ULOOP white paper 09
25/09/2012

Crediting aspects in ULOOP

Introducing ULOOP credits and the virtual currency system developed to provide reward-based cooperation incentives in ULOOP

Alessandro Bogliolo (editor, University of Urbino), **Saverio Delpriori** (University of Urbino), **Lorenz Klopfenstein** (University of Urbino), **Alessandro Aldini** (University of Urbino), **Jean-Marc Seigneur** (University of Geneva), **Waldir Moreira** (Universidade Lusófona)

This white paper is focused on the reward-based incentive system for resource sharing developed within the European project "User-centric Wireless Local Loop" (ULOOP), and on the virtual currency system designed to manage such incentives. In particular, the paper introduces the notion of "ULOOP credits", and it outlines the features and the architecture of the virtual currency system adopted to manage them in order to provide reward-based cooperation incentives.

Contents

Introduction

The European project "User-centric Wireless Local Loop" (ULOOP) [1] has as underlying scenarios *User-centric networks (UCNs)*. UCNs can be seen as networking structures where networking devices often belong to the Internet end-user, and where the links of such structure are formed due to trust interaction, as well as to the willingness of users to share networking resources (e.g., Internet access, printing services). Hence, UCNs are autonomic and self-organizing structures, where social trust derived from the interaction among peers is a main trait.

In fact, the trust management system [2] in ULOOP is fundamental to create broad circles of trust, which in ULOOP are known as communities [5], and the basis to provide adequate quality.

In order to assist in creating broad and robust circles of trust, it is essential to consider an incentive system which can allure new users to join ULOOP communities. Therefore, to fight back the so-called "selfishness of the peers", ULOOP considers, in the context of its trust management block, a specific mechanism to motivate cooperation be it in a pure trust basis, or in a rewarding basis. Within the ULOOP trust management block, the entities that are being implemented to provide such cooperative behavior [2] are, respectively, the *Cooperation Manager* and the *Reward Manager.*

The Cooperation Manager is in charge of *trust-based incentives*, e.g., "the more one shares, the more one gets". While the Reward Manager takes care of *reward-based incentives,* which are used to push the willingness of individuals to share their services/resources beyond the limits of their inherent pro-social attitude. Members who need a reward in order to share their services/resources are called "retailers", while those who do not need any reward are called “volunteers”. Any user can dynamically switch between the two cooperating modes.

Reward-based incentives are used in ULOOP to push cooperation beyond the limit of the pro-social attitude of individuals

This white paper is focused on the rewarding system of ULOOP (i.e., on the retailer model) which we believe is essential to ensure that ULOOP can be quickly disseminated.

Virtual currency has three main advantages w.r.t. real money when used as a cooperation incentive within an online community: first, it provides a more appropriate support to micro-payments; second, it raises less security concerns; third, it can be used without reserve on the Internet. This document focuses on the crediting aspects of ULOOP and outlines the features of the virtual currency system adopted. The rest of this section provides a minimum background on virtual currency systems.

Virtual currency systems

According to the phenomenal analysis conducted by Guo and Chow [4], existing virtual money systems can be classified into four categories: *Type 1* virtual money can be used only to purchase virtual goods and services and cannot be exchanged for real money; *Type 2* virtual money can also be used to purchase real goods and services; *Type 3* virtual money can also be purchased; *Type 4* virtual money can also be sold.

Regardless of the category it belongs to, virtual money is subject to security issues which need to be properly addressed to make it work. The main problems are related to the risks of *forgery* and *double spending*, the prevention of which requires the adoption of countermeasures based on cryptography.

Virtual money systems can be classified based: on their scope, on their need for a centralized trusted authority, and on their capability of supporting offline transactions

For the purpose of this document it is useful to provide also an architectural classification of virtual currency systems, according to two criteria. First, we distinguish between *centralized* and *distributed* systems according to the existence (or not) of a central trusted authority which acts as mint/bank. Second, we distinguish between *offline* and *online* systems, depending on their capability to support (or not) transactions between nodes which are not connected to the Internet. Centralized virtual currency systems are usually online, in that they rely on a trusted third-party which oversees every transaction. These two technical features, together with the phenomenal classification proposed by Guo and Chow, represent the three orthogonal axes of a design space in which to place the ULOOP virtual currency system described in this white paper.

ULOOP Credits

The virtual currency unit used in ULOOP is called “ULOOP credit”. An initial budget of ULOOP credits is assigned to any new member to represent the value that he/she brings to the community due to the network effect at a stage where there is not yet trust established. ULOOP credits are then transferred from a *requester* to a *requestee* whenever a cooperation process takes place between two ULOOP nodes, in order to assist in getting a desired service. According to the cooperation process adopted in ULOOP, credits are offered beforehand by the requester to the requestee in order to reduce the communication overhead of the negotiation phase. If the requestee acts as a volunteer he/she accepts any offer, while if he/she acts as a retailer he/she might ask for more, and eventually, reject the request if the final reward is not enough.

