MEDWIN PUBLISHERS
Committed to Create Value for Researchers

Open Access Journal of Data Science & Artificial Intelligence
ISSN: 2996-671X

A Key Exchange Scheme Using Multicast Cryptography for Inter-Site Communication

Sukegawa T, Akashi S and Matsuzawa T*

Department of Information Sciences, Tokyo University of Science, Japan

***Corresponding author:** Tomofumi Matsuzawa, Department of Information Sciences, Tokyo University of Science, Japan, Tel: +81471229643; Email: t-matsu@is.noda.tus.ac.jp

Research Article
Volume 3 Issue 1
Received Date: December 30, 2024
Published Date: January 10, 2025
DOI: 10.23880/oajda-16000159

Abstract

In recent years, diverse work styles, such as satellite office work and remote work, have become widespread. In order to securely and smoothly connect multiple sites, such as office and home or office and satellite office, it is important to construct a network environment that can realize inter-site communication. At such sites, inter-site VPNs are used to achieve highly reliable communication. We focused on VPNs between multiple sites, which have been studied as the number of sites increases. For VPNs between multiple sites, Dynamic Multipoint VPN, which establishes a tunnel connecting multiple sites, and GET VPN, which shares the same policy with a group, has been proposed. In this study, we proposed a method of sharing policies using Multicast Cryptography. Multicast Cryptography is an encryption scheme that can be decrypted only by receivers selected by the sender. The proposed method does not require a single key management server in the GET VPN, and the sender can share the policy by selecting the receivers. Performance evaluation showed that the proposed method has the same establishment time as existing IPsec implementations and is superior to existing methods when the number of sites increases. We also discussed that the proposed method not only replaces existing multi-site communication, but is very useful for networks with unbalanced privileges, since the sender can choose the receivers.

Keywords: Virtual Private Networks (VPNs); Secure Sockets Layer (SSL); Generic Routing Encapsulation (GRE); Dynamic Multipoint VPN (DMVPN)

Abbreviations

VPNs: Virtual Private Networks; SSL: Secure Sockets Layer; GRE: Generic Routing Encapsulation; GDOI: Group Domain of Interpretation; GET: Group Encrypted Transport; DMVPN: Dynamic Multipoint VPN.

Introduction

In recent years, Virtual Private Networks (VPNs) have been used for security on the Internet. VPN technologies include Security Policy for Internet Protocol (IPsec) Karen S, et al. [1] and the Secure Sockets Layer (SSL) Freier AO, et al. [2]. Such technologies basically assume the establishment of one-to-one tunnels, which are communication paths between senders and recipients. However, the demand for communication between multiple sites has been increasing in recent years, and existing VPN technologies require the establishment of tunnels between multiple sending and receiving sites, respectively. In response to this situation, VPN technologies such as Generic Routing Encapsulation (GRE) over IPsec Rosen EC, et al. [3], Dynamic Multipoint VPN (DMVPN) Alam T, et al. [4], and Group Encrypted Transport VPN (GET VPN) Niazi H, et al. [5] were proposed.

GRE over IPsec and DMVPN use tunnels to support multiple sites, similar to existing methods. GET VPN, on the other hand, did not use tunnels, but instead realized these by configuring a group of secret communications among multiple sites. GET VPN uses Group Domain of Interpretation (GDOI) Hardjono T, et al. [6] for group key management. In GDOI, a key management server shares encryption keys and policies with group members. In this paper, we propose a method to share encryption keys and policies among group members using multicast cryptography in order to establish secret communication groups among multiple sites. The multicast cryptography is an encryption scheme that can be decrypted only by recipients selected by the sender, and it constitutes a secret communication group between the sender and the selected recipients.

Related Research

Multicast Cryptography

The Multicast Cryptography Matsuzawa T [7] is a public-key cryptography scheme that allows only a recipient selected by the sender to decrypt. Figure 1 shows an overview of the Multicast Cryptography. The sender selects several recipients in advance and encrypts using their public keys. The recipient decrypts using its own private key. The selected recipients receive the same plaintext. Unselected recipients cannot decrypt.

