The Architecture of Coupon-Based, Semi-off-Line, Anonymous Micropayment System for Internet of Things

Daniel Wilusz and Jarogniew Rykowski

Department of Information Technology, the Poznań University of Economics
Mansfelda 4, 60-854, Poznań, Poland
{wilusz,rykowski}@kti.ue.poznan.pl

Abstract. In the Internet of Things a lot of business opportunities may be identified. The devices in IoT may create ad-hoc temporary networks to provide services or share some resources. Such services are characterized by a great economical potential, especially while provided at mass-scale and for incidental users. However, the development of paid services or resources in IoT is hampered by relatively big transaction costs of payment operations. To deal with this problem, we propose a novel architecture of coupon-based, semi-off-line, anonymous micropayment system to enable transactions in the scope of Internet of Things. User anonymity and security is assured by the usage of standard cryptographic techniques together with novel architectural design of the payment processes. Utilization of a hash function allows generating and verifying electronic coins in computationally efficient way, so as to be executed even in hardware- and software-restricted environment such as Internet of Things.

Keywords: micropayments, e-money, Internet of Things, Future Internet.

1 Introduction

The Internet of Things (IoT) is the rapidly developing phenomenon, which undoubtedly will influence the society and economy. Originally it was perceived as the intelligent network linking objects, information and people to allow remote coordination of resources by humans and machines [3]. However, nowadays IoT is not only limited to electronic identification of objects, but it is defined as technology integrating physical objects with information network, where these objects may act as active participants in business processes [6].

Multiple applications of Internet of Things have been identified in such economy areas, as manufacturing, supply chains, energy, healthcare, automotive industry and insurance, to mention a few [6]. Moreover, the expansion of Internet of Things outside the internal infrastructures of companies is expected. Such situation should affect the economy by creating human-to-machine (H2M) and machine-to-machine (M2M) markets [14]. In these markets, the machines will match business partners and conclude contracts, according to the preferences of their owners.

In the Internet of Things markets the devices will cooperate by creating temporary networks to exchange data. The devices are expected to provide services on the mass

L.M. Camarinha-Matos, S. Tomic, and P. Graça (Eds.): DoCEIS 2013, IFIP AICT 394, pp. 125–132, 2013.

scale, but the business relations will be temporary, and often formed on an ad-hoc basis. The devices in Future Internet will be used locally, but at mass scale and in many places. Similarly, the particular payments will be made in micro scale, but all transactions will have the global character. One of the features of the services provided by devices from IoT network is activity-based micro-pricing, which means that clients are charged by exact time, amount and sort of services they consume [14]. Therefore, to make the provision of ad-hoc services profitable, an efficient micropayment system is required.

The micropayment system suitable for the transactions in Internet of Things should observe the following requirements. First, it should be possible to implement the system worldwide, by avoiding intermediaries (e.g., a clearing house). Second, the financial institution should bear possible minimal computation costs. Third, a user should be able to make a payment off-line in order to decrease the costs of a network connection, which in particular cases may exceed the value of purchased goods or services (e.g., mobile data transfer under roaming circumstances). Fourth, the vendor should contact a financial institution as seldom as possible. Fifth, the anonymity of the user should be assured by a prevention of payment tracking. Sixth, the security of transaction should be assured by the encryption and the prevention of double spending or forgery.

To deal with the above problems, an anonymous, semi-offline, micropayment system for transactions in Internet of Things is proposed in this paper. The contribution of the proposed solution in the field of anonymous micropayment systems and Internet of Things is described in Section 2. The state of the art of micropayment systems is reviewed in Section 3. In Section 4 overall architecture and main protocols of micropayment system suitable for micro-transactions in Internet of Things are proposed. Finally, Section 5 concludes the paper.

2 Contribution of Proposed System to the Internet of Things

In the paper a new architecture of micropayment system adjusted to the requirements of business transactions in Internet of Things (IoT) is presented. The proposed micropayment system meets the needs of human-to-machine and machine-to-machine markets, where efficient processing of many small-amount transactions is required. Although plenty of anonymous micropayment systems were proposed in the literature, the state of the art reveals that none of them is suitable for transactions in Internet of Things. However, the coupon-based systems, originally proposed to handle pay per view payments on the websites, seem to fit the gap.

A good starting point to realize the idea presented in the paper is related with a micro-payments architecture originally proposed by Wilusz and Rykowski [15]. However, in order to fulfill above-mentioned requirements of IoT transactions, this architecture was significantly modified. First, the clearing house became an unnecessary intermediary and in our proposition a financial institution is sufficient to handle both coin issue and clearing. Second, the coin registration was changed by putting this activity into a vendor task, so that each coin is registered during its first use.

