

Using Game Theory to configure P2P SIP*

Sheila Becker
LORIA - INRIA Lorraine
615, rue du jardin botanique
54602 Villers-les-Nancy,
France
University of Luxembourg
6, r. R. Coudenhove-Kalergi
L-1359 Luxembourg
sheila.becker@uni.lu

Radu State
LORIA - INRIA Lorraine
615, rue du jardin botanique
54602 Villers-les-Nancy,
France
University of Luxembourg
6, r. R. Coudenhove-Kalergi
L-1359 Luxembourg
radu.state@uni.lu

Thomas Engel
University of Luxembourg
6, r. R. Coudenhove-Kalergi
L-1359 Luxembourg
thomas.engel@uni.lu

ABSTRACT

In this paper we propose a framework for the analysis of the security in peer-to-peer Session Initiation Protocol based infrastructures. The proposed approach defines a game theoretical model for both an attacker as well as the defender and uses the Nash equilibrium to derive optimal attack and defensive strategies for both entities. We address the specific threats related to SPam over Internet Telephony, flooding and non-cooperative behavior and assess defensive mechanisms based on thresholds and redundant retransmissions. The paper summarizes the main results based on extensive Monte-Carlo simulations of this game.

1. INTRODUCTION

Peer-to-peer Session Initiation Protocol (P2P SIP) is a promising approach for building scalable and reliable VoIP infrastructures using a standardized protocol (SIP) as a main component. The protocol is standardized following [7] and the location and registration service is leveraging distributed hash tables. As far of today few studies have addressed the reliability and resilience of P2P SIP. Based on the two core-components SIP and distributed hash tables, threats coming from both sides have to be addressed. The relevant threats that we consider in this paper are SPam over Internet Telephony and Denial of Service for the SIP plane and respectively non-cooperative/blocking behavior from peer implementing the distributed hash tables.

*Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

IPTCOMM'09, July 7-8, 2009, Atlanta, Georgia, USA.
Copyright 2009 ACM.

In this paper we propose a game theoretical model to analyze and assess the defensive/attack strategies, that are possible in a P2P SIP environment. We derive optimal defense strategies and respectively "optimal" attacking strategies using the Nash equilibrium [10]. According to the Nash equilibrium, we assume that both parts are rational and try to maximize their respective gain. The main challenges that we address are:

1. what are the key metrics that can characterize the performances of such a service?
2. which are the factors (and to what extent) that have an impact on the previous metrics?
3. what is the best configuration that can achieve a run time optimum for the measure?

We will provide answers to these questions in this paper, which is structured as follows: we start in section 2 with an overview on the P2P SIP communication service. In section 3 we develop a risk modeling framework and derive two important measures related to the availability (blocking probability) and the performance (in terms of delay) for the communication service. We describe in the same section the game theoretical models underlying our work and illustrate the results obtained from an extensive simulation suite. We will describe related work in section 4 and conclude our work in section 5.

2. P2P REAL TIME COMMUNICATIONS

P2P communication algorithms assume that peers will cooperate and provide a joint service. This can happen only at signaling level (the best example being P2P SIP) [21] or at both signaling and data level (with Skype being the notable reference). Our work focusses on the signaling level especially on the P2P SIP protocol.

Session Initiation Protocol (SIP) is a signaling protocol for setting up multimedia communication sessions. Primarily, SIP uses proxies to establish sessions between different clients. This architecture can be viewed as a client/server infrastructure. Such an infrastructure is not scalable due to the centralization. The authors of [21] propose to use a peer-to-peer architecture for SIP, because P2P systems are scalable,

robust and fault tolerant due to decentralization and self-organization of the network. A next step is proposed in [22] where a distributed hash table (DHT) is used for storing user contact locations, and as lookup protocol we use Chord [23] as this protocol is used in most proposals for P2P SIP. Following the Chord protocol, the nodes in our network are ordered clockwise in a ring following their hashed IDs.

In spite of the wide usage of P2P algorithms, performance and reliability assessments are missing. In our threat model, we assume that an attacker can run different types of attacks to affect the network. Obviously, there are many different attacks possible in networks and we focus in this paper on three different attacks most relevant for our work.

One attack is commonly referred to as SPam over Internet Telephony (SPIT) [19] - see Figure 1(a). To release a SPIT attack a malicious node has to find out the location of his victims. Therefore, the malicious node sends lookup-requests to a node of the overlay network. After getting the responses, the malicious node can start calling his victims. This threat is similar to spam in the email systems but is delivered by means of voice calls. This leverages the cheap cost of VoIP when compared with legacy phone systems. Such SPIT calls can be telemarketing calls that sell products. SPIT attacks have high impact on the operability of a network and its nodes, as every time a SPIT session is established, nodes have to establish many useless connections or must accept calls that are annoying. As countermeasure against SPIT attacks, a node could use a throttling mechanism in order to accept only a limited number of requests per second, or to integrate a time-to-live so that a lookup has a limited hopcount in the overlay network.

A second attack could be to flood the network while sending many requests to one or more nodes of the network, so that the destination nodes get distracted from working properly, and the network is heavily loaded due to the increasing traffic - see Figure 1(b). In case of such an attack, throttling mechanism could be used again as countermeasure. Within the throttling mechanism every node has a maximum number of requests it can handle per time unit. If the threshold is reached within the specified time unit, a node will drop further incoming requests.

