Group-Oriented Communication: Concept and Network Architecture

Yousuke Takahashi, Kouhei Sugiyama
Hiroyuki Ohsaki and Makoto Imase
Graduate School of Information Science and Technology
Osaka University
1-5, Yamadaoka, Suita, Osaka 565-0871, Japan
Email: {yosuke-t,k-sugi,oosaki,imase}@ist.osaka-u.ac.jp

Takeshi Yagi and Junichi Murayama
NTT Information Sharing Platform Laboratories
NTT Corporation
3-9-11, Midori-cho, Musashino-shi, Tokyo 180-8585, Japan
Email: {yagi.takeshi,murayama.junichi}@lab.ntt.co.jp

Abstract*—In this paper, we propose a novel communication paradigm called *group-oriented communication*. Different from conventional unicast-based communications, group-oriented communication is entirely based on group-based communication. Our group-oriented communication is essentially a type of many-to-many communication, but it realizes any type of communications including one-to-one, one-to-many, many-to-one and many-to-many communications based on group-based communication. With our group-oriented communication, diverse social activities can be shifted into a communication network in a straightforward way, and users' requirements on security/reliability can be fulfilled. In this paper, we first qualitatively discuss advantages of our group-oriented communication by comparing with the conventional IP-based network. We then discuss four design goals of a network architecture for our group-oriented communication: supporting dynamic entity/group, supporting address operation expression, realization of entity/group findability, and realization of security. After carefully examining these design goals, we design a network architecture for realizing our group-oriented communication. Through quantitative evaluations, we show that the network architecture for our group-oriented communication should be packet-based, that reachability control is the core networking technology, and that the network architecture should have the two-layer structure consisting of transport and control layers.

1. Introduction

In recent years, several social activities have been rapidly shifting into networked environment [1]. Such tendency originates from prompt advancement of information and communication technologies, such as speed improvement and cost reduction in information processing technologies and explosive deployment of networking technologies such as the Internet.

On the contrary, those advanced technologies change the style of communications because of rationalization and diversification of social activities [2], [3]. For instance, several advanced network services and systems, such as electronic commerce, information appliances, and home security systems, have been realized and started to be widely deployed.

Users' requirements on a network have been specialized, and therefore several problems of the existing Internet have been pointed out in recent years [4]. For instance, the Internet is essentially based on one-to-one communication (i.e., unicast), and its primary concern lies in high connectivity and low cost. Consequently, in the Internet, spam mails and phishing have been unintentionally utilized by malicious users, and those have still been serious issues. Such serious issues of the Internet are basically the side effect of its global connectivity. Namely, in the Internet, connectivity among geographically widespread users is realized using the unique address information, the IP address. Hence, once address information is known by a malicious user, it is theoretically difficult to prevent such security attacks.

For shifting several social activities into a network, supporting not only one-to-one (i.e., unicast-based) communication, but also one-to-many (i.e., multicast-based) and many-to-many (i.e., group-based) communications are important. In addition, users' requirements on a network have been gradually changing from connectivity and cost to *security and reliability*. Consequently, many users have been demanding a new type of network, which can provide several types of communications in a secure and reliable fashion.

For realizing several types of communications (i.e., one-to-many, one-to-many and many-to-many communications), several researches on group-based communication have been performed [5]–[10]. There are two types of approaches for realizing group-based communication: network-level and application-level.

Examples of network-level approaches for group-based communication are [6], [7]. In [6], a networking protocol stack called Horus is proposed. In Horus, several networking functions are modularized as blocks, and various types of communications including group-based communication may be constructed by combining those blocks. In [7], a network architecture called MNS (MyNetSpace), which enables construction of end host groups, is proposed. By adding an MNS header for group identification to an IP packet header, MNS realizes compatibility with the conventional IP-based network. However, since these networking protocols are built on top of the conventional IP network, they simply inherit issues of the Internet — lack of security and reliability.

On the contrary, application-level approaches for group-based communication (see [5] and references therein) includes application-level multicast [8], overlay multicast [9] and Publish / Subscribe [11]. For instance, an application-level multicast called TAG (Topology Aware Grouping) is proposed [10]. TAG enables efficient utilization of network resources by constructing a multicast tree so that the end-to-end delay and load between a source and sinks are minimized.

