Bloom Filter-Based Scalable Multicast: Methodology, Design and Application

Xiaohua Tian, Shanghai Jiao Tong University
Yu Cheng, Illinois Institute of Technology

Abstract

Bloom filter based multicast has recently been proposed as a promising methodology for scalable multicasting. The basic idea underpinning this family of multicast mechanisms is to encode the multicast routing information into a Bloom filter carried in the packet. Thus, the routers are relieved from maintaining per-group forwarding states and able to support multicasting with improved scalability, compared to traditional IP multicast. In this article, we first review the evolution path of multicast protocols to shed light on the impetus that had driven the multicasting technology forward. We then discuss several representative Bloom filter based multicast protocols, with revealing their core design issues. While multicast is normally considered the most efficient way for delivering multimedia services, how to fully leverage the advantages of Bloom filter based multicast protocols to facilitate multimedia delivery is still an open issue. In this regard, we present a design that exploits a Bloom-filter based multicast protocol to accelerate the channel zapping in an IPTV system. Moreover, we point out the open research issues hoping to promote new development in the field.

The prevalence of multimedia applications, such as IPTV, video conferencing, online multi-player games, over the Internet has manifested the importance of developing a scalable and efficient networking protocol to disseminate shared data to widely distributed destinations. Recently, Bloom filter based multicast has been proposed as a solution for the need, where routing information is carried in the multicast packet in the format of a Bloom filter. This family of protocols has been gaining an increasing interest in the field due to their desirable scalability over predecessor multicast protocols. This article gives a tutorial of the Bloom-filter based multicast protocols by answering some important questions. What is the fundamental issue hindering the success of the traditional multicast protocols? How has the research on multicast evolved all the way to the current state? What specific benefits can the Bloom filter based multicast bring? How could the Bloom filter based multicast benefit the multimedia applications over IP? What could be the open research issues in the field?

We reveal the impetus behind the evolution path of multicast mechanisms, in order to help understanding how multicast has developed into the current state. The evolution of the multicast mechanism in fact epitomizes the evolution of Internet itself. The early IP multicast is to construct a tree structure by networking routers in a single flat topology [1]. As the domain-based hierarchical architecture adopted by Internet, multicast protocols originally designed for the flat network are extended into the inter-domain scenario, where improving IP multicast scalability has been put many efforts but still can not be thoroughly resolved. This is because the networking node involved in IP multicast has to install a forwarding state for each multicast group it is supporting, and the associated messaging and memory overhead will grow linearly.

The Bloom filter based multicast takes a source routing methodology. The fundamental design is to carry routing information in the multicast packet in the format of a Bloom filter, which is a randomized data structure for representing a set and supporting membership queries [2, 3]. The routing information will be extracted by the intermediate networking node and used to compute appropriate packet copies and output interfaces. Since each node has no need maintaining the group-specific forwarding states, the Bloom filter based multicast has desirable scalability. According to the information encoded into the Bloom filter, these multicast protocols can be categorized as *tree oriented* [4]and *destination oriented* [5], where the former encodes the multicast tree branches while the latter encodes receiver domains' network prefixes. This seemingly slight difference can incur significant distinctions in protocol design and performance, which will be described later in a tutorial manner.

Multicast is normally considered the most bandwidth efficient way for delivering multimedia services, but how to utilize the particular features of Bloom filter based multicast protocols to facilitate multimedia delivery is still an open issue. This article provides a synergetic perspective for designing IPTV systems, where the Bloom filter based multicast not

Xiaohua Tian's work in this article is partially supported by NSFC 61202373, SRF for ROCS by SEM, China Postdoctoral Science Foundation Grant 2011M500774 and 2012T50417, STCSM Grant 12JC1405200, and Open Foundation of State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) (SKLNST-2013-1-16).

