in this case is to build a large group of hosts, which provide the described proxy service

[1] `http://www.anonymizer.com`

for each other in a specific, cascading and randomised way.

Evolving the Mix concept from one-to-one to one-to-many and many-to-many relationships, there are a number of aspects to be considered, especially regarding the implementation details of the protocols used for multicast communication in the Internet. The fundamental open group multicast concept, invented by Deering [2], introduced a range of IP addresses, which no longer identify a single Internet host, but a multicast group. This fact already provides a low level of anonymity for the individual group members, because the receivers can no longer be identified by analysing an IP packet header of a message on its distribution way from the sender. The anonymity characteristic is improved further by the fact, that a multicast packet, transfered from the assigned router into the LAN as a shared medium, could be originally requested and received from any host in this local network. Therefore, by simply analysing the traffic, it is far more difficult to identify a multicast group member, than communciation partners for the point-to-point case.

Nevertheless, further measures are necessary to provide anonymous participation in group communications. Currently the MBone is driven by a set of standard applications used for video and audio conferencing, chat and shared editing. Appropriate tools for these applications demonstrate, how easily the advantages of multicast regarding anonymity could be undermined. In the case of the well known MBone tools, it is a common practice to send membership messages to the multicast address the tool is currently assigned to. All similar applications connected to the multicast group are permanently listening for these reports. Membership reports contain the name, email address and organisation description of the client and the sender could also be identified by the sender address field of the IP packet.

As this is a process automatically executed without knowledge and approval of the user, it shows how easily personal information could be compromised. A reliable and secure anonymisation service necessitates additional measures as presented in this paper.

III. Multicast Receiver Anonymity

The *Dedicated Multicast Anonymiser* (DMCA) is a straightforeward application of the Mix concept, providing receiver anonymity. The core element of this concept is a process, running on a powerful workstation and accepting requests from hosts, which want to participate in a specific multicast group. The request consists of the multicast addresses[2] of the desired media streams and the corresponding information for their forwarding to the receiver by multiple unicast links. So after a first negotiation sequence, the DMCA participates in the group representative for the hosts and forwards the received multicast traffic directly to the clients. The left part of Fig. 1 illustrates the concept.

[2]Throughout this text, the term *multicast address* is always used meaning the (address:port)-pair.

