Overlay AuthoCast: Distributed Sender Authentication in Overlay Multicast

Matthias Wählisch[†]
Freie Universität Berlin
Institut für Informatik
Email: waehlisch@ieee.org

Thomas C. Schmidt
HAW Hamburg
Dept. Informatik
Email: t.schmidt@ieee.org

Gabriel Hege
HAW Hamburg
Dept. Informatik
Email: hege@fhtw-berlin.de

***Abstract*—Multicast services raise significant operational and security challenges not only when deployed on the Internet layer, but also in overlay networks. Large P2P groups as emerging from IPTV applications may be abused by unwanted traffic or denial of service attacks through amplified flooding. In this paper, we introduce a distributed, autonomously verifiable scheme for multicast sender authentication, which does not depend on pre-established trust relationships. Based on cryptographic identifiers and passport packets, any overlay peer is enabled to verify the origin of data prior to forwarding and to repel its misuse. Dynamic ingress filtering and individually established gradual trust allow for a lightweight protection of the distribution system in structured overlays.**

***Index Terms*—Multicast source authentication, cryptographically generated identifiers, P2P, structured overlay multicast**

I. Introduction

Infotainment and collaboration, i.e., voice and video (group) conferencing, as well as large scale content distribution, e.g., IPTV and massive multiplayer games (MMORPGs), are considered the key applications for the next generation ubiquitous Internet. Nevertheless, efficient group services via multicast on the Internet layer are not globally provided, but remain restricted to walled domains. Structured peer-to-peer systems offer multicast services in an infrastructure-agnostic fashion, using deterministically organized key-based routing (KBR) while operating on hash identifiers. They are reasonably efficient and scale over a wide range of group sizes.

Multicast is inherently predestined to facilitate DDoS attacks, as it amplifies traffic on a possibly enormous scale. Threats become even more severe in the context of overlay networks, as these place enhanced stress onto the underlying infrastructure. Approaches to authenticate overlay multicast (OLM) sources are thus desired, and should enable any peer to discard bogus traffic. Complying to incentive-driven self-organization, multicast source authentication should be performed autonomously per peer and on the packet level.

In this paper, we propose a lightweight multicast extension to sender authentication based on cryptographic identifiers, which allows for a cryptographically strong traffic validation at the packet level. This mobility-compliant 'Overlay Authocast' protocol is introduced in section II along with its extension to the case of multiple simultaneous sources within one group and a numerical performance evaluation. A brief discussion of protocol properties is presented within the final conclusions.

This work is supported by the German BMBF within the project *Moviecast* (http://moviecast.realmv6.org).

[†]The author is also with HAW Hamburg, Dept. Informatik.

II. Overlay AuthoCast

Overlay content distribution commonly is organized among independent peers that agree on a distribution scheme and a group identifier. To prevent an abuse of this multicast distribution infrastructure, forwarders need to verify the legitimacy of a sender, i.e., require means to authenticate a source w.r.t. the group. P2P overlay networks are not govern by pre-established trust among peers, but by incentives. It is therefore desirable to enable a peer-wise independent validation of traffic. Due to the multicast nature, any such packet authorization has to proceed within unidirectional signaling, as feedback messages will violate the scalable communication paradigm.

Currently, the only known method for autonomously verifying authenticity is by the use of cryptographically generated identifiers (CGIs). Having its seeds in cryptographically generated IPv6 addresses (CGAs) [1], cryptographic identifiers have been transferred to overlay addressing [2] and do not conflict with current KBR implementations such as Chord or Pastry. CGAs have been recently used in AuthoCast [3] to derive a generic framework for mobile multicast source authentication in IP. The approach of CGI-certified group identities can be extended to overlay multicast source verification as follows.

A. Single-Source Authentication

a) Base Scheme: The creator of a group or group controller that has generated its cryptographic overlay ID from a public-private key pair $(\mathcal{K}_{pub}, \mathcal{K}_{sec})$, will use $\mathcal{K}_{pub}$ to configure the group address G equally as a cryptographic identity. Conflicts within the overlay node ID space can be avoided by adding a counter.

In signing the packets using $\mathcal{K}_{sec}$ and attaching $\mathcal{K}_{pub}$, the group controller will provide cryptographically strong proof of ownership to any receiving peer of the packet: After extracting $\mathcal{K}_{pub}$, an intermediate node can reconstruct source and group address and validate the signature. Having verified that the source is the valid owner of the group, data will be forwarded according to the OLM protocol in use. In any case of failure, the OLM forwarder drops the packet, thereby cutting distribution along multicast branches.

b) Optimized Scheme: Depending on the key length in use, multicast packets may be unreasonably enlarged by the public key piggybacked with data. RSA signature validation in addition is laborious and may not be applicable to every packet traversing. These security overheads can be mitigated by securing multicast forwarding relationships separate from

data and offering peers an option to gradually acquire trust in upstream neighbors.