However, TAG is also built on top of the conventional IP-based network. Its security and reliability are insufficient for realizing social activities in a network.

For alleviating inherent issues of the Internet, in this paper, we propose a novel communication paradigm called *group-oriented communication*. In this paper, group-based communication is defined as a class of many-to-many communications. On the contrary, group-oriented communication is a specific network architecture supporting one-to-one, one-to-many and many-to-many communications as well as advanced features explained in Section 2.

Different from conventional unicast-based communications, group-oriented communication is based on group-based communication. Several conventional unicast-based communications support group-based communication, but it is usually a just extension to unicast-based communication. For instance, IP multicast is an extension to IP unicast. On the contrary, our group-oriented communication is essentially a type of many-to-many communication, but it realizes any type of communications including one-to-one, one-to-many, many-to-one and many-to-many communications based on group-based communication.

In this paper, we first qualitatively discuss advantages of our group-oriented communication by comparing with the conventional IP-based network. We also design a network architecture for realizing our group-oriented communication. We discuss four design goals for our group-oriented communication: supporting dynamic entity/group, supporting address operation expression, realization of entity/group findability, and realization of security. After carefully examining these design goals, we design a network architecture for realizing our group-oriented communication. Through quantitative evaluations, we show that the network architecture for our group-oriented communication should be packet-based, that reachability control is the core networking technology, and that the network architecture should have two-layer structure consisting of transport and control layers.

The primary contribution of this paper is twofold. The first is the proposal of a novel communication paradigm called *group-oriented communication*, which realizes different types of communications simply based on many-to-many communication and naturally solves current issues of the conventional unicast-based communications. To the best of our knowledge, the concept of group-oriented communication is new. We understand that there are many issues to be solved for realizing *real* network architecture such as performance, efficiency, usability, implementation, security, reliability, management and deployment, as will be partly discussed in Section 2. This paper is just the first step toward realizing fully-functioning network architecture for group-oriented communication. However, we believe this step — proposing the concept of a novel communication paradigm — is one of the most important ones for realizing a new type of network architecture.

The second is a sketched design of a network architecture for our group-oriented communication. Our group-oriented communication supports advanced features such as dynamic creation/change/deletion of entities/groups and address operation expression. We find that most of those advanced features can be realized simply by appropriately controlling the reachability of information. Our finding and sketched design of a network architecture clearly suggest that our group-oriented communication with advanced features can be realized by a simple network architecture.

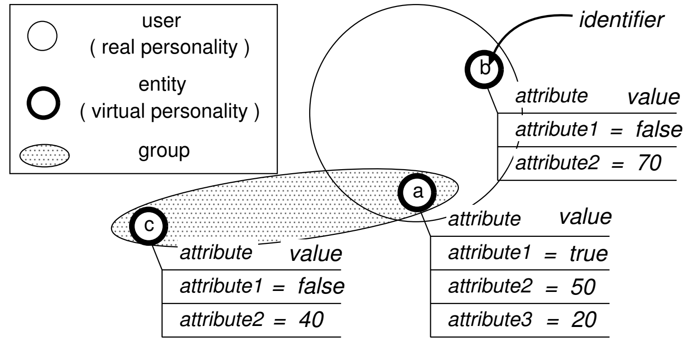

Fig. 1: Definition of terms used throughout this paper

Note that we do not argue that the conventional IP-based network should be replaced by another (and completely different) network architecture. Instead, we claim that the conventional IP-based network is not sufficient for supporting various social activities, and that such a problem can be solved by our group-oriented communication in a straightforward way. Hence, an application-level overlay network realizing group-oriented communication might be a solution. However, detailed discussion on implementation/deployment of our group-oriented communication is outside the scope of this paper.

The organization of this paper is as follows. In Section 2, overview of our group-oriented communication is explained, followed by detailed explanation of its features and characteristics. Section 3 discusses design goals of the network architecture for realizing our group-oriented communication. According to these design goals, the network architecture for our group-oriented communication is designed in Section 4. Finally, Section 5 concludes this paper and discusses future works.

2. Group-Oriented Communication

A. Terminology

We define terms used throughout this paper as follows (see Fig. 1).