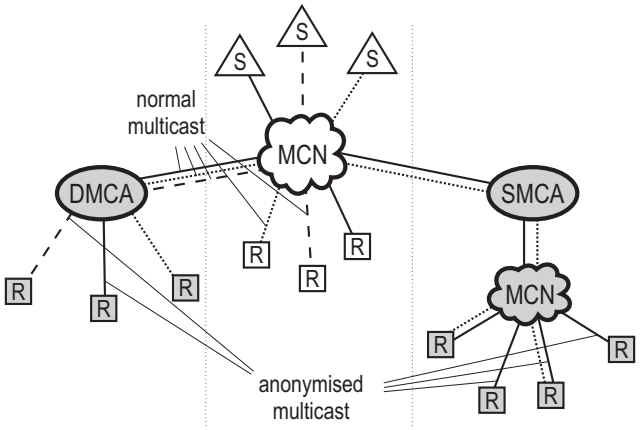


Fig. 1. Dedicated and Shared Multicast Anonymiser

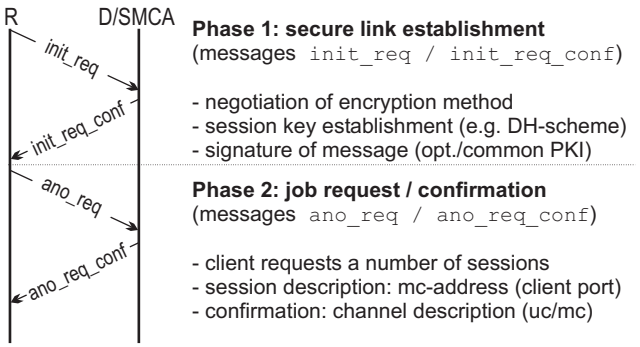


Fig. 2. Simplified initialisation protocol for receiver anonymity

Fig. 2 shows a simplified scheme of the protocol used for starting a new anonymisation session. A minimum of two rounds are necessary for the initial message exchange. First a secure channel is established and thereafter the transmission and confirmation of the session data take place. In the presented example a Diffie-Hellman based scheme is suggested. Both communication partners create and transmit the desired key elements. Optionally the DMCA signs the `init_req_conf` message for ensuring authenticity of the message by using a common PKI. In its second message, the client now transmit the request itself. The message consists of n multicast stream description sets $\{r_1, \ldots, r_n\}$ determining the multicast address/sender pair. The message `ano_req_conf` confirms the request by naming the multicast groups which will be added to the anonymisation service. The basic scheme of this negotiation process remains the same for all modules presented in this paper. The datails of the messages change respectively.

To provide a reliable and secure service, there are a

number of additional aspects to be considered. As described in Chaums paper, encryption, packet renumbering and fill pattern insertion should be applied by the DMCA, to prevent the identification of related media streams by analysis of incoming and outgoing IP packets. It is further necessary, to perform a number of similar tasks in parallel to hide the identity of the packets.

The aspect of session announcement should be considered for completeness, too. The fact, that a client joins the group for a well known announcement address (e.g. MBone SDR channel `sap.mcast.net = 224.2.127.254`) could already be compromising, so that the anonymiser gets the additional task to listen to these channels and provide the information in the initialisation process over a secure link.

The concept of the DMCA has some serious disadvantages. By performing anonymisation tasks individually for each client, the efficiency of the multicast concept gets lost in case several hosts want to participate in the same multicast group. The *Shared Multicast Anonymiser* (SMCA) takes these circumstances into account and improves the concept by introducing the multicast concept for the anonymous receiver group as well.

The right part of Fig. 1 illustrates the scheme. The SMCA accepts requests in the same form, as described before, but instead of establishing a unicast link to the client, it initiates a separate multicast tree for distributing the forwarded media streams to the host. If further clients request anonymisation for the same multicast group, they could simply be added to the existing tree and cause therefore only minimal additional overhead.

The costs for this concept are the additional measures necessary for maintaining session lists, managing the session key for the receiver group (including reliable exclusion) and the distribution of these session keys to the clients. By using standard MBone tools and protocols, the system is flexible enough to integrate any existing method, as introduced e.g. in the papers refered to in chapter I.

IV. Multicast Sender Anonymiser

While DMCA and SMCA provide anonymity for the receivers in a multicast group, the *Shared Sender Anonymiser* (SSA) is a concept for the sender side, based on the same idea. Sender and SSA first establish a secured link and exchange the necessary information before the SSA joins the requested group as substitute for the sender. The SSA receives the encrypted traffic from the sender, decrypts it and forwards it to the corresponding multicast address. Fig. 3 illustrates the SSA concept.

If the anonymised sender of a session is the group initiator at the same time, the problem of session announcement has to be addressed, too. In this case the SSA has to provide the additional functionality of initiating a new

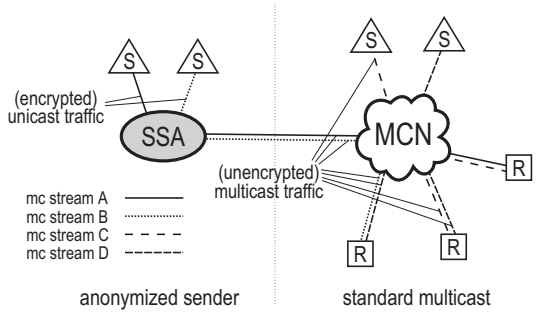


Fig. 3. Shared Sender Anonymiser

multicast session and distributing the information to the well known announcement address. If the sender wishes to receive reply messages, a pseudonym has to be negotiated with the SSA first, so the anonymiser is able to identify messages addressed to the sender and forward them accordingly. It is further possible for the sender to join the group as a normal participant or via a DMCA or SMCA service a second time. This is especially useful, if the group has more than one sender, distributing media streams in a conference session.

