APSITT2008/Copyright 2008 IEICE 07SB0208

On Network Architecture for Realizing Group-Based Communication

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 network architecture for realizing a group-based communication to solve issues of the Internet such as lack of security and low information S/N (Signal to Noise) ratio. We design a network architecture based on a multiple-association model. The proposed network architecture can realize high information S/N ratio by constructing multiple groups for different communication purposes, and can also realize security by logically separating those groups. An existing user terminal cannot be associated with multiple groups. Hence, in our network architecture, multiple groups are terminated at a gateway called SA (Security Agent), which realizes multiple association to several groups. A user terminal is directly connected to a Web concentrator running on SA. Similarly to a portal Web site, a Web concentrator aggregates contents from multiple groups, and transmits the aggregated contents to a user terminal. Several networking technologies for realizing group-based communications have been proposed. From the comparative evaluation of those networking technologies, we show that (1) SSL-VPN is suitable for access networks connecting a user terminal and SA, and that (2) MPLS-VPN is suitable for the backbone network connecting SAs. We also show that the proposed network architecture realizes security and high information S/N ratio for Web-based applications.**

1. Introduction

In recent years, various 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. Moreover, 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. For instance, the Internet is now a part of our society's infrastructure; users can easily access the Internet with just sharing small cost. However, they are faced with security issues by malicious activities (e.g., spam mails and/or phishing mails [4]). 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.

Users' requirements on a network have therefore been gradually changing from *connectivity/cost* to *security/reliability*. Hence, many users have been demanding a new type of network, which can provide several types of communications in a secure and reliable fashion.

We believe a *group-based communication*, which restricts reachability only to users belonging to a specific group, is a promising technology for solving several security issues of the Internet. In a group-based communication, multiple groups are formed for different purposes, and reachability to users outside a group is strictly controlled. This realizes secure communication among users belonging to the same group. However, when multiple groups are formed for different purposes, the number of accessible users is much smaller than that of the Internet. It is expected that by forming groups, unnecessary information (i.e., noise) is not likely to be received by a user. As a side effect, when uses' purposes are further diversified, it is expected that necessary information (i.e., signal) is also not likely to be received by a user. Consequently, inadequate application of a group-based communication may lead to information S/N (Signal to Noise) ratio degradation, resulting in poor communication environment.

For increasing the information S/N ratio while maintaining appropriate level of security, multiple association, where users simultaneously associate with multiple groups, should be one of promising solutions [5]. However, it is not trivial for a user to be associated with multiple groups with the existing networking technologies.

In this paper, we propose a group-based communication architecture for enabling multiple association with conventional networking technologies. In the group-based communication architecture, a gateway called SA (Security Agent) realizes multiple association to multiple groups. User terminals are connected to a *Web concentrator* running on SA. Similarly to a portal Web site, the Web concentrator aggregates contents from multiple groups and transmits the aggregated contents to a user terminal.

Several networking technologies for realizing group-based communications have been proposed. Based on comparative evaluation of those networking technologies, we show that (1) SSL-VPN is suitable for access networks connecting a user terminal and SA, and that (2) MPLS-VPN is suitable for the backbone network connecting SAs.

The organization of this paper is as follows. In Section 2, problems of conventional networking technology and an approach for solving those problems are explained. In Section 3, a proposed network model for realizing a group-based communication is discussed. Section 4 comparatively evaluates several communication technologies, which are applicable to our proposed network model, and discusses the design principle of the network architecture for the group-based communication. Section 5 presents the overview of the proposed network architecture, and qualitatively evaluates its characteristics. Finally, Section 6 concludes this paper.

2. Problems of Conventional Networking Technologies

A. The Internet

The communication model of the Internet is illustrated in Fig. 1. In the Internet, since all users share the unique address space, a user can identify other users based on the address information. For instance, in Fig. 1, when user #1 knows the addresses of users #2 and #3, user #1 can communicate with these users.

However, in the Internet, since reachability to all users is maintained, a user may receive/send information from/to an unexpected user. For instance, in Fig. 1, since user #1 receives information from users #4 and #5, user #1 may receive undesired information such as spam mails. By receiving undesired information from the unexpected user, the amount of noise increases so that the information S/N ratio is degraded. Moreover, since user #1 may send information to an unexpected user #6 due to phishing or misoperation, confidential information of user #1 such as personal information may be disclosed. Possibility to transmit information to an unexpected user degrades security. Global reachability is the essential feature of the Internet, but such global reachability is not always desirable. Hence, in recent years, users' requirements on a network have been gradually changing from *connectivity/cost* to *security/reliability*.