 0890-8044/13/$25.00

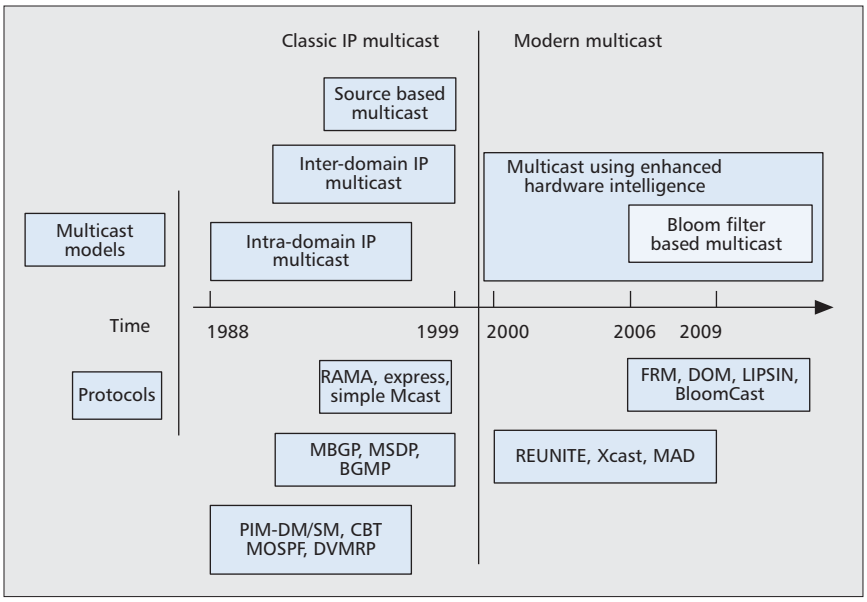

Figure 1. *Evolution path of multicast.*

only provides a scalable transportation scheme, but also accommodates the special demands of the IPTV systems. Specifically, we examine how the Bloom filter based multicast with the source routing approach could be applied to the IPTV system to reduce the channel zapping delay, which is incurred by the video compression scheme and the IP based delivery. The application may shed light on how to further exploit the Bloom filter based multicast for multimedia services.

The source routing feature of Bloom filter based multicast brings both challenges and opportunities. On one hand, encoding routing information in the multicasting packet could incur security breaches, where the potential attacking and corresponding defending schemes for destination oriented approach are still not studied. On the other hand, the source routing mechanism provides an opportunity to improve the reliability for Bloom filter based multicast, where the source could retransmit different lost packets to different receivers by encoding different routing information.

In the remainder of this article, we first present the methodology behind the evolution of multicast mechanisms. We then describe the design of representative Bloom filter multicast mechanisms. A synergetic design for mitigating channel zapping delay with Bloom filter based multicast for the IPTV system is presented, followed by a description of open research issues in the field. Concluding remarks are given at the end.

Methodology

An evolution path of multicast technologies is given in Fig. 1, which can be roughly divided into two stages: the classic IP multicast and modern multicast.

IP Multicast: Constructing the Group-Specific Tree

The essence of IP multicast is to construct a data delivery tree with routers for every group active in the network, where each group ID represents end hosts with shared data. To construct a tree, the sender could first broadcast data packets all over the network to build an all-connected tree, and unintended receivers then send pruning messages in the reverse direction to cut tree branches for unwanted groups, which is known as "broadcast-and-prune" [1]. Receivers can also initiate the tree construction process, where receivers unicast explicit joining messages to a selected core or rendezvous point (RP) to construct the core/RP-rooted tree [1]. These two approaches are widely used in the intra-domain IP multicast protocols, where all networking routers are connected in a flat topology and under the administration of the same network service provider.

With Internet adopting a domain-based hierarchical architecture, providing Internet-wide multicast service is confronted with new challenges. The broadcast-and-prune approach is obviously inapplicable due to its bandwidth inefficiency. The challenge confronted by the approach with explicit joining procedure is the asymmetric routing in the inter-domain environment, i.e., the joining paths are not necessarily valid for data delivery due to administrative reasons [5]. Moreover, data source and core/RP are not necessarily in the same domain, where the receivers in one domain may be unable to receive traffic from the data sources in other domains.

To deal with the issue of asymmetric routing, the protocol for spreading network topology information allowing multicast is developed, known as multiprotocol extensions to BGP-4 (MBGP) [5]. To deal with different placements of the data source and the core/RP, the protocol for informing the core/RP the existence of data sources in other domains is developed, known as multicast source discovery protocol (MSDP) [1]. With such facilitations, each domain could construct a core/RP based multicast tree and these trees in multiple domains can be connected to realize multi-domain multicast. Another solution is to directly construct a domain-level core based tree with the border gateway multicast protocol (BGMP) [1], where the multicast address-set claim (MASC) protocol [1] is developed to support core selection.

The defects of inter-domain multicast solutions above are their complex configuration and unsatisfactory scalability, which are partially incurred by supporting the "more-than-enough" many-to-many communication paradigm. With the argument that many large-scale applications only require delivery from an often well-known source, *source-based* service model with one-to-many paradigm has been proposed, which makes the source the root of the multicast tree, and thus simplifies the complexity and improves the scalability to some extent.

