

Economic Mechanisms for Protecting VoIP Services within the IMS

Gabriel Andrews, Neco Ventura
University of Cape Town,
Electrical Engineering
7700 Rondebosch
South Africa
Tel + Fax 0216505296
gandrews,neco @ {crg.ee.uct.ac.za}

Abstract—The IP Multimedia Subsystem (IMS) is the proposed Next Generation Network (NGN) architecture that will be used to provide revolutionary services based on an IP backbone. For successful IMS deployment, service providers need to ensure that the services offered to customers are protected. This will ensure that customer satisfaction is upheld and that customers are retained within the network. Customer retention is an essential part of ensuring the needed investment into IMS technologies. This paper analyses a VoIP service offered over an IMS network as a revenue maximization problem. Using this technique we show that it is possible to prevent unsolicited sessions and to maintain customer satisfaction. We will provide guidelines that can be used to ensure that customers are protected from abuse which will result in an economically beneficial situation for all parties.

Index Terms— SPIT, SPAM, Economic mechanism, IMS

I. INTRODUCTION

THE Internet Multimedia Subsystem (IMS) is a service delivery platform proposed by the 3GPP as the network architecture for the future NGNs. The proposed architecture is access agnostic and provides a single management interface to provide services to customers attached to it via any medium. The IMS is an all-IP network built entirely on protocols developed by the IETF with necessary extensions to provide QoS, accountability etc. [1].

The main advantage is the rapid and efficient manner in which services are created and deployed. A set of common application service enabler's are to be standardized, these can then be mashed together to create innovative new services. The IMS is the evolution of existing networks and with this creates the impetus for the evolution of the services that we know today. Voice services too will be offered over this network but it will not be in the form as we see it today. Utilizing this IP-based network infrastructure Voice over Internet Protocol (VoIP) is the technology that will be used to provide voice services to users. This technology is already known to many users of the internet with some examples being

Skype, GTalk and AOL's TotalTalk and is known as an inexpensive means to make long distance internet calls. It is currently used by service providers who do not have their own network infrastructure to deliver voice services and compete with traditional telephony services [2]. The inexpensive nature of VoIP that has attracted a great deal of attention from service providers as well as their customers and it is envisaged that this business model will again be utilized within the IMS arena.

This technology is an IP-based service and it falls prey to the same predators as that of any IP-based communication service such as email. Unsolicited communications, or more commonly known as SPAM; in a VoIP domain it is referred to as Spam over Internet Telephony or SPIT. This represents a growing concern for service providers as a barrier for consumer uptake since customer quality of experience can be greatly reduced when they are subjected to unsolicited calls. It is human nature to answer a ringing phone, we normally believe that any call made to our telephone, whether mobile handset or PSTN device, is important. It is this nature that a spammer can abuse in a VoIP system. We have not as yet experienced a problem such as SPAM within the PSTN controlled voice service since it is economically unfeasible to conduct a SPAM attack on such a network, the calls would just be too expensive. This is where the benefit of VoIP becomes a flaw; because it is so inexpensive to use it will lessen the barrier to entry for spammers in this market, creating an entire new customer base for these abusers to plague. To ensure that network providers adopt this architecture it is up to the research community to provide sound business reasons to prove the economic benefits for the major investment and deployment into IMS technologies.

This means that we need to secure this service before it is deployed in a production environment. Solutions to the SPAM problem within email systems have been proposed to thwart spammers within VoIP networks but not all these techniques can be used because of the nature of the technology. Email systems currently employ a filter mechanism which marks incoming mail as either SPAM or legitimate mail and it is left for the email consumer to then choose which mails he/she would like to read. Filters cannot be used with SPIT since we have no way of filtering packets of digitized voice to discover

whether it contains unsolicited communications. Another method currently used in securing IP services are CAPTCHAs, where a user is required to enter mangled letters shown to them as an image. These have been adapted to VoIP where now a user is required to either type in a requested sequence of numbers or to answer a question. Although this solution is very effective it differs greatly from the way voice services are currently used today and this will then become another barrier to uptake since users would have to be retrained into using the service. We would optimally want a solution that requires minimal change from the way voice services are currently used today and which is not too invasive.