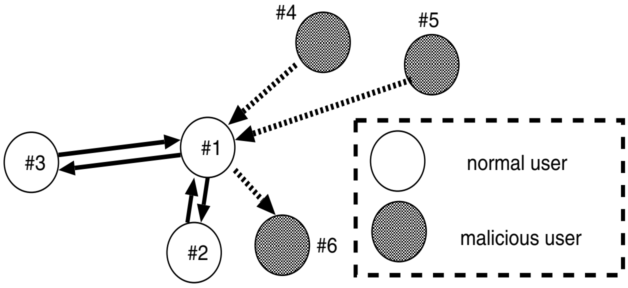

Fig. 1: Communication model of the Internet; since reachability to all users is maintained, a user may receive/send information from/to an unexpected user.

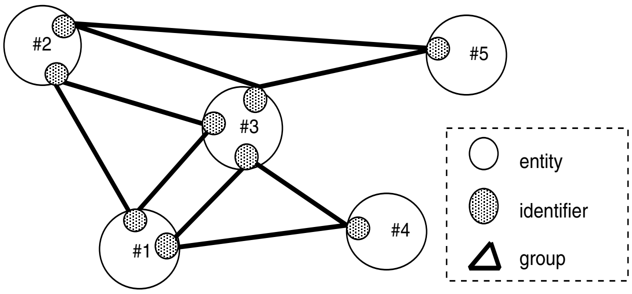

Fig. 2: Communication model of a group-based communication; by restricting connectivity within groups, information leakage to other groups and information receipt from other groups are prevented.

B. Group-based Communication

We believe a group-based communication, which restricts reachability only to users belonging to a specific group, is a promising technology for solving several security issues caused by global reachability of the Internet. In this paper, a *group* is a logical set of entities, and an *entity* is a communication endpoint (Fig. 2). By restricting connectivity within a group, information leakage to other groups and information receipt from other groups are prevented. With a group-based communication, diverse social activities can be shifted into a communication network in a straightforward way.

By forming groups according to user's requirements, it is expected that unnecessary information (i.e., noise) is not likely to be received by a user. As a side effect, when user' requirements are further diversified, it is expected that necessary information (i.e., signal) is not likely to be received by a user. Consequently, inadequate application of a group-based communication may cause degraded information S/N ratio, leading poor communication environment.

C. Multiply Associated Communication

For alleviating the limitation of conventional group-based communications, it is desirable for a user to be able to form multiple groups according to communication requirements, and to be simultaneously associated with those multiple groups. Security is improved by forming a closed group. Also, by selectively associating with multiple groups according to user's requirements, information S/N ratio is improved.

However, it is not trivial for a user terminal to be associated with multiple groups simultaneously with existing networking technologies. For instance, with the VPN (Virtual Private Networks) technology, a user can simultaneously be associated with multiple VPNs (i.e., groups). However, in this case, if the address space overlaps among different VPNs, the destination address of information cannot be identified, leading loss of connectivity.

3. Proposed Network Model

We propose a network model shown in Fig. 3, which realizes multiple association with conventional networking technologies. In this network model, the backbone network is composed of multiple groups (e.g., VPNs). Each group is terminated by a gateway called *SA (Security Agent)*. SA is logically associated with every user terminal. SA enables a user to be associated with multiple groups according to user's requirements.

Also, SA provides a function called a *Web concentrator*. Web concentrator provides a function of virtual tab browsing for a Web browser running on a user terminal. A user terminal and its associated SA are connected using a point-to-point communication. For maintaining security, it is desirable that the connection between a user terminal and SA is constructed by a group-based communication (e.g., VPN).

A Web concentrator aggregates contents from multiple groups, and provides a function of virtual tab browsing to a user terminal. Thus, a user can access multiple groups in a straightforward way. A user terminal is the device operated by a user participating in the group-based communication. A user communicates with multiple groups using a general-purpose Web browser running on a user terminal. Several operations to groups (e.g., selection, creation, change, and deletion) are performed through a Web interface. Thus, a Web concentrator provides an intuitive user interface for the group-based communication. Since a user utilizes a general-purpose Web browser, no change to a user terminal is necessary.

