Bounds and Constructions for A_3-code with Multi-senders

Rei Safavi-Naini and Yejing Wang

School of IT and CS
University of Wollongong, Northfields Ave.
Wollongong 2522, Australia
[rei, yejing]@cs.uow.edu.au

Abstract. We extend authentication codes with arbiter to the scenario where there are multiple senders and none of the participants, including the arbiter, is trusted. In this paper we derive bounds on the probability of success of attackers in impersonation and substitution attack, and give constructions of codes that satisfy the bounds with equality.

1 Introduction

Authentication systems with multiple senders were originally introduced in [1]. In these systems there are multiple senders and construction of a codeword requires collaboration of a subset of them. Authentication system with arbiter, called A^2-codes, were introduced in [6] and further studied in [2]. In these systems sender and receiver do not trust each other and there is an honest arbiter in the system, who knows the transmitter and the receiver's key information and can arbitrate in the case of dispute. If the arbiter is dishonest, the system is called A^3-system.

We consider the following scenario: there are n senders u_1, u_2, ..., u_n, a receiver R, and an arbiter A. There is a combiner C which is a public algorithm. To construct an authentic message an authorised group, B, of senders send their partial codewords to the combiner who composes the codeword that is sent to the receiver. The receiver uses his encoding rule to verify the authenticity of the codeword. When a dispute between R and u_i occurs, the arbiter uses its encoding rule to arbitrate. Possible attackers are an outsider O, arbiter A, receiver R, and groups of senders who do not from an authorised group. We consider impersonation and substitution attack. Some of the senders in an authorised group might launch a denial attack. Note that we do not assume that A is trusted during the transmission phase. However the senders and the receiver trust in the A's arbitration in the dispute phase. We consider Cartesian codes only.

Partial codewords are sent to the combiner who composes the codeword and sends it to the receiver. We assume that information in both channels can be intercepted. The channels between the senders and the combiner are called channel 1, and the channel between the combiner and the receiver is called channel 2. In this paper we assume that the attacks are only on channel 2. We study the following attacks.
Impersonation attack by the opponent: Before any transmission by an authorised group of senders, the opponent puts a codeword into the channel. He succeeds if both $R$ and $A$ accept his codeword as authentic. The success probability of this attack is denoted by $P_{O_0}$.

Substitution attack by the opponent: Opponent constructs a codeword after observing an authentic codeword sent by $C$ and all partial codewords sent by an authorised group of senders. The opponent succeeds if both $R$ and $A$ accept this codeword as authentic. The success probability of this attack is denoted by $P_{O_1}$.

Impersonation attack by the arbiter: This attack is similar to the impersonation attack from the opponent. The arbiter succeeds if the receiver accepts the codeword as authentic. Because the arbiter has more information about the keys than the opponent, he will have a better chance of success than the opponent. His success probability is denoted by $P_{A_0}$.

Substitution attack by the arbiter: This attack is similar to the opponent’s substitution. Arbiter success probability is denoted by $P_{A_1}$.

Impersonation attack by the receiver: Before any codeword is sent by the senders, the receiver puts a codeword into the channel. He succeeds if the arbiter, using the arbiter’s encoding rule, arbitrates that the receiver must accept this codeword. The success probability of this attack is denoted by $P_{R_0}$.

Substitution attack by the receiver: Having received a codeword sent by $C$ and knowing partial codewords sent by an authorised group of senders, the receiver claims that he has received another codeword. He succeeds if the arbiter, using the arbiter’s encoding rule, arbitrates that he must accept this codeword. The success probability of this attack is denoted by $P_{R_1}$.

Impersonation attack by an unauthorised group of senders: A group of senders who do not form an authorised group put a codeword into the channel. They succeed if both $R$ and $A$ accept this codeword as authentic. The success probability of this attack is denoted by $P_{U_0}$.

Substitution attack by an unauthorised group of senders: After observing an authentic codeword sent by $C$, and all the partial codewords sent by an authorised group of senders, some senders not forming an authorised group put another codeword into the channel. They succeed if both $R$ and $A$ accept this codeword as authentic. The success probability of this attack is denoted by $P_{U_1}$.

Denial attack by an authorised group of senders: After sending a codeword by $k$ senders in an authorised group, some of them deny that they have sent the codeword. The attack succeeds if the receiver $R$ presents the codeword to $A$, and $A$, using the arbiter’s encoding rule, arbitrates that $R$ must accept this codeword. The success probability of this attack is denoted by $P_{U}$.

An $A^2$-code with multi-senders was constructed in [2]. An $A^3$-code with a single sender was presented in [6]. In this paper we study $A^3$-code with multiple senders. We derive bounds on the probability of success in the attacks (Section 2), and then present a construction of the code (Section 3).