As long as ULOOP credits are used as cooperation incentives within a specific community they can be regarded as a *Type 1* or *Type 2* virtual money, depending on the nature of the traded services/resources. In practice, ULOOP credits work as a guarantee of reciprocity, since the credits earned by providing a service/resource can then be used to purchase other services/resources. No conversion is needed to this purpose. On the other hand, role swapping avoids end-users to run out of credits.

ULOOP credits provide a guarantee of reciprocity within the community

ULOOP communities, however, doesn’t work in isolation. Rather, it is part of the Internet supply chain. Typical application scenarios for user-centric wireless networks, in fact, include 3G offloading and wireless extensions of infrastructured access networks.

Therefore, when considering interoperability to the access, reciprocity cannot be guaranteed in the same way it is guaranteed in ULOOP communities, since there are end-users interested in taking advantage of ULOOP services without having any resource to share, or established operators providing their services for business without being interested in the services/resources shared by ULOOP members. In order to allow ULOOP to become part of the Internet value chain, ULOOP considers a model where end-users can buy ULOOP credits, and established operators and service providers can sell the credits they earn. This process is called "monetization" in ULOOP.

ULOOP credits can be converted at the borders of ULOOP

In order to avoid speculation, ULOOP credits either assigned to a new member or bought by an end-user cannot be monetized directly. Rather, ULOOP credits earned by providing a service can be traded for money. This means that ULOOP credits purchased or assigned need to be spent within the community. In spite of these limitations, ULOOP credits have to be regarded as a *Type 4* virtual money.

Functional Specification

The ULOOP crediting system provides the support for credit assignment, rewarding, and monetization, as detailed below. Each one of the three phases entails both a decision about the amount of credits involved, and the management of such credits.

Credit assignment

As mentioned earlier, a given amount of ULOOP credits is automatically assigned (computed locally on each device) to any new member when he/she joins the community. In principle, this amount represents the value that the new member brings to the community because of network effect. Due to the cooperative nature of the ULOOP community, the added value brought by a new member depends on his/her willingness to cooperate, which is expressed by the so-called *dispositional trust* [2]. Hence, the amount of credits to be assigned to any user is computed by taking into account his/her dispositional trust. Please refer to specific white papers for further details [2][3].

From a technical point of view, the ULOOP credits to be assigned to a new user need to be minted and made available to that user avoiding forgery and theft. Moreover, the assigned credits have to be labeled as unmonetizable in such a way that the label cannot be removed by the assignee.

Rewarding

Reward computation is performed by the two parties – requester and requestee - the parties involved in any cooperation process. The requester computes the amount of credits to be offered beforehand based on his/her trust on the requestee: the higher the trust, the higher the offered reward for the service requested. The requestee (when he/she operates in retailer mode) computes the reward needed to provide a service based on his/her trust on the requester: the higher the trust the lower the reward. This tight relationship between trust-based and reward-based incentives strengthens the cooperation patterns in ULOOP, as detailed in the specific white papers [2][3].

From a technical stand point, once an agreement is found between a requester and a requestee, the agreed reward has to be paid. There are three main issues to be addressed when implementing a payment system: *forgery*, i.e.use of false credits; *double spending*, i.e.,use of credits already spent; *cheating* , i.e. refusal to pay.

Monetization

Monetization, which is the conversion of ULOOP credits in real money, is needed at the boundaries of ULOOP to allow the ULOOP community to interact with the outside world. In principle, conversion can be done either at a fixed rate, or based on current market values. The virtual currency system adopted in ULOOP has to be flexible enough to support both strategies, allowing the ULOOP community to decide which one to adopt.

From a technical stand point, monetization entails credit transfers (with the same issues mentioned about rewarding) with the additional complexities raised by the use of real money and by the need to distinguish between monetizable and unmonetizable credits.

Architecture

ULOOP credits are managed by a virtual currency system with a *centralized offline* architecture: it relies on a trusted authority (namely, the *Bank*), but transactions can take place even if the trusted authority is not online.

ULOOP adopts a centralized offline virtual-money architecture

The details of the credit management system are hidden by a software component (the *Reward manager*) which runs on each node and provides an interface to the crediting functionalities described in the previous section. Encapsulation makes it possible to transparently change the implementation of the underlying virtual currency system without affecting the applications which rely on it.

In the current implementation ULOOP credits are not managed as digital coins. Rather, they are managed by means of bank accounts locally mirrored by the wallets installed on each node.