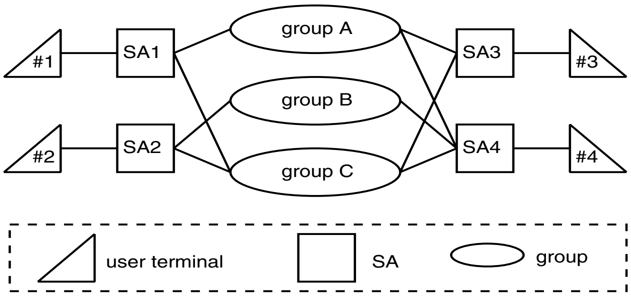

Fig. 3: Proposed network model, which realizes multiple association with conventional networking technologies.

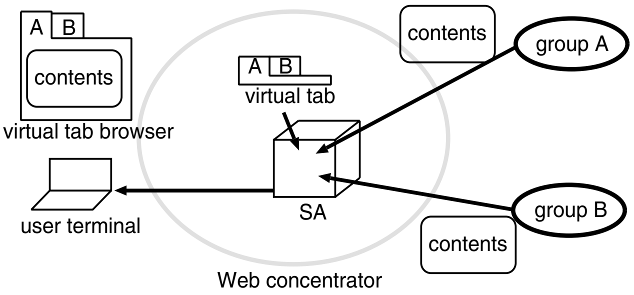

Fig. 4: A Web concentrator aggregates contents from multiple groups, and provides a virtual tab browsing feature to a user terminal.

4. Networking Technologies for Group-based Communication

For implementing the proposed network model, it is quite important to design access networks and the backbone network appropriately.

We therefore discuss suitable communication technologies for implementing the proposed network model by examining general requirements for a group-based communication and comparatively evaluating conventional communication technologies.

A. Requirements for Group-based Communication

In this paper, for taking account of emergent requirements on security and safety, we focus on connectivity, generality, and security among all general requirements for a group-based communication.

- Connectivity
  For connectivity, both portability and scalability are required. In a group-based communication, it is desirable to realize several types of communications among entities by connecting not only fixed terminals but also mobile terminals. So, portability is required. Moreover, since it is important to accommodate many

groups and many user terminals in the network, scalability is also required.

- Generality
  It is necessary to think of generality from two different viewpoints: operating layer and performance. In a group-based communication, it is desirable that a user can communicate with entities using generic applications, and for realizing high compatibility with the conventional networking technologies. Therefore, it is desirable for a group-based communication to be implemented at a lower layer. Moreover, for enabling audio and video applications, it is desirable that communication performance between entities is high enough to accommodate those bandwidth-demanding applications.
- Security
  For security, closed communication and encryption are required. One of the goals of the group-based communication is security. By restricting reachability within a specific group, security issues such as spam mails and phishing can be solved. However, when a closed network is constructed as an overlay network on a public network infrastructure, restricting reachability with a specific group is not sufficient for preventing malicious users from intercepting/falsifying communication. It is necessary to prevent such malicious usage. In a group-based communication, it is therefore necessary to encrypt communication contents.

B. Comparative Evaluation

Based on these requirements, we comparatively evaluate conventional networking technologies. As evaluation criteria, we focus on connectivity (portability and scalability), generality (operating layer and performance), and security (closed communication and encryption).

For each criterion, seven major communication technologies (i.e., MPLS-VPN [6], IPsec VPN [7], SSL-VPN [8], SNS [9], SMTP [10], JXTA [11], and MyNetSpace [12]) are evaluated. Table I summarizes our evaluation results.