In summary, the methodology of IP multicast is simple: constructing a multicast tree for each multicast group, either within a domain or over multiple domains. It is worthy note that the tree constructed is group specific, which means that the number of multicast forwarding states need to be maintained at each networking node will linearly grow with the number of multicast groups being supported by the node, so do the messaging and memory overhead. This is the root cause of scalability problem suffered by IP multicast.

Modern Multicast: Exploiting Network Intelligence

IP multicast has not been widely deployed due to its scalability issue and other marketing reasons, which invites the emergence of application-layer overlay multicast [6]. However, more efforts are made to solve the scalability problem of IP multicast based on the network-layer approach. This is because multicast is a generic service commonly used by a wide variety of multimedia applications, and a scalable and efficient multicast mechanism should be one of the infrastructural functionalities provisioned by the network. Meanwhile,

the rapid development of hardware and software technologies provides an opportunity for streamlining the design of the network.

In most of the modern multicast protocols, the group-specific forwarding states maintained at each router, as adopted by IP multicast protocols, are traded with packet-carried information and corresponding computation at each router for better scalability. REUNITE [7] enables initiating multiple unicast within the network to implement multicast, where the branching routers require complicated processing to reduce the per-group forwarding states. Xcast [8] encodes the destinations list in the packet header and enhances the router with the capability of modifying the in-packet destinations list. The networking routers in MAD [9] could switch between the network layer overlay multicast and IP multicast mode, depending on the group scale and frequency of message exchange.

The free riding multicast (FRM) protocol [4] is the seminal work stimulating the research on Bloom filter based multicast protocols. The fundamental idea of FRM is to compute a domain-level multicast tree, and to carry the tree in the packet in the format of a Bloom filter, which is for space efficiency [2]. The Bloom filter is a randomized data structure for representing a set and supporting membership queries, as shown in Fig. 2. An empty Bloom filter is a bit vector consists of m bits that are all set to 0. To represent a set of n elements, each element is hashed using k hash functions to k bit positions, and the corresponding bits are to be set to 1. To query the Bloom filter if an objective is an element of the original set, the objective is to be hashed using the same hash functions. If any 0 bits are found in corresponding positions, the objective is definitely not a member of the original set; however, it may happen that the Bloom filter falsely report that the objective is a member of the set when obtained bits are all 1s, which is referred to as f*alse positive*.

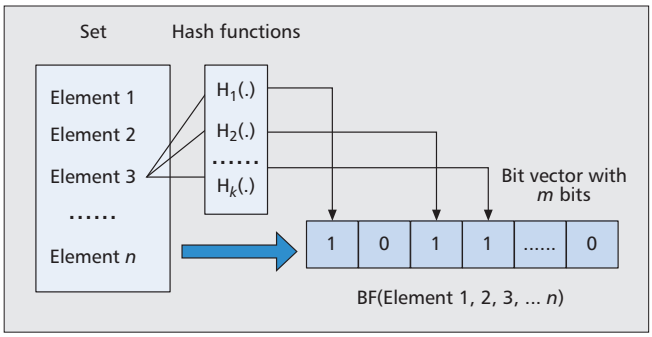

Figure 2. *Principles of the Bloom filter.*

Design

Depending on which routing information, multicast tree branches or destination network prefixes, are encoded in the Bloom filter of the packet, different service models are in the front and different designs have been developed, which to be described in detail in the following.

Service Model

The tree oriented approach (TOA) and the destination oriented approach (DOA) are illustrated in Fig. 3. As Bloom filter based multicast focuses on inter-domain environment, we use the designated border router to represent each domain for convenience of demonstration. In the tree oriented approach (TOA), the border gateway protocol (BGP) advertisements [4], originally used for exchanging reachability information for each domain, is augmented at the receiver domain with a description of the multicast groups currently active within the domain. These advertisements spread to the entire network, with the membership information notified to other domains. The source domain detects the destination domains for an active group, and computes a domain-level multicast tree for that group through combining unicast path vectors to all destination domains, with scanning local BGP routing table. The tree will then be encoded using a Bloom filter and inserted into each multicast packet. When receiving such a packet, the transit domain border router examines each of its neighboring domain-level edges against the attached Bloom filter to compute appropriate packet copies and output interfaces. The representative protocol with the TOA model is the free riding multicast protocol [4].