Moreover, this solution strengthened user anonymity, by an elimination of a possibility of user (e.g., his personal device) tracking. Third, the coin blocking procedure was improved by setting the final date for blocking a coin by a vendor. Fourth, the user and vendor specify together in anonymous way the account to be credited, which, by an application of cryptographic methods, improves security of the proposed solution.

According to the long tail concept [2], the Internet of Things has a huge economic potential of services or resources being sold for micro-price in huge amounts to plenty of incidental clients. The potential areas of application of micropayments in IoT are as follows: transportation services (pay per exact distance or number of stops), services concerning augmented reality (virtual guides in a museum or multimedia concerning cultural heritage objects), a reduction of external effects in public spaces (payments for using a car in city centers), and services in public spaces (vending machines, toilets or waiting rooms), to mention a few. However, because of the lack of efficient payment method, high transaction costs strongly limit IoT market. The proposed architecture will allow implementing an efficient micropayment system suitable for payments in IoT. The system, once become de facto standard, will cause the IoT market to flourish on international scale.

3 State of the Art

There were proposed numerous micropayments schemes in the literature. However, to our best knowledge none of them is suitable for the payments in the IoT environment.

Most of already implemented micropayment systems are based on the prepaid account and aggregation of particular payments by single payment system operator (e.g., Amazon Flexible Payment Service [1] or GeldKarte [5]). In this approach vendors and clients are bound to a single payment service provider, which consolidates clients' micropayments into macropayments made to the sellers at the end of specified period. The micropayments aggregation by one entity is not proper for IoT transactions, as purchases happen rather irregularly, incidentally and should be possible worldwide. Moreover, this solution lacks anonymity, as service provider can track each payment [13].

Another sort of micropayment schemes applies probability approach to make micropayments effective (e.g., schemes proposed by Micali and Rivest [8] or Lipton and Ostrovsky [10]). The foundation of these systems is based on an assumption that users make a lot of purchases and vendors have huge volume in sales. Under this assumption, it is enough to provide a coin, which with probability of s will be payable amount of $1/s$ to assure that users will pay and vendors will get amount close to their expenses and earnings. However, there are following drawbacks of such a solution. First, no anonymity is assured, as each user is obliged to sign transaction details. Second, the probabilistic scheme has features of a wager (one may win or lose depending on result of some activity) rather than sale (getting goods or services for an amount of money). Third, both user and vendor are required to have PKI certificates.

The third group of micropayment schemes is coupon-based, which utilizes the idea of hash chains [7] (e.g. PayWord [12], Payeras-Capella et. al. scheme [11] or Wilusz and Rykowski architecture [15]). In coupon-based systems an electronic coin is represented by the last output of a hash function applied iteratively to some seed. This approach enables the electronic coin to be spent in fractions, by presenting the vendor a set of chain nodes. Although, the general scheme presented by Rivest [12] missed the anonymity and allowed user to exceed their bank-account limits, it was improved by Payeras-Capella et al. [11] by an application of Chaum's blind signature protocol [4]. However, in this scheme, a user needs to contact financial institution directly before the payment in order to produce merchant-specific hash chain. Moreover, the Authors do not mention what happens with unspent tokens of merchant specific hash chain, and it appears that unspent value is lost in favor of the financial institution. Wilusz and Rykowski [15] proposed improved, anonymous coupon based micropayment system. In their proposition the user contacts the financial institution only during coin issue phase. During the payment process only the vendor needs to stay on-line. The proposition of locking the coin by the vendor at the clearing house solved the problem of double spending, and in advance to the Payeras-Capella et al. [11] scheme, there is no need to generate merchant-specific coins. Moreover, unspent fraction of the coin may be used in further transactions, provided that the coin was unblocked by the merchant. However, there are still some drawbacks of this system. First, the presence of the clearing house increases transaction costs and hampers the worldwide expansion of the system. Second, there is a serious risk, that the vendor will not unblock the coin after the payment.

The decentralized micropayment systems such as Bitcoin [9] are becoming more popular. However the decentralized systems appear to be of limited trust, as there is no central authority controlling the supply of virtual currency. Moreover, the security of Bitcoin system is preserved under condition that the majority of Bitcoin network nodes are honest. The botnet attack poses a real risk of Bitcoins forgery or doublespending. The above mentioned traits of Bitcoin system cause, that this solution is not suitable for mass scale payments in the Internet of Things.