The third attack, that we consider is, that a node can silently drop messages that must be routed. In a pure P2P environment, nodes can significantly affect the service by blocking messages that must be forwarded, see Figure 1(c). In this case, using replication could be a possible defense strategy to increase reliability. The source node will send the request to two or more different nodes to assure receiving a response to the sent request. One request is sent to several entries of the fingertable of the overlay network protocol Chord. This replication mechanism is used for instance by the Slapper worm [3]. We consider the P2P algorithm of the Slapper worm in our work due to its interesting mode of operation. The messages are forwarded and at the same time the identity of the source node gets anonymized. Messages are forwarded to two random nodes until the hop-count has reached zero. If the hop-count reaches zero, the message is sent directly to the destination. We generalize this approach by allowing k successive nodes of the fingertable to

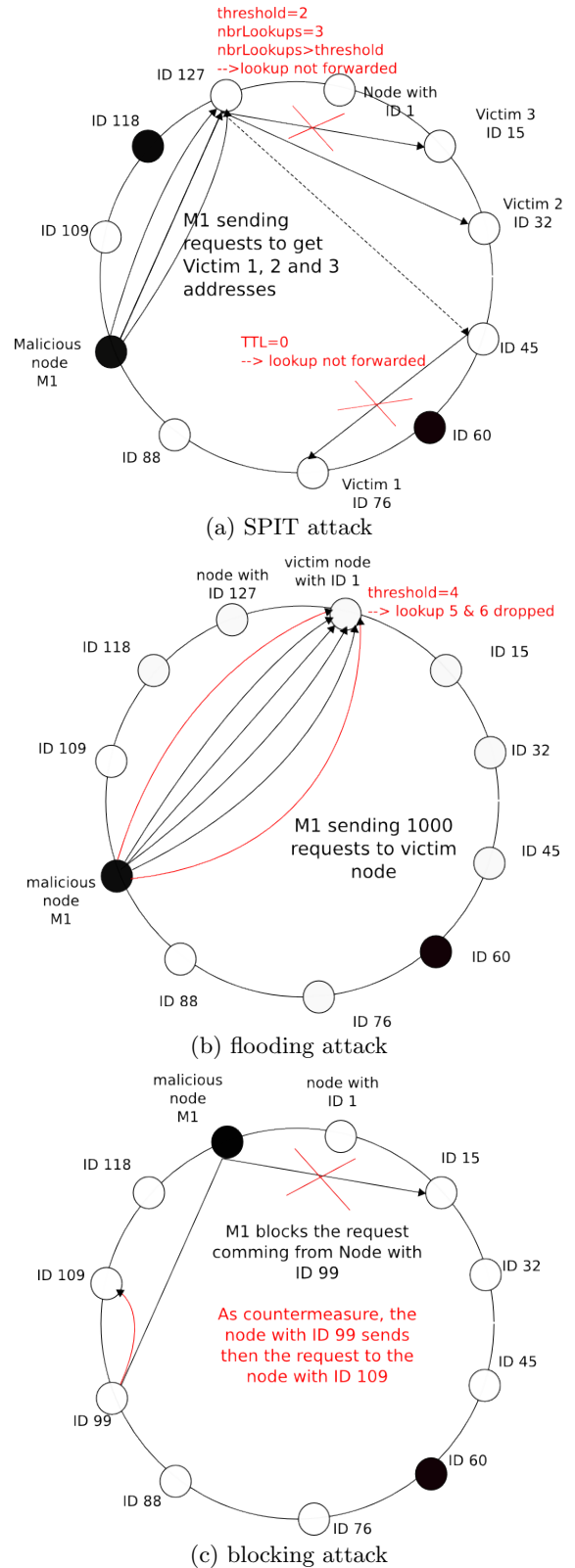


Figure 1: P2P SIP

be used. We call k the replication factor. One contribution of this paper is the choice of the optimal replication factor

and its impact on the defense strategy. To summarize, our main contribution is to provide a framework based on game theory which captures and models the defender and the attacker. This framework can be used to establish optimal strategies for both attacker and defender, assuming rational behavior.

The use of the different defense strategies are illustrated in the following pseudocode.

Algorithm 2.1: DEFENDER STRATEGIES()

```

if lookup
  then if lookupTTL > 0
    then if nbrRequests < threshold
      then
        if lookupHopcount > 0
          then {forwarding lookup to k nodes
                hopcount --
              }
        else forwarding lookup to dest
      nbrRequests ++
      updateNbrRequestsTimeUnit

```

3. OVERALL FRAMEWORK

Risk is considered as a state of uncertainty eventually involving a loss, catastrophe, or undesirable outcome [13]. Whereas uncertainty is defined as the lack of complete certainty, when more than one possibility exists. Uncertainty is measured with a set of probabilities assigned to a set of possibilities. Risk, on the other hand, is measured with a set of probabilities with quantified possibilities and quantified losses. We use the terminology of risk in P2P SIP to quantify threats and in our case the threats are information loss and information delay. There are two sources of uncertainty in P2P SIP communications. The first one is analogous to the blocking probability in telecommunication networks and gives the probability of a call not being established. In telecommunication networks, such a blocking can occur when the available resources are not sufficient to allow more calls. In P2P SIP networks, such a blocking can happen because of a malicious node dropping or tampering the relayed message. This happens when a node is not capable to send the request to the destination target. A second source of uncertainty comes from the time of reception. Long communication delays are unacceptable and thus, the number of hops relaying a message is a risk factor.