- *Entity* is an endpoint of communication. Generally, a user or an application running on an end host corresponds to an entity. A user may have multiple entities (e.g., user's virtual personalities) for different purposes.
- *Group* is a logical set of one or more entities. Note that group construction is completely free from physical restrictions of a network (e.g., geographical restrictions).
- *Identifier* is a name used for identifying an entity or a group.
- *Attribute information* is information with which characteristics of an entity or a group are represented. Examples of the attribute information for an entity includes user information (e.g., name, sex, address and age), user's

geographical information (e.g., latitude, longitude and altitude).

B. Overview

To meet various communication demands, both types of communications, entity-to-entity communication and group-to-group communication, are required. Hence, even in a group-based communication protocol, both entity-to-entity communication and group-to-group communication must be supported.

In conventional group-based communication protocols, two different types of communication endpoints, an entity and a group, are discriminated and therefore differently realized. In such protocols, since two types of communications, entity-to-entity and group-to-group communications, are separately realized, the network architectures are inevitably complicated. However, an entity and a group have similarities, and similar network functions are provided for both an entity and a group.

In our group-oriented communication, an entity is recursively defined as *either an endpoint of communication or a set of entities*. Network architecture can therefore be quite simplified since only an entity needs to be realized as an endpoint of communication.

Based on such an idea, we propose a novel communication paradigm called *group-oriented communication*. Group-oriented communication is based on group-based communications. Our group-oriented communication is essentially a type of many-to-many communication, but it realizes any type of communications including one-to-one, one-to-many, many-to-one and many-to-many communications based on group-based communication. The key idea of our group-oriented communication is utilizing the fact that one-to-one, one-to-many and many-to-one communications are special cases of many-to-many communication.

In our group-oriented communication, since groups can be combined flexibly and dynamically, different types of communications among entities can be realized. Our group-oriented communication supports creation, change and deletion of entities/groups according to user's different purposes. Our group-oriented communication also supports search of entities/groups from their attribute information.

Since our group-oriented communication is a type of group-based communication, it can intentionally restrict information reachability within a group. Namely, our group-oriented communication can solve current security issues (e.g., spam mails and phishing) of the conventional unicast-based communications.

With our group-oriented communication, we believe that diverse social activities can be shifted into a communication network in a straightforward way, and users' requirements on security/reliability can be fulfilled.

C. Features

In what follows, features of our group-oriented communication are explained.

Address Operation: In our group-oriented communication, a user can flexibly and dynamically combine groups using a novel dynamic addressing called *address operation* (see Fig. 2). Various communications among many entities can be realized using address operation. Specifically, in our group-oriented communication, a user can specify an *address operation expression*, which is composed of entity/group identifiers and set operations, as a source or destination address. With such a mechanism, for instance, a user can send information to set of members belonging to multiple groups but excluding specific persons.

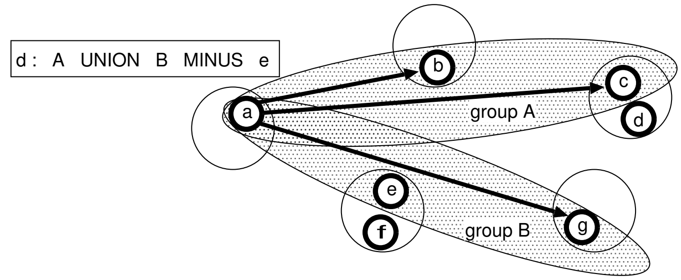

Fig. 2: A user can flexibly and dynamically combine groups using address operation

The notion of an address operation expression is derived from set operations in SQL (Structured Query Language) [12]. In an address operation expression, a user can specify a set operator (e.g., `UNION` (union of set), `INTERSECT` (set intersection), or `MINUS` (difference set)) as an operator, and an identifier of an entity/group as its operand. Figure 2 illustrates an example of an address operation expression. A user can deliver information to set union of the group `A` and the group `B` while excluding the entity `e` with

```
A UNION B MINUS e
```

In an address operation expression, a user can also specify a conditional expression using a conditional operator `WHERE` for restricting information reachability to a subset of entities/groups. For instance, if entity's age is registered as its attribute information, a user can send information only to people of older than 20 with

```
A UNION B MINUS e WHERE age >= 20
```

where `age` is the attribute information of an entity.