The analysis of the state of the art in micropayment systems indicate that there is no solution meeting all the requirements of transactions in the Internet of Things. However, the Wilusz and Rykowski solution [15] has a potential, after some modification, to meet the needs of H2M and M2M markets. In this paper, we propose some extensions and improvements to this approach, to be described in the next section.

4 Architecture of Micropayment System for Internet of Things

The architecture and protocols of a micropayment system for Internet of Things, presented in this section, are the results of significant improvements of the proposition of Wilusz and Rykowski [15]. The introduced changes enabled the system to meet the requirements of micro transactions on both H2M and M2M markets.

The proposed system is coupon-based, which means that the hash chain concept is used to produce divisible coin. Such a solution decreases computation costs of a financial institution, as it is enough to sign the coin once and further this coin may be spent in fractions. The anonymity is assured by an application of Chaum's blind signature scheme. In the result, a financial institution is not able to link the coin identifier with a user. Additionally, the vendor stands for an entity to register a coin at financial institution, which strengthens the user anonymity, as no IP tracking of end-user device is possible. The financial institution *F* generates the coin in return for money, so the coin bears obligation of *F* to accept it and pay the holder (e.g. by banking transfer). As a result there is no need to involve a clearing house in the payment process, as the financial institution, that issued a coin, takes care of coin clearing. What is more, a user needs an Internet connection only to get new coins from *F*. In Internet of Things, a user (a person or a device) contacts a vendor (a person or a device) by a short-range radio communication. Moreover, the vendor *V* uses the Internet, to contact *F*, only when blocking the coin or finishing the transaction. The idea of indexing and blocking of coins together with storing the last spent token in financial institution database, prevents the double spending issue. In the system a coin may be blocked only till specified date *T*. Additionally the user *U* specifies who should be credited by using vendor's certificate, which prevents any eavesdropper from gaining benefit.

Figure 1 presents the participants of the system and their interactions. In the next sections the coin generation protocol and payment protocol are described in details.

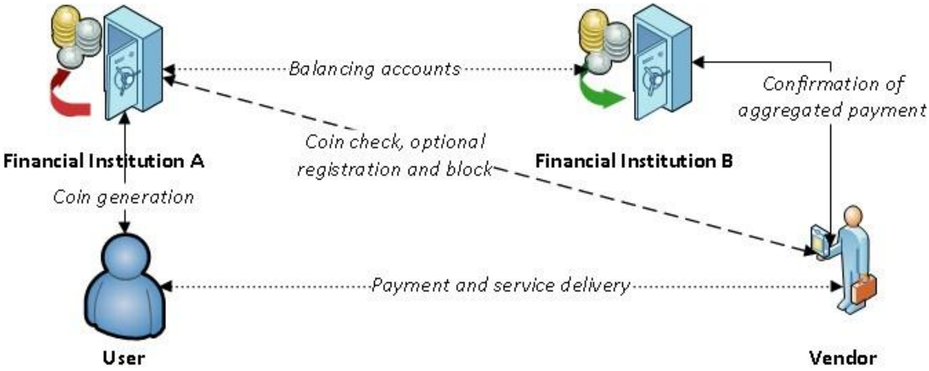
Balancing accounts
Confirmation of aggregated payment
Coin check, optional registration and block
Financial Institution A
Financial Institution B
Coin generation
Payment and service delivery
User
Vendor

Fig. 1. Overall system architecture

4.1 Coin Generation Protocol

In the proposed system, the coins generated by a financial institution are of fixed value *M* and may be divided into *n* fractions (tokens). Each token has specified value equal to *M/n*. The divisibility of a coin is achieved by an application of hashchain concept, while the anonymity is assured by the use of Chaum's blind signature scheme. The coin generation protocol consists of three phases: blind coin generation, blind coin signing and a removal of a blind factor.

In the first phase, the user *U* generates a random seed *S,* which is kept in secret. Then, hash function *H()* is performed iteratively on the seed. Next, the user generates random blinding factor *r* and finds its reverse modulo *N* (where *N* is modulus of financial institution RSA public key). Finally, blinding factor *r* is encrypted with financial institution RSA public key e and multiplied modulo N by the coin identifier (last value of hash chain $H^n(S)$). As a result of this operation a blinded coin $H^n(S)r^e \mod N$ is produced.

During the second phase, the user is authorized in the payment system and sends the blinded coin to the financial institution, which in turn debits user account and signs blinded coin with RSA decryption key d. Then, the signed blinded coin $H^n(S)^d r^{ed} \mod N$ is returned to the user U.