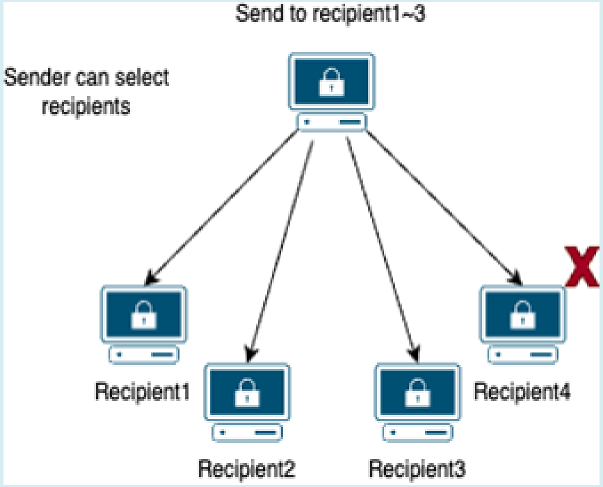

Figure 1: Multicast Cryptography.

Dynamic Multipoint VPN

Dynamic Multipoint VPN (DMVPN) is a technology that enables VPN between multiple locations. Figure 2 shows an overview of DMVPN operation. This is achieved by using a hub-and-spoke configuration. The hub acts as a central hub and relays communications, while the spokes connect to the hub for communication. In previous methods, communication between spoke-spokes had to go through the hub. However, DMVPN establishes tunnels between hub-spokes and spoke-spokes, respectively. Tunnels are established on-demand between spoke-spokes.

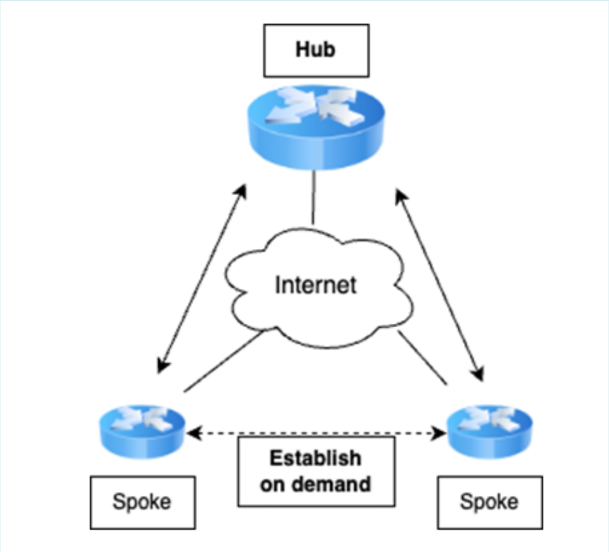

Figure 2: An overview of DMVPN operation.

Group Encrypted Transport VPN

Group Encrypted Transport VPN (GET VPN) Niazi H, et al. [5] is a technology that enables VPN without using tunnels. Figure 3 shows an overview of GET VPN operation. Group Domain of Interpretation (GDOI), a group key management protocol by communicating over a common SA, VPN between multiple sites is possible without using tunnels.

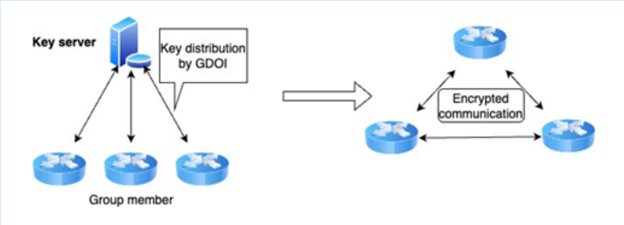

Figure 3: An overview of GET VPN operation Groups share IPsec Security Associations (SA) using.

Group Domain of Interpretation

Group Domain of Interpretation (GDOI) Hardjono T, et al. [6] is a protocol for group key management. Figure 4 shows an overview of GDOI. The GDOI has the roles of key management server and group member, which distribute and update group keys using the key management server. The group member uses the Pull method to establish a SA for Push and a SA for data between the key management servers. The key management server shares the updated SA for data and the updated key with the group members using the method Push. The purpose of GDOI is to share encryption keys and policies to configure group SAs used in GET VPN.

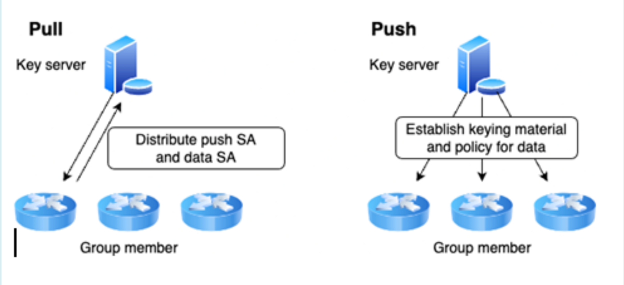
Pull
Key server
Distribute push SA and data SA
Group member
Push
Key server
Establish keying material and policy for data
Group member

Figure 4: An overview of GDOI.

