# Protocols to Prevent Illegal Information Flow in Peer-to-Peer Publish/Subscribe Systems

NAKAMURA, Shigenari

(出版者 / Publisher)
法政大学大学院理工学・工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学・工学研究科編 / 法政大学大学院紀要. 理工学・工学研究科編
(巻 / Volume)
58
(開始ページ / Start Page)
1
(終了ページ / End Page)
3
(発行年 / Year)
2017-03-31
(URL)
https://doi.org/10.15002/00014348

# Protocols to Prevent Illegal Information Flow in Peer-to-Peer Publish/Subscribe Systems

Shigenari Nakamura
Supervisor Professor Makoto Takizawa
Graduate School of Science and Engineering, Hosei University

In a peer-to-peer (P2P) type of topic-based subscribe/publish (P2PPS) model, each peer (process) can be a publisher and subscriber. Here, a peer publishes an event message and then the event message is notified to a target peer which is interested in the event message. Publications and subscriptions are specified in terms of topics. In the topic-based access control (TBAC) model proposed in our previous studies, only a peer granted publication and subscription access rights is allowed to publish event messages with publication topics and subscribe events, respectively. In our previous studies, the illegal information flow relation among peers is defined and the subscription-based synchronization (SBS) protocol is proposed to prevent illegal information flow. Here, topics carried by event messages are just accumulated in the target peers and notification of event messages which may cause illegal information flow are banned in each target peer. The more number of event messages are published, the more number of event messages are not notified in the system. In this paper, we newly propose a subscription initialization (SI) protocol where topics accumulated in peers are removed to reduce the number of notifications banned. We show the number of notifications banned is reduced in the SI protocol compared with the SBS protocol in the evaluation.

***Key Words** : Information flow control, Peer-to-peer (P2P) model, Publish/subscribe (PS) systems, Subscription initialization (SI) protocol, Implicit topics, Topic-based access control (TBAC) model*

## 1. INTRODUCTION

In distributed systems, information in objects flow to other objects by transaction's manipulating the objects. In order to prevent illegal information flow, types of synchronization protocols are discussed based on the role-based access control (RBAC) model [1], [2], [3], [4]. On the other hand, a publish/subscribe (PS) systems are getting important as a general framework of a distributed system. In this paper, we consider a peer-to-peer (P2P) model of PS system (P2PPS model) where each peer can both publish and subscribe event messages. Here, a peer publishes an event message and then the event message is notified to a peer which is interested in the event. Publications and subscriptions are specified in terms of topics as discussed in topic-based PS systems. The *topic-based access control* (*TBAC*) model in PS systems is proposed [5]. A peer is allowed to manipulate topics in publish (*pb*) and subscribe (*sb*) operations. In our previous studies [5], we newly propose a subscription-based synchronization (SBS) protocol to prevent illegal information flow. Here, the notification of an event message which may cause illegal information flow are banned at each target peer. In this paper, we newly propose a *subscription initialization (SI)* protocol to reduce the number of banned notifications. We show the number of notifications banned is reduced in the SI protocol compared with the SBS protocol.

## 2. TBAC MODEL

In the TBAC model, an TBAC access rule $\langle p_i, t, op \rangle$ means that a peer $p_i$ is allowed to manipulate a topic $t$ in an operation $op$. Here, an operation $op$ is subscribe (*sb*) or publish (*pb*). A pair $\langle t, op \rangle$ of a topic $t$ and an operation $op$ shows an access right in the TBAC model. A peer $p_i$ is allowed to perform an operation $op$ on a topic $t$ only if an access right $\langle t, op \rangle$ is granted to the peer $p_i$.

## 3. LEGAL INFORMATION FLOW

The publication $p_i.P$ of a peer $p_i$ is a subset of topics on which a peer $p_i$ is allowed to publish an event message. The subscription $p_i.S$ of a peer $p_i$ is a subset of topics on which a peer $p_i$ is allowed to receive event messages.

**[Definition 1]** A peer $p_i$ *flows* to a peer $p_j$ ($p_i \rightarrow p_j$) iff (if and only if) $p_i.P \cap p_j.S \neq \phi$.

