An Extended Service Filtering Technique for Mass Calling-Type Services Using Intelligent Peripheral in an SCP-Bound Network

Kwang-Jae Jeong, Tae-Il Kim, and Go-Bong Choi

CONTENTS

ABSTRACT

This paper proposes an extended service filtering technique to prevent overload in service control point (SCP) due to televoting (VOT) or mass calling (MAS) services with the heavy traffic characteristics. Also, this paper compares this extended technique with the existing overload control techniques, and calculates steady state call blocking probabilities in intelligent network (IN) under overload conditions. The proposed technique considers SCP overload and IN Capability Set (CS)-1 services (such as VOT or MAS service) that have to use the specialized resources of intelligent peripheral (IP). This technique uses first an activating step in which SCP requests service filtering to service switching point (SSP). Then, in the filtering step, SSP sends filtering results to SCP periodically or each N-calls. Also, when filtering time-out expires, SSP stops service filtering, and sends service filtering response to SCP in the deactivating step. This paper applies this technique to VOT/MAS service, and calculates SCP and SSP-IP (circuit) call blocking probabilities by using an analytical VOT/MAS service model. With the modeling and analyzing of this new technique, it shows that this technique reduces the traffic flow into SCP from SSP and IP prominently.

I. INTRODUCTION

The telecommunications industry has paid considerable attention for the past several years to the concept of rapid deployment of new services in the telecommunication networks through the use of IN technology. To meet rapidly evolving market demands and requests for customized service, we have experienced IN SSP, SCP, and IP prototype systems to ensure competence of the major IN network elements for the effective deployment of target set of IN CS-1 services defined in International Telecommunications Union - Telecommunication standardization sector (ITU-T) Recommendation Q.12xx series [1]-[3].

Operation, administration & management (OAM), especially, traffic management functionality is a very important part of IN to prevent overload as well as to make efficient use of the network resources. There are two approaches [4]:

- Network-node-controlled traffic management mechanism reduces traffic to avoid overload of resources of an IN and of the underlying network [4].
- Service-logic-controlled traffic management mechanism influences the traffic dependent on service-subscriber-specified parameters. There are three approaches [4] :
  - limiting of calls to customer destinations
  - limiting of resources
  - customer service filtering

The first two approaches control the traffic to specified customer destinations according to the service logic executed by SCP. The customer service filtering approach is based on the localization of some service control functionality at SSP [4]. However, the existing service filtering technique cannot reduce the signaling traffics that flow into SCP from IP, when IN services such as Free Phone (FP) service, VOT service and MAS service are heavily utilized and required for IP resources. Therefore, there are some problems of SCP overload due to the signaling traffics from SSP/IP.

The intention of this paper is to propose an extended service filtering technique that includes IP, and that considers not only the localization of some service logic at SSP but also SCP overload. In addition, we solve SCP overload prevention problems due to VOT/MAS service calls that have the heavy traffic characteristics and are caused by the specialized resources of IP, especially. Also, this paper intends to calculate SCP call blocking probability through the application of this new technique to VOT/MAS service. Section II covers the concept and architecture of IN. Also, network interfaces between IN elements such as SSP, SCP and IP are mentioned in this section. Section III introduces the existing service filtering method, and describes its defects. This extended technique involves three steps, namely, the activating step, the filtering step, and the deactivating step. These are presented in Section IV of this paper. Also, this section makes service scenarios by using INAP operations defined in ITU-T INCS-1. Section V constructs an analytical VOT/MAS service model by using analytical modeling technique [7], [8], and calculates steady state SCP call blocking probabilities and SSP-IP(circuit) call blocking probabilities under overload conditions. By calculating the blocking probabilities of SCP and SSP-IP(circuit) that have the extended service filtering capability, this paper aims to demonstrate the reduction of the signaling traffics from SSP/IP to SCP. Finally, we conclude this paper in Section VI.

II. IN ARCHITECTURE

Figure 1 shows the IN functional architecture for VOT/MAS service. The physical entities considered in this architecture are SCP, SSP, and IP. The IN architecture as defined by ITU-T provides the following attributes[1]-[3]:

- Signaling System No.7 (SS7) is a core requirement for the IN that provides signaling connection(i.e., message transfer part (MTP), signaling connection control part (SCCP), transaction capability application part (TCAP) and intelligent network application protocol (INAP)) between SCP and SSP/IP.
- In addition to provide with access to the network and performing any necessary and flexible switching functionality, SSP allows access to the set of IN capabilities and contains detection capability to detect requests for IN-based services. Also, SSP contains capabilities to communicate with other physical entities (PEs) such as SCP and IP, and to respond to instructions from the other PE. Functionally, SSP contains call control function (CCF) and service switching function (SSF). Also, SSP may optionally contain call control agent function (CCAF), service control function (SCF), and service data function (SDF)[9]-[11].
- SCP provides centralized call processing and thus minimizes changes to the underlying switching infrastructure such as local or toll exchange. SCP contains the service logic programs (SLPs) and data that are used to provide IN-based services. SCP is connected to SSPs, and optionally to IPs, through the signaling network. SCP supports SCF and SDF.
- IP provides resources such as customized and concatenated voice announcements, voice recognition and dual tone multi-frequencies (DTMF) digit collection, and contains switching matrix to connect users to these resources. IP is used for flexible information interactions between a user and the IN(i.e. SCP). IP may directly connect to one or more SSPs, and may connect to the signaling network. Functionally, IP contains SRF, and provides the following capabilities [5], [6], [12], [13]:

- User interactive dialogue support of the IN SCP for processing of IN calls during IN dialogues;
- Collection of user input such as voice input or DTMF;
- Playing customized and mass announcements;
- Basic errors handling such that plays retry announcement and re-collects user input under the control of SCP.

VOT service included in ITU-T IN CS-1 service is defined as following [1].

