Christos Solomonides and Mark Searle

An Intelligent Network-Based E-Commerce Protocol

This paper describes a protocol for electronic payments using existing intelligent network (IN) infrastructure. This is of particular benefit to network operators who already have a large investment in IN infrastructure. Through this protocol they can extend their existing billing systems to support electronic commerce (e-commerce). Users can be charged for micro-payments on their telephone bill. This way they may enjoy the benefits of having an easy, relatively accepted and recognised billing system.

Introduction

Most European and United States operators have invested heavily in intelligent network (IN) platforms to support key bearer control services such as freephone and premium rate. Such systems have complex structures for interfacing with existing billing systems that are resilient and trusted by the end users. In contrast there is still much mistrust over the security of the Internet.

Currently, many electronic payment systems require the use of a credit card. Although reported instances of fraud are rare there is still reluctance by individuals to divulge their credit card details. This framework is limiting both for end users and businesses.

The purpose of this paper is to describe a protocol for electronic payments using existing intelligent network infrastructure. This allows users to charge for micro-payments on their telephone bills. The paper firstly presents the protocol designed and simulated using Java. It then goes on to talk about the relationship between the proposed system and existing electronic payment systems. The final part of the paper presents a number of other applications where IN systems can be used in support of the Internet.

Christos Solomonides:
c.solomonides@ee.ucl.ac.uk
Mark Searle:
m.searle@ee.ucl.ac.uk
Both authors are at:
University College London,
Torrington Place,
London WC1E 7JE.

The Intelligent Network-Based E-Commerce System

The protocol allows users to perform on-line commerce, including micro-transactions, without the need for credit cards. Currently most electronic payment systems require the use of a credit card. However a lot of studies have shown that users are uncomfortable with submitting their credit card information on-line. This has been one of the most limiting factors regarding the widespread use of on-line shopping.

A restriction is imposed by the high transaction costs of credit cards. These arise because of the overheads involved in processing credit card transactions. An impracticality arises from the requirement that, in most situations, users must enter their credit card number, expiry date, cardholder name as well as their address. This is tedious, time consuming and is a deterrent for such transactions. Credit cards are therefore uneconomical and impractical for use in micro-transaction services. However such micro-transactions are common in IN services like freephone where the cost per transaction is very low to support such services.

Operators who have implemented IN infrastructures will have essentially invested in a set of interfaces to complex management systems such as billing, customer services systems etc. It is in establishing such interfaces that much of the cost of IN deployment cost is expended and such systems represent important and reusable assets.

The application described in this paper allows end users to perform on-line commerce without the limiting requirement that they must be credit-card holders. The system reuses the telephone billing mechanism, which has for the most part been accepted by, and is trusted by, end users as a means of charging end users. Three parties are involved in the system: a network operator, Internet shops and end users. The scenario is outlined as follows: a network operator is responsible for managing an Internet shopping mall. Internet shops wishing to be part of this mall must sign a contract with the network operator and reach an agreement regarding the transfer of funds from the network operator to the Internet shop. The network operator also provides end users with a small application that is used when they wish to use the system.

The framework provides some degree of protection to end users because they feel they have the protection of the intermediary party—that of the network operator. A shop can use a combination of credit card billing for larger payments or where a user is happy to divulge credit card details, and use the micro-payment system for other transactions.

The Protocol: High-Level Architecture View

The protocol is divided into two phases: a registration phase and a transaction-processing phase. During the registration phase, the identity of the end user is established and authenticated so that payments can be billed to the home telephone bill. Having passed the registration phase, end users can

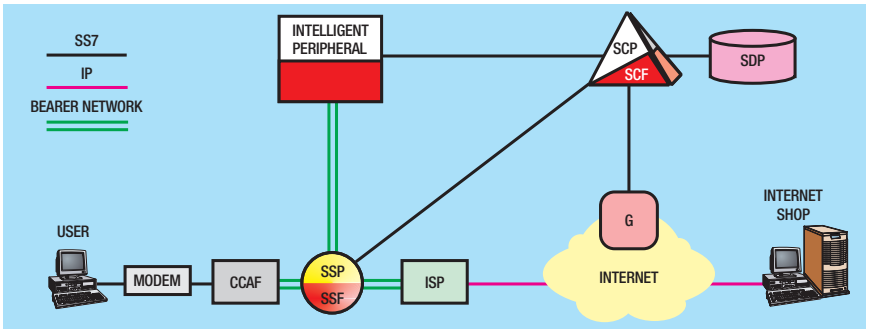


Figure 1—High-level architecture view

perform on-line transactions. The transaction phase can also be subdivided into two phases, an information interchange stage and a billing stage. Figure 1 depicts the high-level architecture view of the system. The Call Control Agent Function (CCAF) may be viewed as a terminal through which a user interacts with the network.