V. Closed Groups

Authentication and privacy are the most important security services needed for pay-tv transmission or secure business conferencing. The anonymisation model developed in this paper incorporates the different security concepts by adding a further module, the *Access Control Anonymiser* (ACA).

For controlling a closed user group in the context of multicast, it is a common technique, to add two functional entities on the sender side. The *Group Authority* (GA) initiates and "owns" the group. It decides upon the membership of clients and provides an access control list (ACL) to the *Group Controller* (GC). The GC is responsible for managing the group, by generating and distributing session keys.

If a client wants to join a group anonymously, it first contacts the ACA and formulates a request, containing the necessary information for getting an access control certificate (ACC) from the GA of the specific group. This ACC could be used later for requesting the current session key from the GC and proving the legality of the demand. Again the ACA could be used as an intermediate instance to hide the identity of the client.

Fig. 4 finally shows the overall concept, especially illustrating its flexibility. In the example presented, nearly all different types of senders and receivers are included. Some senders/receivers use the anonymisation services ($S_{3/4}, R_{3/4}$), the others not. Two senders ($S_{2/4}$) provide data for a closed user group and the other two not. It must be stressed, that the multicast network cloud (MCN) rep-

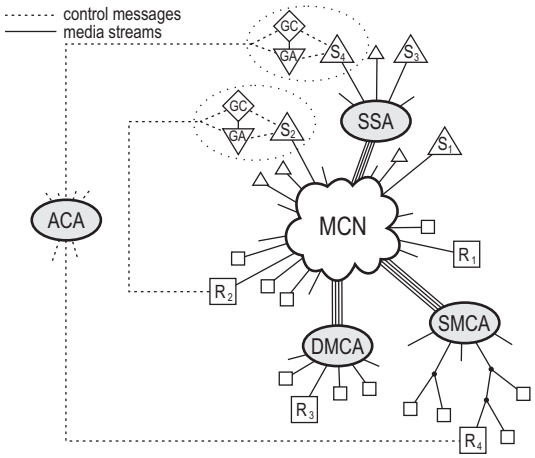


Fig. 4. Integrated Model

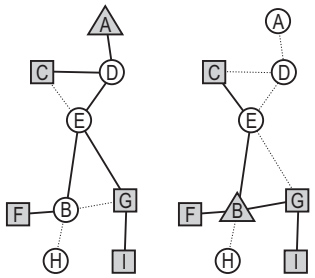
resents a standard IP multicast network and therefore no changes to existing transport protocols or router functions/protocols are necessary.

VI. Optimisation

The presented concept provides anonymisation of multicast sessions by introducing intermediate servers, located anywhere in the Internet. Obviously additional traffic is generated: packets travelling detours for passing the anonymiser, encryption and integration of fill pattern and the intruduction of specific negotiation protocols for session initialisation. The analysis of the concept includes several aspects. The degree of reliability and security of the service is one main topic, the performance aspects for sender, receiver, anonymiser and the network the other. In this paper a solution for reducing the additional network load is introduced. This is done be finding a location for the anonymiser, which implies minimal multicast trees.

The question of additional network load for the models introduced was first analysed by introducing a simulation scheme basing on models of different real network topologies (e.g. the german MBone). The simulation results confirmed the obvious observations, that the additional network load depends on the topology of the multicast group, i.e. the location of sender and anonymiser and the number and location of the receivers as well. While sender and receiver distributions are dynamic and nearly impossible to influence, the location of the anonymiser could be possibly choosen in a given network. The fundamental question in this case is to determine a network node for which the multicast trees for average member distributions show optimal characteristics.