We performed Monte Carlo type of simulations to obtain the results presented in this paper. Monte Carlo simulation is defined as generating a large number of scenarios [13]. We varied the strategies, configuration settings, number of attacking hosts and averaged the two metrics : blocking probability and delay. Each simulation consists in an observation of the network for a maximum amount of iterations. We simulated the network with different configuration settings, but for this paper we used as configuration that the network contains 200 nodes, 7 of these 200 nodes we consider to be malicious as 7 is the result of the logarithmic function of 200. The simulation consists of 120 iterations, as the simulation run two minutes and every second another iteration is created. In each simulation 4000 messages are transferred

between the nodes. At each iteration, each node applies the specified strategy. We estimate the blocking probability by randomly selecting pairs of nodes to communicate at each iteration. Finally, an average blocking probability for the whole simulation track is computed. Similarly, we estimate the delay, by monitoring for randomly selected pairs of nodes, the minimal time (in terms of iterations) required to successfully relay testing messages.

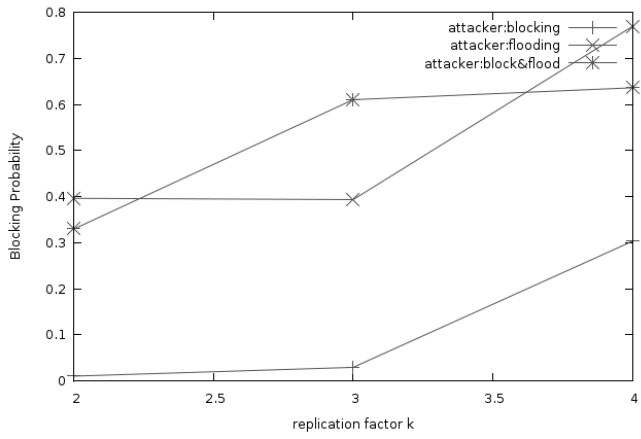
The impact on the blocking probabilities for configuring the replication factor is illustrated in Figure 2(a). The X-axis represents the replication factor k , that can be increased in order to improve the reliability of the communication. The Y-axis represents the respective blocking probabilities. The different lines in the figure specify different attacker strategies. We can see that for all attack strategy increasing the replication factor from 2 to 3, and 4 has as a consequence higher blocking probabilities. This behavior of the blocking probability shows that increasing the replication factor should be used sparingly due to the caused traffic. When the attacker uses flooding as a strategy, the blocking probabilities increase sharp with increasing replication factor. This happens because defender nodes amplify the flooding attacks by forwarding them to many nodes at once.

A similar analysis can be done in terms of the delay and is illustrated in Figure 3(a). When calculating the average hopcount we also take into account the lost requests by adding the longest possible path to the average hopcount. This is done to avoid a falsified impression on the network behavior, as otherwise a small average hopcount value would be considered to be very good without noting that the request never reached the destination. We observe that the average hopcount increases for increasing replication factor which is a consequence for the lost requests.

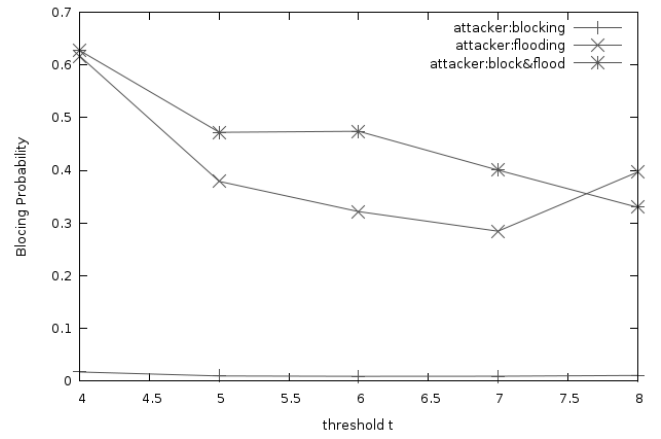
If we consider the impact of the threshold value (see Figure 2(b)), we observe that by increasing the threshold value, the blocking probabilities decreases. We also can see that the blocking strategy of the attacker has no great impact on the blocking probability. A similar analysis in Figure 3(b) illustrates the decreasing average hopcount when increasing the threshold.

We have shown that from the perspective of the defender, several strategies are possible. Each strategy has some advantages when confronted to malicious attackers, but there is no panacea. Some strategy might help against a flooding attack and at the same time be an amplifier for a blocking attack. For instance, using small replication factors will avoid to propagate a flood to the rest of the network. When confronted with attacking nodes that block and do not forward traffic, the same strategy is no good remedy. It is thus natural to inquire about the best strategy that can be used in such a context, assuming a determinate and rational adversary. Such an optimal strategy can be used to perform risk mitigation in order to guarantee reliability of the communication infrastructure. We will leverage concepts from game theory in order to derive the best strategies for both the attacker and the defender. These strategies are obtained by determining the Nash equilibrium of the game.