A key point regarding the protocol is the link between the service switching point (SSP) and the service control point (SCP). This is a Signalling System No. 7 (SS7) link, which is relatively resilient and suitable for allowing the secure identification of the user. The link between the intelligent peripheral and the SSP is used as a means of collecting information from the user. Also the final link between the gateway (G) and the SCP, which is again an SS7 link, is used for the billing phase.

An important element depicted in Figure 1 is the element between IP networks and the IN infrastructure (marked G). There are a number of possible ways for implementing such a gateway, two of which are described in reference 1. The authors take the view that the gateway should be considered as a standardised IN entity with SSP capabilities.

Registration phase

The registration phase of the protocol makes use of the existing SS7 network. During the registration phase, the user calls the Internet service provider (ISP) as depicted in Figure 2, flow 1. The number assigned to this service constitutes a service access number (SAN). The service switching function (SSF) will recognise the number as a SAN (universal access number) and will query the service control function (SCF) for call-handling support, flow 2. The SCF will then instruct the specialised resource function (SRF) to collect the personal identification number (PIN) of the user using the *PromptAndCollectUserInformation* operation[2], flows 3 and 4. The *ReceivedInformationArg* returned by the operation will then contain the PIN number entered by the user, flow 5. The SCF must now check the PIN number of the user stored in the service data point (SDF). For this, the SCF will use the 'query' operation to check for a match in the SDP, flow 6. If a correct match is made, the user is authenticated and the SCF will provide the user with a connection number, flows 7 and 8. This number is used in the final stage of the protocol for the billing.

Figure 2—User calls Internet service provider

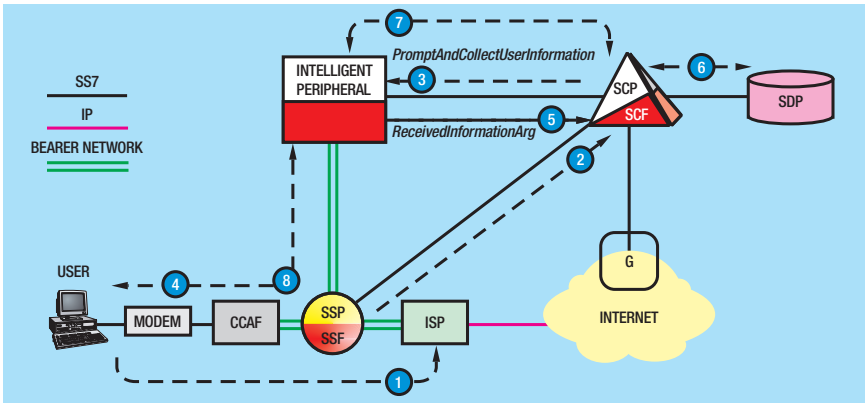
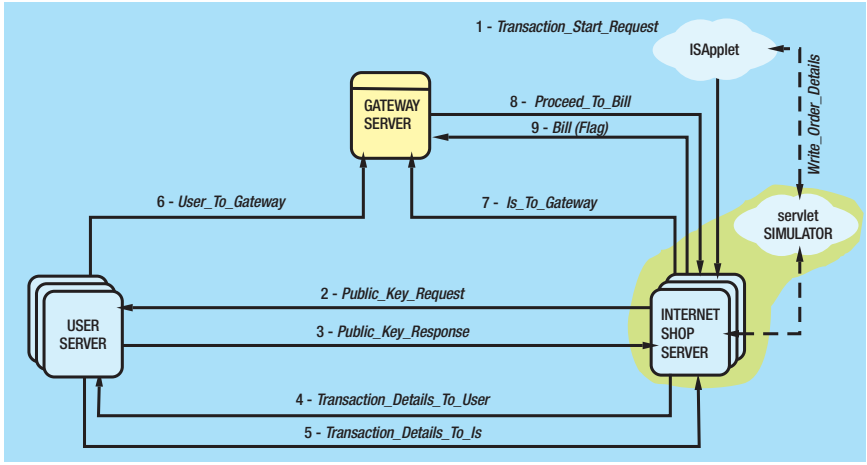