A peer $p_i$ is *compatible* with a peer $p_j$ ($p_j \rightharpoonup p_i$) iff the peer $p_i$ does not flow to the peer $p_j$ , i.e. $p_i \nrightarrow p_j$. There is no information flow relation among the peers $p_i$ and $p_j$ if

$p_i \rightharpoonup p_j$. A pair of peers $p_i$ and $p_j$ are compatible with one another ($p_i \rightleftharpoons p_j$) iff $p_i \rightharpoonup p_j$ and $p_j \rightharpoonup p_i$.

**[Definition 2]** A peer $p_i$ *legally flows* to a peer $p_j$ ($p_i \Rightarrow p_j$) iff one of the following conditions holds:

1) $p_i.S \neq \phi$, $p_i \rightarrow p_j$, and $p_i.S \subseteq p_j.S$.

2) For some peer $p_k$, $p_i \Rightarrow p_k$ and $p_k \Rightarrow p_j$.

**[Definition 3]** A peer $p_i$ *illegally flows* to a peer $p_j$ ($p_i \mapsto p_j$) iff $p_i \rightarrow p_j$ but $p_i \not\Rightarrow p_j$.

## 4. SYNCHRONIZATION PROTOCOLS

(1) Subscription-based synchronization (SBS) protocol

A peer $p_i$ is granted topics in the publication $p_i.P$ and subscription $p_i.S$. A peer $p_i$ is associated with subsets $p_i.PP$ and $p_i.PS$ of the topics granted to the peer $p_i$. A pair of the topic subsets $p_i.PP$ and $p_i.PS$ are referred to as *purpose* of a peer $p_i$. A peer $p_i$ is allowed to issue a publication operation $pb$ on a topic $t$ only if $t \in p_i.PP$. In addition, a peer $p_i$ is allowed to issue a subscription operation $sb$ on a topic $t$ only if $t \in p_i.PS$. In our previous studies, a subscription-based synchronization (SBS) protocol is discussed to prevent illegal information flow in the TBAC model [5]. In the SBS protocol, the notifications which may cause illegal information flow are banned.

**[Subscription-based synchronization (SBS) protocol]**

A peer $p_i$ publishes an event message to a peer $p_j$.

1) If $p_i.S \Rightarrow p_j.PS$, $p_j.S = p_i.PS \cup p_j.S$ and the event message is notified to a peer $p_i$.

2) Otherwise, the notification to the peer $p_j$ is banned.

(2) Subscription initialization (SI) protocol

In this paper, we newly propose a *subscription initialization (SI)* protocol. In the SI protocol, if an event message $e$ issued by a peer $p_i$ is not notified, i.e. banned at some target peer $p_j$, the topics accumulated in $p_i.S$ of the peer $p_i$ are initialized, i.e. removed in order to reduce the number of notifications to be banned.

**[Subscription initialized (SI) protocol]**

1) If $p_i.S \Rightarrow p_j.PS$, $p_j.S = p_i.PS \cup p_j.S$ and the event message is notified to a peer $p_i$.

2) Otherwise, if some number of the notifications of the event message $e$ are banned, the subscription $p_i.S$ of the peer $p_i$ is initialized, i.e. $p_i.S = \phi$.

We consider an initialization parameter $\alpha$ to allow a peer $p_i$ to initialize its subscription $p_i.S$. If the ratio of number of notifications banned to the total number of notifications in a publication is equal to or more than $\alpha$, the subscription $p_i.S$ is initialized.

## 5. EVALUATION

We evaluate the SI protocol compared with the SBS protocol in terms of number of notifications banned. In the evaluation, we consider twenty topics ($tn = 20$) and fifty peers ($pn = 50$). First, a collection $P$ of fifty peers are randomly generated on twenty topics. $en$ shows the number of event messages published. Here, $0 \leq en \leq 500$. The number $en$ of event messages are performed on the topic set $T$. We randomly create a peer set $P$ on the topic set $T$ seven hundred times for each $en$. Here, the number of topics in subscription purpose of each peer $mpstn$ is randomly selected out of numbers $0, \cdots, 8$. One peer $p_i$ is randomly selected in the peer set $P$ and one topic $t$ is randomly selected in $p_i.PP$. Then, the peer $p_i$ publishes an event message $e$ with the topic $t$. The event message $e$ is notified to a target peer $p_j$. Then, the legal information flow condition is checked. If not satisfied, the notification of the event message $e$ is banned. This step is iterated $en$ times. For a given peer set $P$ and the both protocols, $en$ event messages are published seven hundred times. Then, we calculate the average ratio for the both protocols.

