Incentive-Based Cooperative and Secure Inter-Personal Networking

Karim El Defrawy, Magda El Zarki and Gene Tsudik
University of California, Irvine
{keldefra,elzarki,gene.tsudik}@.uci.edu

ABSTRACT

In this paper we describe a framework for enabling a "stranded" mobile user to negotiate connectivity and networking resources through another user's devices. (A "stranded" user is one who has no direct means to access a network for communication purposes or other computing services.) The entity under consideration in this paper is the Wireless Personal-Area Network (WPAN). We regard the user's WPAN as an entity that negotiates short-term contracts on behalf of the user for access services through WPANs of other users that act as bridges to locally available resources. This collaborative approach allows on-the-go users to be always connected, even in locations where their service providers offer no coverage.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]:
wireless communication, network communication.

General Terms

Design, Security.

Keywords

Personal Area Networks, always connected, security

1. INTRODUCTION

The future of networking lies in the ability to provide a communication link to anyone, anywhere, at anytime, to send or obtain information, e.g., for emergency, health, security, or entertainment services. 4th-generation networking technology does not consist of a new physical layer or a new network interface; it embodies the essence of seamless internetworking that enables the "always connected" dream. To achieve this goal we have to address two prominent challenges. First, we need to enable devices to communicate, over a multitude of interfaces and share resources within well-defined policies. Second, we have to instill trust in the end-users and offer incentives that will encourage them to cooperate in a communication infrastructure that guarantees the desired level of privacy and security. Due to the explosive growth of wireless technologies any urban area will be soon covered with at least two wireless technologies, e.g. WiFi and GSM. With the WiMAX technology already available in fixed form and expected soon with mobility support, the wireless market will continue to grow at least at the same rate.

However, access to, and use of, a particular technology normally requires the user to subscribe with a service provider that offers service with that technology. Users today are literally "stranded" if they happen to be in a location that is covered by a service provider for which they do not have a contract. Another common problem occurs when a user has a device that does not have an interface for the technology available at the current location. Dual-mode (e.g. WiFi-GSM, GSM-CDMA, WiFi-CDMA) and even triple-mode (e.g. WiFi-GSM-CDMA) devices have emerged as a solution to this problem. Although multi-mode devices may solve part of the problem, they will require the user to be registered with several service providers. Having subscription with several operators might not be economically feasible, as a user might not need more than one of these technologies most of the time. And additionally, having a multi-mode device does not always guarantee connectivity, since there are always some locations that fall outside the coverage area of the user's subscribed operators.

Today, an increasing number of users are carrying more than one device – a direct consequence of the shrinking size and decreasing cost of portable devices. Most current devices have at least one interface which can be used to establish a communication channel with another device. With this proliferation of personal portable devices, we envision a world where people have a Wireless Personal Area Network (WPAN) that facilitates seamless device-to-device communication. Active devices in a WPAN establish direct communication with each other by forming an (possibly multi-hop) ad hoc network. The composition of the WPAN undergoes changes as the owner adds, removes or de-activates personal devices. The ad hoc topology has to guarantee connectivity between devices that have an association (e.g., a cell phone and a headset) and must be power-aware, minimizing energy consumption for those devices that are battery-constrained.

Besides establishing and maintaining internal communication links, a WPAN can also have connectivity to the outside world via one or more personal device. In Figure 1, we depict an envisaged scenario of a WPAN with at least one device acting as the gateway to the outside in order to provide connectivity to the public Internet as well to the user's office, home, and vehicle networks. A personal network begins from a WPAN bubble that can be expanded and shrunk depending on the user's demands and environment.

MobiOpp'07, June 11, 2007, San Juan, Puerto Rico, USA.