Figure 3—Protocol implementation



At this stage a user has a normal IP connection but the software on the user's machine holds a connection number, which can be used to perform the on-line transactions. When the connection is terminated, the software on the user's machine will invalidate the connection number.

A user is free to browse web pages and make selections for purchase by filling a shopping basket. The transaction phase is triggered when a user has finished making selections and wishes to place an order with the Internet shop. The user may initiate this by clicking on an icon to place the order. The transaction phase is described in the next section.

Transaction phase

The transaction phase of the protocol is depicted in Figure 3. Three servers have been set up, representing the gateway, an end user and an Internet shop (IS). The simulation was implemented in Java. For the simulation a servlet simulator was used (using a server), as the web server available did not support servlets. The shaded area in Figure 3 indicates the fact that the *servletSimulator* and the Internet shop server (ISServer) are running on the same PC. In a commercial implementation of the system, the

UserServer (UServer) is supplied to the user as part of the provided software package. The network operator is responsible for implementing the gateway server (GServer). Internet shops are required to implement their own servers, which would operate on a clean interface provided by the network operator to them.

The transaction phase is triggered when a user has finished shopping and has selected to proceed with placing the order. This causes the Internet shop (IS) Applet (ISApplet) to send a *Transaction_Start_Request* to the ISServer. The ISApplet also submits the details of the order to the ISServer using the *write_order_details* packet. This flow is not required if a servlet is running on the ISServer.

Packet 1 causes the ISServer to send a *Public_Key_Request* to the UserServer (UServer) to which the UServer replies by sending the public key. The request sent by the ISServer also contains the IP address of the IS. This is required in order for the UServer to know to which IS the reply must be sent.

The next stage is for the ISServer and the UServer to exchange information. This is achieved by the sending of packets 4 and 5. These packets contain information regarding the transaction cost, the connection number assigned by the SCP to the user during the registration phase and the unique transaction numbers generated by the IS and the user.

Having exchanged information, both parties must now submit the information to the gateway. These packets are encrypted using the public key of the network operator, which is known by all users and Internet shops. Once the GServer has received a matching pair of packets, it checks the information contained within the packets and makes sure that all the transaction details match. Another check performed by the GServer is the authentication of the ISServer as an authorised Internet shop through agreement with the network operator. This is achieved using the IP of the Internet shop, which is contained in packet 6, as well as interrogating the originating address of packet 7.

Following the correct matching of this information, the GServer will send a final *Proceed_To_Bill* message to the ISServer. The need for this packet is for the ISServer to perform a concluding check that the transaction

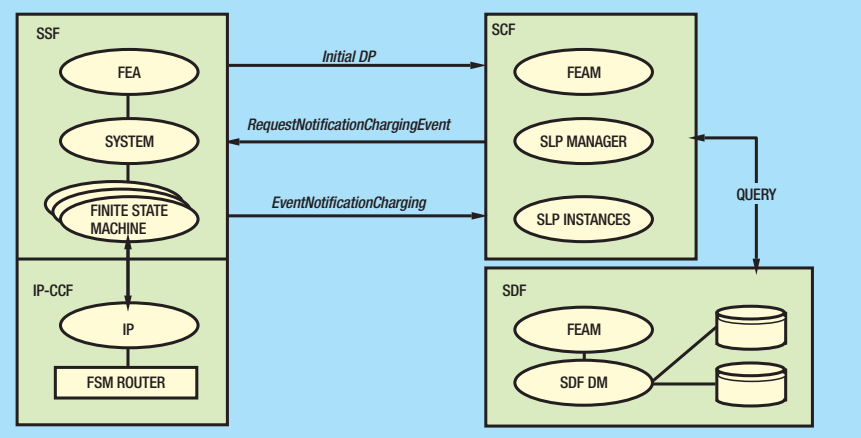


Figure 4—Billing stage of protocol

number contained within the packet is valid and allows the ISServer to check stock levels by interfacing to existing stock control systems etc. The ISServer will then reply to the GServer by returning a true/false flag to the GServer. A false flag will cause the cancellation of the transaction. A true flag will cause the protocol to move to the final stage of billing. This is discussed in the next section.