Fig. 5 illustrates the problem. In both examples an anonymiser is represented by the sender symbol (A and B). The original senders and optional additional participants connected via standard multicast are omitted, because they are of no relevance for the problem itself. For the comparison of the two scenarios different characteristics could be calculated. To simplify matters, a homogeneous network with equally weighted links is assumed, so that the topologie could be modelled by a bidirectional graph $G = (K, E)$. Regarding the SMCA or SSA models, the tree weight is measured by the number of links involved in the distribution of the stream from the sender to all clients. Although this method is quite simple, its output suffices for a rough estimation.



	A	B
tree weight	7	5
perc.of network	70 %	50 %
avg. dist	1,5	3,25

Fig. 5. Example trees for different sender locations

From the table in Fig. 5 it could be seen, that the differences for the scenarios are remarkable. Because of its unfavourable location, the weight for sender A is about 28% higher than that for sender B. The value for the average distance from the sender to all members, measured in numbers of links to pass, even differs by a factor greater than 2. This example illustrates, that a deliberate choice of the location of an anonymiser instance could lead to a remarkable reduction of network load and optimisation of traffic characteristics like packet latency.

But how could an optimal location for a multicast sender or anonymiser be found? As mentioned above, this paper concentrates on the two aspects of network load and average distance. Obviously there are different solutions for each problem, so a decision has to be made, which aspect is of most importance. Otherwise a compromise solution may be suitable, too.

For finding an optimal location to ensure minimal route length for an average multicast tree, there are well known and efficient algorithms like the ones from Dijkstra or Floyd-Warshall. E.g. if the outcome of the Floyd-Warshall algorithm, $d^n(e_i, e_j)$ describes the minimal distances between any two pairs of nodes $e_i, e_j \in E$, the average distance for each sender $s \in E$ results in

$$\bar{d^n}(s) = \frac{1}{n-1} \sum_{i=1}^{n} d^n(s, k_i) \quad \text{with} \quad k_i \neq s. \qquad (1)$$

If we further determine the minimum of these values, the optimal solution for this problem has been found. Although it could be guessed that for a lot of network topologies a strong correlation between this definition of "centrallity" and the one regarding minimal average network

load exists, the formal dependency is somewhat more complex. The main idea is to determine the probability of the involvement of each network link in an average distributed multicast tree for a sender s and a specific group size t.

A connected and undirected graph $G = (E, K)$ with $E = \{e_1, \ldots, e_n\}$ and $K = \{k_1, \ldots, k_m\}$ representing network nodes and links shall be given. For a designated sender $s \in E$, the directed subgraph $G_s \subseteq G$ with $E_s = E$ and $K_s \subseteq K$ denotes the full shortest path tree (SPT) from s to all other nodes $e_i \in E \setminus s$. For each link $k \in K$, the function $e : E, K \rightarrow \mathbb{N}_0$ denotes the number of nodes, which will be potentially connected downstream in a shortest path multicast tree for the sender $s \in E$. Thereby $e(s, k_i)$ equals the size of the subtree $G_{s,a}$ with a, the indexed endpoint of the link k_i, being the root of the subtree. $|G_{s,a}|$ could easily be determined by standard graph algorithms, e.g. a recursive depth first search run. Fig. 6 shows the known example graph with sender node A, where all nodes participate in the group. In this case, the links are weighted by $e(A, k_i)$.