The Nash Equilibrium [10] is a strategy profile specifying

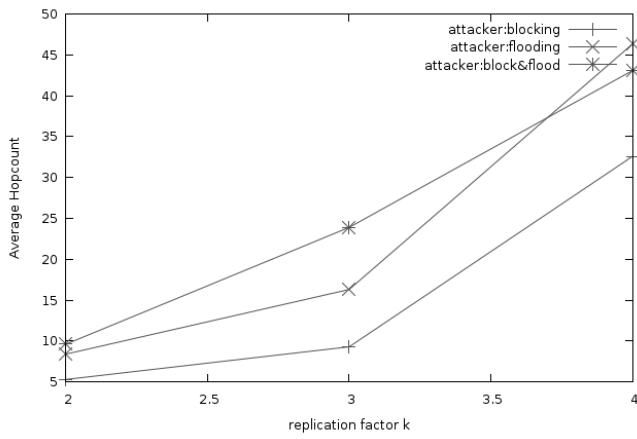


(a) replication factor

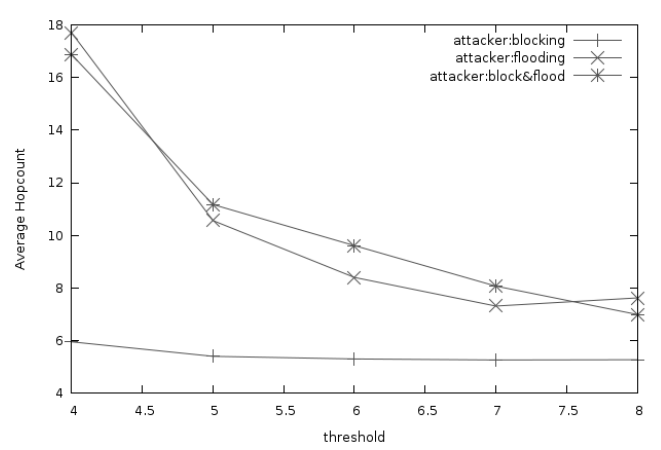


(b) threshold

Figure 2: Risk Analysis - blocking probability



(a) replication factor



(b) threshold

Figure 3: Risk Analysis - average hopcount

optimal strategic choices for all players by reason that none of the players has any motivation to diverge from the Nash equilibrium because one player can not gain greater payoffs by choosing another strategy when all the other players choose the strategies given by the profile. To calculate the Nash equilibrium we need N as a set of players, A_i as a finite strategy set, and R_i as a payoff function.

- N : set of n players
- A_i : finite strategy set ($a_i \in A_i$)
- R_i : payoff function $A \rightarrow \mathbb{R}$, where $A = A_1 \times \dots \times A_n$

A Nash equilibrium can either have a pure strategy, which provides a complete definition of how a player will play a game, or a mixed strategy, that is a randomization over a set of pure strategies. A mixed strategy set for player i is the set of probability distributions over the action set A_i described by the simplex operator Δ .

$$\Delta(A_i) = \{ q_i : A_i \rightarrow [0, 1] \mid \sum_{i=0} q_i(a_i) = 1 \}$$

for mixed strategies: (i : player 1; $-i$: player 2)

$$Q = \prod_i \Delta(A_i) \quad \text{and} \quad q = (q_i, q_{-i}) \in Q$$

Expected payoffs for player i from strategy profile q in mixed strategies are:

$$\mathbb{E}_{a \sim q}[R_i(a)] = \sum_{a \in A} q(a) R_i(a)$$

where $q(a) = \prod_{j=1}^N q_j(a_j)$

The essential meaning of a mixed strategy is that randomized actions can achieve a better average payoff, and the equilibrium in mixed strategies is associated with the probability distribution over the set of actions, where this equilibrium can be achieved. In a mixed strategy, actions are performed randomly according to the probability distribution function.

In our context, a game can be formulated in terms of blocking probability and delay as payoff values. We will assume that both the attacker and the defender are rational, in that both will perform in order to maximize their payoff. The attacker and the defender have opposite goals: the defender tries to maintain his P2P infrastructure, while the attacker is motivated by inducing high blocking probabilities and large per message hop counts on the target network. The interaction between an attacker and a defender can be modeled as strategic games.

3.1 Dealing with obstructive non-cooperative peers

We derive an equilibrium condition for the different attack and defensive strategies based on the blocking probability, meaning the probability of requests not reaching the destination, as payoff function. For the attacker we use the

blocking probability as payoff function and for the defender we use 1-blocking probability, the probability that a communication is established, as payoff function. For convenience we have scaled the payoff function based on the blocking probability to the interval $[0, 100]$. The attacker strategies are blocking, flooding, and blocking and flooding. On the defensive site, the possible actions are to adjust the replication factor - the number of nodes (k), to which a message is forwarded (where the possible choices are 2, 3, and 4 and to adapt the throttle value).