"Using this service, the network operator can temporarily allocate a single directory number to the served user. Each time a call is made to this number by an end user, the user be played an announcement and asked to input a further digit to indicate a preference. The choice made will be recorded and a count incremented. When the service has ceased, the network operator will supply the details of the total "votes" cast for each preference to the served user and the special number will be reallocated. Calls made to this special number may be charged at varying rates."

Also, MAS service included in ITU-T IN CS-1 service has the same characteristics as VOT service [1].

SSP detects that end-users request VOT/MAS service, and notifies SCP to invoke the related SLP. Also, SSP provides the routing capability for IP and relays between the end-user and IP. SCP provides

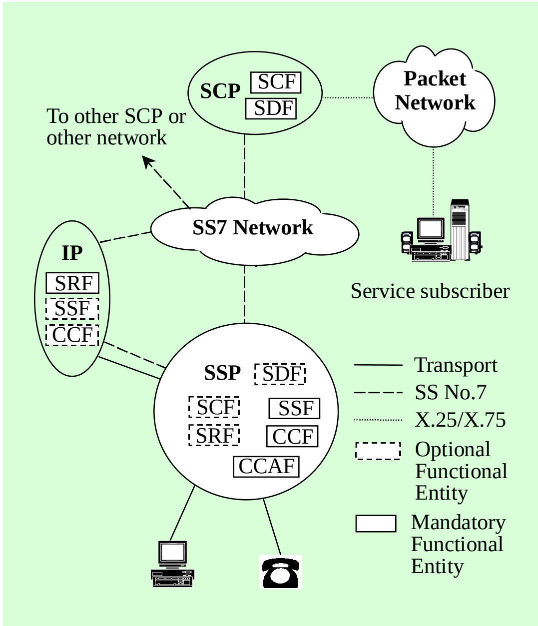

Fig. 1. The IN functional architecture for VOT/MAS service.

the service logic and data related to the service that is requested by the end user, and processes VOT/MAS service under the control of service logic. IP preserves network resources such as announcements, speech recognition and text-to-speech related to service processing. Also, IP provides end-users with network resources under the control of SCP, and collects digits from the end-users. SS7 Network transfers SS No.7 messages between SCP and SSP.

III. EXISTING SERVICE FILTERING

VOT/MAS service may generate extraordinary high traffic during short time intervals, especially during the first seconds after service activation. This leads to peaks of initial DP (IDP) operations from a number of SSPs to one SCP, as shown in Fig. 2. During a short time frame these traffic peaks together with the traffic related to other IN services may exceed the processing capacity of the SCP and/or the capacity of the underlying SS7 network if a large number of SSPs are involved. Such overload situations are handled by the overload control mechanisms (i.e. call gapping schemes) discussed in the papers [14], [15], [16] and [17]. As the result of the activation of these mechanisms the quality of service provision will be decreased because the service is made unavailable for a number of calling parties.

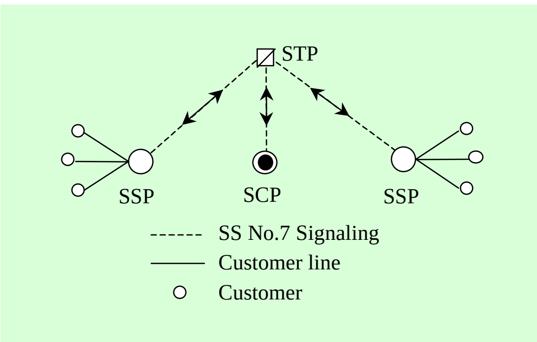

Fig. 2. SCP overload situations only including SSP and SCP.

To solve these problems, service filtering techniques are proposed [4]. The existing service filtering approach can provide the capability to reduce the number of IDP operations that have to flow into one SCP from one or more SSPs. However, it is impossible to reduce the number of INAP operation between one or more IPs and one SCP. Service calls may "experience" blocking in either (circuit switched) trunk subnetworks or signaling subnetworks although SCP has the existing customer service filtering technique. The existing technique means that simple registration functionality and announcement control functionality necessary in some applications are engaged at SSP through sending activate service filtering (ASF) operation [2]. This approach makes efficient use of the resources on IN systems including only SSP and SCP. VOT/MAS service may be used with service filtering capability as well as without this feature depending on service subscriber's choice.

However, we cannot apply this technique to IN topology including a number of IPs because the traditional techniques do not support the filtering of service calls connected to the specialized resources of IP. Also, the old technique cannot provide the service filtering capability that enable to reduce the traffic flows into SCP from many IPs. If VOT/MAS services are using the resources of IP, the existing approach cannot be applied to these services because there are many interactions such as assist request instruction (ARI), prompt and collect user information (PCUI) and collect user information (CUI) operations between IP and SCP through the signaling network. When VOT/MAS service subscriber would like to investigate public opinion with a single VOT/MAS directory number and various question items, it is more effective to provide a large number of sophisticated and customized announcements [5], [6] by using IP instead of SSP. Therefore, it is necessary to extend the existing service filtering approach.

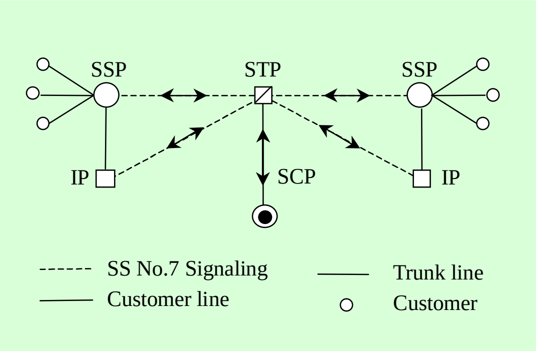

Fig. 3. SCP overload situations including SSP, IP and SCP.