$e(s, k_i)$ could now be used to determine the involvement probability $i(s, k_i, t)$, which is calculated as the ratio of the number of member distributions $p(s, k_i, t)$ with a minimum of one member connected downstream of k_i to the number of all possible distributions $v(t)$:

$$i(s, k_i, t) = p(s, k_i, t)/v(t) \quad \text{with} \tag{2}$$

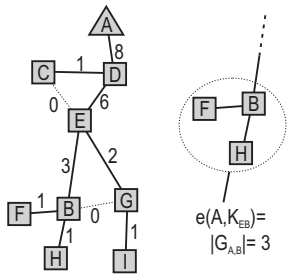
$$p(s, k_i, t) = v(t) - \bar{p}(s, k_i, t)$$

$$= \begin{pmatrix} n-1 \\ t \end{pmatrix} - \begin{pmatrix} n-1-e(s,k_i) \\ t \end{pmatrix}. \tag{3}$$

The overall weight for an average multicast tree could now be calculated as $w(s, t) = \sum_{i=1}^{n} i(s, k_i, t)$. By finding the minimum average tree size for all possible sender nodes $s \in E$, an optimal location for a multicast sender or an anonymiser could be determined, with the parameter t set to a suitable group size. The calculated values for the example in Fig. 6 could be learned from the corresponding table. It shows the average distances as well as the function results for $w(s, t)$ and $t = \{3, 4\}$. In these cases, node E could be clearly identified as the preferable choice, but in general multiple suitable solutions are possible. Finally it should be noticed that this result is applicable for multicast tree optimisation in general. The method is not limited to anonymisation problems.

VII. Conclusion

This paper focused on anonymisation of multicast senders and receivers as one previously unregarded security element of group communication. A framework of several modules has been introduced and an- optimisation concept regarding network load and average distance has been presented. For practical evaluation, a prototype of the model has been implemented in Java und successfully



t	$w(s,t)$ 3	$w(s,t)$ 4	$\phi d(i,j)$
A	9,93	11,43	2,88
B	8,18	11,11	1,62
C	9,21	11,00	2,13
D	8,67	10,43	2,00
E	7,96	10,00	1,50
F	9,43	11,11	2,50
G	8,61	10,40	1,75
H	9,43	11,11	2,50
I	9,79	11,40	2,62

Fig. 6. $e(s, k_i, t)$ for sender node A and $w(s, \{3, 4\})$ and the mean average distance for all possible senders.

demonstrated in an experimental environment. Further research work concerning this topic is in progress.

Acknowledgement

The research work presented in this paper has been done at the Department of Communication Systems of the FernUniversität Hagen. The author thanks Prof. Dr.-Ing. Firoz Kaderali for the supervision of his work.

References

[1] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, Vol. 24(Nr. 2), 2 1981.

[2] Stephen Deering. Host extensions for ip multicasting. *IETF Request for Comment 1112*, 8 1989.

[3] David Goldschlag, Michael Reed, and Paul Syverson. Onion routing for anonymous and private internet connections. *Communications of the ACM*, Vol. 24(Nr. 2), 2 1999.

[4] Li Gong and Nachum Shacham. Elements of trusted multicasting. In *IEEE Proceedings of International Conference On Network Protocols, Boston*, 10 1994.

[5] Christian Grosch. Security measures in ip-multicasting-classification and comparison. In *Proceedings of the European Conference on Networks & Optical Communications (NOC'99)*, 6 1999.

[6] Suvo Mittras. Iolus: A framework for scalable secure multicasting. In *Proceedings of ACM Conference of the Special Interest Group on Data Communication (SIGCOMM '97), Cannes*, 9 1997.

[7] Michael Reiter and Aviel Rubin. Crowds: Anonymity for web transactions. *DIMACS Technical Report 97-15, AT&T Labs-Research, Murray Hill*, 8 1997.

[8] Andreas Rieke and Thomas Demuth. Janus: Server-anonymität im world wide web. In *Horster, Patrick: Sicherheitsinfrastrukturen:Grundlagen, Realisierungen, Rechtliche Aspekte und Anwendungen*, 1999.

[9] Debby M. Wallner, Eric J. Harder, and Ryan C. Agee. Key management for multicast: Issues and architectures. *IETF Internet Draft: draft-wallner-key-arch-01.txt*, 9 1998.