Entity/Group Creation/Change/Deletion: In our group-oriented communication, an entity/group can be flexibly and dynamically created, changed and deleted according to user's requirements (see Fig. 3).

For instance, a user can create multiple entities, each of which corresponds to each virtual personality, and simultaneously utilizes those entities for different purposes. Also, users can create multiple groups according to their requirements. Similarly, an entity/group can be flexibly and dynamically deleted. For instance, a user can delete unnecessary entities (e.g., virtual personalities) and groups.

Attribute information of an entity/group can also be flexibly and dynamically updated. For instance, a user can update the attribute information of entities and groups.

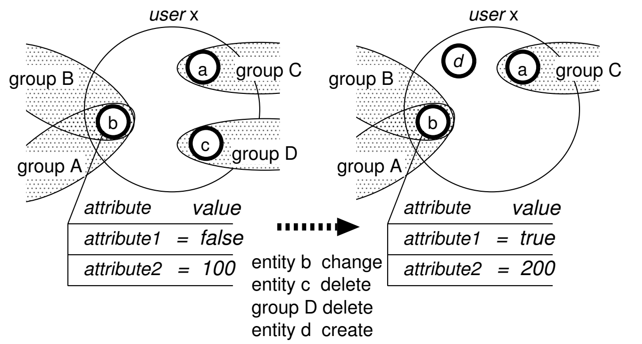

Fig. 3: An entity/group can be flexibly and dynamically created, changed and deleted according to user's purposes

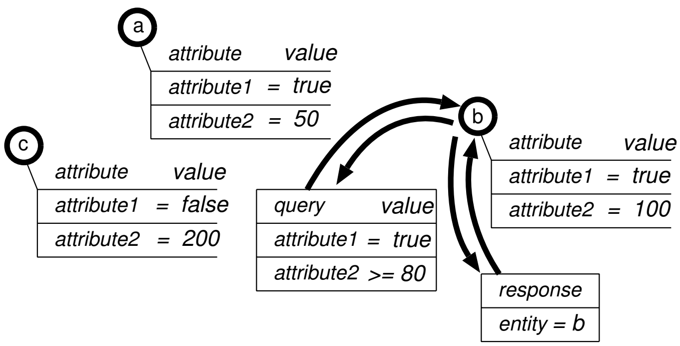

Fig. 4: Entities/groups can be searched from their attribute information

Entity/Group Findability: In our group-oriented communication, entities/groups can be searched (see Fig. 4). Specifically, an entity can be searched from its identifier and/or attribute information. For instance, if entity's geographical information is registered as its attribute information, a user can search geographically-close entities using their attribute information.

Similarly, a group can be searched from its identifier and/or attribute information. For instance, if group's organization name is registered as its attribute information, a user can search the corresponding group using its attribute information.

For preventing communication from an unexpected third person, access to identifier and attribute information of an entity/group can be freely controlled by a user. Thus, for instance, a user can selectively disclose its identifier and/or attribute information to designated people.

Security: In our group-oriented communication, reliable and secure communication can be provided among entities/groups (see Fig. 5). For instance, a user can securely exchange information with specific entities/groups. Since our group-oriented communication is a type of group-based communication, it can intentionally restrict information reachability within a group, leading reduced risk for security issues (e.g., spam mails and/or fishing mails) [13].

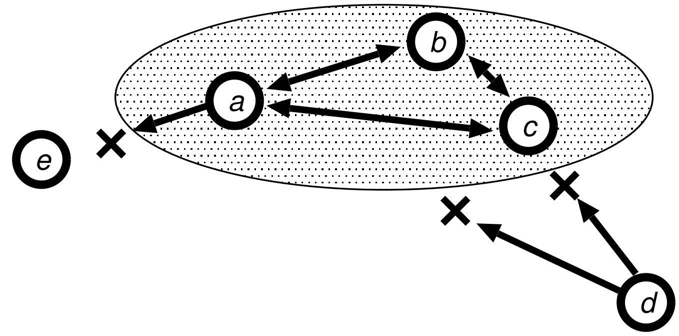

Fig. 5: Reliable and secure communication can be provided among entities/groups

D. Group-oriented Communication vs. IP-based Network

In what follows, we discuss characteristics of our group-oriented communication by comparing with the conventional IP-based network. According to our terminology, an entity in the IP network corresponds to a *network interface*, and its identifier corresponds to an *IP address*. Also, a group corresponds to a *multicast group*, and its identifier corresponds to a *multicast IP address*.