The destination oriented approach (DOA) explicitly sends joining messages to the data source domain for membership management, and the joining messages establish forwarding states that will be utilized for later data forwarding. The multicast packet with DOA encodes only destination network prefixes into the Bloom filter. When receiving a packet, the forwarding states installed at each interface are compared against the in-packet Bloom filter for computing packet copies and output interfaces. It is worthy note that the states in intermediate nodes are network prefixes in the format of the Bloom filter; therefore, even if a given node is supporting thousands of groups active in a receiving domain, it only needs to maintain one forwarding state for the domain. The representative protocol developed with the DOA model is the destination oriented multicast (DOM) protocol [5, 10].

Core Design Issues

Eliminate Forwarding Anomalies — The false positives in Bloom filter based computation may incur forwarding anomalies such as packet storms, loops and duplicate flows [11], which could be eliminated using both stateful and stateless mechanism in TOA. With the stateful scheme, each link is assigned multiple link IDs and the multicast tree is constructed using chosen IDs with lowest estimated false positive rate [12]. Moreover, when receiving a packet, the router analyzes the in-packet Bloom filter to check if it contains a path that may lead the packet to return. If positive, the packet and its incoming interface will be cached for checking following packets for potential loops.

With the stateless mechanism, the *bit permutation* is used to reduce the false positive rate of Bloom filter based forwarding. The tree is constructed from leaves in a link-by-link manner, where each link of the tree is first encoded into a Bloom filter and then re-mapped to a different arrangement. A unique multicast tree is built at the data source side by ORing all cumulatively permuted Bloom filters. During the forwarding, the falsely delivered packet can not be correctly demapped through the bit permutation thus to be dropped.

The problem of stateful scheme is that the router caching the suspect packet is not necessarily the origin of the forwarding anomalies; therefore, the false positive traffic may not be fully truncated. The stateless scheme assumes symmetric routing environment where it works smoothly; however, inter-domain routing is usually asymmetric as we mentioned earlier. Moreover, it still can not identify the origin of the forwarding loop. Bit permutation can only mitigate the probability of the forwarding loop rather than totally prevent it.

DOA exploits the features of its own routing scheme to eliminate forwarding anomalies: first, the number of elements encoded in the in-packet Bloom filter normally keeps decreasing at each hop, and it will not increase at least; second, the falsely forwarded traffic will definitely be received by some receivers due to the way the forwarding states are installed. If keep decreasing, the remained 1-bit positions in the Bloom filter will be unable to match any at-interface forwarding