To establish source-specific authentication to forwarding relations throughout the multicast distribution network, the source initially sends a 'passport' packet down the multicast routing path, once. This signed passport contains the complete CGI extensions, including the public key. Peers store this passport, and augment multicast forwarding states by $\mathcal{K}_{pub}$, as well as by the verified overlay source address. In the absence of churn and group dynamics, any peer is thus enabled to match a group address to the valid source address *and* to its public key. Subsequent data packets need not carry $\mathcal{K}_{pub}$, but only the signature to allow for authentication. Whenever multicast branches change, or in the presence of mobility or churn, a peer may face new downstream neighbors. To them, it simply forwards the passport packet which will allow for a fully authenticated maintenance of augmented states at newly arriving peers.

To further avoid the overhead of signature verification, overlay nodes may simply check for the cached source address. This however will raise the threat of global impersonation. To prevent spoofing, peers can establish ingress filters with respect to the underlay address of their upstream neighbor. In structured overlays, packet forwarding deterministically follows the KBR, and upstream neighbors are well defined. Each peer can reliably restrict source-specific traffic to the legitimate upstream forwarder of a group by verifying the address triple of group, source and ingress port. The need for cryptographic signature validation ceases to apply with increasing trust in the upstream forwarder.

As each peer can detect unwanted traffic from invalid signatures, it can individually decide on a strategy of gradual trust establishment or continued validation. In the presence of overlay multicast schemes that allow for multipath transport, a node may even employ this degree of trust for a dynamic path selection.

B. Multi-Source Authentication

Multiple multicast senders contributing to the same multicast group require admission by the group controller. This admission authority has created the cryptographically generated group address. Before an additional multicast source S injects data, it requests a certificate. The group controller authenticates the sender and – according to an application policy – issues the certificate, which includes S, the peer membership of G and an optional lifetime. The certificate is signed with the private key corresponding to the creation of G. A multicast source that wants to transmit data attaches this certificate and signs packets with its own private key. An OLM router verifies whether the group certificate is valid and the group address G has been generated from the group public key. Additionally, the router authenticates the source CGI according to the certificate and the peer identifier as described in the single-source case. All optimizations derived from extended state caching at forwarding peers remain likewise applicable.

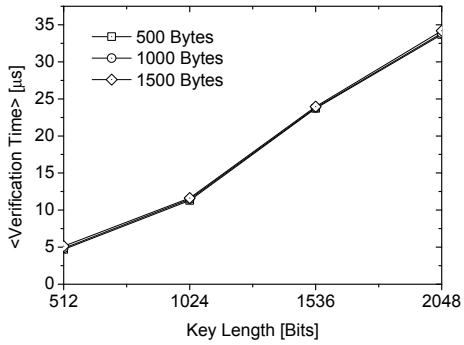

Fig. 1. Processing times for CGI signature verification

C. Protocol Performance

To quantify the processing overhead of the CGI verification, we have implemented the scheme on a standard Linux platform (2.4 GHz AMD Athlon X2 processor) using the OpenSSL library. For typical ranges of key lengths and packet sizes we measured absolute processing times. Averages were taken over 50 randomly generated keys, each of which employed to verify 10.000 packets. Results are displayed in figure 1. Strikingly, processing costs remain independent of data packet sizes, since the overhead of evaluating SHA-1 hashes is negligible as compared to RSA signature verification. Processing overheads are in the order of $10 - 20\ \mu s$ and appear compliant to the overall routing performance attained in overlay networks.

III. Discussion & Conclusion

We have presented Overlay Authocast, an extension of CGI-based host authentication to multicast sources in structured P2P networks. This protocol enables overlay peers to detect unauthorized data independently and on an individual packet level. An efficient caching of authentication credentials, and protected upstream neighbor relations mitigate security overheads, and offer a path to gradual trust establishment at individual peers. Any peer that decides for traffic validation will not only protect itself from unwanted forwarding loads, but will keep subsequent overlay members free of malicious flows. In offering shared benefits, this scheme nicely follows a co-operative P2P paradigm where the incentive offered to the individual enhances the overall system quality.

This fully distributed and autonomously verifiable method remains valid under varying node and forwarding conditions. In particular, it can be equally applied in schemes of multipath multicast transport, as well as in the presence of mobile multicast parties, thereby encouraging the belief that Overlay Authocast is a candidate for real-world deployment.

References

[1] T. Aura, "Cryptographically Generated Addresses (CGA)," IETF, RFC 3972, March 2005.

[2] I. Baumgart, "Peer-to-Peer Name Service (P2PNS)," P2PSIP, IETF Internet Draft – work in progress 0, November 2007, expired.

[3] T. C. Schmidt, M. Wählisch, O. Christ, and G. Hege, "AuthoCast — a mobility-compliant protocol framework for multicast sender authentication," *Security and Communication Networks*, vol. 1, no. 6, pp. 495 – 509, December 2008.