GET VPN Issues

GET VPN has three problems. The first is that it requires a centralized key management server. A centralized key management server can be a single point of failure, and there is also the possibility of concentrated access.

The second is the cost of creating groups. In GET VPN, if the members of a group change even a little, it is necessary to create a new group, and each time it is necessary to access the key management server.

Each time, it is necessary to access to the key management server. Third, it is difficult to control access to multicast communication within a group. If the number of group members increases, it is necessary to create a new group with only a limited number of recipients.

Therefore, this study shares the same encryption key and policy among multiple sites, similar to GDOI, in order to establish a secret communication group for inter-site communication. As a means to achieve this, multicast encryption is used to enable secret communication between the sender and selected recipients.

Proposed Method

Overview

Figure 5 shows an overview of the proposed method. The proposed method uses multicast encryption to share the common key and policy. It acts like GDOI in GET VPN, but only between the sender and selected recipients to form a group.

The non-selected recipients also receive the ciphertext, but since they do not have the corresponding secret key, decryption are not possible. Since the common key is managed for each sender, a single key management server is not required.

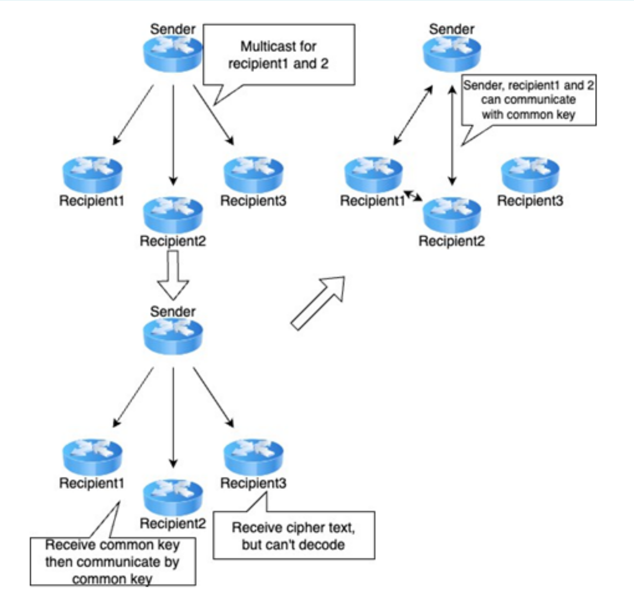
Sender
Multicast for recipient1 and 2
Recipient1
Recipient3
Recipient2
Sender
Sender, recipient1 and 2 can communicate with common key
Recipient1
Recipient3
Recipient2
Sender
Recipient1
Recipient3
Recipient2
Receive common key then communicate by common key
Receive cipher text, but can't decode

Figure 5: An overview of the proposed method.

Protocol

Figure 6 shows the communication protocol of the proposed method. In the proposed method, the key and other parameters are encrypted and transmitted by using a multicast cipher. The selected recipient then decrypts it using its own secret key. This procedure enables the sender and recipient to communicate using symmetric key encryption.

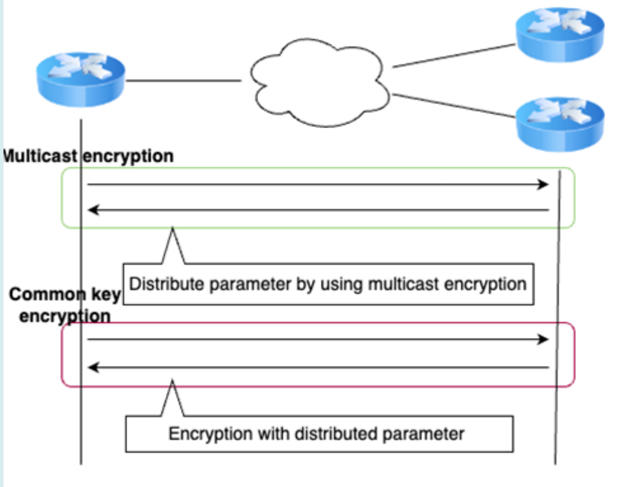
Multicast encryption
Distribute parameter by using multicast encryption
Common key encryption
Encryption with distributed parameter

Figure 6: Protocol of the proposed method.