- set of players N : {attacker, defender}
- set of strategies A_i :
 - $A_{attacker}$: {block, flood, block & flood}
 - $A_{defender}$: { $k:2 \setminus t:4$, $k:2 \setminus t:6$, $k:2 \setminus t:8$,
 $k:3 \setminus t:4$, $k:3 \setminus t:6$, $k:3 \setminus t:8$,
 $k:4 \setminus t:4$, $k:4 \setminus t:6$, $k:4 \setminus t:8$ }

The instance of " $k:2 \setminus t:4$ " means that the defender strategy has a k of 2 and a threshold of 4.

- payoff function R_i is illustrated in table 1

In order to calculate the Nash equilibrium we used the free software Gambit¹ that allows us to evaluate the strategies. The Nash Equilibrium and the resulting strategy profiles are:

- $q_{defender}(k : 2 \setminus t : 4) = 0$
- $q_{defender}(k : 2 \setminus t : 6) = \frac{133}{438}$
- $q_{defender}(k : 2 \setminus t : 8) = \frac{305}{438}$
- $q_{defender}(k : 3 \setminus t : 4) = 0$
- $q_{defender}(k : 3 \setminus t : 6) = 0$
- $q_{defender}(k : 3 \setminus t : 8) = 0$
- $q_{defender}(k : 4 \setminus t : 4) = 0$
- $q_{defender}(k : 4 \setminus t : 6) = 0$
- $q_{defender}(k : 4 \setminus t : 8) = 0$
- $q_{attacker}(block) = 0$
- $q_{attacker}(flood) = \frac{721}{1095}$
- $q_{attacker}(block \& flood) = \frac{374}{1095}$

The game admits a mixed solution, where:

- the defender should randomly apply two strategies: the first one consists in using ($k=2$, $t=6$) and ($k=2$, $t=8$) with the probabilities $133/438$ and $305/438$ respectively.

¹gambit.sourceforge.net

Defender strategy	Attacker strategy	$R_{defender}$ (%)	$R_{attacker}$ (%)
k:2\t:4	block	98,30	1,70
k:2\t:4	flood	38,37	61,63
k:2\t:4	block & flood	37,30	62,70
k:2\t:6	block	99,12	0,88
k:2\t:6	flood	67,85	32,15
k:2\t:6	block & flood	52,60	47,40
k:2\t:8	block	98,95	1,05
k:2\t:8	flood	60,37	39,63
k:2\t:8	block & flood	67,02	32,98
k:3\t:4	block	81,82	18,18
k:3\t:4	flood	20,15	79,85
k:3\t:4	block & flood	33,40	66,60
k:3\t:6	block	91,45	8,55
k:3\t:6	flood	66,77	33,23
k:3\t:6	block & flood	37,52	62,48
k:3\t:8	block	97,05	2,95
k:3\t:8	flood	60,65	39,35
k:3\t:8	block & flood	38,97	61,03
k:4\t:4	block	55,07	44,93
k:4\t:4	flood	34,47	65,53
k:4\t:4	block & flood	40,35	59,65
k:4\t:6	block	64,90	35,10
k:4\t:6	flood	38,62	61,38
k:4\t:6	block & flood	36,62	63,38
k:4\t:8	block	69,70	30,30
k:4\t:8	flood	23,10	76,90
k:4\t:8	block & flood	36,40	63,60

Table 1: Payoffs using blocking probability - defender strategies are both k and the threshold

Defender strategy	Attacker strategy	$R_{defender}$	$R_{attacker}$
k:2\t:4	block	-0,95	5,95
k:2\t:4	flood	-12,70	17,70
k:2\t:4	block & flood	-11,87	16,87
k:2\t:6	block	0,07	4,93
k:2\t:6	flood	-3,40	8,40
k:2\t:6	block & flood	-4,61	9,61
k:2\t:8	block	0,08	4,92
k:2\t:8	flood	-2,62	7,62
k:2\t:8	block & flood	-1,99	6,99
k:3\t:4	block	-15,12	20,12
k:3\t:4	flood	-45,86	50,86
k:3\t:4	block & flood	-35,20	40,20
k:3\t:6	block	-4,29	9,29
k:3\t:6	flood	-11,30	16,30
k:3\t:6	block & flood	-18,90	23,90
k:3\t:8	block	-1,01	6,01
k:3\t:8	flood	-8,77	13,77
k:3\t:8	block & flood	-12,12	17,12
k:4\t:4	block	-57,03	62,03
k:4\t:4	flood	-69,73	74,73
k:4\t:4	block & flood	-55,93	60,93
k:4\t:6	block	-27,57	32,57
k:4\t:6	flood	-41,32	46,32
k:4\t:6	block & flood	-38,07	43,07
k:4\t:8	block	-17,68	22,68
k:4\t:8	flood	-37,04	42,04
k:4\t:8	block & flood	-28,18	33,18

Table 2: Payoffs using delay - defender strategies both k and the threshold

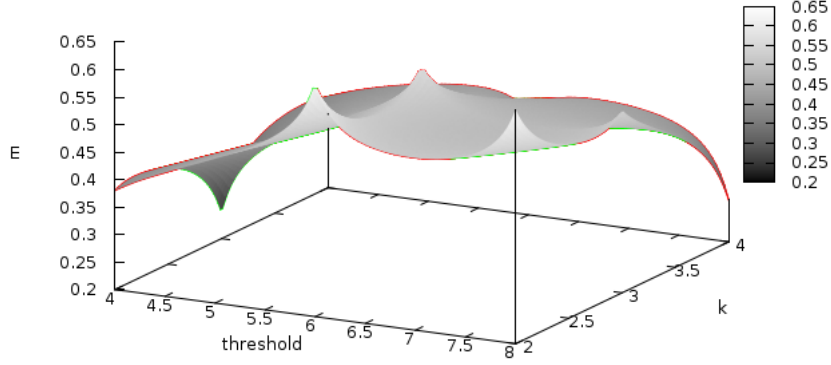


Figure 4: defender - payoff distribution

- the attacker should randomly apply two strategies (flood, block and flood) with the probabilities 721/1095 and 374/1095 respectively.