IV. EXTENDED SERVICE FILTERING TECHNIQUE

Since VOT/MAS service requires a large number of customized announcements, it is more effective to provide this service by utilizing the useful resources such as play-announcement, the customized recorded announcement or DTMF detection. This case also leads to peaks of ARI, PCUI, PA (play announcement) and CUI at SCP-IP interface as shown in Fig. 3. Therefore, we propose this extended service filtering technique that can support a simple registration functionality of SSP and an announcement control of IP necessary for some applications. This approach makes more efficient use of the resources on IN systems including SSP, SCP and IP than existing approach.

1. Service Filtering Activation

SCP or network operator can activate the service filtering technique for a certain VOT/MAS subscriber in order to prevent No.7 traffic congestion and SCP overload. SCP sends the extended ASF operations, proposed in this paper, with specified filtering parameters to SSP. These filtering parameters are as follows :

- filteredCallTreatment
  - ipRoutingAddress (i.e. called party number): new defined parameter in this paper
  - serviceFilteringBillingChargingCharacteristics
  - informationToSend
  - collectedInformation: new inserted parameter in this paper
  - maximumNumberOfCounters
  - maximumNumberOfCalls: new defined parameter in this paper
  - releaseCause
  - disconnectFromIpForbidden: new inserted parameter in this paper
- filteringCharacteristics
  - interval or numberOfCalls
- filteringTimeout
  - duration or stopTime
- filteringCriteria, and

  - dialedNumber, callingLineID, serviceKey or addressAndService (called address value, service key, calling address value, location number)
- startTime

The service filtering is activated immediately or at the specified point in time (startTime). If startTime parameter is omitted, SSP starts filtering immediately.

The parameter group filteredCall Treatment specifies how filtered calls are to be treated. It includes information about what announcement should be played, how they are to be charged, how many counters should be used for counting filtered calls and what release cause should be applied to filtered calls. Specially, it indicates whether SSP is to connect to IP. Also, collectedInformation defines the information that will be collected from users.

The parameter group filtering Characteristics indicates the severity of the filtering to be applied and the point in time when the service filtering report will be sent. filteringCharacteristics are either Interval or numberOfCalls. If interval is set, then a call will be allowed through and a SFR operation will be sent to SCP at periodic intervals. If numberOfCalls is set, then every n-th call will be allowed through, and an SFR operation will be sent to SCP.

The parameter group filteringTimeout defines the maximum of the filtering. When the timer expires, a service filtering response is sent to SCP. It is a choice of specifying either the duration or a stop time.

The parameter group filteringCriteria is a choice of dialed number, calling party number or service key. It is used to specify those calls, which are to be filtered out.

2. Counting

If ipRoutingAddress parameter is NULL, then every detected VOT/MAS call to a destination with active service filtering causes SSP to increment the counter assigned to this destination. Also, the calling party will be connected to a customer-specified announcement (like, for example, “Your vote has been counted. Thank you for your call. Good-bye”).

However, if ipRoutingAddress parameter contains a called party number, then every detected VOT/MAS call to a destination with active service filtering causes SSP to route the call to the specified IP address using the initial address message (IAM) with filteredCallFlag[TRUE]. If IP receives IAM with filteredCallFlag[TRUE] for bearer channel setup, then IP waits for information request (INR) ISUP (ISDN User Part) message from SSP. On receiving the INR message including collectedInformation and disconnectFrom IpForbidden parameters, IP connects to the calling party via SSP, plays a customer-desired announcements, collects the digits dialed by the service user, and sends the information (INF) message including the dialed digits to SSPU. SSP increments the counter assigned to this destination by using the received INF message.

Every n-th call will be allowed through SCP and processed in a different manner, if desired. For example, a service user can be connected to the subscriber and has a dialogue with him or her.

3. Service Filtering Deactivation

Service filtering may be deactivated in three ways :

(a) filteringTimeout timer in SSP expires, and causes SSP to send the SFR operation with the lastResponse parameter and to stop counting.

(b) Call counters value exceeds maximumNumberOfCalls, and causes SSP to stop counting.

(c) Network operator or service provider force to deactivate the service filtering for operation and management.

4. Scenarios Using Information Flows

VOT/MAS service counts the number of calls to customer-specified dialed numbers and the number of votes for each question item. Each call is registered and the calling party is connected to a specific announcement of IP, in most cases. Some calls may also be routed to the destination for every n-th call if desired (for example, n = 10,000 calls). Therefore, it is not necessary to send an IDP INAP operations from SSP to SCP and to exchange an ARI, PCUI or CUI INAP operations between SCP and IP for each call to the related VOT/MAS service because SSP, SCP and IP have this extended service filtering capability. In other words, SSP detects the filtered calls, and send the IDP/SFR operations to SCP if only the n-th calls arrive after the service filtering is activated.

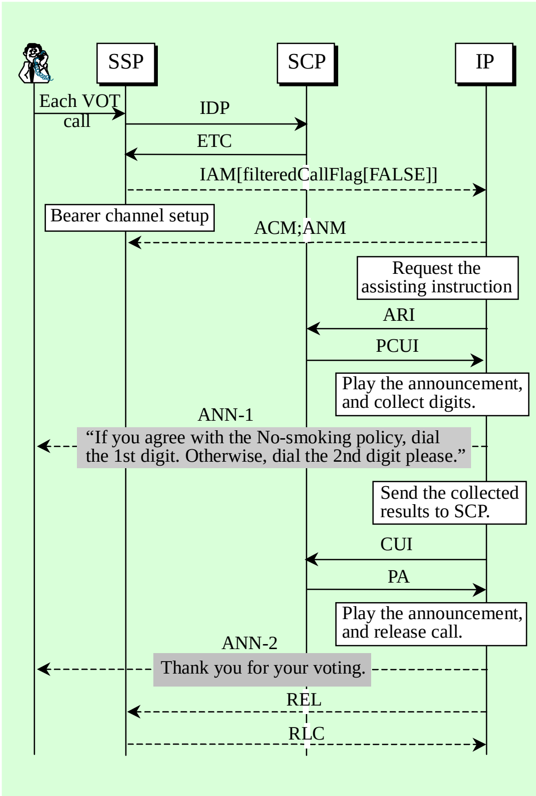

Fig. 4. Information flows before the extended service filtering technique is activated.