Decisions about the amount of credits to be assigned or awarded are also taken by the *Reward manager*, which directly interacts with the Cooperation manager [2].

Bank

The Bank encompasses the roles of *mint*, *bank*, and *trusted third party*.

New credits are created only when they need to be assigned to a new ULOOP member. The Bank makes available to the ULOOP community a web service which can be invoked with a signed credit assignment request (signature is based on the CryptoID used as unique identifier in ULOOP [3]). The Bank checks the validity of the signature of the new member and creates an account for the new user with the initial assignment of unmonetizable credits.

The Bank is the trusted third party that manages ULOOP credit accounts

A payment consists of a transfer of credits from the account of the payer to the account of the payee, triggered by a credit transfer request signed by both parties. Both monetizable and unmonetizable credits can be used to pay for services. Hence, the specified amount of credits is taken from the account of the payer using unmonetizable credits first. Regardless of the nature of the credits taken from payer's account, all the credits earned by the payee are monetizable.

The role of the Bank in monetization is similar to the role it plays in rewarding: it manages the transfer of credits from account of a selling user to the account of a selling user. Notice that the ULOOP Bank doesn't manage real money. Hence, it takes care only of transferring ULOOP credits. The way credits are converted in real money is independent of the Bank and will be discussed in next section. As for the Bank, the only difference between monetization and rewarding is that credits have to be taken from the amount of vendor's monetizable credits and added to the amount of buyer's unmonetizable credits. This is schematically represented in Figure 1, where bank accounts are represented as pairs of reservoirs for unmonetizable (left) and monetizable (rights) credits.

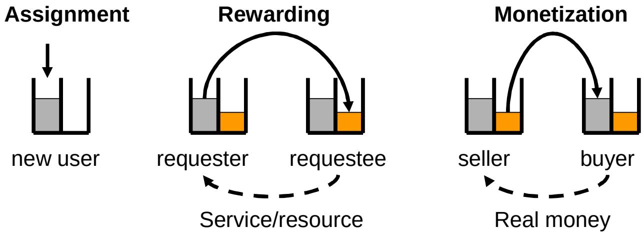

Figure 1. Schematic representation of credit transfers among bank accounts.

Wallet

The Wallet installed on a node works as a mirror of the corresponding bank account. Local mirroring is used to relax the online constraint and to allow ULOOP members to engage in cooperation processes even if they are temporarily disconnected from the Bank.

The Wallet is a software component which maintains a local copy of a Bank account to enable offline transactions

Needless to say, as long as the trusted third party is offline ULOOP members cannot operate on their Bank accounts. Hence, payments can only be promised by the requester to the requestee based on the credits available on their wallets. A promise of payment is nothing but a credit transfer request issued and signed by the payer and sent to the payee. The amount to be transferred is taken from the local wallet of the payer and added to the local wallet of the payee, but such operations remain in a pending status until the credit transfer is forwarded by the payee to the Bank and processed by the Bank as described in previous subsection.

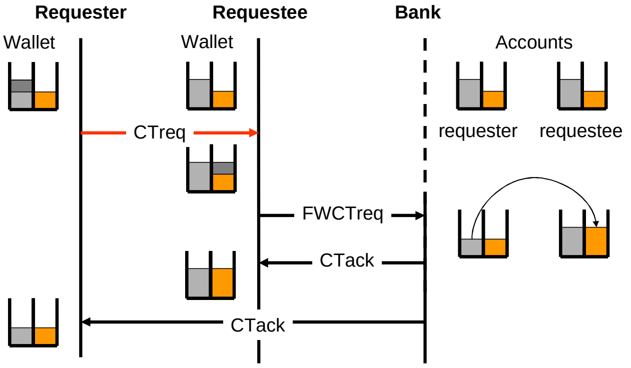

Figure 2. Sequence diagram of an offline transaction which entails a credit transfer from the Requester to the Requestee. "CT" is used in the sequence diagram to denote credit transfers.

Wallets need to synchronize with the Bank either periodically, or whenever a pending transfer is completed. In the current implementation, synchronization can be performed by invoking a specific web service made available by the Bank.

Otherwise, credit transfer notifications can be sent back by the Bank to both parties. This is the case represented in Figure 2, where pending payments are represented in dark grey.

Although the Wallet has been described so far as a simple data structure keeping a local copy of a bank account, the exact nature of this software component may vary depending on the actual implementation of the virtual currency system. This module however is only used by the Reward manager and provides high-level primitives for managing the status of the user's account. The interface to the wallet is not visible outside of the Reward manager and is not reflected in the final user interface.

