Parameterisation of a reputation system for VoIP in P2P networks for improved communication quality and security

Markus Fiedler, Charlott Eliasson, Tomasz Ciszkowski, Wojciech Mazurczyk and Zbigniew Kotulski

***Index Terms*—Reputation, Covert Channel, VoIP, Utility Function, Quality of Service, Quality of Experience.**

I. Introduction

In this paper, we propose how to parameter and maintain a reputation system that, based on the current network conditions, supports the selection of the optimal communication end-to-end path for VoIP communication in P2P network. Each node's reputation is formed based on three factors: (1) *performance reputation* (own experience from passive measures of the network conditions); (2) *security reputation*; and (3) *information reputation* consisting of recommendations from other nodes. Reputation data is periodically updated from continuous lightweight monitoring of path quality and security and also from information exchange between the nodes. When network conditions deteriorate, the reputation system enables switching, if possible, to another available path for further communication.

The proposed reputation system is a component of the SecMon system [1], which is intended especially for VoIP service over P2P networks. SecMon features lightweight QoS parameter monitoring, authentication and data integrity services. The exchange of monitoring information represents a low-bandwidth consumption solution that is transparent to the users and possesses a self-organizing capability. The above-mentioned exchange features are accomplished by utilizing two information hiding techniques: digital audio watermarking and network steganography. These techniques are used to create *covert channels* that serve as transport channels for lightweight QoS measurement's results.

Moreover, in this paper, we present results of the simulations that were performed to investigate how the proposed reputation system is performing for simple two-path case scenario. Additionally, we show how different network condition negative effects like delays and packet losses affect the proposed reputation system and how they are modeled with utility functions. Results of the simulations also illustrate the approaches to thresholds that trigger path changes.

II. Reputation and Utility Functions

The reputation associated to a path determines its usefulness in terms of quality and security. If at least two parts were available, the path with the higher reputation is chosen. Reputation is calculated as outlined in [SecMon], the full formula and the corresponding discussion will be found in the full version of this paper.

Basically, the reputation is split into several parts:

1. *Performance reputation*, which can be derived from lightweight comparative end-to-end measurements of averages and standard deviations of user-perceived throughput over *averaging intervals* of duration ΔT and *observation windows* of duration $\Delta W = \mathrm{n}\,\Delta T$ as described in [AutoMon2]. The SecMon infrastructure allows for the transmission of sender reports at the end of *exchange intervals* $\Delta E \le \Delta W$, containing (quantized) throughput averages m and standard deviations s over the most recent ΔW, using covert channels. Changes of throughput averages between sender and receiver reflect loss and are captured by the *m-utility function* U_m. Changes of the coefficient of deviation $c = s/m$ reflect jitter and loss and are captured by the *c-utility function* U_c. Denote for instance the coefficient of variation at the inlet (outlet) of the path as c_{in} (c_{out}). A simple linear approximation of the *s*-utility function can be expressed as
$$U_c = \max\{1 - k_c(c_{\text{out}} - c_{\text{in}}), 0\},\ k_c > 0 \qquad (1)$$
2. *Security reputation*, which can analogously be expressed by a binary security utility function that indicates whether the hash of the received data matches the one of the sent data, which is conveyed via another covert channel:
$$U_{\text{sec}} = \begin{cases} 1, & \text{hash correct} \\ 0, & \text{else} \end{cases} \qquad (2)$$
3. *Information reputation*, capturing the reliability of monitoring data, expressed as follows:
$$U_{\text{info}} = \begin{cases} 1, & \text{monitoring data received} \\ 0, & \text{else} \end{cases} \qquad (3)$$

Blekinge Institute of Technology, Dept. of Telecommunication Systems, Sweden {markus.fiedler | charlott.eliasson}@bth.se

Warsaw University of Technology, Institute of Telecommunications, Poland, {T.Ciszkowski | wmazurczyk | zkotulsk}@ tele.pw.edu.pl

III. Bottleneck Simulator

Within the SecMon project, the bottleneck simulator is aimed to provide an experimental tool for quantifying the effect of quality and security problems (implying delays and losses), which will help to parameterise the SecMon system.

This underlying model for the simulator is based on the description of queueing through an *equivalent bottleneck* as introduced in [3]. Both inlet traffic entering and outlet traffic leaving the bottleneck are described by data rates in form of packets per averaging interval (ppΔT), forming the time series $\left\{R_q^{\text{in}}\right\}_{q=1}^{n}$ and $\left\{R_q^{\text{out}}\right\}_{q=1}^{n}$, respectively. If both time series match, the bottleneck is said to be transparent. Deviations of R_q^{out} from R_q^{in} reflect typical queuing problems. Assume that some traffic D_q is delayed beyond the end of interval q and arrives during the next interval q+1. Assume furthermore that some traffic L_s is lost during interval q. The we can express the data rate at the outlet of the equivalent bottleneck as a function of the data rate at the inlet, the delay process $\{D_q\}$ and the loss process $\{L_q\}$ as follows:

$$R_q^{\text{out}} = R_q^{\text{in}} - \frac{D_q + L_q}{\Delta T} + \frac{D_{q-1}}{\Delta T} \qquad (4)$$