We feel that the economic techniques which have been proposed within the email solution space are the solutions that hold the most promise for securing VoIP services. Another benefit of these solutions is that they allow one to analyze the system from a business perspective and can be linked directly to a specific business model. This paper will aim at doing just that, we will model an IMS-VoIP market as a revenue-maximization problem and show that it is possible to prevent SPIT and at the same time encourage the use of the system for legitimate users. This will then facilitate uptake of IMS based services and foster customer buy-in to the IMS.

The structure of the paper is as follows. Section II is a literature review highlighting previous work done in the field which relates most to this paper. In Section III we describe the model that will be used for the analysis and the derivation of results. Section IV we discuss some results that were derived using the model and section V shows how these results can be applied in a service provisioning setting. Section VI then concludes the paper.

II. LITERATURE REVIEW

Economic solutions to the SPAM problem within email systems have been discussed within literature albeit not extensively. The literature has described the problem in two broad solution concepts; being that of an asymmetric-information problem or market efficiency problem. In the asymmetric information solution space we use the observation that the sender has more information regarding the validity of the message than the receiver and therefore has to decide legitimacy of the message before consuming it.

Researchers have also noted that the market inefficiency that is displayed in an email system is similar to what is known in economic terms as the 'tragedy of the commons'. This is when a common good, e.g. fish, is over-utilized within the market resulting in a market inefficiency in which the resources are not optimally allocated e.g. fish stock depletion. The solutions developed in economic literature are then applied to the communications network setting.

[3] used the asymmetric information approach and proposed a solution in which an attention bond is paid by senders to an external escrow service before a mail message is sent to the receiver's inbox. This system is effective in reducing both false positives and false negatives. It could be an

implementable solution but the effects of currency differences could pose problems in a production system.

[4] used a game-theoretic approach, they analyzed the effects on SPAM mail due to increased message costs, increased filter effectiveness and the incorporation of a do-not-spam registry.

[7] performed an information-economic analysis on a model of a Unsolicited Commercial Message (UCM) industry. The concept of an email user's attention endowment was used to determine the effect that different technologies have on SPAM email. The most striking result is that an increase in the effectiveness of a filter leads to an increase in the amount of UCM sent within the system. Thus increasing the network level cost of SPAM even though the amount of SPAM-delivered to a specific user's email box is reduced.

[5] have developed a game-theoretic model for the UCM system and have used the results to tune their email filters.

[6] has modeled a user's attention as the scarce resource that the agents compete for within the email system and they have shown that unsolicited commercial e-mail reduces the effectiveness of communication.

[8] also does an economic analysis but focuses on the legal aspects. He develops a model incorporating the property rights of both email users and spammers and analyses the social welfare under these different approaches to email SPAM law.

[9] focused on the economic aspects of email service providers stopping the spam that they send out of their networks. They proved that by increasing the cost of messages and by employing a customer feedback system one can drastically reduce the amount of spam within ones network. They also have proved an interesting result in that by presenting an email user with a Turing Test for every k (e.g. $k=100$) messages and limiting the amount of these test to d (e.g. $d=10$), proves to be as effective to presenting the user with one Turing test for $k*d$ times every time a message is sent. This would then be less annoying to legitimate user but still be a headache to spammers.

Our model borrows much from these but is most similar to [9] and [4] but we have chosen to analyze a market where the service provider is also a peddler of commercial advertisement messages since this is where the revenue for the service will come from. Hence ironically the service provider is a potential spammer as well. They have also all only focused on email spam and have not touched on what changes are affected when the messages are carried in a VoIP market.

III. THE MODEL

There are z_T customers within the system. These customers are customers of an IMS network provider and subscribe to the IMS-VoIP service provided by the IMS-VoIP Service Provider (VSP). We assume that the revenue that the IMS-VSP generates is through advertising only and that there is no subscription cost. The exclusion of subscription costs will be made since we are not trying to determine an optimum subscription cost for this service and the inclusion of this parameter will only serve to increase the complexity within the model. We will also assume that the customer's have the

option to choose to receive solicited commercial advertising. The portion of the customer base that agrees to this will be represented by z_{IN} and the probability for any customer to have chosen to receive advertisements is $\sigma = z_{IN}/z_T$. The amount of people that respond to these advertisements is z_{RES} and the response rate for advertisements within the system will be the ratio of amount of people who respond within the total population, we will represent this by $\mu = z_{RES}/z_T$. We will call the amount of calls made within the system N_{total} . Of these calls some will be legitimate calls or solicited advertisements, represented by N_{leg} and others will be unsolicited, represented by N_{illeg} . The total number of calls is the sum of the two. The probability that any customer receives an unsolicited commercial session will then be represented by $\zeta = N_{illeg}/N_{total}$.