Address Operation: In our group-oriented communication, a user can flexibly and dynamically combine groups using the address operation. Since a user can specify various combinations of entities using the address operation expression, our group-oriented communication realizes various types of communications among entities.

On the contrary, in the conventional IP-based network, a user can specify only a single identifier (i.e., IP address) as a destination address. With the source routing of IP protocol options or XCAST [14], a list of multiple destination addresses can be specified if all routers along the path supports such an extension. However, their usages are quite limited.

Entity/Group Creation/Change/Deletion: In our group-oriented communication, a user can freely create, change and delete entities. Such a dynamic entity/group operation is realized by separation of entity's identifier from its physical address.

On the contrary, in the conventional IP-based network, since entity (i.e., network interface) is statically mapped to entity's identifier (i.e., IP address), dynamic entity/group operation is impossible.

In our group-oriented communication, access to an entity/group identifier can be freely controlled by a user. Hence, by selectively disclosing identifier of an entity/group, communication from an unexpected third person can be prevented, and security can be improved.

In our group-oriented communication, a user can also freely create, change and delete groups. In the conventional IP-based network, a multicast group can be freely created, changed and deleted using the IGMP protocol. However, for realizing such a dynamic group management, all routers along the path must be IGMP-aware. Note that several security issues of the IGMP protocol such as its vulnerability to attacks have been pointed out [15].

Entity/Group Findability: In our group-oriented communication, an entity can be searched from its identifier and/or attribute information. For instance, if entity's name, address, age and sex are registered as its attribute information, an entity can be searched from its attribute information. With such a mechanism, advanced network services can be easily developed, and various social activities can be easily shifted into a network.

On the contrary, IP provides very limited mechanism for searching the identifier of an entity (i.e., IP address). Although hostname-to-address and address-to-hostname resolutions are possible with the DNS, its usage is quite limited. Even though the attribute information can be registered to the DNS using SRV RR (resource records) [16], it is not suitable for managing dynamic attribute information.

In our group-oriented communication, a group can be searched from its identifier and/or attribute information. For instance, if group's name, location and purpose in a real society are registered as its attribute information, a group can be searched from its identifier and/or attribute information.

On the contrary, IP provides no mechanism for searching identifier of group (i.e., multicast address). A multicast address is just an IP address. Hence, as discussed above, attribute information of a group (i.e., multicast group) cannot be registered, so that a group cannot be searched from its attribute information.

Security: In our group-oriented communication, secure and reliable communication among entities/groups can be realized.

On the contrary, IP is a communication protocol primarily designed for unreliable data delivery. Although there several existing security extensions such as IPsec and SSL/TLS, those are not part of the IP protocol itself. Also, since an entity in the conventional IP-based network corresponds to a network interface, a user cannot know whether the corresponding entity/group is active or not. Just limited status of a network interface can be known using ICMP messages.

As addressed above, our group-oriented communication is a novel communication paradigm for solving several issues of the conventional IP protocol. However, such advantages of our group-oriented communication are derived from its advanced features. Hence, it is quite important to address its feasibility; i.e., whether a network architecture for our group-oriented communication can be realized.

In the following section, we therefore discuss how the network architecture for our group-oriented communication should be designed.

3. Design Goals

In this section, we discuss several design goals of a network architecture for our group-oriented communication. Generally, design goals are classified into two categories: performance-related (e.g., transmission speed and efficiency), and functionality-related (e.g., flexibility and security).

Although performance-related design goals are important, most of those goals can be fulfilled with progress of hardware and software technologies. In this paper, we therefore focus on functionality-related design goals of a network architecture for our group-oriented communication.

Supporting Dynamic Entity/Group

For mapping services and organizations in a real society to a network, it is necessary for a user to be able to flexibly and dynamically operate an entity/group. Namely, it is necessary for a user to be able to dynamically create and delete entities/groups, and to be able to dynamically update attribute information of an entity/group.

It is also desirable for a user to be able to dynamically create and change the identifier of an entity/group, and to be able to create aliases to the identifier of an entity/group. Moreover, a user should be able to dynamically control access to the identifier of an entity/group.

