Principles of Soft Verification

Natasa Zivic, Department Electrical Engineering and Computer Science, Institute for Digital Communications Systems, University of Siegen, Siegen, Germany

ABSTRACT

This paper considers messages protected with the Message Authentication Code (MAC) for the sake of authenticity. The standard forward error correcting channel code is assumed, which reduces the error rate, but no repeat mechanism exists to correct the remaining errors. The uncorrected errors cause the rejection of messages with a wrong MAC, as a successful MAC verification ("hard" verification) demands errorless message and errorless MAC. This paper introduces the extension of "hard" verification of MACs, whose result is "true" or "false", to "soft" verification, that outputs additionally a trust level as verification result. This allows the acceptance of corrected messages and their MACs, even if a few bits of the MAC are different from the expected value. The costs are a loss of trust, as trust is defined for the successful standard or "hard" verification, i.e. for errorless message and its MAC. Therefore "Trust Output" is accompanied with the output of the verification process. A definition of "Trust Level" will be given, together with an algorithm of "soft" verification, which provides such Trust Output. This algorithm is based on a Soft Output channel decoder, which provides a reliability value for each bit, which is used as soft input for the proposed algorithm, "Soft Input Trust Output". Simulation results show an essential improvement of the acceptance rate of MACs - at the cost of a reduced trust level. The reduction can be calculated and the maximum permitted reduction of the trust level can be preset.

Keywords: *Data Integrity, Forward Error Correction, Hamming Distance, Hard Message Authentication Code (H-MAC), Message Authentication Code (MAC), Soft Input Decryption, Soft Input Soft Output (SISO) Channel Decoder, Trust Level*

INTRODUCTION

This paper is an extended version of (Živić, 2012), which includes discussion about differences between hard and soft verification, as well as application possibilities of the presented algorithm and analysis of the possibilities for future work. Its subjects are cryptographic check values (CCV), for example Message Authentication Codes (MAC) (ISO/IEC 9797-1, 1999; Ruland, 1993) and hash function based Message Authentication Codes (H_MAC) (ISO/IEC 9797-2, 2002) provide secure information transfer.

Channel codes use redundancy for the recognition and correction of errors that occur during the data transfer over a noisy channel, for example convolutional or turbo codes. Not all errors are corrected by the channel decoder, but there will be a remaining bit error rate after channel decoding depending on the channel characteristics, i.e. the signal-to-noise-ratio.

DOI: 10.4018/jdst.2013010101

The remaining bit errors will cause the rejection of messages secured by CCV´s, and the information is lost. It is assumed that no ARQ mechanisms is possible for correction of the remaining errors by repetition of the message – may be caused by a very low S/N, which will again produce a message with errors, by real time requirements or by one way communication, which is used in deep space or broadcast applications.

Redundancy generated by the channel code as well as by the data integrity mechanism has been used for Joint Channel Coding and Cryptography (Živić, 2008) and will be also exploited for Soft Input Trust Output.

Cryptographic mechanisms are standard components of nowadays' communication systems and distributed applications (Figure 1). In this paper the mechanisms of an en-/decryptor are used to generate/verify the CCV of a message M using a shared secret key.

The channel decoder is assumed to be SISO (Soft Input Soft Output). SISO is a concept of channel decoding, which was originally used in iterative and turbo coding, because soft output is fed back internally (Giuiletti et al., 2003; Lin et al., 2004). Soft output of the channel decoder is used here as soft input for the cryptographic verification process, called Soft Input Verification. Soft output of the channel decoder is usually expressed as a reliability or L-value of each output bit u' (Figure 1):

$$L(u') = \ln \frac{P(u=1)}{P(u=0)} \tag{1}$$

Reliability can be used in different applications and defined in different manners (Raza & Vidyarthi, 2001). In the case of L-values, L(u') expresses the reliability of the decision of the channel decoder, if the sent bit u was 1 or 0 (Barbulescu, 2002). The sign of the L-value shows the hard output of bit u' (1 or 0) and |L| is used as reliability value of the hard decision. Example: if L is positive, the hard output is 1, otherwise 0. As higher |L|, as more reliable is the hard decision and vice versa: a lower |L| means a less reliable decision. When the L-value is equal to 0, the probability of the correctness of the decision is 0.5.

In this paper CCV verification is used as part of Soft Input Decryption (Ruland, 2006) for the correction of the received message M' and the CCV'. Soft Input Decryption is explained, after explanation of differences between hard (standard) and soft verification. The extended algorithm of Soft Input Decryption providing soft verification, and called Soft Input Trust Output (SITO), is shown in the next section. Afterwards the maximum Hamming distance used by the extended algorithm is estimated and discussed. Trust level and trust output will be introduced in the section following Hamming distance discussion. Results of simulations

Figure 1. Modular block diagram of the coding model