A Multi-party Rational Exchange Protocol

Almudena Alcaide, Juan M. Estevez-Tapiador,
Julio C. Hernandez-Castro, and Arturo Ribagorda

Computer Science Department – Carlos III University
Avda. Universidad 30, 28911, Leganes, Madrid
{aalcaide,jestevez,jcesar,arturo}@inf.uc3m.es

Abstract. In recent years, existing computing schemes and paradigms have evolved towards more flexible, ad-hoc scalable frameworks. Nowadays, exchanging interactions between entities often takes place in non-structured environments where the number and nature of the different participants are unknown variables. In this context, traditional *fair* exchange protocols cease to be a feasible solution to the exchanging problem, as they are not sufficiently adaptable to offer the same guarantees in such new scenarios. *Rational* exchange protocols represent a real alternative to fair exchange exchange. In this paper, we propose the first multi-party rational exchange protocol, giving solution to the exchange problem in a context where the number of entities could vary in each different instance of the protocol and where rational (self-interested) parties, exchange their items without the involvement of a trusted third party (TTP). We also formally analyze our new scheme by applying some Game Theory concepts. Besides the simplicity of our model and a restrictive set of initial assumptions, several real life scenarios can be resolved with the proposed scheme.

1 M-RES Protocol

A multi-party rational exchange protocol is a cryptographic protocol allowing several parties to exchange commodities in such a way that, if one or more parties deviate from the protocol description, then they may bring other correctly behaving participants to a disadvantageous situation, but they cannot gain any advantages by doing so.

Initial Assumptions

- *Electronic items exchanged:* An entity U aims to collect a series of electronic items from different entities E_i, $i \in \{1, \ldots, n\}$. The nature of these items must be such that their utility only become available when the corresponding token is delivered in return. Additionally, no item in isolation is of any value to entity U. In other words, U is interested in collecting all or none of these items.
- *Providers of e-items:* Participant entities E_i providing with the electronic items must be part of a visible and recognizable PKI (Public Key Infrastructure). Messages forth and from these entities must be digitally encrypted and

R. Meersman, Z. Tari, P. Herrero et al. (Eds.): OTM 2007 Ws, Part I, LNCS 4805, pp. 42–43, 2007.

signed respectively. No other trusted or semi-trusted parties are involved in the scheme. Note that this is not a restriction on entity U, who can maintain anonymous his real identity.
- *Repeated scenarios:* The scheme will render rational exchanges when executed in repeated scenarios. Participants E_i must be assumed to run the protocol in multiple instances with different participants. In this context, an informal reputation factor is indirectly implemented, ensuring entities with good reputation a continuity in their trading activity.

Two Phase Protocol. The M-RES protocol consists of two main phases.

- Phase I: Customer U sends entity E_1, a message including a set D with descriptions for all the required items. Entity E_1 produces a customized item $item_1$, according to the appropriate token description and destined to U. It also establishes who would be the next entity to satisfy the next requirement described in set D. Finally, entity E_1 sends E_2 a message containing $item_1$ and the set D with the remaining description-tokens. The process is repeated from any E_i to E_{i+1} until all requirements are satisfied. The last entity E_n sends U all items $\{item_i\}_{1,\ldots,n}$ completing the first phase of the exchange.
- Phase II: User U produces n payment-tokens, one for each participant entity. U sends entity E_1 the set of payments P. When a participant E_i receives a message with a set of payments P, it takes the appropriate payment token, deletes it from the list and forwards the message to the next entity.

Protocol Formal Analysis. In Game Theory, backward induction is one of the dynamic programming algorithms used to compute *perfect equilibria* in sequential games. The process proceeds by first considering the last actions of the final player of the game. It determines which actions the final mover should take to maximize his/her utility. Using this information and taking the induction one step backward, one can then determine what the second to last player will do, to also maximize his/her own utility function. This process continues until one reaches the first move of the game. Our formal analysis of the M-RES protocol is based on applying backward induction to the *protocol-game* derived from M-RES description. Rationality is then inferred from entities following strategies which conform an equilibrium in the game.

2 Conclusions

Our future work is directed to transform other problems, such as multiple access control or shared secret distribution, into an M-RES framework in which rationality can be formally proven to be guaranteed.