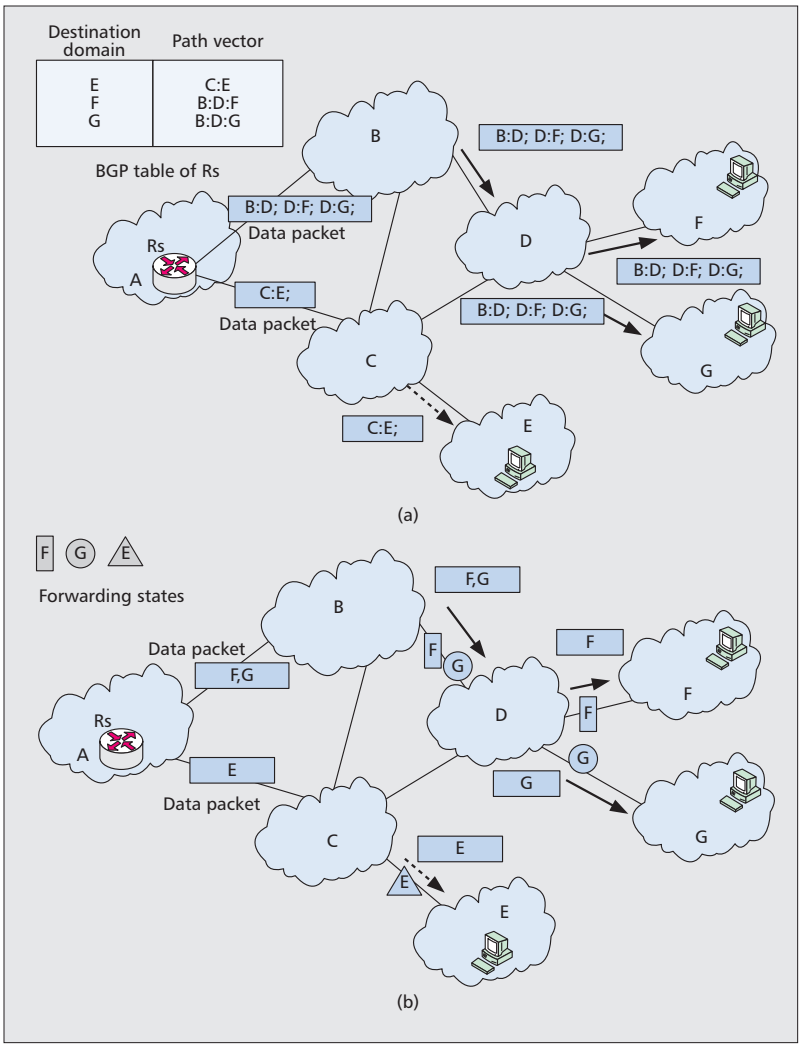

Figure 3. *Service model: a) TOA model; b) DOA model.*

states eventually, and the forwarding loop will automatically be eliminated. If the 1-bits keep unchanged, the second feature needs to be used. When receiving the falsely forwarded traffic, the receiver could trace back the packet to its source hop by hop, and turn off the source of false forwarding. The trace-back message will trigger intervening nodes to sample group ID from the passing traffic, where a small number of group-specific states are needed to block the falsely forwarded traffic [13].

The DOA could completely eliminate the forwarding loop (once occurred) by the false positive. Because of the trace-back scheme, the origin of the false forwarding will be accurately identified and turned off. The scheme can work in both symmetric and asymmetric routing scenario, where the BGP information could be of great help [13].

Transparentize Asymmetric Routing with BGP Information — TOA computes the data delivery tree at the source domain, which in most cases supports multicasting in the asymmetric routing scenario. However, BloomCast protocol [11] is an exception, where receivers send explicit joining message to subscribe to a source with performing bit permutation at each hop. How to deal with asymmetric routing is not specified in BloomCast.

DOA utilizes the source domain BGP routing information to handle the asymmetric routing issue. The idea is to make receiver side border router informed of the path vectors perceived at the source side. The joining message can then be delivered along the path reverses to the notified path using source routing [10]. With this scheme, a fast-join mechanism can be derived in DOA, where the data traffic could be steered to the receiver upon the joining message hits any node currently forwarding the requested traffic [10]. Consequently, the receivers in DOA may observe a shorter data access delay compared with TOA, for which the joining process must be accomplished at source node.

Security Solutions — The difference between forwarding anomalies prevention and security mechanism is that the former deals with the accidental events while the latter defends hostile attacks specifically waged for the Bloom filter based multicast protocols. Two main hostile attacks are the chain reaction attack and the target path attack [14]. The first is to trigger occurrence of forwarding anomalies, and the second is to converge as many packet flows as possible on a particular path with a large number of zombie hosts. Currently, there are three security mechanisms for Bloom filter based multicast: limiting the number of 1-bits in the Bloom filter, varying the structure of the Bloom filter, and encrypting the link IDs or the Bloom filter, where the essence of them all is to mitigate the false positive rate.

Networking nodes need to check the Bloom filter's *fill factor* ρ_{max}, defined as the proportion of 1 bits in the bit vector, before any further packet processing operation. The typical value of ρ_{max} is set to approximately 0.5, which strikes a balance between space efficiency and false positive rate [14]. Varying the structure of the Bloom filter such as the number of hash functions or the order of 1-bit positions can also improve the security level. Encrypting link IDs or the Bloom filter is to make routing information secret and prevent target path attack. The node could dynamically compute each packet a different Bloom filter for the same link ID, where the computation involves some context information including input/output interface, secret key of the time, flow ID of the packet and some parameters for performance optimization [14].

We summarize and compare the major features of TOA and DOA in Table 1.

Application

This section illustrates how the source routing feature of the Bloom filter based multicast could benefit multimedia applications, with IPTV as an example.

IPTV systems deliver the TV program as a compressed multicast data stream over IP-based networks, where the stream is usually a series of groups of pictures (GOPs) and play-out can only start with an I-frame at the beginning of each GOP [15]. The IPTV channel zapping is the act of leaving a stream and joining in another. The time it takes for the picture of the new TV channel to start displaying since the zapping request has been issued is *zapping time*, which is a critical quality of experience (QoE) metric for IPTV systems. As the zapping request possibly occurs at any time in a GOP of the new channel stream, the time between the arrival of the request and the first I-frame (*first I-frame Delay, FID*) could

Features	TOA	DOA
Asymmetric routing	Source routing with encoded multicast tree branches [7]; bit permutation needs to deal with asymmetric routing [5]	Handled with BGP-view based approach [13]
Memory efficiency	Depends on the number of neighboring links of the router [7]	Depends on the number of destination domains can be reached through the router [12, 13]
Bandwidth efficiency	Depends on the number of tree branches encoded in the packet [7]	Depends on the number of destination domain prefixes encoded in the packet [12, 13]
Joining operation	Has to be completed at source node	Can be accelerated with fast joining [13]
Falsely forwarded traffic	Can be constrained with probability [8, 9]	Can be completely blocked
Forwarding loops	Can be constrained with probability [8, 9]	Can be completely removed
Security	Subject to chain reaction attack and target path attack [11]	Security issue has not been studied in this context

Table 1. *Features comparison between TOA and DOA.*

be up to a few seconds, which is a significant contributor to the IPTV channel zapping time [16].

