ERCIM "Alain Bensoussan" Fellowship Scientific Report

Fellow: Suzana Andova
Visited Location : Department of Telematics, Norwegian University of Science and Technology - NTNU, Trondeheim, Norway
Duration of Visit: 9 months (01.09.2005-31.05.2006)

I - Scientific activity

During the ERCIM fellowship at the Department of Telematics, NTNU I have been mainly focused on the following research areas:

1. **Security**

1.1. This research has been on formal modelling and verification of security protocols and security properties. We have worked on an extension of a formal model and its tool support (originally developed by our collaborators from the Security group at TU/e in Eindhoven) with features to express composition of security protocols. We have obtained several interesting results about sufficient conditions under which a ***composition of security protocols*** preserves certain security properties, possessed by the components of the composition when considered in isolation. Currently we are finishing a paper to be submitted to a journal: *Sufficient conditions for composing security protocols,* by authors Suzana Andova, Cas Cremers, Kristian Gjøsteen, Sjouke Mauw, Stig F. Mjølsnes, Saša Radomirović.

1.2. We have successfully applied a standard formal language (developed for specification and verification of communication systems with data) to prove ***secure realization*** in the Universal Composability security framework. The result has been published in the proceeding of the Workshop on Formal and Computational Cryptography, 2006.

2. **Cryptography**: we have proposed a new crypto primitive called ***Cryptcoding*** which has a feature to encrypt and encode (and decrypt and decode) in a single logical step. We have analized few (exsisting in the literature) realizations of this primitive, with a special focus on the one based on quasigroup transformation. Using the advantages of this function we have proposed 14 ***security schemes*** that can be used for secure document menagement. The results have been summirized in two papers, one published in the proceeding of the 2006 International Conference on Security & Management, and the other published in proceeding of the 2nd International Conference on Internet and Society.

3. **Verification of probabilistic systems**: this work has been a continuation of my previous research. It is focused on investigating weak and branching ***bisimulations*** that can be used to prove equivalent behaviour of two probabilistic systems. The result is published in the proceeding of the 17th International Conference on Concurrency Theory, 2006.

II- Publication(s) during your fellowship

Please insert the title(s), author(s) and abstract(s) of the published paper(s). You may also mention the paper(s) which were prepared during your fellowship period and are under reviewing.

1. S. Andova, K. Gjøsteen, L. Kråkmo, S. F. Mjølsnes, S. Radomirović, *An example of proving UC-realization with formal methods,* In Proc. of the Workshop on Formal and Computational Cryptography, FCC 2006, Venice, Italy, 2006

   Abstract: In the universal composability framework we consider ideal functionalities for secure messaging and signcryption. Using traditional formal methods techniques we show that the secure messaging functionality can be UC-realized by a hybrid protocol that uses the signcryption functionality and a public key infrastructure functionality. We also discuss that the signcryption functionality can be UC-realized by a secure signcryprion scheme.

2. D. Gligoroski, S. Knapskog, S. Andova, *Cryptcoding - Encryption and Error-Correction Coding in a Single Step,* In Proc. of the 2006 International Conference on Security & Management as a part of WORLDCOMP'06, Las Vegas, USA, 2006

   Abstract: In this paper we re-open a 25 years old question of joint encryption and error-correction coding, named here as *Cryptcoding*. Cryptcoding is a procedure in which encryption/decryption and error-correction coding/decoding are performed in a single step. We discuss the advantages of this approach over the traditional First-Encrypt-Then-Encode approach. To our knowledge only three different realizations of cryptcoding can be found in literature: the McEliece's public key encryption system using Goppa codes, the Kak's joint encryption and error-correction coding using D-sequences and the recently developed quasigroup random error-correcting codes. We briefly discuss the first two and mainly focus on the last one. We give two examples in which cryptcoding is efficiently employed for secure document management.

3. D. Gligoroski, S. Knapskog, S. Andova, *Schemes for Secure Management of Digitally Produced Documents,* In Proc. of the 2nd International Conference on Internet and Society, Southampton, UK, 2006

   Abstract: By means of a recently proposed encryption and error correcting system we define schemes for building secure protocols for a number of different scenarios for management of digitally produced documents. The documents are both encrypted and robust against a certain amount of intentional or non-intentional errors. Some of the schemes are based on the property of the system that the introduced redundant information needed for error-correction is not algorithmically predetermined but can arbitrarily be chosen, i.e. it can be given a semantical meaning if necessary or if desired by the user.

4. S. Andova, J. Baeten, T. Willemse, *Complete axiomatization of branching bisimulation for probabilistic systems*, 17th International Conference on Concurrency Theory, CONCUR'06, Bonn, Germany, 2006

Abstract: We consider abstraction in probabilistic process algebra. The process algebra can be employed for specifying processes that exhibit both probabilistic and non-deterministic choices in their behaviour. We give a set of axioms that completely axiomatises the branching bisimulation for the strictly alternating probabilistic graph model. In addition, several recursive verification rules are identified, allowing us to remove redundant internal activity.

Using the axioms and the verification rules, we have successfully conducted a verification of the *Concurrent Alternating Bit Protocol*. This is a simple communication protocol, slightly more `sophisticated' than the well-known Alternating Bit Protocol. As channels are lossy, sending continuous streams of data through the channels is a method to overcome this possible loss of data. This instigates a considerable level of parallelism (parallel activities) and as such requires more complex techniques for proving the protocol correct. Using our process algebra we show that after abstraction of internal activity, the protocol behaves as a buffer.

III -Attended Seminars, Workshops, and Conferences

Please identify the name(s), date(s) and place(s) of the events in which you participated during your fellowship period.

Seminars organized at the department and active working seminars of our research team organized during the visit of our collaborator from TU/e, Eindhoven.