Supporting Address Operation Expression

For realizing various social activities on a network, it is necessary to realize not only one-to-one communication, but also one-to-many and many-to-many communications. In our group-oriented communication, these types of communications are realized using address operation.

Thus, for realizing several types of communications among various combinations of entities/groups, it is necessary for a user to be able to specify an address operation expression as a source or destination address.

Realization of Entity/Group Findability

It is important for a user to be able to quickly and easily find the desired entity/group (i.e., findability). For realizing reliable communication with a suitable entity/group, it is necessary for a user to be able to dynamically search an entity/group from its identifiers and/or attribute information.

Realization of Security

Users' requirements on a network have been specialized and concern on safety has been increasing. Hence, it is necessary for a user to be able to safely exchange confidential information with others. Thus, realization of security is essential to a network architecture for realizing our group-oriented communication.

For communicating only with reliable entities, it is necessary that all users need to be authenticated and that accesses to those entities are dynamically controlled. In addition, falsification of communication contents must be prevented, or at least falsification of communication contents must be detected. Also, for avoiding interference from a third party, both existence and contents of communication among entities/groups can be concealed.

For realizing reliable communication, it is desirable for a user to be able to instantly know whether the corresponding entity/group is active in real-time. For realizing reliable communication, records of communications should be concretely stored and preserved for realizing communication traceability. For securely communicating among entities/groups, communication contents should be inspected so that viruses and malicious mails are eliminated.

4. Designing Network Architecture

In this section, we design a network architecture satisfying the design goals discussed in Section 2.

A. Assumptions

In this paper, we assume that *the core network is managed by a network service provider* and *compatibility with IP is not mandatory*. First, validity of these assumptions is discussed.

In this paper, our network architecture is designed based on the PPVPN (Provider Provisioned Virtual Private Network) framework [17]. In the PPVPN framework, the core network is managed by a service provider, so that it becomes possible to realize secure VPN services. For realizing a secure network, the essential part is controlling the chain of trustworthiness. If the core network is managed by a service provider, it becomes possible to build the secure core network, so that the chain of trustworthiness can be tightened. Moreover, since network devices in the core network are under control of the service provider, two important functionalities — network traceability and exclusion of malicious users — can be realized.

Our group-oriented communication is quite different from the conventional IP-based network. As discussed in Section 1, it is not trivial for the network architecture of a group-based communication to have compatibility with the conventional IP-based network. In our group-oriented communication, a user can freely specify various combinations of sources/destinations using an address operation expression, which enables many-to-many communication. Such advanced communication is difficult to be realized with the same addressing and/or API (e.g., BSD-based socket API) as the IP. As discussed above, in this paper, we assume that the core network is managed by a network service provider. Hence, it is thought that compatibility with the conventional IP-based network is not mandatory.

B. Circuit Switching vs. Packet Switching

We discuss the design of a network architecture for our group-oriented communication from a viewpoint of a communication model.

The network architecture for group-oriented communication should be a type of packet switching networks. One of the notable features of our group-oriented communication is its address operation expression, which enables for a user to flexibly and dynamically specify the sources/destination address. Network architecture supporting such dynamic address operation expression well matches not static circuit switching but dynamic packet switching. Conversely, dynamics of address operation expression is difficult to be realized on a circuit switching network. Also, circuit switching is stateful, so that with a circuit switching network, it is difficult to realize scalability in terms of the number of entities/groups. Namely, for realizing scalability (e.g., creation/change/deletion of a large number of entities/groups), a packet switching network is advantageous to a circuit switching network.

C. Core Networking Technology

So, what is the key networking technology for realizing our design goals for group-oriented communication on a packet switching network?

Recall that the essence of any types of communication is transmitting information. Our key finding is that most design goals discussed in Section 3 can be classified into two categories: *information delivery* (i.e., how to deliver information to its destination) and *information non-delivery* (i.e., how to restrict spreading of information).