The loss process is composed from a constant term A_q, reflecting *systematic* losses e.g. due to overload or attacks, and a random term, drawn from a discrete uniform distribution:

$$L_q = A_q + \text{DU}(0, B) \qquad (5)$$

Observe that A_q can be adjusted per interval q in order to provoque transients, e.g. a suddenly starting DoS attack. The delay process is also generated from a discrete uniform distribution:

$$D_q = \text{DU}(0, C) \qquad (6)$$

IV. Examples for Performance Reputation

The examples shown in this section limit themselves to performance reputation, captured by the change of performance parameters due to bottleneck behaviour. We assume

- an averaging interval of ΔT = 200 ms;
- an observation window of $\Delta W = 10\ \Delta T$ = 2 s;
- an exchange interval of $\Delta E = 5\ \Delta T$ = 1 s;
- VoIP traffic with 50 pps = 10 ppΔT at the inlet.

If we apply a quantization of 0.1 ppΔT combined with region-of-interest-based coding, the lightweight monitoring traffic amounts to not more than 10 bps, which is well-adapted to the capabilities of the covert channel.

As quality criterion, we propose (1) with k_c = 5. This implies a halving of the utility U_c = 0.5 for c_{out} = 10 %. The latter boundary applies for Quality of Experience of both streaming and elastic traffic. Reference [4] reports – for Skype via UMTS – that a growth of the coefficient of variation of the throughput by 10 % implies a decrease in PESQ from about 2.5 to 2.0 (10 %). And [5] hints that satisfactory TCP behaviour implies a coefficient of variation of not more than 10 %.

Tab. 1. Time-dependent behaviour of the utility function per observation interval in face of a sudden permanent loss, described by parameter *A*.

A [ppΔT]	1	2	3	4
$U_c(\tau + 1\text{ s})$	0.72	0.41	0.07	0.00
$U_c(\text{t} + 2\text{ s})$	1.00	1.00	1.00	1.00

Tab. 1 illustrates how a sudden increase of loss by *A* ppΔT that starts at 0 s is seen from the *c*-utility function. After the transition has happened, the coefficient of variation relaxes. In the following, the unit ppΔT will be ommitted.

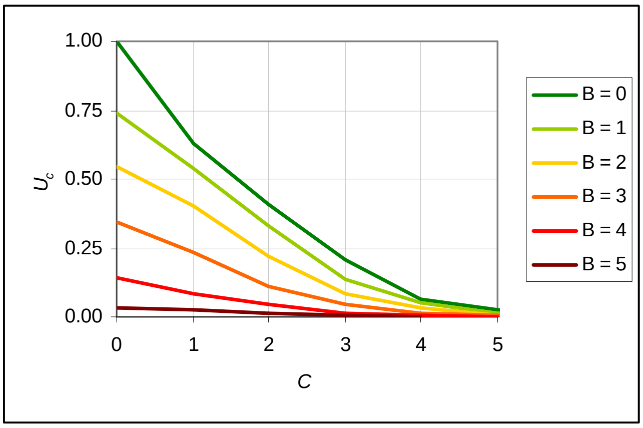

Fig. 1. *C*-utility function as a function of delay parameter *C* for different loss parameters *B* (standard deviation of the shown values between 0.02 and 0).

Fig. 1 shows how the *c*-utility function is affected by the parameters (*B*, *C*). Obviously, only the combinations (0, 1), (1, 0), (1, 1), (2, 0) yield a utility of at least 50 %.

V. Conclusions and Outlook

We have presented key parameters for a reputation system targeting quality and security of VoIP in a P2P context. Results obtained with aid of a bottleneck simulator show that the *c*-utility function is capable of the impact of loss and delay. There is obviously not much room for disturbances in order to keep the Quality of Experience on an acceptable level.

Further results, amongst others demonstrating the reputation-based link choice, will be shown in the full version of the paper.

References

[1] T. Ciszkowski, C. Eliasson, M. Fiedler, Z. Kotulski, R. Lupu, and W. Mazurczyk: *SecMon: End-to-End Quality and Security Monitoring System.* Submitted for journal publication.

[2] M. Fiedler, K. Tutschku, S. Chevul, L. Isaksson, and A. Binzenhöfer. The Throughput Utility Function: Assessing network impact on mobile services. *Proc. of 2nd EuroNGI IA.8.2 Workshop*, Lake Como, Italy, July 2005, edited by Springer Verlag (LNCS series).

[3] M. Fiedler, K. Tutschku, P. Carlsson, and A.A. Nilsson. Identification of performance degradation in IP networks using throughput statistics. *Proc. of 18th International Teletraffic Congress* (*ITC-18*), Berlin, Germany, Sept. 2003, pp 399–407.

[4] T. Hoßfeld, A. Binzenhöfer, M. Fiedler, and K. Tutschku. Measurement and Analysis of Skype VoIP Traffic in 3G UMTS Systems. *Proc. of IPS-MoMe 2006*, Salzburg, Austria, Feb. 2006, pp. 52–61.

[5] S. Landström and L.-Å. Larzon. Revisiting Wireless Link Layers and In-order Delivery. *SNCNW'08*, Karlskrona, Sweden, April 2008.