The defender strategies regarding the resulting Nash Equilibrium calculated with respect to the blocking probability are illustrated in the following pseudocode.

Algorithm 3.1: DEFENDER STRATEGIES()

```

i ← random(1)
if i ≤ 133/438
  then threshold ← 6
  else threshold ← 8
if lookup
  then if lookupTTL > 0
  then if nbrRequests < threshold
  then
    {
      if lookupHopcount > 0
      then {forwarding lookup to 2 nodes
            hopcount --
            }
      else forwarding lookup to dest
    }
    nbrRequests ++
    updateNbrRequestsTimeUnit

```

The attacker strategies regarding the resulting Nash Equilibrium calculated with respect to the blocking probability are illustrated in the following pseudocode.

Algorithm 3.2: ATTACKER STRATEGIES()

```

i ← random(1)
if i ≤ 374/1095
  then strategy ← block&flood
  else strategy ← flood

```

The expected payoffs are:

- defender:

$$\begin{aligned}
& - \mathbb{E}_{a \sim q}[R_{defender}(k : 2 \setminus t : 4)] \\
& = q_{attacker}(block)R_{defender}(k : 2 \setminus t : 4, block) \\
& + q_{attacker}(flood)R_{defender}(k : 2 \setminus t : 4, flood) \\
& + q_{attacker}(bl\&fl)R_{defender}(k : 2 \setminus t : 4, bl\&fl) \\
& = 98,3\% * 0 + 38,37\% * \frac{721}{1095} + 37,30\% * \frac{374}{1095} \\
& = 38,00\%
\end{aligned}$$

$$\begin{aligned}
& - \mathbb{E}_{a \sim q}[R_{defender}(k : 2 \setminus t : 6)] = 62,64\% \\
& - \mathbb{E}_{a \sim q}[R_{defender}(k : 2 \setminus t : 8)] = 62,64\% \\
& - \mathbb{E}_{a \sim q}[R_{defender}(k : 3 \setminus t : 4)] = 24,68\% \\
& - \mathbb{E}_{a \sim q}[R_{defender}(k : 3 \setminus t : 6)] = 56,78\% \\
& - \mathbb{E}_{a \sim q}[R_{defender}(k : 3 \setminus t : 8)] = 53,25\% \\
& - \mathbb{E}_{a \sim q}[R_{defender}(k : 4 \setminus t : 4)] = 36,48\% \\
& - \mathbb{E}_{a \sim q}[R_{defender}(k : 4 \setminus t : 6)] = 37,94\% \\
& - \mathbb{E}_{a \sim q}[R_{defender}(k : 4 \setminus t : 8)] = 27,64\%
\end{aligned}$$

- attacker:

$$\begin{aligned}
& - \mathbb{E}_{a \sim q}[R_{attacker}(block)] = 0,99\% \\
& - \mathbb{E}_{a \sim q}[R_{attacker}(flood)] = 37,36\% \\
& - \mathbb{E}_{a \sim q}[R_{attacker}(bl\&f)] = 37,36\%
\end{aligned}$$

Due to these results we can conclude that it would be meaningless to take another strategy except those satisfying the Nash equilibrium, because the payoff would be less than for the proposed strategies. The strategies with the greatest payoff are: defender playing 'k:2 with threshold 6' and 'k:2 with threshold 8', attacker playing 'flood' and 'block&flood'. That are also the proposed strategies by the Nash equilibrium.

3.2 Accounting for Delay

If we consider the delay as critical factor, then a similar analysis can establish optimal strategies for the players. For the attacker we use the average delay of the messages as payoff function and for the defender we use the maximum

hopcount-average delay as a payoff function. The objective of an attacker is to delay as much as possible the reception of messages, while the defender will try of minimize the same measure.

We have also modeled this game, where on the defensive site, multiple actions are allowed: the defender can adjust both k and the threshold. The attack strategies are the same as before.

- set of players $N : \{\text{attacker, defender}\}$
- set of strategies A_i :
 - $A_{\text{attacker}} : \{\text{block, flood, block \& flood}\}$
 - $A_{\text{defender}} : \{k:2\backslash t:4, k:2\backslash t:6, k:2\backslash t:8, k:3\backslash t:4, k:3\backslash t:6, k:3\backslash t:8, k:4\backslash t:4, k:4\backslash t:6, k:4\backslash t:8\}$
- payoff function R_i illustrated in table 2

The Nash Equilibrium admits a pure solution, where:

- the defender should use for k the value 2 and for the threshold the value 8
- the attacker should flood the network

The defender strategies regarding the resulting Nash Equilibrium calculated with respect to the delay are illustrated in the following pseudocode.

