ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

SECURE MULTIPARTY ELECTRONIC PAYMENTS IN MOBILE COMPUTING

Dr.K.Ravikumar[1], A.Udhayakumar[2]

Assistant Professor & UGC-NET Coordinator, Departmet of Computer Science, Tamil University ((Established by Government of Tamil Nadu), Thanjavur-613010, India[1]

Assistant Professor, Department of computer Science,A.M.JAIN College, Meenambakkam, Chennai-600114, Research Scholar,Karpagam University,Coimbatore-641021,India[2]

ABSTRACT:

As Mobile communications become increasingly sophisticated and ubiquitous .traditional mobile billing with its implicit trust relationships Will no longer be adequate .with a large number of different sizes mobile Networks, a huge variety of value added service provider and many millions Of roaming user, it is desirable to remove any unnecessary trust in order to Increase security and provide incontestable charging. Billing allowance each Party involved in a call to eventually receive a share of the revenue generated. An examination of network billing techniques reveals a number of critical shortcomings and emerging problem. Address these issue by designing a multi-party electronic payment scheme that allows are parties involved in a Call to be paid in real-time. The mobile user releases an ongoing stream of low valued micro payment tokens into the network in exchange for the requested Services. Dynamic pricing is supported by the association of a pricing contract With the call which specifies the cost of leg of the call route. Any user with a mobile device and monetary value can use and pay for network access and services in any mobile network into which they roam. The need to authenticate the user or contact a distant home network for billing purposes. Extensions to the basic scheme provide mobile wallet functionality and allow user-to-user payments. In addition solutions are designed to cope with frequent handovers between independent piccolos, to aggregate several payment streams into one in the core network, and to inter-work with networks using legacy billing techniques. A detailed survey of micropayment techniques forms part of the design Process and a number of a new micro payment contribution result from observation made. In order to choose appropriate techniques for payment a performance comparison of micropayment schemes is presented based on benchmark measurement taken for the underlying cryptographic algorithms. The multi-party micropayment protocol is prototyped wireless environment where it is used to pay for user traffic from existing internet applications. the proposed scheme has the potential to revolution mobile communication by allowing the emergence of many independent inexpensive high speed picocell networks and by allowing any network entity to sell value added services. Mobile user will be able to select the most appropriate access network and services wherever they roam, paying all parties for resources as they are provided.

KEYWORDS: Micropayment, Multi-party, Mobile computing, Security, Authentication.

I. INTRODUCTION

CRYPTOGRAPHY:

One of the main Challenges in this area is to establish a common level of security top priorities of this frame-work is to provide method to implement secure policy negotiation. Cryptographic operations provider the developer the ability to ensure confidentiality, integrity and authenticity of message exchanged between peers. The cryptography component provides functions such as key storage and generation, asymmetric and symmetric encryption, certificate and signature validation, remote service authenticity validation and secret sharing to other components. All cryptographic algorithm (except secret sharing) are configurable and exchangeable without having a modify the source code for authentication is one of the major issues in network security.

II.SECURITY REQUIREMENTS POLICY

The security requirements will consist of confidential communication, message authentication a privacy protection, remote access logging and cryptography.Since Policies for negotiation are provided by applications installed on the bidders.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

Such as. A service is needed to allow applications to manage the policies. Multiple applications may define identical policies. Policies are unique and grouped by type. During negotiation, peers negotiate policies of each type sequentially. Table I contains example of policies for the video conference scenario given in subsection.

In the scope of this of paper, a policy describes a data structure binding attributes to values. Each policy of the same type consists of the same attributes. Each attribute is unique and has a value j £ N: $1 < J \leq 10$. For example the policy "enc video" feature the possibility the cooperate using encrypted video telephony. This provides to the user to cooperate very efficiently. As such, the value for the attribute "cooperation" is the maximum value of 10. Since the communication is encrypted, the parameter "security" also has the value 10. However, encryption and video telephony require a lot of power, hence the value for "energy saving" is 1. Here, these values are just raw estimations for the sake of demonstration but in [18] we have shown how correct values for such attributes can be determined and used. The performance of the proposed algorithm is evaluated using communication overhead and memory requirements per system for public key authentication.