To complete the model we will include the network provider in the role of a social planner. The network provider rents part of its capacity to the service provider in fixed amounts, it is assumed that the service provider cannot request more resources but has to form a new agreement with the network provider, for the purposes of the model the network provider has a fixed amount of capacity and he wants to maximize the return from this investment. This is a fixed cost and is thus external to the dynamics of the market being analyzed.

Using these definitions we will now describe the payoff for each player within the network. The IMS uses the Session Initiation Protocol (SIP) to setup sessions within the network, we will use the term unsolicited commercial sessions (UCS) to describe all sessions that are created by the spammers.

A. The IMS-VoIP Service Provider

We will assume that the IMS-VSP has paid for a fixed portion of capacity from the Network provider, for the model we will average this cost on a per session basis, this cost will then be represented by $N_{total}C_{VSP}$, where N_{total} is the total number of sessions made and C_{VSP} is the average cost per session. We assumed that the service provider did not charge the customers for the service and that the revenue will be generated via advertising, this is represented by σB_{VSP} . We assume that an opt-in policy is used and represent this opt-in ratio by σ , B_{VSP} represents the benefit the VSP receives for each correctly delivered non UCS. For completeness we also include a term for any benefit received by the IMS-VSP for delivering UCS. It is rational to expect that some customers that have not opted to receive advertisements from the VSP but still do. The VSP receives some benefit for this but the customer still regards this as SPIT. The portion of population affected by this is $(1-\sigma)$, and the benefit that the IMS-VSP receives from this is

$(1-\sigma)\zeta\mu B_{VSP}$ where B_{VSP} is the average benefit received by the IMS-VSP for each UCS delivered to it's customers and μ is the amount of probability that a customer responds to the UCS. The total payoff that the IMS-VSP receives is

$$U_{VSP} = -N_{total}C_{VSP} + z_T (\sigma B_{VSP} + (1-\sigma)\zeta\mu B_{VSP}) \quad (1)$$

B. The IMS-VoIP customer

The customers are the valuable commodities within this market and t is essentially their attention we are targeting [6]. We will, for now, ignore situations where the customers pay an extra amount for the bandwidth that they consume. Although this will be a direct cost for the user, the income generated will be gathered by the IMS network provider and thus for our purposes we can ignore this as an externality. The cost for using the service is very low or zero but the customers who receive unsolicited sessions experience a negative benefit. We define this as a cost for the customer by C_R , where C_R is the average cost per UCS that is received. A distinction is stressed here, in that it is rational to expect that there will be a portion within the population that will see these sessions as solicited and respond to these messages.. Hence the benefit for this portion is $\zeta\mu B_{RI}$, where ζ is the probability that a customer receives UCS and B_{RI} is the average benefit received from these sessions per user and μ is the response rate. Since the IMS-Service Provider will also be advertising to the customers the users will receive a benefit for correctly delivered solicited sessions. The benefit for this component is σB_R , where B_R is the benefit received by each customer and σ is the opt-in ratio. To complete the model we will also include a benefit for the customers that correctly receive non UCS, we model this by B_{RL} . The complete model is thus

$$U_R = z_T (-\zeta C_R + \sigma B_R + \zeta\mu B_{RI} + B_{RL}) \quad (2)$$

C. The IMS-VoIP spammer

The spammer initiates UCS hoping to attract users to the stores that the spamming campaign is promoting. It receives a benefit, B_S , for each person that responds to his advertisement; we will use μ to represent the response rate and the benefit per session is $z_T\mu B_S$. We will assume that the spammer is also a user (or abuser) of the IMS-VoIP service hence his cost C_S is only his opportunity cost that he derives from sending SPIT. Since sending SPIT earns a greater income for the same amount of effort than other industries this will be very low, hence the incentive to SPIT. Collecting all the terms, the total payoff to the spammer is

$$U_S = \zeta N_{total} (-C_S + z_T\mu B_S) \quad (3)$$

, where ζN_{total} is the total number of UCSs.