We find that the source routing feature of the Bloom filter based multicast could be utilized to give a simple but effective solution. The service model of the solution is shown in Fig. 4. Each video channel is accompanied by several time-shifted sub-channels (sCHs) that are generated through replicating the main channel (mCH) media stream. There are $X = \lceil s/T \rceil$ sCHs coexisting with the mCH, where T is the time space between two adjacent sCHs and s is the size (in time units) of the largest GOP in the video stream. With the setting, a joining request can always find an appropriate sCH to join at any time, which will provide an I-frame within T time units. Take the scenario in Fig. 4 for example, the zapping request arrived at t could subscribe to sCH 1 to get an I-frame within T, where $X = 2$ in the case.

The challenge of the model is that sCHs will consume network resources continuously if they are always active, which could be conveniently overcome by exploiting the source routing property of the Bloom filter based multicast. The sCH could be configured a higher data rate and its subscribers can change to join in the mCH after the sCH catches up with the mCH, and the sCH can be deactivated then. The membership migration in the Bloom filter based multicast is very simple, where the only need is to change corresponding routing information carried by the multicast packet, instead of constructing new trees compared to traditional IP multicast [15].

We have implemented the service model with the destination-oriented multicast (DOM), a Bloom filter based multicast protocol with DOA [15]. We note that the DOA has a particular advantage over TOA in the scenario. DOA just needs to put destination prefixes associated with a sCH in the Bloom filter, while TOA needs to recalculate delivery tree each time subscribers of sCHs migrate to the mCH, which could be difficult in a highly dynamic context. The visual effect of the implemented scheme compared with an existing multicast instant channel change (MICC) mechanism is depicted in Fig. 5 [15], where the first pictures received after the zapping request and the pictures received just before the migration from auxiliary channel to main channel are shown. The user experience of the implemented scheme is obviously better than the MICC on the right of each sub-figure. This application indicates that the Bloom filter based multicast, especially the DOA approach, may provide an opportunity to gain more benefits for IP video delivery systems with a synergetic design.

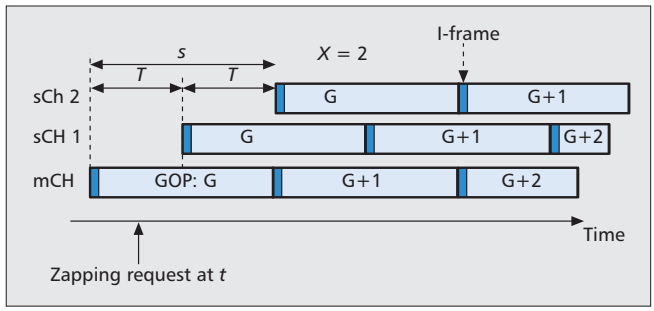

Figure 4. *IPTV channel zapping acceleration.*

Open Research Issues

Bloom filter based multicast works with source routing instead of with hop-by-hop routing as in IP multicast, which brings both challenges and opportunities. On one hand, encoding the entire multicast routing information could incur security breaches that could influence TOA and DOA in different ways. For example, in the TOA scenario, having known the topology of an area of network and a number of zombie hosts under control, the attacker can let zombie hosts to subscribe to each other and collect the Bloom filter formatted paths; it is very possible to reverse engineer the Bloom filter that represents certain link by ANDing those Bloom filter formatted paths with considering the intersections of those paths in the topology. However, as DOA encoding destination domain prefixes in the Bloom filter, the reverse-engineer attack does not work. Could we conclude that the DOA provides higher security level than TOA? What attacking pattern could happen in the DOA? These questions are interesting and still unanswered.

On the other hand, the source routing property of the Bloom filter based multicast provides an opportunity for the reliable multicast mechanism design. Intuitively, the basic principle of reliable data transfer is to acknowledge the sender if some data needs retransmission, such as that in transmission control protocol (TCP) that targets at point-to-point communication. One of the challenges for reliable one-to-many communication is that different receivers may need the source to resend different lost data packets. In the source routing based multicast schemes, this could be easily imple-

mented as the data source only needs to encode different routing information in the packet for different receivers. Moreover, the source node has the chance to aggregate the retransmission requests from different receivers to save bandwidth. Recent work has shown the Bloom filter based multicast could be applied in the datacenter network [17], it could be very interesting to find out if the Bloom filter based reliable multicast could benefit the datacenter network.