To illustrate the above, an example of extended service filtering with IP interactions is described as shown in Fig. 4∼7 using INAP protocol defined in ITU-T IN CS-1/CS-2 and ISUP messages of blue book specified by ITU-T. In the case of active service filtering SCP instructs SSP how to handle calls to specific destinations. SSP provides functionality to restore call history, to count calls to the specified called party addresses and to connect the calling parties to the pre-specified IP routing address as well. Also, SSP accumulates the number of votes for each question. IP plays the specific announcement, collects digits from users, and sends these digits to SSP. This new service filtering helps avoiding the SCP overload situations because it strongly decreases the number of IDP operations to be processed as well as the load of SS No.7 network. By using information flows (IFs) at SSP-SCP-IP interface, different scenarios of VOT/MAS are seen:

(a) Before the extended service filtering technique is activated.

Each VOT/MAS call immediately causes the IDP operation to be sent from SSP to SCP as shown in Fig. 4. SCP sends the Establish Temporary Connection (ETC) operation to SSP. According to SCP instruction, SSP attempts to set up a bearer channel with IP. After the bearer channel setup is completed, IP sends the ARI operation to SCP. Then, SCP sends the PCUI operation to IP under the control of the invoked VOT/MAS service logic. IP plays a specific announcement to the end user, collects digits dialed from the caller, and sends the CUI operation to the SCP.

(b) After the extended service filtering technique is activated.

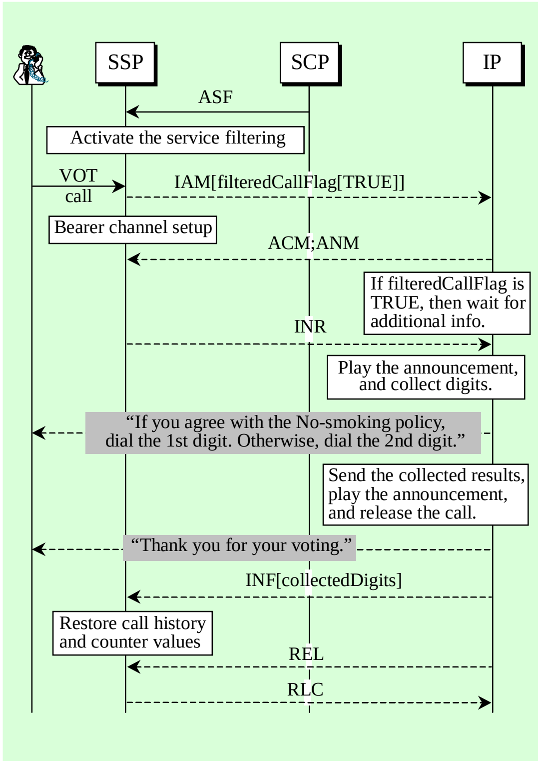

Fig. 5. Information flows after the extended service filtering technique is activated.

No call causes an IDP to be sent from SSP to SCP as shown in Fig. 5. According to the SCP instruction [i.e., ASF operation] that specifies how to handle the filtered calls, SSP processes the VOT/MAS service without SCP query. The value of numberOfCalls N or Interval T is set to the largest possible value.

(c) In the case of the n-th call arrival after the extended service filtering technique is activated.

Only each n-th VOT/MAS call or each T interval causes an IDP operation and additionally one service filtering response

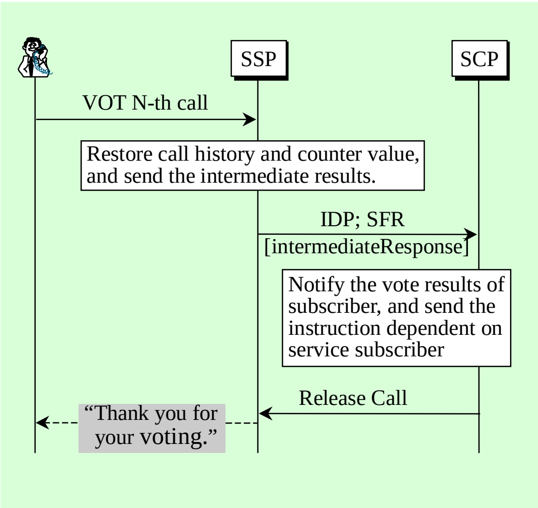

Fig. 6. Information flows in the case of the n-th call arrival after the extended service filtering technique is activated.

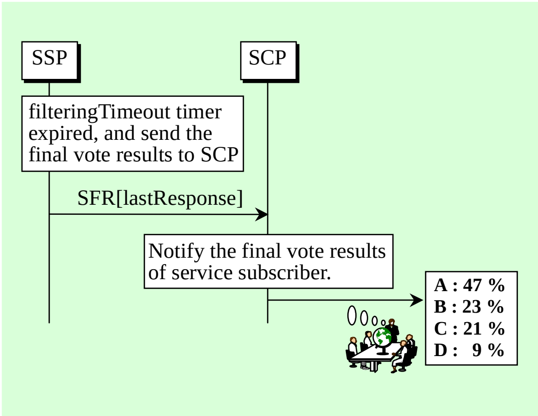

Fig. 7. Information flows after deactivating service filtering in the extended service filtering technique.

(SFR) operation to be sent from SSP to SCP as shown in Fig. 6. The value of numberOfCalls N or Interval T is chosen by the service subscriber.

(d) After the extended service filtering technique is deactivated.

When filteringTimeout timer expire, SSP reports the vote results to SCP through SFR[lastResponse] operation. Then, SCP notifies the service subscriber of these results, as shown in Fig. 7.