III.ELECTRONIC MICRO PAYMENT SYSTEM:

PROBLEM DEFINITION:

Authentication is one of the major topics in Micro Payment System. Dynamic billing allows each party involved in a call to eventually receive a share of the revenue generated. An examination of network billing techniques reveals a number of critical shortcomings and emerging problems.

IV. NEGOTIATION

Every auction algorithm is designed and implemented in form of a separate component. The frame work defines a standardized procedure to implement new protocol based on finite state machines. These are designed using a model driven approach. Only the negotiation itself is described using this component. For calculating prizes resulting from different auction protocols and reimbursing peers the reimbursement component should be used.

The auction protocols depend on the previously on the previously described mechanism for accessing remote services. Upon initialization, bidders wait for the availability of an auctioneer. Once an auctioneer is available, all bidders try to authenticate the auctioneer using credentials based on asymmetric cryptography which bind the auction service to a verifiable identity. The credentials are provided by the auctioneer.

Once the authentication process is completed successfully. The bidders short the auctions state machine and provide an auction service to the auctioneer. This service providers access to registered policies and is furthermore used to get bids from the participate and to announce the result of an auctions. All communications between the auctioneer and the bidders confidential. In order provide message authenticity, integrity and confidentiality, a symmetric session key is exchanged between each bidders and the auctioneer using the auctioneers' credentials.

One shoot auctions, like the vickrey auctions, recover each peer to provide exactly one bid. This is a desirable property since each message exchange takes time and drains the battery of mobile devices. Other protocols, like the English or the Dutch auction, usually require significantly more messages to establish the result since multiple between rounds are conducted. These protocols are less suitable for scenarios with resource-constrain devices and limited available bandwidth.

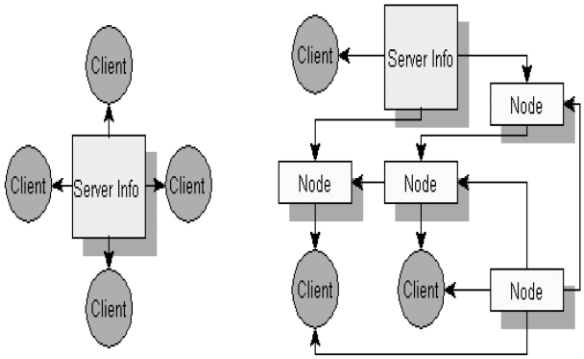

Fig.1.Relationship between client and Server node

V. USER INTERFACE

Since the result auctions is based on individual performance, support for user interfaces is required to allow applications developers using the frame work to provide user with the ability to modify the behavior and to set individual performance values. In our prototype, we integrated frontends for bidders running on mobile devices and for auctioneer, running on a normal desktop PC.While the mobile device frontends provide comprehensive interaction with the framework, the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

auctioneer frontends features rudimentary user interface to start and stop the host and to export on easily parse able history of negotiation process. These frontends have just been created for demonstration purposes and applications developers who use framework might want to provide their own GUIs or even let the negotiation run without any possibility of user interaction at all.

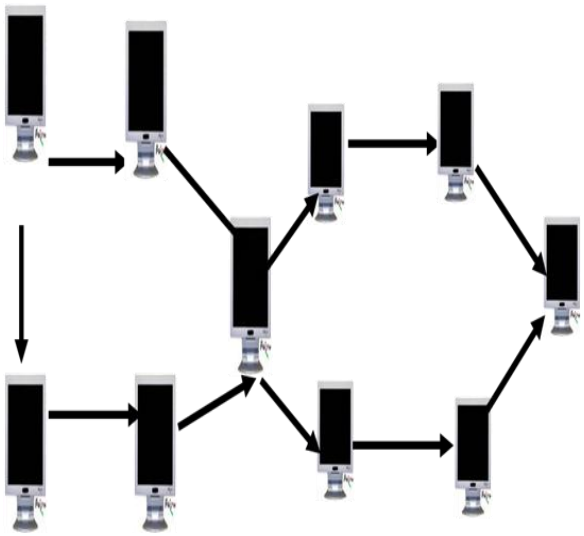

Fig.2.Social Computing and its Application

VI.ADVANTAGE OF PROPOSED SYSTEM:

Confirmation of received data

End to end delay is less

High delivery ratio

Enhance the reliability

High performance

Avoid packet collision

Reducing broadcast redundancy.