Billing stage

Figure 4 depicts the information flows and operations sent from the Gateway to the SCF in order to bill the customer. Firstly there is an *InitialDP* operation from the gateway (SSF) to the SCF. The *InitialDPArg* contains the serviceKey argument, which will be used by the SCF to trigger the service logic. The SCF will then reply by sending a *RequestNotificationChargingEvent* (after it has sent a query to the SDP). The final stage involves the gateway sending an *EventNotificationCharging* operation to the SCF to perform the billing.

Characteristics of the Protocol as an Electronic Payment System

The proposed protocol does not require an operator to make changes to the intelligent network application protocol (INAP) or SS7. Standards CS-1 information flows are used. The network operator needs to create a billing service logic script in the SCP and associated announcements and digit collection procedures in the intelligent peripheral. This should be a relatively simple procedure with a standards service creation environment.

One new functional element is required for the system, the gateway. This device allows IP-based applications to trigger SSP-like transactions. However, once implemented, the gateway can be used to support a number of new services. Much of the gateway functionality can be reused in other applications. The system also requires the end user to install billing software, which is provided by the service provider or network operator.

System security is a major issue. Password information and secure keys are transmitted over a relatively secure link and is not transported over the Internet. Clearly, the first phase of the protocol is in isolation from the Internet. However, unlike most systems, which utilise a network that is in isolation, it does not require the setting up of a complete network infrastructure. It makes use of existing SS7. The use of the SS7 network for high-value data is a concern to network operators. Currently SS7 networks are not particularly the targets of malicious intent but sending billing information can lay it open to future attack. The second phase of the protocol, which makes use of the Internet, is relatively insecure for intrusion. Hence, the use of public keys transmitted over the secure link is essential.

Currently, there is the restriction that the user can only make purchases via their own home telephone line. Hence the PIN number entered by the use identifies them with the home line. It is acknowledged that this is restrictive. Universal personal telecommunications are a set of standards for allowing user registration on any terminal; such mechanisms could be used to support the billing application in future.

Another option open to the network operator or service provider is to configure the web

browser, given to the user, so that the user is only able to surf the web pages of shops that are registered with the operator. This would reduce the risk of rogue shops pretending to be authorised shops. This would provide the user with a more secure feel for the system than if a normal 'open' browser was used. In any case, through the use of public key encryption and digital signatures the second phase is secured.

Low transaction cost

The system has a low transaction cost. This is because the on-line clearance that is required is obtained by the gateway after it requests an authorisation from the SCP. The SCP only needs to make a database enquiry in the SDP to check the credit limit of the customer before it authorises the transaction. The protocol could also be enhanced to operate as a form of a prepaid service, where the subscriber buys credit from the operator in advance and therefore further limits the need for on-line clearance.

Traceability of payments

Concerning the traceability of payments, the protocol could be adopted from conditional to user-controlled traceability. This means the user can choose whether or not his/her identity is revealed to the Internet shop. From the user's perspective to the network operator, the first phase of the protocol is classified as being unconditionally traceable (that is, the transaction generates a record that identifies the buyer, seller and the amount). This is due to the fact that the PIN number is associated with the physical connection. However, from the Internet shop's perspective the system could be classified as offering a user-controlled traceability (that is, the user can control the level of traceability). If the user is buying a service, then the system is totally user-controlled. However, if the user is buying goods then the Internet Shop needs to know the delivery address of the user. Currently the protocol offers unconditional traceability in this respect (that is, payer and payee are always identified). This can be changed and instead of the user providing the information to the Internet shop, the information could be sent to the gateway, submitted to the network operator, who in turn arranges for the delivery of the goods.

Acceptability

Concerning the acceptability (that is, the universal applicability and widespread use) of the system, it will obviously be available only to Internet shops that sign an agreement with the network operator. However, different network operators can reach agreements between them therefore allowing a wider choice to the subscriber. Of course this would require a higher communication overhead between the involved network operators, and thus slightly increasing the transaction cost of the system. At present the system does not offer transferability of funds (that is, the transfer of funds between the parties involved) and there should be no need to do so.