- MPLS-VPN [6]
  An entity in MPLS-VPN corresponds to a virtual network interface, and it is identified by a layer 3 address (i.e., IP address). A user terminal is generally connected to a network managed by a carrier or a network service provider. Communication contents are not encrypted. Security cannot be maintained when a user terminal moves out of a LAN managed by a VPN gateway. It is difficult to utilize MPLS for remote access; i.e., MPLS lacks portability. It has high scalability since MPLS has a label stacking feature.
- IPsec VPN [7]
  An entity in IPsec VPN corresponds to a virtual network interface, and it is identified by a layer 3 address (i.e., IP address). IPsec VPN can be used on many OSs, but it lacks flexibility regarding change in a user terminal due to its complexity and difficult configuration. So, portability of IPsec VPN is not sufficient. Since IPsec VPN adopts a client-server architecture, an IPsec VPN server is likely to be the bottleneck; i.e., IPsec VPN lacks scalability in terms of the number of user terminals. Since IPsec VPN is used on the Internet, communication contents are generally encrypted.
- SSL-VPN [8]
  An entity in SSL-VPN corresponds to an SSL module, and it is identified by an IP address and a port number. Since SSL-VPN adopts a client-server architecture, it lacks scalability. Generally, communication contents are encrypted using SSL. SSL-VPN is similar to IPsec VPN, but they operate at different layers. Since SSL-VPN can be utilized with a general-purpose Web interface, it is superior to IPsec VPN in terms of portability.
- SNS [9]
  An entity in SNS corresponds to a user's virtual personality, and is identified by its account information. Even though SNS is generally based on a client-server architecture, it may realize high scalability by aggregating processing for different users at a server. Since SNS can be utilized with a general-purpose Web interface, it has high portability.
- SMTP [10]
  An entity in SMTP corresponds to an MUA (Mail User Agent), and it is identified by a mail address. Since SMTP virtually constructs a connectionless network, it has high scalability. SMTP has high portability since access from an arbitrary site can be realized by maintaining reachability from a user terminal to a mail server. In SMTP, communication contents are generally not encrypted.
- JXTA [11]
  An entity in JXTA corresponds to a peer, and it is identified by a peer identifier. Since JXTA adopts a P2P architecture, it has high scalability. In JXTA, communication contents are encrypted using SSL. Since JXTA can be utilized with an application running on a Java VM (Virtual Machine), it has high portability.

TABLE I
COMPARATIVE EVALUATION OF CONVENTIONAL COMMUNICATION TECHNOLOGIES

		MPLS	IPsec VPN	SSL-VPN	SNS	SMTP	JXTA	MyNetSpace
connectivity	portability	×	△	○	○	○	○	×
	scalability	○	×	×	○	○	○	×
generality	operating layer	3	3	5	7	7	7	3
	performance	○	×	×	×	×	×	○
security	closed communication	○	○	○	○	×	○	○
	encryption	×	○	○	×	○	○	×

○: possible △: partly possible ×: impossible or require non-standard mechanism

- MyNetSpace [12]
  An entity in MyNetSpace corresponds to a network interface, and it is identified by an IP address. Since MyNetSpace adopts a centralized network architecture, it lacks scalability. Since MyNetSpace requires non-standard and OS-specific feature and configurations, it lacks portability. In MyNetSpace, communication contents are not encrypted.

C. Networking Technology for Access Networks

According to our evaluation results, we choose the most desired communication technology for implementing access networks of our proposed network model. For access networks, portability, encryption, and operating layer are particularly important.

- Portability
  In our proposed network model, SA operates as an access point for a user terminal. It is necessary to accommodate not only fixed terminals but also mobile terminals. Therefore, it is desirable for our proposed network model to be accessible not only from fixed terminals but also from mobile terminals.
- Encryption
  For fulfilling portability, supporting accesses from different terminals and from different locations is necessary. Thus, encryption of the communication contents is mandatory for realizing security.
- Operating layer
  Since a Web-based access is assumed from a user terminal to SA, operating layer should be lower than layer 7. Otherwise, type of usable applications is limited.

Since we assume one-to-one mapping between a user terminal and SA, scalability is not required.

From these observations and our evaluation results in Tab. I, we conclude that SSL-VPN is suitable for access networks connecting a user terminal and SA.

D. Networking Technology for Backbone Network

According to our evaluation results, we choose the most desired communication technology for implementing the backbone network of our proposed network model. For the backbone network, scalability and performance should be of great importance.

- Scalability
  For realizing various social activities on our proposed network model, it is necessary to support a large number (e.g., millions) of SAs. Also, it is necessary to support a large number (e.g., ten of thousands) of groups.
- Performance
  Since the backbone network is shared by many users for different purposes, transmission performance for supporting various types of applications, such as video and voice applications, is required. However, since network resources are shared by different types of users, it is not necessary to realize completely equal fairness; instead, network resources should be allocated to each user according to their requirements using, for example, a sort of priority control.

Since we assume that the backbone network is managed by a carrier or a network service provider, encryption of the communication contents is not mandatory. Also, since we assume SA is fixed, portability is not required.

From these observations and our evaluation results in Tab. I, we conclude that MPLS-VPN is suitable for the backbone network connecting SAs.

5. QUANTITATIVE EVALUATION

Finally, we present the overview of our network architecture based on the multiple-association model, and quantitatively evaluate its effectiveness.