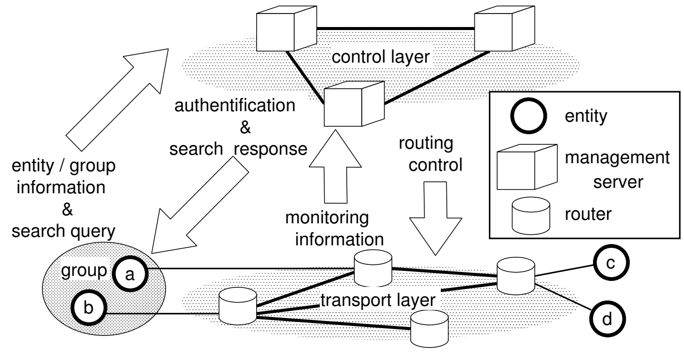

Fig. 6: Network Architecture for Group-Oriented Communication

This finding results in a simple idea: *most design goals for our group-oriented communication can be fulfilled, if reachability of information is appropriately controlled.* For instance, by appropriately controlling reachability from a third party, access from malicious users is prohibited, leading high security. Also, by appropriately controlling reachability from an entity, authentication/authorization of an entity can be realized. By controlling reachability of information within a group of entities, secure group communication within those closed groups can be realized. By appropriately controlling reachability to entity's identifier, access control to entity's identifier can be realized.

D. Layered Network Architecture

As discussed above, we found that reachability is the core networking technology for realizing design goals. However, if various features are realized simply by reachability, a network architecture might be complicated due to increased network functionalities.

For avoiding unnecessary complication, the network architecture should be composed of two layers: transport layer and control layer (see Fig. 6). Namely, the network architecture for group-oriented communication should not be integrated as like an IP-based network but be separated as like an MPLS-based network.

The transport layer covers packet transmission, including packet switching and monitoring. On the contrary, the control layer covers network control, including *reachability control* (i.e., control of packet switching policy), management of entities/groups, identifiers and attribute information.

Transport Layer: The transport layer is composed of routers, which perform high-speed packet switching.

The routing table of a router in the transport layer is controlled by the control layer. Creation and deletion of groups is realized by changing routing tables. Similarly, reachability from a malicious entity to other entities is restricted by appropriately managing routing tables, and abuse can be eliminated. Moreover, reachability to an entity belonging to a different group is restricted by appropriately managing routing tables, and group-based communication is realized.

In the transport layer, for realizing traceability and communication inspection, traffic is monitored. Communication inspection is realized by monitoring payload of packets. Thereby, exclusion of virus and spam mails is realizable. However, generally, for preventing degradation of transmission speed, only traffic to a specific entity/group network should be monitored. Traceability can be realized by notifying to the control layer payload of the monitored packets in the transport layer and by appropriately storing saves that information in the control layer.

Moreover, it is detectable whether an entity is active by monitoring amount of traffic transmitted from the entity. Existence of entity can be realized by notifying to the transport layer this information.

Control Layer: The control layer is composed of management servers, which control reachability, and manage entities/groups.

A management server of the control layer controls the routing table of a router in the transport layer. For instance, when a group is created/deleted, a management server updates routing tables.

Moreover, when an entity newly connects with a network, a management server of the control layer authenticates an entity. Only when an entity is authenticated, the routing table of a router in the transport layer is updated, and the entity is permitted to access the network.

A management server of the control layer manages an entity/group. When an entity/group is created, changed or deleted, a management server updates directory information on an entity/group. For instance, when an entity is created, identifier of an entity is newly registered as directory information. Similarly, when attribute information of an entity/group is registered or changed, directory information on an entity/group is updated. Presence information on an entity notified from the transport layer is also registered as directory information on an entity/group. When directory registers and manages information on an entity/group, feature to search entities/groups can be also realized.

Address operation is realized by utilizing such directory information. If packets specified address operation expression as destination address reach a router, the control layer updates the routing table of a router based on calculation result of an address operation expression. The calculation result of an address operation expression can be easily derived by storing directory information on an entity/group in form of database, and by using the set operation of a database.

5. Conclusion

In this paper, we proposed a novel communication paradigm called group-oriented communication. Different from conventional unicast-based communications, group-oriented communication is based on group-based communications. Our group-oriented communication is essentially a type of many-to-many communication, but it realizes any type of communications including one-to-one, one-to-many, many-to-one and many-to-many communications based on group-based communication. The key idea of our group-oriented communication is utilizing the fact that one-to-one, one-to-many and many-to-one communications are special cases of many-to-many communication. In this paper, we qualitatively discussed advantages of our group-oriented communication by comparing with the conventional IP-based network. We also designed a network architecture for realizing our group-oriented communication. Through quantitative evaluations, we showed that the network architecture for our group-oriented communication should be packet-based, that reachability control was the core networking technology, and that the network architecture should have two-layer structure consisting of transport and control layers.