V. VOT/MAS SERVICE MODELING – CASE STUDY

1. VOT/MAS Service Model

To analyze the traffic characteristics of IN topology including two pairs of SSP-IPs, and one SCP, this paper models VOT/MAS service by using the analytical service modeling technique proposed in [7] and [8]. Also, in order to calculate the SCP call blocking probability and SSP-IP(circuit) call blocking probability before or after applying new extended service filtering to VOT/MAS service respectively, we assume VOT/MAS service action as shown in Table 1 [Refer to Fig. 7∼10.], and present VOT/MAS service model shown in Fig. 8. In this service model, customers reattempt actions are considered.

It is assumed in the paper that the trunk subnetwork and the signaling subnetwork have the same distribution characteristics with call requests rates forming Poisson process. Also, we assume that service requests produced by customer actions are treated as Poisson processes, and that the external reasons for blocking are the lack of a free circuit in the trunk subnetwork and the blocking caused by SCP overload. In

Table 1. Mapping between service actions and INAP/ISUP operations for VOT/MAS service.

Action	Comments	MSU type
a(0)	Dummy action.	
a(1)	SSP detects the filtered call, and accumulates the counters; SSP checks whether the call is the n-th call.	
a(2)	The n-th call; SSP attempts to send the query to SCP.	IDP; or IDP; SFR (SSP→SCP)
a(3)	Not the n-th call; SSP attempts to find a free circuit between SSP and IP.	IAM(SSP→IP)
a(4)	SSP query blocked; reattempt?	
a(5)	SSP query succeeded; SSP attempts to find a free circuit between SSP and IP.	ETC or Connect (SCP→SSP); IAM(SSP→IP)
a(6)	No free circuit; reattempt?	
a(7)	Free circuit found; SSP sets up a bearer connection with IP; IP interacts with SCP; IP plays ANN-1, collects digits from caller, and sends the digits to SCP; IP play ANN-2 to caller, and attempt to release the call.	ACM; ANM(IP→SSP); ARI(IP→SCP); PCUI(SCP→IP); CUI(IP→SCP); PA(SCP→IP)
a(8)	Free circuit found; SSP sets up a bearer connection with IP; SSP sends the additional instruction to IP; IP plays ANN-1, collects digits from caller, and sends the digits to SSP; IP play ANN-2 to caller, and attempt to release the call.	ACM; ANM(IP→SSP); INR(SSP→IP); INF(IP→SSP); PA(SCP→IP)
a(9)	Caller hangs up first; The occupied circuit released.	REL(SSP→IP); RLC(IP→SSP)
a(10)	IP hangs up first; The occupied circuit released.	REL(IP→SSP); RLC(SSP→IP)
a(11)	Dummy action	

order to calculate call blocking probabilities caused separately by the lack of circuits and by SCP overload, the followings are needed:

(a) layout of actions which represent part of the service functionality [7],

(b) probability to reattempt a failed call, and

(c) rates of services invoked by customers.

Let us denote by λ_S the rate at which a service is invoked by customers. It is the fresh input rate of calls from service subscribers into two pairs of SSP-IPs. In the n-th iteration, an action $a(i)$ is caused by another action $a(j)$ at a rate $\lambda(n-1)(j,\ i)$. The total rate $\lambda(n)(i)$, at which the action $a(i)$ is invoked by other actions in the n-th iteration, can be calculated as follows [7]:

$$\lambda^{(n)}(i) = \sum_{j\,=\,0}^{11} \lambda^{(n-1)}(j,\ i),$$

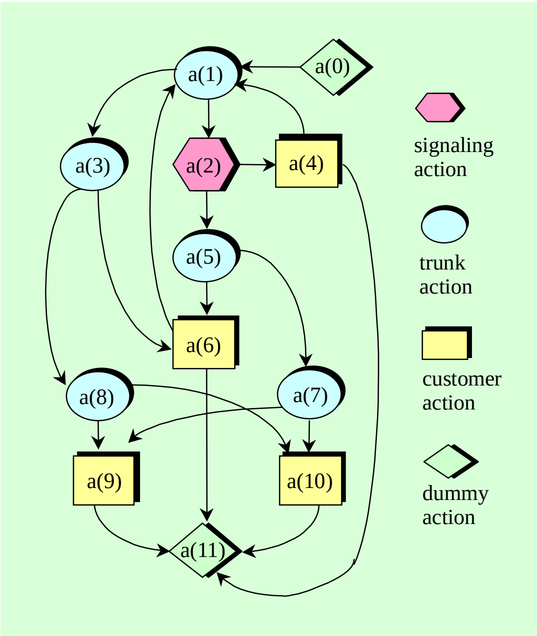

Fig. 8. VOT/MAS Service Model.

$$i = 1,\ 2,\ \cdots,\ 11,\ \text{and } i \neq j \qquad (1)$$

The action $a(i)$ invokes in turn another action, $a(j)$, with the output rate $\lambda(n)(i,\ j)$ which is obtained using:

$$\lambda(n)(i,\ j) = \lambda(n)(i)\ P(n)(i,\ j),$$
$$i = 1,\ 2,\ \cdots,\ 10,\quad j = 1,\ 2,\ \cdots,\ 11,$$
$$\text{and } i \neq j \qquad (2)$$

where $P^{(n)}(i,\ j)$ is a transition probability with which an action $a(i)$ invokes an action $a(j)$.

A. The Iteration Procedure

It is additionally assumed in the paper that the action $a(0)$ invokes the next action in turn at the rate λ_S in all iterations. The iterative procedure consists of the following steps:

Step 0: Preset action output rate :

$$\lambda^{(0)}(i,\ j) = 0,$$
$$n = 1,\quad i = 1,\ 2,\ \cdots,\ 10,$$
$$j = 1,\ 2,\ \cdots,\ 11,\ \text{and } i \neq j \qquad (3)$$

Step 1: For all actions, calculate input rates using (1).