In our proposed network architecture, MPLS-VPN is applied to the backbone network for realizing high scalability and performance. Multiple VPNs are constructed for different purposes. These VPNs are terminated by SAs. SA terminates multiple VPNs according to user's requirements. SSL-VPN is used for access networks connecting a user terminal and SA for realizing high portability. A Web concentrator is equipped on SA. A Web concentrator aggregates contents from multiple groups, and transmits the aggregated contents to a user terminal. A user can selectively access multiple VPNs using tab browsing interface.

For the group-based communication, connectivity, generality, and security are important factors. In what follows, effectiveness of our proposed network architecture in terms of these three factors is discussed.

- Connectivity

  Our proposed network architecture has high portability; it enables for users to access SAs from an arbitrary site via the Internet using SSL-VPN.

  Scalability of the proposed network architecture simply depends on the scalability of MPLS-VPN itself since a large number of SAs must be accommodated in the network. MPLS-VPN has high scalability because of its label stacking feature, so that a large number of SAs can be accommodated in the network.
- Generality

  Our proposed network architecture has modest generality; since our proposed network architecture relies on a Web concentrator for realizing multiple association, only Web-based applications can be used on our proposed network architecture.

  Performance of the proposed network architecture should be limited not by the performance of the backbone network but by the performance of a Web concentrator in access networks. Performance of a Web concentrator is a sort of design issues; there should be some trade-offs among performance and cost. Note that the performance of a Web concentrator can be improved by parallelization of multiple Web concentrators.
- Security

  Our proposed network architecture realizes high security using VPNs in both access networks and the backbone network. In access networks, communication contents are encrypted with SSL. In the backbone network, communication contents are not encrypted since SAs are managed by a career or a network service provider.

From these quantitative evaluation results, we conclude that, even though its usage is limited to Web-based applications, our proposed network architecture can realize secure communication with high information S/N ratio using the conventional user terminals.

6. Conclusion

In the Internet, global reachability is provided. However, several issues, such as lack of security and low information S/N ratio, have been caused by such global reachability. To solve these issues, we have proposed a network architecture for realizing a group-based communication. Our proposed network architecture is based on a multiple-association model. In this network, multiple groups are terminated at SAs, which realizes multiple association to several groups. A user terminal is directly connected to a Web concentrator. Similarly to a portal Web site, a Web concentrator aggregates contents from multiple groups, and transmits the aggregated contents to a user terminal. From comparative evaluation results of conventional networking technologies, we have shown that (1) SSL-VPN is suitable for access networks connecting a user terminal and SA, and that (2) MPLS-VPN is suitable for the backbone network connecting multiple SAs. We have also shown that, even though its usage was limited to Web-based applications, our proposed network architecture could realize secure communication with high information S/N ratio using the conventional user terminals.

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, pp. 39–50, Dec. 2007.

[2] D. Jefferson, A. D. Rubin, B. Simons, and D. Wagner, "Analyzing Internet voting security," *Communications of the ACM*, vol. 47, pp. 59–64, Oct. 2004.

[3] "Communications usage trend survey in 2005 compiled." http://www.johotsusintokei.soumu.go.jp/tsusin_riyou/data/eng_tsusin_riyou02_2005.pdf, May 2005.

[4] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, pp. 94–100, Oct. 2007.

[5] O. Honda, H. Ohsaki, M. Imase, J. Murayama, and K. Matsuda, "A Prototype Implementation of VPN Enabling User-Based Multiple Association," in *Proceedings of the Ninth IASTED International Conference on Internet & Multimedia Systems & Applications (IMSA 2005)*, pp. 59–64, Aug. 2005.

[6] E. Rosen, A. Viswanathan, and R. Callon, "Multi-protocol Label Switching Architecture," *Request for Comments (RFC) 3031*, Jan. 2001.

[7] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," *Request for Comments (RFC) 2401*, Nov. 1998.

[8] T. Dierks and C. Allen, "The TLS Protocol Version 1.0," *Request for Comments (RFC) 2246*, Jan. 1999.

[9] R. Gross, A. Acquisti, and H. J. H. III, "Information revelation and privacy in online social networks," *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pp. 71–80, Nov. 2005.

[10] J. B. Postel, "Simple Mail Transfer Protocol," *Request for Comments (RFC) 821*, Aug. 1982.

[11] B. Traversat *et al.*, "Project JXTA 2.0 Super-Peer Virtual Network," May 2003. Also available as https://research.sun.com/spotlight/misc/jxta.pdf.

[12] 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*, pp. 290–294, Nov. 2005. (in Japanese).