As future work, we are planning to do further detailed investigation of the network architecture for group-oriented communication designed in this paper, development of a group-oriented communication protocol, and mathematical analysis of group-oriented communication.

References

[1] M. J. Jensen, J. N. Danziger, and A. Venkatesh, "Civil society and cyber society: The role of the internet in community associations and democratic politics," *The Information Society*, vol. 23, no. 1, pp. 39–50, Dec. 2007.

[2] "Communications Usage Trend Survey in 2005 Compiled," May 2005, also available as http://www.johotsusintokei.soumu.go.jp/tsusin_riyou/data/eng_tsusin_riyou02_2005.pdf.

[3] "WHITE PAPER information and communications in japan," May 2007, also available as http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2007/2007-index.html.

[4] D. Jefferson, A. D. Rubin, B. Simons, and D. Wagner, "Analyzing internet voting security," *Communications of the ACM*, vol. 47, no. 10, pp. 59–64, Oct. 2004.

[5] A. El-Sayed, V. Roca, I. Rhone-Alpes, and L. Mathy, "A survey of proposals for an alternative group communication service," in *Proceedings of IEEE Network*, vol. 17, Jan. 2003, pp. 46–51.

[6] R. van Renesse, K. P. Birman, and S. Maffeis, "Horus: a flexible group communication system," *Communications of the ACM*, vol. 39, no. 4, pp. 76–83, Apr. 1996.

[7] N. Mimura, Y. Tobioka, H. Morikawa, and T. Aoyama, "A user-controlled network construction using service-orieted grouping mechanism," in *Proceedings of The 13th DPS Workshop, Sponsored by IPSJ SIG-DPS*, Nov. 2005, pp. 290–294, (in Japanese).

[8] M. Castro, P. Druschel, A.-M. Kermarrec, and A. I. T. Rowstron, "Scribe: a large-scale and decentralized application-level multicast infrastructure," *Selected Areas in Communications, IEEE Journal on*, vol. 20, no. 8, pp. 1489–1499, Oct. 2002.

[9] S. Banerjee, C. Kommareddy, K. Kar, B. Bhattacharjee, and S. Khuller, "Construction of an efficient overlay multicast infrastructure for real-time applications," in *Proceedings of INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, vol. 2, Apr. 2003, pp. 1–11.

[10] M. Kwon and S. Fahmy, "Topology-aware overlay networks for group communication," in *Proceedings of the 12th international workshop on network and operating systems support for digital audio and video*, May 2002, pp. 127–136.

[11] P. T. Eugster, P. A. Felber, R. Guerraouiu, and A.-M. Kermarrec, "The many faces of publish/subscribe," *ACM Computing Surveys*, vol. 35, no. 2, pp. 114–131, Jun. 2003.

[12] J. Melton, "Database language SQL," in *Handbook on Architectures of Information Systems*, P. Bernus, K. Mertins, and G. Schmidt, Eds. Springer Berlin Heidelberg, 1997, pp. 105–132.

[13] B. Gleeson *et al.*, "A framework for IP based virtual private networks," *Request for Comments (RFC) 2764*, Feb. 2000.

[14] R. Boivie *et al.*, "Explicit multicast (xcast) concepts and options," *Request for Comments (RFC) 5058*, Nov. 2007, also available as http://tools.ietf.org/html/rfc3376.

[15] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan, "Internet group management protocol, version 3," Oct. 2002, also available as http://tools.ietf.org/html/rfc3376.

[16] A. Gulbrandsen and P. Vixie, "A DNS RR for specifying the location of services (DNS SRV)," Oct. 1996, also available as http://tools.ietf.org/html/rfc2052.

[17] M. Carugi and D. E. McDysan, "Service requirements for layer 3 provider provisioned virtual private networks (PPVPNs)," Apr. 2005, also available as http://tools.ietf.org/html/rfc4031.