IV. MODEL DISCUSSION

We will now use the model to derive some general results which are peculiar to the market as described above. We will firstly be looking at the conditions under which the spammer benefits from sending UCS to customers. This will then provide a goal to be used in a UCS prevention strategy. Secondly we will then determine whether it is beneficial for the IMS-VSP to protect its client base from receiving UCS. This will be used as a reason for the need for UCS prevention to be considered as part of the service offered to the users. Finally we will be looking at the conditions under which a customer will actually use the service. Using these parameters we can determine the environment needed to correctly and efficiently deploy an IMS-VoIP solution.

A. Marginal utility for sending UCS

We will now calculate the marginal utility earned by the spammer by sending more UCS into the market. This will then reflect the extra utility that the spammer gains in sending one more message. If this quantity is always positive then the spammer's rational behavior will be to send an ever increasing amount of SPIT since he receives greater utility. If on the other hand this quantity is negative then the spammer will be better off flipping burgers at McDonald's. Hence the marginal utility is an important variable that needs to be evaluated critically. The partial derivative of the spammer's utility with respect to the number of UCS is trivial to calculate. It is simply

$$\frac{\delta U_S}{\delta N_{illeg}} = -C_S + z_T \mu B_S = -C_S + z_{RES} B_S \quad (4).$$

For this result to be positive it requires that $z_{RES} B_S > C_S$ and for this to be negative it is required that $C_S > z_{RES} B_S$. We know that as long as the spammers utility increases by sending more UCS, i.e. the marginal utility is positive, the spammer will continue to send UCS. Thus to prevent this from happening we need to increase the costs to send UCS. This result concurs with those produced in the reviewed literature.

It must be stressed here that this cost was defined not as a monetary cost that a user pays to the IMS-VSP but rather as an opportunity cost. Thus one can for instance increase the time it takes to send a message by introducing CAPTCHAs or via computational puzzles. An increase in the amount of time it takes the spammer to send messages lessens the amount of messages that a spammer can send which results in a potential loss for the spammer.

B. Marginal utility for protecting customers

The previous analysis predicted that when costs are not prohibitively large it is rational to expect the spammer to increase the amount of UCS sent into the system. The IMS-VSP has to decide whether it is in its best interests to protect its users from this onslaught of UCS. By analyzing the marginal utility of the IMS-VSP with respect to the number of illegitimate sessions we can determine what the rational behavior of a VSP should be.

The marginal utility with respect to N_{illeg} is calculated to be

$$\frac{\delta U_{VSP}}{\delta N_{illeg}} = -C_{VSP} + \frac{\zeta}{N_{total}} z_{RES} (1 - \sigma) B_{VSP} \quad (5)$$

This result predicts that under certain conditions i.e. the average benefit per UCS per respondent is greater than the cost of delivering the UCS, it is beneficial for the IMS-SP to allow more UCS to enter the system. Although this might increase the utility for the VSP it will negatively impact the customers who do not respond to UCS. Customers would be ill-advised to join the service at these times since they would stand a greater chance of receiving UCS.

It is interesting to note that there are circumstances in which the utility of the service provider increases when there is an increase in UCS. This is not an intuitive result but does bear credence to the theory that some service provider's benefit from SPAM, which is a reason as to why it is so prevalent in today's networks.

C. Marginal utility for using the system

We have analyzed the conditions which need to occur in which a) spammers will send UCS into the system and b) the IMS-VSP will actually benefit from delivering these UCS messages. We will now find the conditions necessary for the customers to gain greater utility for using the service. To derive this result we must calculate the marginal utility of the customers with respect to the number of non UCS initiated. This was calculated to be

$$\frac{\delta U_R}{\delta N_{leg}} = \frac{\zeta}{N_{total}} (z_T C_R - z_{RES} B_{RI}) \quad (6).$$

Hence we can see that as long as the total cost to the network for SPIT is greater than the benefit that is received by the UCS, the customers will benefit from initiating non UCS. This is an intuitive result which lends to the validity of the chosen model. Further calculation indicated that the marginal utility with respect to number of UCS is the negative of the above quantity.

V. APPLICATIONS OF RESULTS

The results gathered from the model can be used to ensure the efficiency of the market. They represent guidelines that if followed ensure the optimal use of all resources within the network. I will now outline how these results can be interpreted and applied in the network setting as described.