Comparisons with Commercially Available Systems

This system, unlike some currently available systems does not require the user to open an 'account' with each of the Internet shops. In does require the user to subscribe to the e-commerce system with the network operator/service provider. The billing account is already in place and in a sense the user is pre-vetted as an existing telephone customer. Unlike other systems it does require for the providing organisation (network operator) to form alliances and reach an agreement with each of the shops. However, since the shops themselves are not responsible for managing the per-transaction billing their overheads are very low. They also have the advantage of having a large customer base being given over to them.

Also an advantage of this system in comparison to existing ones is that it does not use credit cards and hence completely avoids the existing controversy present among the public of whether submitting credit card information over the Internet is safe or not. It could easily be marketed as a system that does not require credit cards because such systems are not secure.

IN Infrastructure and IP Services

This section presents a brief overview of two further potential applications that are being considered where an existing IN system can be used in support of the Internet. The first of these provides support for mobility through the domain name system (DNS). The SCP can treat the DNS as a service data function. Hence, since CS2 provides enhanced support for user interaction and service profile customisation the user could register a binding between the IP address and URL through the IN. Number translation services are relevant to the Internet. The DNS currently services as a resolution protocol allowing the translation of fully qualified domain names to IP addresses. In this sense the DNS is an IN platform. The difference is that the end terminal rather than the switch (SSP) interrogate the DNS. A structure such as the DNS has the potential of being an interworking function for the control of services in the Internet. In such a scenario the DNS could be used to provide personal and terminal mobility services.

The second application treats the SCP as a general certification authority. The SCP can provide access for all manner of secure information such as passwords that could be used in Internet applications.

Finally, the role of application programming interfaces (APIs) such as Parlay[3] should be acknowledged. The Parlay Organisation is a working group formed by a number of leading telecommunication companies as well as software developing organisations. Its aim is to produce an open, technology-independent and extensible API specification for access to telecommunications control equipment. Parlay is currently defining interfaces to enable third-party service providers to provide customised access to telecommunications equipment such as SCPs. Parlay interfaces are object oriented and are described using Unified Modelling Language and Interface Definition Language. The potential of Parlay and other APIs is to allow other IP-based applications to make use of existing management and control interfaces in a way that is potentially more powerful that the INAP-based solutions described in this paper.

Conclusions

This paper has presented a system that utilises existing IN infrastructure to support an e-commerce protocol. The clear advantage of this system is the incorporation of existing billing mechanisms, which are accepted by end users. In this

way, the controversy surrounding the security of credit card use on the Internet is sidelined.

This protocol nicely fits with the current trend of mergers and acquisitions between traditional PSTN network operators and Internet service providers. It can easily be used to complement the network operator's product portfolio by also providing e-commerce solutions in a manner acceptable by the end users.

References

1 SOLOMONIDES, C.; and SEARLE, M. Relevance of Existing Intelligent Network Infrastructure to the Internet, Lecture Notes in Computer Science 1597, Springer.
2 ITU-T Recommendation Q.121x Series on Intelligent Networks for CS-1, Geneva 1995.
3 Parlay API Specification—Issue 1.01. The Parlay Organisation, 14 Jan. 1999.

Biographies

Christos Solomonides
University College London

Christos Solomonides is working toward his Ph.D. in telecommunications from the Department of Electronic and Electrical Engineering, University College London (UCL). His dissertation concerns the issues surrounding the area of service creation in open networks with multi-vendor, multi-network APIs. He received his B.Eng in Software Engineering from the University of Manchester Institute of Science and Technology (UMIST) and his M.Res. in Telecommunications from UCL.

Mark Searle
University College London

Mark Searle was awarded the degrees of B.Sc. and Ph.D. at the University of Manchester Institute of Science and Technology in 1982 and 1989 respectively. He is currently involved in research and development in the area of telecommunications. He is currently engaged in a number of topics connected with Signalling System No.7, intelligent networks and the relevance of the control plane to the Internet. He is also currently the Director for the Telecommunications for Industry Programme based at UCL.