Step 2: For all actions, calculate output rates using (2).

Step 3: Check the following convergence criteria :

$$\frac{\lambda^{(n)}(i,\ j) - \lambda^{(n-1)}(i,\ j)}{\lambda^{(n)}(i,\ j)} \leq \varepsilon,$$
$$i = 1,\ 2,\ \cdots,\ 11,\quad j = 1,\ 2,\ \cdots,\ 11,$$
$$\text{s.t. } i \neq j \text{ and } \lambda^{(n)}(i,\ j) \neq 0, \qquad (4)$$

where ε is an arbitrarily small, positive value (in this paper, $\varepsilon = 10^{-8}$). If all these criteria are successful, then the iterations are finished. Otherwise, go to Step 4.

Step 4: $n = n+1$. Go to Step 1.

B. Case Study

We consider two pairs of SSP-IP and one SCP shown in Fig. 3, and assume that the network is SCP-bound but not IP-bound. From the network point of view, a call set-up may not succeed due to external or internal reasons. But, we assume that blocking of calls within the signaling subnetwork due to other reasons than SCP overload is negligible. Also, we consider only the blocking of calls due to the lack of a free circuit in the trunk subnetwork.

SCP, when overloaded, invokes the call gapping (CG) load regulation procedures in both signaling points (SPs) which also perform SSP functions for intelligent services. This is a typical approach to combat persistent overloads in SCPs (for example, see [14]). The type of the CG scheme considered, assumes that time is divided into equal intervals at most one call request is allowed to be sent from the SSP to the SCP in any interval. This type is not the most effective amongst the CG schemes, but it has already been implemented in a real network [17]. CG scheme sets a limit on the rate at which calls are accepted – one per gapping interval, where we choose the gapping interval to give the desired performance.

This paper's aim is to evaluate call-blocking probabilities caused separately by the lack of circuits and by the SCP overload. Therefore, it is assumed in the paper that our SCP uses the call gap control mechanism [14], [15] with the length of one time gap to calculate the blocking probabilities for the simplified IN topology. The Erlang (B) loss formula is used to calculate the call blocking probability due to the lack of circuits between SSP and IP.

$$P_B(cir) = \frac{(\lambda_{cir} T_{cir})^{N_{cir}} / N_{cir}!}{\sum_{k=0}^{N_{cir}} \frac{(\lambda_{cir} T_{cir})^k}{k!}}, \qquad (5)$$

where λ_{cir} is the total input traffic of call requests for circuits, N_{cir} is the total number of circuits between SSP and IP, and T_{cir} is the average circuit holding time.

Considering the layout of call requests, it is apparent that :

$$P^{(n)}(1,2) = 1/N, \qquad (6)$$

$$P^{(n)}(1,3) = 1 - P^{(n)}(1,\ 2), \qquad (7)$$

$$P^{(n)}(3,6) = P^{(n)}(5,\ 6) = P_B(cir), \qquad (8)$$

$$P^{(n)}(3,8) = P^{(n)}(5,\ 7) = 1 - P_B(cir), \qquad (9)$$

and

$$\lambda_{cir} = \lambda^{(n)}(1,\ 3) + \lambda^{(n)}(2,\ 5), \qquad (10)$$

where N is the number of calls for the filteringTimeout parameter which specifies the filtering period.

It is assumed in the paper that SCP has the overload control scheme proposed in the paper [17]. Under the assumption, we can easily calculate the call blocking probability, $P_B(SCP)$, by using the following formula [17]:

$$P_B(SCP) = \frac{\lambda_{SCP} T_{GAP} - 1 + e^{-\lambda_{SCP} T_{GAP}}}{\lambda_{SCP} T_{GAP}}, \qquad (11)$$

where λ_{SCP} is the total traffic of call requests directed from SSP/IP to SCP, and T_{GAP} is the time gap length used for call gapping scheme.

Considering the layout of call requests, it is seen that :

$$P^{(n)}(2,\ 4) = P_B(SCP), \qquad (12)$$

$$\lambda_{SCP} = \lambda^{(n)}(1,\ 2) \qquad (13)$$

and

$$\lambda^{(n)}(0,\ 1) = \lambda_S, \qquad (14)$$

where λ_S is the fresh input traffic rates by customer.

2. Analytical Results

Using (5)∼(14) and applying the iterative method described above in this section, the SCP blocking probabilities and the SSP-IP(circuit) call blocking probabilities can be obtained. The following parameters, partly taken from Kwiatkowski [7], [8] and Skoog [18], are chosen for this paper. It is assumed that the dialogue time is exponentially distributed with the mean of 150 sec. Half of successful calls are finished when the caller hangs up first. If a call fails, the probability of a call reattempt is set to 0.7. Also, we assume that the total number of trunk circuits is equal to 2000, and that the SCP call gapping interval is set to 0.2 second. However, because the papers [7] and [8] proved that the analytical results by the analytical modeling technique are almost equal to the simulation ones, we omit the simulation to confirm our analytical results.

Figure 9 depicts the successful call traffic rate as a function of λ_S and N. It is obvious that the successful call rate increases as N grows. When N is equal to 1 (*i.e.* the extended service filtering is not applied), the successful call rate is less than 5 call/sec. However, after service filtering is activated a higher number of calls are served. Also, it's seen that the completed call rate is saturated at the 13.3 call/sec rate, even if N is set to a very large number, as we guess these results from the Erlang(B) loss formula. Anyway, the successfully served calls increase with applying service filtering technique.