A. Increasing message cost

As seen in the model, increasing the costs for imitating sessions within the network will be a sufficient mechanism to prevent unwanted UCS. This though is not as simple as it sounds since this increase in cost will impact the legitimate users' as well. But what does help is that there is a significant difference in spammers call patterns than legitimate users [10]. This reflects their differing behavior or attitude towards communication that these two groups have. Spammers see communication as a means to earn a living but legitimate users view communications as a tool to increase their connectedness. One of the most significant differences, as highlighted in [10],

is that spammers tend to create large numbers of messages within a short amount of time. Assuming this behavior carries over from the email to VoIP domain, it is a fact that should be used. If the costs of creating sessions were strongly correlated to session frequency then we would have created a cost function that punishes the behavior pattern of spammers, whilst not impacting on legitimate users too significantly.

B. Monitoring zeta

It is also necessary from a global perspective to ensure that the benefit received from the responses to UCS does not exceed the costs of receiving UCS and the cost of delivering the UCS. As operators or service providers we do not have direct control over the user's response to stimulus, but it could be prudent for the network providers providing to monitor user complaints. If a mechanism was introduced for a user to identify if it receives UCS the network provider could tax the service provider. This would create an economic incentive for the service provider to monitor its network and the amount of UCS it delivers.

This will be beneficial for network operators in that the service provider acts as a proxy for the reliability of the network provider. If customers become dissatisfied with their experience with the service provider this will result in their confidence in the network provider dropping as well. This could then lead to customers leaving the network and utilizing services offered by other networks. The economic benefits of future NGN's will be dependant on the returns received from the customers. Customer retention must be an important goal of any network operator to ensure its return on investment.

VI. CONCLUSION

The economic benefits of deploying IMS technologies depend greatly on the customer experience. Customer retention is key to ensuring RoI. The main revenue generation streams of a NGN will stem from services offered by service providers. It is important for these services to be protected from abuse. A VoIP service suffers from abuse called SPIT, if such a service is to be deployed the service provider must ensure that it protects itself from this. We have provided an economic analysis of such a market and shown that this can be achieved by:

1. Increasing cost of creating sessions based on call frequency and
2. By creating a feedback mechanism for identifying UCS, service provider's can be taxed for not protecting customers, thus shifting the cost of UCS from the customers to the service providers.

These results can be applied by various mechanisms using technology which already exists. This paper shows that these mechanisms will result in an economically beneficial situation for all parties concerned; that is besides users who create UCS.

REFERENCES

- [1] Th. Magedenz and F. C. de Gouvêa, "IMS – the IP Multimedia System as NGN Service Delivery Platform," *e & i Elektrotechnik und Informationstechnik*, vol. 123, Aug. 2006, pp 271 -276.

- [2] N. Bila, "Dealing with SPAM in Voice over IP," unpublished. Available: <http://www.cs.toronto.edu/~nilton/pubs/spit.pdf>
- [3] T. Loder, M. van Alstyne, and R. Wash, "An Economic Answer to Unsolicited Communications," *ACM Electronic Commerce*, May 2004, pp. 40 -50.
- [4] E. Reshef and E. Solan, "The Effects of Anti-Spam Methods on Spam Mail," *Conference on Email and Anti-Spam 2006*, July 2006.
- [5] I. Androutsopoulos, E. F. Magirou, and D. K. Vassilakis, "A Game Theoretic Model of Spam E-Mailing," *Conference on Email and Anti-Spam 2005*, July 2005.
- [6] O. V. Pavlov, N. Melville, R. Plice, "Unsolicited Commercial Email: An Attention Resource Perspective," in *Proc. 11th Annu. Conf. on Computing in Economics and Finance*, Washington D.C, 2005.
- [7] R. K. Plice, O.V. Pavlov, and N. Melville, "Spam and beyond: An information-economic analysis of unwanted commercial messages," *Journal of Organizational Computing and Electronic Commerce*, submitted for publication.
- [8] D. W. Khong, "An Economic Analysis of Spam Law," *Erasmus Law and Economics Review*, vol. 1, February 2004, pp 23-45.
- [9] J. Goodman and R. Rounthwaite, "Stopping Outgoing Spam," *ACM Electronic Commerce*, May 2004, pp. 30-39.
- [10] H. Husna, S. Phithakitnukoon, S. Palla, R. Dantu, "Behavior Analysis of Spam Botnets" *IEEE 3rd. Int. Conf. on Communication Software and Middleware 2008*, submitted for publication.

Gabriel Andrews graduated with his BSc. in Electrical and Computer Engineering from the University of Cape Town in 2006. He is currently completing his MSc. in Electrical Engineering at the University of Cape Town.