Conclusions

This article gives a comprehensive study of Bloom filter based multicast from the aspects of methodology, design and application. We have revealed the impetus behind the evolution of multicast mechanism to help understanding how multicast has developed into the current state. A tutorial description of representative Bloom filter based multicast protocols has been given, where core design issues for the protocols have been analyzed. Moreover, we have proposed a synergetic scheme to accelerate the channel zapping of IPTV systems, where the source routing feature of the Bloom filter based multicast is seamlessly utilized. We have pointed out that the security issue in the context of destination oriented approach and the reliable Bloom filter based multicast could be possible research directions.

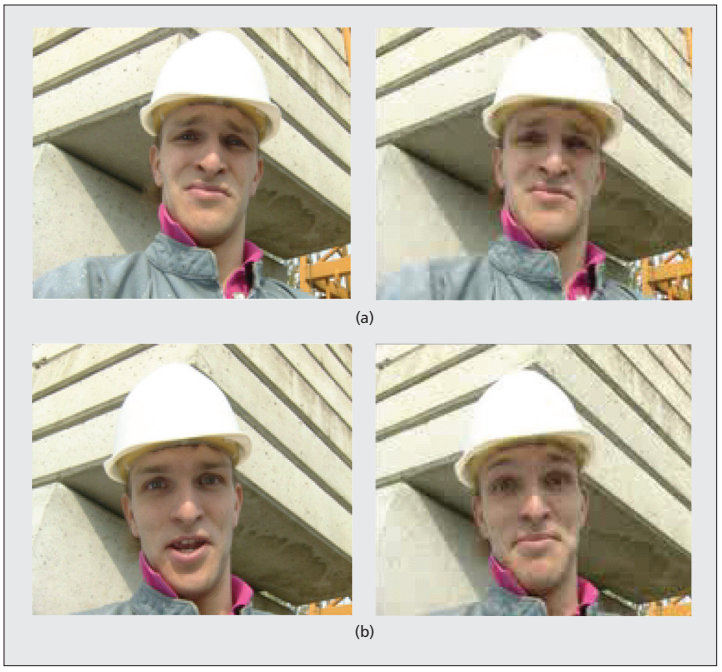

Figure 5. *Visual effects (left: proposed scheme, right: MICC): a) first pictures observed; and b) pictures observed just before migration.*

References

[1] K. C. Almeroth, "The Evolution of Multicast: from the MBone to Interdomain Multicast to Internet2 Deployment," *IEEE Network*, vol. 14, no. 1, Jan.–Feb. 2000, pp. 10–20.

[2] S. Tarkoma, C. E. Rothenberg, and E. Lagerspetz, "Theory and Practice of Bloom Filters for Distributed Systems," *IEEE Trans. Commun. & Tutorials*, vol. 14, no. 1, Jan. 2012, pp. 131–55.

[3] B. Xiao and Y. Hua, "Using Parallel Bloom Filters for Multi-Attribute Representation on Network Services," *IEEE Trans. Parallel and Distributed Systems*, vol. 21, no. 1, Jan. 2012, pp. 20–32.

[4] S. Ratnasamy, A. Ermolinskiy, and S. Shenker, "Revisiting IP Multicast," *Proc. ACM SIGCOMM*, Aug. 2006, pp. 15–26.

[5] X. Tian, Y. Cheng, and B. Liu, "Design of A Scalable Multicast Scheme with an Application-Network Cross-Layer Approach," *IEEE Trans. Multimedia*, vol. 11, no. 6, Oct. 2009, pp. 1160–69.

[6] S. Fahmy and M. Kwon, "Characterizing Overlay Multicast Networks and Their Costs," *IEEE/ACM Trans. Net.*, vol. 15, no. 2, Apr. 2007, pp. 373–86.

[7] I. Stoica, T. S. E. Ng, and H. Zhang, "REUNITE: A Recursive Unicast Approach to Multicast," *Proc. IEEE INFOCOM*, vol. 3, Mar. 2000, pp. 1644–53.

[8] R. Boivie *et al.*, "Explicit Multicast (Xcast) Basic Specification," Internet draft, Mar. 2001.

[9] T. W. Cho *et al.*, "Enabling Content Dissemination Using Efficient and Scalable Multicast," *Proc. IEEE INFOCOM*, Mar. 2009, pp. 1980–88.