In the last phase, the user removes the blinding factor. As the $r^{ed} \mod N$ is equal to $r \mod N$ it is sufficient to multiply the blinded coin by the r reverse modulo N ($r^{-1} \mod N$), because the following congruence is met $rr^{-1} \equiv r^0 \equiv 1 \pmod N$ [4].

Coin generation protocol

U→F:	user credentials, H^n (S) r^e mod N
F→U:	H^n $(S)^d$ r^{ed} mod N

4.2 Payment Protocol

At the beginning of a transaction, the user U and the vendor V both agree on the date T of finishing transaction (the final date till which the coin will be blocked at a financial institution). Additionally, the vendor provides to the user its certificate C containing credentials and bank account details. The user sends to the vendor the following items: the signed coin, encrypted concatenation of the last unspent token $H^{n-m}(S)$ (where $n>=m$) with T, and encrypted concatenation of $H^{n-m}(S)$ with C. This proves that U (the only entity knowing $H^{n-m}(S)$) authorizes vendor V identified by certificate C to block the coin identified by $H(S)^d mod\ N$ till the date T.

In the next step vendor V sends C, T, the coin $H^n(S)^d \mod N$ and both concatenations $(H^{n-m}(S)\|T)^e \mod N$ and $(H^{n-m}\ (S)\|C)^e \mod N$ to the financial institution F. Then, the financial institution F uses its encryption key e, in order to obtain coin identifier $H^n(S)$ from signed coin $H(S)^d mod\ N$. Next, the financial institution F decrypts $(H^{n-m}(S)\|T)^e mod\ N$ and $(H^{n-m}(S)\|C)^e mod\ N$ with its decryption key d and retrieves $H^{n-m}(S)$. Then, the financial institution F checks if the coin was already registered. In the case of a new coin, the financial institution F checks if $H(H^{n-m}(S))$ *is* equal to $H^n(S)$. If this checking succeeded, the coin $H^n(S)$ is registered in the database by storing the coin $H^n(S)^d \mod N$, coin identifier $H^n(S)$, and first token $H^{n-1}(S)$ (in this case $m=1$). If the coin was already registered, the financial institution F checks if the token $H^{n-m}(S)$ is the predecessor of the previously spent token $H^{n-m+1}(S)$ by verification of the following equation $H^{n-m+1}(S)=H(H^{n-m}(S\ ))$. In the next step, the coin is blocked for the period T for the vendor V identified by the certificate C. Then, financial institution F sends to the vendor V the last spent token $H^{n-m}(S)$ and a position (n-m) of this token in the hashchain. The position of the token in hashchain determines the remaining value of the coin ($(n-m)M/n$).

After having validity and blocking of the coin confirmed by financial institution F, the vendor V starts charging the user U the micro prices by requesting tokens representing particular value. Then the user U provides the vendor V the token

$H^{n-m-q}(S)$ of value qM/n and the order number $n-m-q$ (where $n>=m+q$). The token is verified by the vendor V by checking if $H^q(H^{n-m-q}(S))= H^{n-m}(S)$. If the checking is positive, the goods or services may be provided. The request and validation of the tokens may be repeated during the consumption of services or goods purchase, in the case when the user U is charged on the pay per use (or unit) basis. For a next service use, the user U is requested for next token $H^{n-m-q-p}(S)$ of value pM/n. The vendor V provides proper token and this process continues till the end of the transaction.

At the end of the payment the vendor V sends to the financial institution F the coin $H^n(S)^d$ *mod* N, last received token $H^{n-m-q-p}(S)$, and order number $n-m-q-p$ (where $n>= m+q+p$). The financial institution F locates the coin in its database and stores the last token. Then, the coin is unblocked and vendor's bank account may be credited. If the total value M of the coin is spent (in the case of $n-m-p-q = 0$), it is marked as invalid.

Payment protocol

V→U: T, C
U→V: $H^n\,(S)^d$ mod N , $(H^{n-m}\,(S)\|T)^e$ mod N, $(H^{n-m}\,(S)\|C)^e$ mod N
V→F: T, C, $H^n\,(S)^d$ mod N , $(H^{n-m}\,(S)\|T)^e$ mod N, $(H^{n-m}\,(S)\|C)^e$ mod N
F→V: $H^{n-m}\,(S)$, n-m
V→U: Request for tokens
U→V: $H^{n-m-q}\,(S)$, n-m-q
V→U: Request for tokens
U→V: $H^{n-m-q-p}\,(S)$, n-m-q-p
V→F: $H^n\,(S)^d$ mod N, $H^{n-m-q-p}\,(S)$, n-m-q-p