Algorithm 3.3: DEFENDER STRATEGIES()

```

threshold ← 8
if lookup
  then if lookupTTL > 0
    then if nbrRequests < threshold
      then
        if lookupHopcount > 0
          then { forwardinglookupto2nodes
                hopcount – –
              }
          else forwardinglookuptodest
        nbrRequests ++
        updateNbrRequestsTimeUnit

```

The attacker strategy regarding the resulting Nash Equilibrium calculated with respect to the blocking probability is illustrated in the following pseudocode.

Algorithm 3.4: ATTACKER STRATEGIES()

```

strategy ← flood

```

The payoff distribution for the defender and its strategies is shown in Figure 4. This figure shows 2 peaks, one for replication factor 2 and threshold value 6 and another for replication factor 2 and threshold value of 8.

4. RELATED WORK

Assessing security risks can be approached using different methodologies. One way for assessing risk is to use attack graphs. In [24], authors use attack graphs to model the threats, counter measures and relationships among vulnerabilities, threats and configuration settings of a system, which is important to monitor security level and risks and to identify high impact vulnerabilities. They propose a cost effective automated solution for hardening the network. In [26], a framework is presented to measure various aspects of network security using attack graphs in order to take into account the interaction between different network components and different vulnerabilities. An attack resistance metric, to indicate the level of security of a system, is given in [25]. Complementary, an extended attack tree is proposed in [5] to be the support in a game theory model. This approach for assessing risk of a system considers to have a complete view on the exact chaining of possible attack actions, that is very complex and on must have deep knowledge of the systems infrastructure. Furthermore, one must be a domain expert to evaluate the outcome. This is opposite to our approach for risk assessment, we do not suppose an expert to assess the outcome of a scenario and we do not integrate a complete attack graph. Our approach is to use game theory by constructing payoffs from multiple simulations and associated monitored performance.

From a monitoring point of view, this topic has been addressed by the network management community [1,2], where precise metrics and indicators for the overall security of a network were defined in order to predict future vulnerabilities and to build an analytical model from a sample of observations. In [11,18] a Monte Carlo simulation is used to identify risk. This Probabilistic Risk Analysis approach comes close to our work. [12] integrates Game Theory to Probabilistic Risk Analysis by integrating behavioral dimension. The idea is to merge behavioral theory of conflict with physical world to produce more accurate estimates of system reliability. The different terms like survivability, reliability, dependability and availability are assessed in [15]. For a good introduction to game theory, the authors of [10] provide a good background reading.

Using peer-to-peer architecture for SIP is first presented in [21], where a pure P2P architecture for the Session Initiation Protocol (SIP) based IP telephony systems is proposed as P2P systems have a better scalability, robustness and fault tolerance compared to client/server infrastructures. Furthermore in [22] an OpenDHT architecture is used for storing user locations. The authors assume in [22] that DHT nodes are not malicious and correctly perform DHT operations. Moreover, the author of [20] gives a good overview of the security issues in P2P SIP, while considering more general security aspects of P2P [6]. SPIT in general is addressed in [19], it proposes a prevention framework based on media and signaling content interception. Our approach is not considering the content in order to prevent SPIT. A holistic intrusion detection and prevention system for VoIP is presented in [14] where a combined honeypot and monitoring schedule is proposed. The concept of VoIP honeypot for P2P SIP is a promising idea, which will be addressed in future work. VoIP flooding attacks are addressed in [16]. A generic security architecture to monitor, detect, analyze and

counter measure for a SIP based VoIP infrastructure is proposed in [9] with the goal to detect attacks against the SIP infrastructure. In [9] a framework is elaborated to prevent respectively mitigate attacks. [17] proposes another method for detecting attacks in SIP, which consists in a self-learning system to detect new and unknown attacks by identifying anomalous content in SIP messages. Another approach for assessing security aspects in P2P SIP is presented in [8] by proposing a hybrid solution called Cooperative SIP where SIP server and a DHT cooperate together instead of using a pure P2P SIP solution. So far, no risk assessment has been performed for P2P SIP using a DHT as lookup-service.

In our previous work [4] generic risk assessment with simple game theory models have been investigated. We did not consider in that work the specific of VoIP communications and did cover simple games with fewer parameters.

5. CONCLUSION AND FUTURE WORK

In this work we proposed a modeling framework for P2P SIP, allowing to capture obstructive behavior of peers, as well as VoIP specific attacks SPIT or DoS attacks. On a defensive side we modeled defensive operations based on throttling mechanisms as well as redundant retransmissions piggybacked on standard DHT. Our model is based on game theory and we assume rational behavior from both sides. The model is capable to derive optimal strategies using the Nash Equilibrium.

To our knowledge this is the first approach for modeling P2P SIP with game theory while accounting for VoIP specific threats. We performed our analysis on a simulated testbed. Our future work will consist in implementing these strategies in a real VoIP testbed. We also plan to bootstrap our simulation with realistic settings and traffic profiles - obtained from the testbed. At conceptual level we will extend our model towards evolutionary game theory and model thus more complex strategies where both attacker and defender can learn from passed experiences.

Acknowledgement

We acknowledge the partial support from the EU-project EFIPSANS (F1R-CSC-PEU-0801EF).