[10] X. Tian, Y. Cheng, and X. Shen, "DOM: A Scalable Multicast Protocol for Next-Generation Internet," *IEEE Network*, vol. 24, no. 4, July 2010, pp. 45–51.

[11] M. Särelä *et al.*, "Forwarding Anomalies in Bloom Filter-based Multicast," *Proc. IEEE INFOCOM*, 2011, pp. 2399–407.

[12] P. Jokela *et al.*, "LIPSIN: Line Speed Publish/Subscribe Inter-Networking," *Proc. ACM SIGCOMM*, 2009, pp. 195–205.

[13] X. Tian and Y. Cheng, "Loop Mitigation in Bloom Filter-based Multicast: A Destination-Oriented Approach," *Proc. IEEE INFOCOM*, 2012, pp. 2131–39.

[14] M. Särelä *et al.*, "Bloomcasting: Security in Bloom Filter-based Multicast," *Info. Security Tech. for Applications Lecture Notes in Computer Science*, vol. 7127, 2012, pp. 1–16.

[15] X. Tian, Y. Cheng, and X. Shen, "Fast Channel Zapping with Destination-Oriented Multicast for IP Video Delivery," *IEEE Trans. Parallel and Distributed Systems*, vol. 24, no. 2, Feb. 2013, pp. 327–41.

[16] Y. Bejerano and P.V. Koppol, "Improving Zap Response Time for IPTV," *Proc. IEEE INFOCOM*, 2009, pp. 1971–79.

[17] D. Li *et al.*, "ESM: Efficient and Scalable Data Center Multicast Routing," *IEEE Trans. Net.*, vol. 20, no. 3, June 2012, pp. 944–55.

Biographies

XIAOHUA TIAN received his B.E. and M.E. degrees in communication engineering from Northwestern Polytechnical University, Xi'an, China, in 2003 and 2006, respectively. He received the Ph.D. degree in the Department of Electrical and Computer Engineering (ECE), Illinois Institute of Technology (IIT), Chicago, in Dec. 2010. He is currently an Assistant Professor in Department of Electronic Engineering of Shanghai Jiao Tong University, China. He won the Highest Standards of Academic Achievement 2011 of IIT and Fieldhouse Research Fellowship 2009 of IIT, which is awarded to only one student over IIT each year. His research interests include application-oriented networking, Internet of Things and wireless networks. He serves as the guest editor of International Journal of Sensor Networks, publicity co-chair of WASA 2012. He also serves as the Technical Program Committee member for Wireless Networking Symposium, Ad Hoc and Sensor Networks Symposium of IEEE GLOBECOM 2013, Ad Hoc and Sensor Networks Symposium of IEEE ICC 2013, Wireless Networking Symposium of IEEE GLOBECOM 2012, Communications QoS, Reliability, and Modeling Symposium (CQRM) of GLOBECOM 2011, and WASA 2011.

YU CHENG received the B.E. and M.E. degrees in Electrical Engineering from Tsinghua University, Beijing, China, in 1995 and 1998, respectively, and the Ph.D. degree in Electrical and Computer Engineering from the University of Waterloo, Waterloo, Ontario, Canada, in 2003. From September 2004 to July 2006, he was a postdoctoral research fellow in the Department of Electrical and Computer Engineering, University of Toronto, Ontario, Canada. Since August 2006, he has been with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, Illinois, USA, and he is now an Associate Professor. His research interests include next-generation Internet architectures and management, wireless network performance analysis, network security, and wireless/wireline interworking. He received a Postdoctoral Fellowship Award from the Natural Sciences and Engineering Research Council of Canada (NSERC) in 2004, and a Best Paper Award from the conferences QShine 2007 and ICC 2011. He received the National Science Foundation (NSF) CAREER AWARD in 2011 and IIT Sigma Xi Research Award in the junior faculty division in 2013. He served as a Co-Chair for the Wireless Networking Symposium of IEEE ICC 2009, a Co-Chair for the Communications QoS, Reliability, and Modeling Symposium of IEEE GLOBECOM 2011, a Co-Chair for the Signal Processing for Communications Symposium of IEEE ICC 2012, a Co-Chair for the Ad Hoc and Sensor Networking Symposium of IEEE GLOBECOM 2013, and a Technical Program Committee (TPC) Co-Chair for WASA 2011. He is a founding Vice Chair of the IEEE ComSoc Technical Subcommittee on Green Communications and Computing. He is an Associated Editor for *IEEE Transactions on Vehicular Technology*.