Public Key Distribution

Figure 7 shows the public key distribution scheme of the proposed method. In the proposed method, the sender must know the public key of the recipient it wants to send. A new member joining a multicast group distributes its own way members of a multicast group can know each other's public keys.

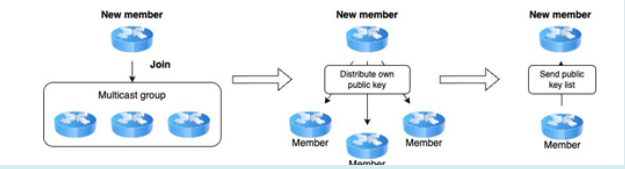

Figure 7: Public key distribution in the proposed method.

Experiments

Comparison of establishment time between existing and proposed methods. DMVPN is used as the existing method. The purpose of this experiment is to measure the establishment time of the secret communication group of DMVPN and the proposed method, and to show whether there are practical problems or not.

DMVPN

DMVPN was implemented by using vyos1 on GNS3. vyos is an open source network operating system. It can be installed on physical machines, virtual machines, and cloud platforms. Figure 8 shows the measurement range of the experiment with DMVPN. In this experiment, we measure the time from start to finish of IKE Kaufman C, et al. [8].

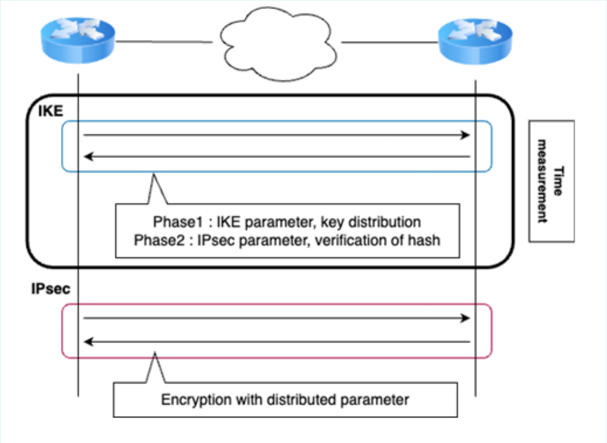
IKE
Phase1 : IKE parameter, key distribution
Phase2 : IPsec parameter, verification of hash
Time measurement
IPsec
Encryption with distributed parameter

Figure 8: The experiment with DMVPN.

Experiments to Evaluate the Proposed Method

We implemented the proposed method using Python on Ubuntu on GNS3. Since the devices are not authenticated, this is a simplified implementation for key public key exchange. Multiple nodes are prepared and joined to the same multicast group. One of them is the sender and the remaining nodes are the recipients. Figure 9 shows the measurement range of the proposed method. The time from when the sender encrypts the common key with the multicast cryptography to when the recipient decrypts the ciphertext to obtain the common key is measured. The encryption method of the multicast cryptography uses the RSA cipher. It allows the use of existing RSA public and private keys.

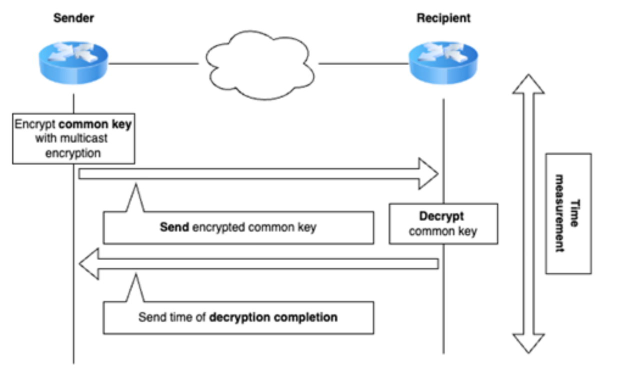
Sender
Recipient
Encrypt common key with multicast encryption
Send encrypted common key
Decrypt common key
Send time of decryption completion
Time measurement

Figure 9: The experiment with the proposed method.

Results

Table 1 shows the experimental results of the proposed method. In this experiment, 1, 2, 9, and 19 recipient nodes for the proposed method were prepared, and the average of the results of five experiments each was calculated. Results show that the time required to establish a group increased as the number of units increased. In the case of 1 and 2 units, the time required remained almost unchanged. In addition, the size of the ciphertext increased in proportion to the increase in the number of units. As a comparison, Table 2 shows the experimental results for DMVPN.