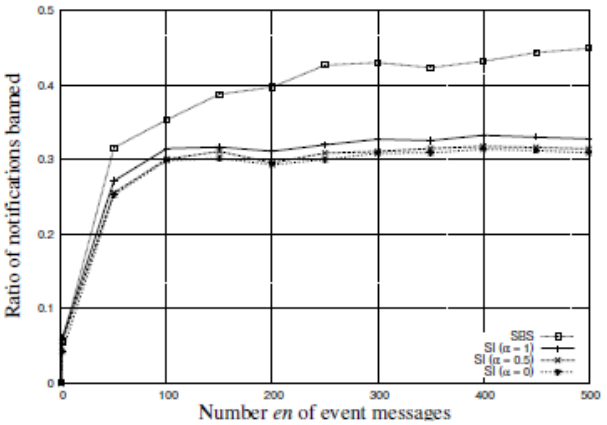


Figure 1. Ratio of notifications banned in the SI and SBS protocols.

Figure 1 shows the ratios of the number of notifications banned to the total number of notifications for the number $en$ of event messages in the SI and SBS protocols. The number of notifications banned in the SI protocol is fewer than the SBS protocol in any value of the initialization parameter $\alpha$. For example, about 43% of notifications are banned in the SBS protocol, but about 33%, 31%, and 33% are in the SI protocol for three hundred event messages ($en = 300$).

## 6. CONCLUDING REMARKS

In this paper, we discussed the legal information flow among peers in a P2PPS model based on the topic-based access control model, TBAC model. We first defined the legal information flow relation $p_i \Rightarrow p_j$ among a pair of peers $p_i$ and $p_j$. This means, if an event message published by a peer $p_i$ is notified to a peer $p_j$, no illegal information flow occur. In our previous studies [5], we discussed the SBS protocol. In the SBS

protocol, the notifications of event messages which may cause illegal information flow are banned. In this paper, we newly proposed the subscription initialization (SI) protocol to prevent illegal information flow in a system. In the SI protocol, the notifications which may cause illegal information flow are banned and then the subscription of a peer which publishes the event message is initialized. We evaluated the SI protocol compared with the SBS protocol in terms of number of notifications banned. In the evaluation, the fewer number of notifications are banned in the SI protocol than the SBS protocol.

ACKNOWLEDGMENT

We would like to thank Prof. Makoto Takizawa for supervising our thesis.

## REFERENCES

1) S. Nakamura, D. Duolikun, and M. Takizawa, “Read-abortion(RA) Based Synchronization Protocols to Prevent Illegal Information Flow,” *Journal of Computer and System Sciences*, Vol.81, No.8, pp.1441–1451, 2015.
2) S. Nakamura, D. Duolikun, T. Enokido, and M. Takizawa, "A Write Abortion-based Protocol in Role-based Access Control Systems," *International Journal of Adaptive and Innovative Systems*, Vol.2, No.2, pp. 142-160, 2015.
3) S. Nakamura, D. Duolikun, T. Enokido, and M. Takizawa, "A Flexible Read-Write Abortion Protocol to Prevent Illegal Information Flow among Objects," *Journal of Mobile Multimedia*, Vol.11, No.3&4, pp. 263-280, 2015.
4) S. Nakamura, D. Duolikun, T. Enokido, and M. Takizawa, "A Read-Write Abortion (RWA) Protocol to Prevent Illegal Information Flow in Role-based Access Control Systems," *International Journal of Space-Based and Situated Computing*, Vol.6, No.1, pp. 43-53, 2016.
5) S. Nakamura, T. Enokido, and M. Takizawa, "Information Flow Control Models in Peer-to-Peer Publish/Subscribe Systems," *Proc. of the 10-th International Conference on Complex, Intelligent, and Software Intensive Systems*, pp. 167-174, 2016.