Reward manager

The Reward Manager is the main component of the ULOOP crediting system. It takes decisions on the amount of credits to be offered/accepted as rewards and it provides an interface which makes available to the Cooperation Manager high-level credit transfer functionalities while hiding all the details of the back end. Not only the Bank, but also the Wallet are hidden behind the Reward Manager.

> **The RewardManager works with the CooperationManager to take decisions about the amount of credits to be used as a reward**

The interface of the Reward manager is outlined in next section.

Object-oriented model

This section describes the object-oriented model and the general interface of the Reward Manager from which the different implementations are derived.

The `RewardManager` is the central module in an ULOOP node that handles credit transfers, also called *payments* in the virtual currency system. `Payment` objects (see below) are described by an opaque object that should (and cannot) be examined by other modules: objects of this type will be crypted and serialized via a custom procedure before being sent to another node. Only the `RewardManager` has the facilities to create or decode any of these objects, through the methods `acceptCreditTransfer` and `createCreditTransfer`.
The `acceptCreditTransfer` method also decides whether a payment can be accepted as an incentive to provide a service, according to the operating mode of the node (volunteer or retailer).

The `Wallet` is a very simple container for the amount of credits kept by the Reward Manager and has no important additional logic.

The Reward manager maintains a reference to the CryptoID of the current user of the ULOOP device (which is needed as an identity reference for the bank account) and a reference to the central authority (Bank).

The Bank is initially needed when initial credits are assigned (which will attempt to create a new account, by default). If the account already exists, the Bank will ignore the account creation and keep the existing account unchanged. Otherwise, the account is created and initial credits are assigned to the newly created record (if they exceed a limiting amount of credits, account creation is deemed fraudulent and fails). In both cases, once the account exists and has been verified, the Wallet is synchronized with the bank account and the effective amount of credits is set.

Afterwards, the Bank is contacted periodically inside the `periodicalSynchronization` method, to synchronize any pending payment registered by the `RewardManager` (both incoming and outgoing). Issued payments are internally identified by an unique ID (a `GUID` value), allowing the Bank to track confirmations for the same payment by both payer and payee. Once the payment is confirmed, the saldo of payer and payee are updated by the bank. When the `RewardManager` performs synchronization, the Wallet status is also synchronized to the current saldo on the Bank.

Discussion

The virtual currency system described in this document is the result of a tradeoff between security and usability. In the context of user-centric networking, usability imposes both to minimize the computation/communication overhead and to relax the constraints on the operating conditions. Both the centralized offline architecture of the virtual-currency system and the cooperation paradigm adopted [2] meet usability requirements at a cost of a reduction in security which needs to be discussed.

> **The virtual currency system adopted in ULOOP is the results of a tradeoff between usability and security**

In particular: i) the presence of a trusted third party reduces the computational requirements of pure distributed systems; ii) the offer made beforehand by the requester reduces the communication overhead; iii) the possibility of making offline transactions increases the availability of the system. In such a system, the requester takes the risk of making an advance payment, while the requestee, in case of offline trusted authority, takes the risk of delivering a service against a payment to be verified.

Security issues are addressed by reducing the value of atomic transactions and by exploiting the trust-management system to isolate cheating users

The risks are mitigated by the granularity of the transactions, the average value of which is expected to be of a few cents, and by the trust management system, which provides an effective mean to isolate cheating users.

References

[1] EU IST FP7 ULOOP – User-centric Wireless Local Loop. Gr. Nr. 257418, 2010-2013. http://uloop.eu/.

[2] P. Mendes *et al*., "Coopeartive Networking in User-Centric Wireless Networks", *ULOOP white paper*, 2012.

[3] C. Bellester *et al*., "Trust Management in ULOOP", *ULOOP white paper*, 2012.

[4] J. Guo and A. Chow, "Virtual Money Systems: A Phenomenal Analysis", in Proceedings of IEEE CEC, 2008.

[5] R. C. Sofia (Ed.), ULOOP D2.3: Overall Specification , *ULOOP Consortium*, September 2011.

The research leading to these results has received funding from the EU IST Seventh Framework Programme (FP7/2007-2013) under grant agreement n 25741, project ULOOP (User-centric Wireless Local Loop), participants: Alcatel-Lucent Bell Labs, (FR), COFAC/University Lusófona (PT), Huawei Technologies Duesseldorf GmbH (DE), ARIA S.p.A (IT), Caixa Mágica Software (PT), FON Wireless Ltd (UK), Technische Universität Berlin (DE), University of Kent (UK), Université de Genève (CH), Level7 srlu (IT), University of Urbino (IT).

For further information please visit http://www.uloop.eu/, join the **FP7 ULOOP Project** group on LinkedIn, follow **@uloopproject** and look for **#uloopproject** on Twitter.