Recipients	Establishment (ms)	Size (byte)
1	42.3	256
2	38.8	512
9	61.6	2304
19	71.9	4864

Table 1: Time Measurement (Proposal).

Connection Node	Tunnel establishment time (ms)
Hub-Spoke	45.2
Spoke-Spoke	35.9

Table 2: Time Measurement (DMVPN).

Since DMVPN establishes tunnels on a one-to-one basis, the establishment time per node does not change as the number of nodes increases. Three nodes were prepared and the time required to establish tunnels between hub-spoke and spoke-spoke was measured. Five measurements were taken and the average was computed. DMVPN tunnel establishment time occurs at any time with each additional node when the number of nodes is increased.

Discussion

Usability

The proposed method can use existing RSA public key pairs. It also does not require a single key management server. This makes it easier for users to deploy the system and eliminates the need to access a single server when updating keys. Thus, usability is improved.

Functionality

In existing methods, a trusted group of members is constituted and between those members, sending and receiving are allowed. However, in the proposed method, the sender can select the recipient to form a group for secret communication. This can provide a new functionality where the sender selects the recipient and can distinguish between sending and receiving privileges.

Connection Establishment

Tables 1 & 2 shows that when the number of nodes is 2 or 3, the time required for establishment are almost the same, so there is no practical problem. In the existing method, establishment is performed as needed as the number of nodes increases, so the establishment time increases proportionally. However, since the proposed method can establish using multicast, the establishment time does not increase proportionally. As a result, the time required for establishment is less than that of the existing method when the number of units increases. In the proposed method, the sender can select the recipient. Such characteristics allow us to separate groups of senders and recipients, and each base can be authorized to send and receive data. This allows a one- way network to be configured in which a certain base is allowed to receive data, but not to transmit from that base. Currently, no method for utilizing such a network has been proposed, but it will be a very useful method when the demand for such a network arises in the future.

Future work

As a future direction, it is necessary to propose a method that utilizes a one-way network. This will further improve the usefulness of the proposed method. One concern is that the proposed method achieves encryption for multiple recipients by calculating the recipients' public keys as a direct product, which increases the ciphertext size. As shown in Table 1, the ciphertext size increased proportionally as the number of locations increased in the experiment. The number of sites used in the experiment does not exceed the maximum size of 65535 bytes, which is the size of IP and UDP packets. In practical use, the case where the maximum size is exceeded must be considered.

Conclusion

In recent years, sites use inter-site VPNs to provide reliable communication. In this study, we focused on multi-site VPNs, which are being studied as the number of sites increases. For VPNs between multiple sites, methods of establishing a tunnel connecting multiple sites or sharing the same policy among a group of sites were proposed. In this study, we proposed a method to share policies using multicast encryption. The proposed method does not require a single key management server in a GET VPN, and the sender can share the policy by selecting the recipient. Experimental results show that the proposed method has the same establishment time as existing IPsec implementations and outperforms existing methods when the number of sites increases. In addition, the proposed method not only replaces existing inter-site communication. Since the sender can choose the recipient, it is possible to construct a network with unbalanced privileges. The proposed method is even more useful for such networks with unbalanced privileges.

References

1. Karen S, Kent S (2005) Security Architecture for the Internet Protocol. Network Working Group RFC4301.
2. Freier AO, Karlton P, Kocher PC (2011) The Secure Sockets Layer (SSL) Protocol Version 3.0. RFC 6101.
3. Rosen EC, Worster T, Rekhter Y (2005) Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE). RFC 4023.
4. Alam T, Refat CMM, Imran AZ, Rashid SZ, Kabir H, et al. (2018) Design and Implementation of a Secured Enterprise Network using Dynamic Multipoint VPN with HSRP Protocol. In 2018 International Conference on Innovations in Science, Engineering and Technology (ICISET), pp: 367-371.
5. Niazi H, Shah N, Zhou B, Sethi V, Shastry S, et al. (2018) Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide. Technical report, Cisco Systems.
6. Hardjono T, Rowles S, Weis B (2011) The Group Domain of Interpretation. RFC 6407.
7. Matsuzawa T (2021) Proposal for Multicast Cryptography and Its Prototype Cipher. Inter J Computer Software Engineering 6(168): 1-5.
8. Kaufman C, Hoffman P, Nir Y, Eronen P, Kivinen T, et al. (2014) Internet Key Exchange Protocol Version 2 (IKEv2). IETF RFC8793.