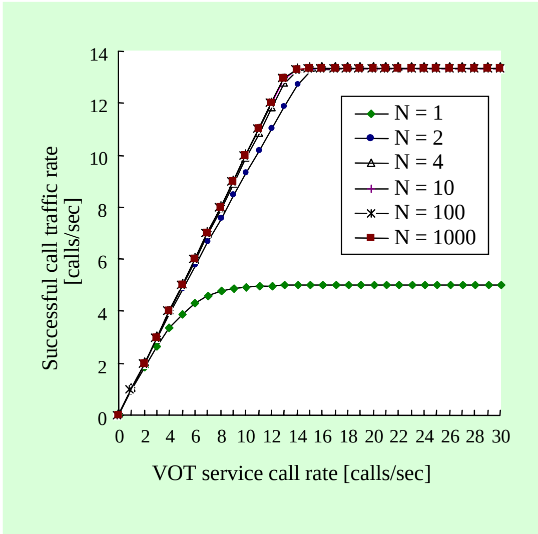

Fig. 9. The successful call traffic rate.

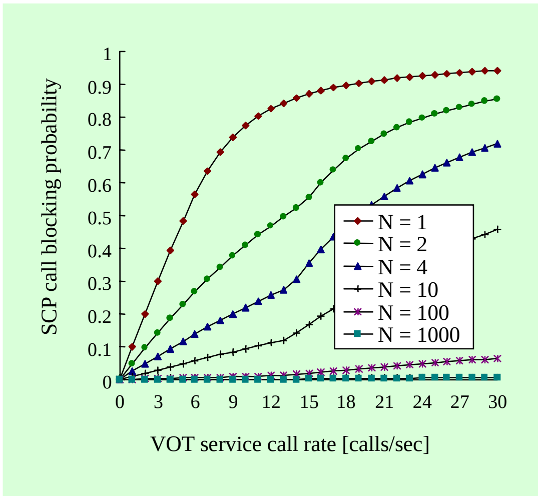

Fig. 10. SCP call blocking probability.

Figure 10 shows SCP call blocking probabilities before and after the extended service filtering activation, as a function of λ_S and N. It can be seen that $P_B(SCP)$

decreases after service filtering activation. As N increases, the traffic rate at signaling subnetwork is decreased. Also, in case that filtering period N is greater than 100, most calls that need to communicate with SCP are not blocked by call gapping scheme. Therefore, from the analytical results it's seen that the proposed service filtering technique prominently reduces the traffic rate of signaling subnetwork including IP.

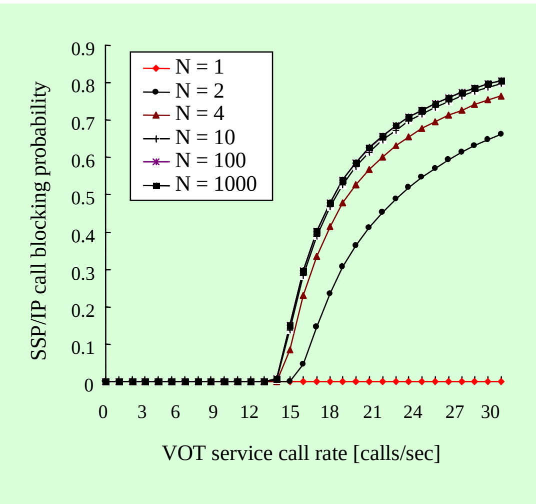

Fig. 11. SSP-IP(circuit) call blocking probability.

Figure 11 shows the SSP-IP(circuit) call blocking probabilities before and after the extended service filtering activation as a function of λ_S and N. When the number of calls N is equal to 1 (i.e. no service filtering is applied) $P_B(cir)$ is nearly equal to 0 call/sec, the successful call rate is less than 5 call/sec (Fig. 9) and $P_B(SCP)$ increases as the fresh input rate λ_S increases (Fig. 10). From these facts, it's seen that SCP blocks most signaling requests of service calls in order to avoid the overload of SCP and signaling subnetwork. Eventually most calls are not served because of the overload of the signaling subnetwork.

Also, after the extended service filtering technique is applied, the circuit call blocking probability $P_B(cir)$ abruptly increases at the rate of nearly 13.3 call/sec, since customer calls with the call arrival rate $(1 - 1/N)\ \lambda_S$, arrive at the trunk subnetwork without the SCP call gapping scheme. This means that the number of calls blocked by the SCP call-gapping scheme is decreased as N increases. Eventually, since the service calls that SCP query are succeeded are increased, the number of blocked calls due to the lack of trunk circuits is overall increased for each N. In other words, most of the SS7 traffics from many SSPs to one SCP is distributed over many SSP-IP interfaces. Therefore, a higher number of VOT/MAS calls are served. Also, the increase of $P_B(cir)$ due to the lack of trunk circuit can be solved by providing a higher number of circuits.

As a side effect of the analytical results, we can obtain the value N needed to preserve SCP call blocking probability within 1 percent. If N is more than $5\lambda_S\, T_{GAP}$, SCP can process most of service calls with 0.01 call blocking probability.

VI. CONCLUSIONS

This paper proposed the extended service filtering technique for IP. If the

VOT/MAS service is provided through an IP resource, this will lead to traffic congestion of signaling subnetwork. In addition, while the existing service filtering scheme can be applied only to both the SSP and the SCP, the extended service filtering technique can be applied to the SSP, SCP and IP as well, which reduces the traffic in the signaling subnetwork and increases the number of billed calls. Finally, the extended service filtering will increase the efficiency of network resources. Figure 9∼11 apparently illustrate these results. Therefore, we can apply the extended service filtering technique to the high traffic volume services like VOT or MAS service in IN topology, and plan to implement this technique in our large-scale IP which has the capacity to process 100,000 BHCA(busy hour call attempts). Also, because the ITU-T IN CS-1 does not specify the proposed service filtering technique, we plan to propose this technique in ITU-T IN CS-2. Especially, the description of ASF IF and ASF operation procedure in ITU-T Q.1224/Q.1228 recommendation document must be modified for the purpose of applying service filtering to IN service calls which require the specialized resources of IP.