Reducing user traffic

VI.CONCLUSION

Thus the research analysis, design and implementation phase has been described for our research. We proposed framework architecture for the Secure Multiparty Electronic Payments in mobile computing in order to support self-protection in Aml scenarios. The architecture of our framework is device-and platform independent and focuses on the use of auctions protocols for electronic payments policies. The top priority was the security of the auctions. All secret information that is exchanged between the auctions host and the peers is encrypted and protected against illegitimate modifications.

To show the architecture design is sensible, we implemented a prototype for Google and for the J2SE Desktop platform. The prototype feature two parameterized auctions protocols which were designed in a model-driven way and added in form of modules to the proposed framework: an all-pay auction and a Vickrey auction protocol. Using our prototype implementation we were able to show that both protocols are suitable for a secure multi-party policy negotiation in the exemplary setting of a mobile collaboration platform. Altogether, from our experience we deem mechanism design in general and auctions in particular as a promising approach to cope with the heterogeneity of Ambient Intelligence applications.

As part of our future work, we will extend the modularity of the proposed framework in order to allow individual utility functions and a replaceable module for determining the winning policy. Further, the integration of our framework into the refinement process of semantic high-level policies is in progress.

REFERENCES

[1] G. Anthes, “mechanism design meets computer science,” communications of the ACM, vol. 53, pp. 11-13, aug.2010.

[2] V . conitzer, “making decisions based on the preferences of multiple agents,” communication of the ACM, vol. 53, pp. 84-94, mar. 2010.

[3] “OSGi ”service platform-core specification,” September. 2009. Release 4.2.

[4] P.fishpern, the theory of social choice. Princeton, NJ, USA,: Princeton univ. prees,1973.

[5] “web service policy 1.5 – framework.” W3C recommendation, September, 2007.

[6] .K.lawerence et al., “ws-sequrity policy 1.2.” OASIS, July 2007 .

[7] A.samir “ how to share a secret,” communication of the ACM, vol. 22, no 11, pp.612-613, 1979.

[8]. S. russel and p.norvig, artificial intelligence : a modern approach . upper saddle river, NJ, USA: prentice hall, 2009.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

[9] A.mases-colell, m.winston, and j. green, microeconomics theory. Oxford university press newyork, 1955.

[10] K. Drexler and m. miller, "incentive engineering for computational resource managemet," the ecology of computation, pp. 231-266, mar. 1988.

BIOGRAPHY

Dr.K.Ravikumar's Qualifications is MCA.,M.Phil.,B.Ed.,Ph.D.,UGC-NET passed.He is presented paper in 50 International and National Conferences.He is Completed UGC Research Project.He is writted 16 DDE Books in Tamil University Thanjavur.He is 12 years Teaching and Research Experience.He is having UGC-NET Coaching Co-ordinator for UGC XI Plan.His Research Areas is Network Security,Cryptography,Mobile Computing,Cloud Computing.

Mr.A.Udhayakumar received his B.Sc and M.Sc degree in computer science from the Bharathidasan University in 2003 and 2005 respectively.He received his M.Phil degree in computer science from Alagappa University in the year 2009.He is pursuing his Ph.D research in Karpagam University,Tamilnadu,India,focusing on *"Multiparty Mobile computing security"*.He joined as an Assistant Professor in the Department of computer science,A.M.JAIN college,Meenambakkam,Chennai-114 affiliated to the University of Madras Tamilnadu,India in the year 2005.He is the author/co-author for more than 10 National papers.He is the co-author of *"Elements of Computer Network"*.His papers have received a wide range of awards in the National seminars and conferences.His area of interest is in the field of *Networking security.One international Journals publishedtitled titled "Performance Analysis for Electronic payment system".*