5 Conclusions

In this paper, an anonymous semi-off-line micropayment system for transactions in Internet of Things is proposed. The improvements described in the text allowed simplifying the architecture, strengthening user anonymity and protocols security. The intermediary clearing house became unnecessary and was removed from the architecture, which caused a simplification of communication and transactional overheads of the proposed solution. The original approach of the vendor being the entity who registers the coin at a financial institution has been applied. This solution caused an increase of the user-anonymity level by disabling communication tracking possibilities. Moreover, the coin management in payment process enhanced security of the solution, for at least two reasons. First, encrypted concatenation of token with blocking date prevents the suspension of coin in financial institution database. Second, the concatenation of token with vendor's certificate ensures that the vendor gets the payment, because any malicious intervention in the protocol cannot change the beneficiary.

The proposed system meets the specific needs of financial transactions in Internet of Things by decreasing transaction costs concerning the payment process. What is more, proposed solution may be implemented on wide range of payment instruments concerning smartcards or smartphones. The payment protocol is easy to be executed by even small devices, and users are required only to formulate an intention of a payment. Additionally, a coin management system may be proposed, which would optimize the choice and strategies of coin spending with different vendors. We do hope that the proposed micropayment system will allow several new, commercial innovations to emerge within the scope of Internet of Things.

References

1. Amazon FPS Aggregated Payments Quick Start, https://payments.amazon.com/sdui/sdui/business?sn=devfps/aggregated
2. Anderson, C.: The Long Tail, http://www.wired.com/wired/archive/12.10/tail.html
3. Brock, D.L.: The Electronic Product Code (EPC) A Naming Scheme for Physical Objects, Auto-ID Center, http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-002.pdf
4. Chaum, D.: Blind signature for untraceable payments. In: Chaum, D., Rivest, R., Sherman, A. (eds.) Advances in Cryptology: Proceedings of CRYPTO 1982, Santa Barbara, California, USA, August 23-25, 1982, pp. 199–203. Plenum Press, New York (1983)
5. Facts and figures on GeldKarte, http://www.geldkarte.de/_www/en/pub/geldkarte/press/facts_and_figures.php
6. Haller, S., Karnouskos, S., Schroth, C.: The Internet of Things in an Enterprise Context. In: Domingue, J., Fensel, D., Traverso, P. (eds.) FIS 2008. LNCS, vol. 5468, pp. 14–28. Springer, Heidelberg (2009)
7. Lamport, L.: Password Authentication with Insecure Communication. Communication of the ACM 24(11), 770–772 (1981)
8. Micali, S., Rivest, R.: Micropayments Revisited. In: Preneel, B. (ed.) CT-RSA 2002. LNCS, vol. 2271, pp. 149–163. Springer, Heidelberg (2002)
9. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, http://bitcoin.org/bitcoin.pdf
10. Lipton, R.J., Ostrovsky, R.: Micro-payments via efficient coin-flipping. In: Hirschfeld, R. (ed.) FC 1998. LNCS, vol. 1465, pp. 1–15. Springer, Heidelberg (1998)
11. Payeras-Capella, M., Ferrer-Gomila, J., Huguet-Rotger, L.: An Efficient Anonymous Scheme for Secure Micropayments. In: Cueva-Lovelle, J.M., González-Rodríguez, B.M., Labra Gayo, J.E., del Puerto Paule Ruiz, M., Aguilar, L.J. (eds.) ICWE 2003. LNCS, vol. 2722, pp. 80–83. Springer, Heidelberg (2003)
12. Rivest, R., Shamir, A.: PayWord and MicroMint: Two Simple Micropayment Schemes. In: Crispo, B. (ed.) Security Protocols 1996. LNCS, vol. 1189, pp. 69–87. Springer, Heidelberg (1997)
13. Sherif, M.H.: Protocols for secure electronic commerce. CRC Press, Boca Raton (2004)
14. Yamabe, T., Lehdonvirta, V., Ito, H., Soma, H., Kimura, H., Nakajima, T.: Activity-Based Micro-pricing: Realizing Sustainable Behavior Changes through Economic Incentives. In: Ploug, T., Hasle, P., Oinas-Kukkonen, H. (eds.) PERSUASIVE 2010. LNCS, vol. 6137, pp. 193–204. Springer, Heidelberg (2010)
15. Wilusz, D., Rykowski, J.: Requirements and general architecture of a payment system for Future Internet. Business Informatics (24), 91–103 (2012)