ACKNOWLEDGMENTS

This study has been funded by Korea Telecom and performed as a part of the R&D activities for the AIN IP system. Also, we thank Dr. M. Kwiatkowski for his long-standing and detailed review of this paper.

REFERENCES

[1] ITU-T Q.1211, *Introduction to Intelligent Network CS-1,* Apr. 1995.

[2] ITU-T Q.1214, *Distributed Functional Plane for Intelligent Network CS-1,* Apr. 1994.

[3] ITU-T Q.1218, *Interface Recommendation for Intelligent Network CS-1,* Apr. 1995.

[4] D. Carl and R. Rieken, "Congestion Control and Overload Prevention in Intelligent Networks," *ICIN'92(International Conference on Intelligence in Netwarks)*, Bordeaux, France, Mar. 3-5, 1992, pp. 280-285.

[5] Y.H. Seo, G.B. Choi, C.K. Lee, and H.G. Bahk, "A Design and Implementation of the IP in Korea," *APSITT'93*, Bangkok, Thailand, Nov. 11-12, 1993, pp. 28-31.

[6] Y.H. Seo, G.B. Choi, and C.M. Han, "IP: Intelligent Peripheral for IN," *ISITA'94(International Symposium on Information Theory & its Applications)*, Sidney, Australia, Nov. 20-24 1994, pp. 531-534.

[7] M. Kwiatkowski, "Steady State Performance Analysis of Intelligent Networks Under Overload," *GLOBECOM'94(IEEE Global Telecommunications Conference)*, 1994, Vol. III, pp. 1269-1273.

[8] M. Kwiatkowski, "Mean Delay in Intelligent Networks Under Overload," International Conference on Telecommunications Systems Modeling and Analysis, Nashville, USA, 1995.

[9] G.B. Choi, H.H. Lee, Y.S. Kim, and H.G. Bahk, "A Service Switching Point for Intelligent Networks," *ICCC'92*,Tampa, U.S.A., May 4-6, 1992, pp. 268-274.

[10] H.H. Lee, T.I. Kim, G.B. Choi, C.K. Lee, and H. G. Bahk, "Development of a SSP System for Intelligent Networks," *INFOCOM'93*, Bombay, India, Nov. 25-27, 1993, pp. 117-140.

[11] K.R. Kim, H.J. Lim, M.S. Cho, H.H. Lee, T. I. Kim, and G.B. Choi, "IN Call Processing of the Service Switching Point," *APCC'95(Asia-Pacific Conference on Communications)*, Vol. I, Japan, June 14-16, 1995, pp. 108-112.

[12] S.K. Jain, "Intelligent Peripheral: Signaling and Protocols", *ISS'90(XIII International Switching Symposium)*, Vol. III, Oct. 1992, pp. 117-121.

[13] R. Soh, H.G. Jeong, H.H. Lee and D.S. Park, "IP-Based Interactive Voice Services in Advanced Networks," *JTC-CSCC'94(Joint Technical Conference on Circuits/Systems, Computers and Communications)*, Vol. II, Kongju, Korea, July 11-13, 1994, pp. 902-907.

[14] G. Hebuterne, L. Romoeuf and R. Kung, "Load Regulation Schemes for the Intelligent Network," *ISS'90(XIII International Switching Symposium)*, Vol. V, Stockholm, 1990, pp. 159-164.

[15] N. Tsolas, G. Abdo and R. Bottheim, "Performance and Overload Considerations When Introducing IN into an Existing Network," *International Seminar on Intelligent Network*, Zurich, 1992, pp. 407-414.

[16] X.H. Pham and P.J. Kuhn, "Congestion Control Intelligent Network," *International Seminar on Intelligent Network*, Zurich, 1992, pp. 407-414.

[17] P.M.D. Turner and P.B. Key, "A New Call Gapping for Network Traffic Management," *13th International Traffic Congress*, Copenhagen, 1991, pp. 121-126.

[18] R.A. Skoog, "Study of Clustered Arrival Processes and Signaling Link Delays," *13th International Traffic Congress*, Copenhagen, 1991, pp. 61-66.

Kwang-Jae Jeong was born in Chonju, Korea in 1968. He received his B.S. degree in Chon-buk National University, Chonju, Korea in 1989 and received M.S. degree in electronic engineering from Chon-buk National University, Chonju, Korea in 1991. Since he joined S/W Engineering Division of ETRI in 1991, he has served as a research staff to develop TDX-10 Service Switching Point (SSP) and Advanced Intelligent Network Intelligent Peripheral (AIN IP). His research interests include AIN, braodband intelligent network and telecommunication management network (TMN).

Tae-Il Kim received the B.S. degree in computer science from Soongsil University in 1983. He obtained the qualification for professional engineer in 1992. Since 1983, he has been a principle member of research staff in Switching Technology Division of ETRI. He has participated in a number of research projects including development of TDX-1, TDX-10, TDX-10 SSP, and AIN IP. He is currently leading an AIN service research project. His research interests are in AIN, IMT-2000, software design of communication systems, and software engineering.

Go-Bong Choi graduated from Kyungpook National University, Taegu, Korea in 1980 and received his Ph.D. degree in electronic engineering from Sungkyunkwan University, Seoul, Korea in 1995. He joined ETRI in 1983, where he is the head of AIN Switching Section. He served as a research staff to develop TDX-1, TDX-10 and TDX-10 SSP system. From 1987 to 1989, he was a visiting engineer at Bell Telephone/Alcatel in Belgium, and worked on the development of S1240 digital switching system. In his academic role, he is a member of the Korean Institute of Telematics and Electronics and Korean Institute of Communication Sciences where he has been the secretary of communication software committee since 1996. He was appointed as the chairman of organizing committee for AIN'95, COMSW'96, COMSW'97 and NCS'97 conferences.