6. REFERENCES

- [1] Mohammad Salim Ahmed, Ehab Al-Shaer, and Latifur Khan. A novel approach quantitative approach for measuring network security. In *Proceedings of IEEE Infocomm 2008*. IEEE, 2008.
- [2] Mohammad Salim Ahmed, Ehab Al-Shaer, Mohamed Taibah, Muhammad Abedin, and Latifur Khan. Towards autonomic risk-aware security configuration. In *Proceedings of IEEE Network Operation and Management Symposium NOMS 2008*. IEEE, 2008.
- [3] Ivan Arce and Elias Levy. An analysis of the slapper worm. In *proceedings of IEEE Security & Privacy*, 2003.
- [4] S. Becker, R. State, and T. Engel. Defensive configuration with game theory. Accepted to IEEE/IFIP IM 2009, May 2008.
- [5] Stefano Bistarelli, Marco Dalli Aglio, and Pamela Paretto. "Strategic games on defense trees". In *Proceedings of FAST 2007*, pages 1–15. LNCS, 2007.
- [6] John R. Douceur and Judith S. Donath. The sybil attack. pages 251–260, 2002.
- [7] J. Rosenberg et al. Rfc3261, sip: Session initiation protocol. 2002.
- [8] Ali Fessi, Heiko Niedermayer, Holger Kinkelin, and Georg Carle. A cooperative sip infrastructure for highly reliable telecommunication services. In *IPTComm '07: Proceedings of the 1st international conference on Principles, systems and applications of IP telecommunications*, pages 29–38, New York, NY, USA, 2007. ACM.
- [9] Jens Fiedler, Tomas Kupka, Sven Ehlert, Thomas Magedanz, and Dorgham Sisalem. Voip defender: highly scalable sip-based security architecture. In *IPTComm '07: Proceedings of the 1st international conference on Principles, systems and applications of IP telecommunications*, pages 11–17, New York, NY, USA, 2007. ACM.
- [10] Amy Greenwald. Matrix games and nash equilibrium. 2007.
- [11] Kjetil Haslum and Andr Arnes. "Multisensor real-time risk assessment using continuous-time hidden markov models. In *Proceedings of LNAI 2007*, pages 694–703. LNCS, 2007.
- [12] Kjell Hausken. *Risk Analysis*, chapter Probabilistic Risk Analysis and Game Theory. Blackwell Publishing, 2002.
- [13] Douglas W. Hubbard. *How to Measure Anything: Finding the Value of 'Intangibles' in Business*. Wiley, 2007.
- [14] Mohamed Nassar, Saverio Niccolini, Radu State, and Thilo Ewald. Holistic voip intrusion detection and prevention system. In *IPTComm '07: Proceedings of the 1st international conference on Principles, systems and applications of IP telecommunications*, pages 1–9, New York, NY, USA, 2007. ACM.
- [15] Yi Qian, James Joshi, David Tipper, and Prashant Krishnamurthy. *Information Assurance*. Morgan Kaufmann, 2007.
- [16] Yacine Rebahi, Muhammad Sher, and Thomas Magedanz. Detecting flooding attacks against ip multimedia subsystem (ims) networks. In *IEEE/ACS International Conference on Computer Systems and Applications*, pages 848–851, 2008.
- [17] Konrad Rieck, Stefan Wahl, Pavel Laskov, Peter Domschitz, and Klaus-Robert Müller. A self-learning system for detection of anomalous sip messages. pages 90–106, 2008.
- [18] Mehmet Sahinoglu. Security meter: A practical decision-tree model to quantify risk. *IEEE Security & Privacy*, 2005.
- [19] R. Schlegel, S. Niccolini, S. Tartarelli, and M. Brunner. SPam over Internet Telephony (SPIT) Prevention Framework. In *IEEE Global Telecommunications Conference*, pages 1–6, 2006.
- [20] Jan Seedorf. Security Challenges for Peer-to-Peer SIP. In *IEEE Network*, pages 38–45, 2006.
- [21] Kundan Singh and Henning Schulzrinne. Peer to peer telephony using SIP. In *Proceedings of the International Workshop on Network and Operating System Support for Digital Video and Audio 2005*, pages 63–68. ACM, 2005.
- [22] Kundan Singh and Henning Schulzrinne. Using an external dht as a sip location service. 2006.
- [23] I. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, M. F. Kaashoek, F. Dabek, and H. Balakrishnan. Chord: a scalable peer-to-peer lookup protocol for Internet applications. In *IEEE/ACM Transactions on Networking*, pages 17–32, 2003.
- [24] Lingyu Wang, Steven Noel, and Sushil Jajodia. Minimum-cost network hardening using attack graphs. *Comput. Commun.*, 29(18):3812–3824, 2006.
- [25] Lingyu Wang, Anoop Singhal, and Sushil Jajodia. Measuring the overall security of network configurations using attack graphs. *Data and Applications Security XXI*, pages 98–112, 2007.
- [26] Lingyu Wang, Anoop Singhal, and Sushil Jajodia. Toward measuring network security using attack graphs. In *QoP '07: Proceedings of the 2007 ACM workshop on Quality of protection*, pages 49–54, New York, NY, USA, 2007. ACM.