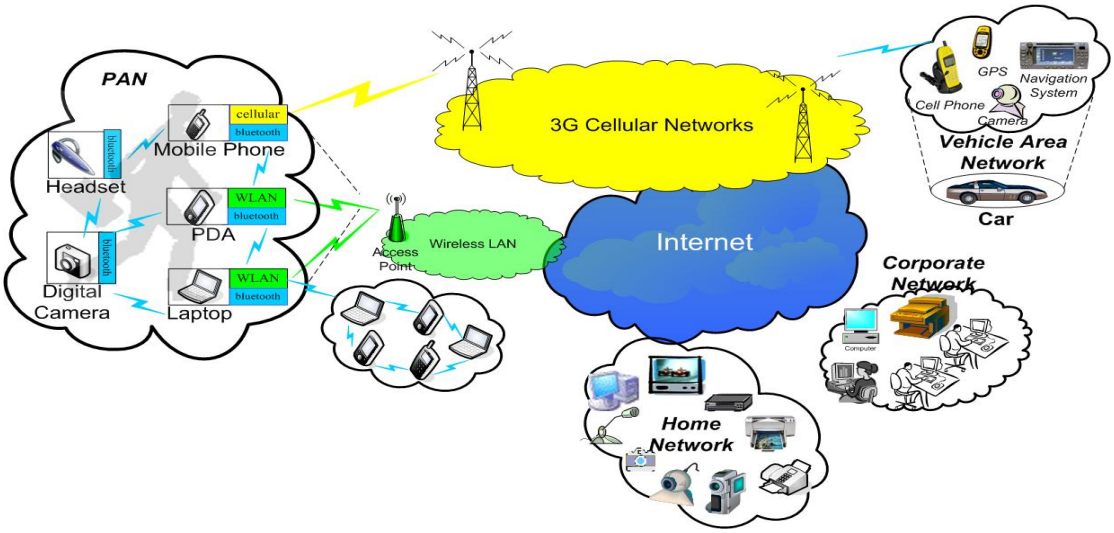

Figure 1 Hybrid Communication Environment

Situations where a user is unable to find a suitable interface for external connectivity are not uncommon. One example setting is an airport where a user's WPAN consists of a cell phone and a Bluetooth-enabled laptop with WiFi (IEEE 802.11). The only local communication service is a cellular network for which the user has no subscription. However, another nearby user does have cellular service. This second user's WPAN can act as a relay and allow the first user to gain external connectivity. Some issues arising in this context have already been addressed in prior work such as power consumption of relay devices, connection parameters – maintaining QoS. Whereas other issues are new and have not been considered before:

- *Cooperation with incentives*: why would User B want to help User A? What are the usage policies of the service being provided?
- *Security and anonymity*: Can the users trust each other? What guarantees does a user have that it will be rewarded/paid for cooperation? How private will the transmission be for a user? How safe is a user WPAN from malicious acts committed by another user?
- *Mobility*: How to ensure seamless and uninterrupted service as either (or both) user(s) moves?

In this paper, we suggest a framework to enable integrative solutions that hide the underlying networking technologies from the end-user who only needs to provide ownership in conjunction with usage policies. The premise is that any user can opt to "sell" (or barter) unused bandwidth and services to other users. We believe that this can markedly improve ubiquitous connectivity and Internet access. Enabling users to exchange services directly, securely and efficiently will also lay the ground for a new flavor of peer-to-peer applications in the wireless market.

2. FRAMEWORK OVERVIEW

The envisaged framework should enable devices in one WPAN to coordinate their efforts to dynamically select the best current gateway to provide outside connectivity. This connectivity should be negotiated under requirements specified in the user's (owner's) policy for the WPAN. Once the gateway is selected, it should be responsible for negotiating with other WPANs' gateways in the vicinity and selecting the best-suited among them. The framework should allow anonymous communication, if desired by the WPAN owner. At the same time, there has to be an incentive for users to provide connectivity and services to others. We propose using a secure micro-payment scheme as a means of paying for opportunistic connectivity. Micro-payments will ensure that, if a user does not provide negotiated service or provides unsatisfactory service, the other party can quit the contract with minimal damage. Issues, such as power management and QoS, of course, have to be taken into consideration when negotiating services and in all algorithms comprising the framework. Also, users should be able to easily cash in collected micro-payments at their service providers (at a later time). We intend for the framework to incorporate the means for both non-repudiation and accountability for all transactions, to ensure secure and robust operation.

2.1 Proposed Framework Operation

In our framework, A WPAN starts negotiating with another WPAN to obtain connectivity such that respective requirements of both users (specified in their policies of use) are satisfied. This first requires coordination between devices inside each WPAN to exchange information about their interfaces and available peer-providers on these interfaces. A collective decision is then made about which interface to use to connect to which peer-provider. Exchange of (public key) certificates is carried out next, to enable mutual authentication and establishment of trust metrics. Once the contract between the customer and peer-provider is negotiated, the micro-payment algorithm is initiated in order to pay for the obtained service from peer-provider.

2.2 Related Work

This section describes related work in the literature. The MOPED project in [1] [2] [3] [4] focuses on enabling several devices belonging to the same user to coordinate obtaining always-best connectivity. This project developed successful methodologies and algorithms for solving this problem. The work in [5] introduces the concept of a personal router (PR). A PR is responsible for connecting a user's WPAN to the Internet and negotiating service; it handles all issues regarding outbound Internet connectivity. While this project successfully addressed several issues such as

policy and security, its two main shortcomings are: (1) single point of failure (PR) and (2) requirement for an additional device (again, PR).

Other proposals [6] [7] [8] [9] [10] [11] [12] address the challenges of having several networks join and deliver services to each other. We can view our framework as a general case of this concept. One of the goals is to allow the WPANs of two different users to collaborate together and provide additional functionality to each of the users. The proposals above are still at early stages of developing requirements and identifying important issues for successful operation.

In [18], a so-called Mobile Bazaar (MoB) framework is developed to allow collaborative networking between users based on incentives. MoB is an open market architecture where mobile users opportunistically and flexibly trade various services. MoB uses a payment system to manage resource trades. However, MoB supports only a single device per user [18] since its main focus is on a user having only one device and getting all service through this device. In other words, MoB does not handle our key scenario of a whole WPAN obtaining service from another WPAN. (MoB can be viewed as a special case of our approach). The open market in MoB is implemented in a "laissez faire" mode with no control or regulations over advertised services and their corresponding prices. In order to enable such a market the MoB system requires: (1) a reputation and trust management system, and (2) a billing and accounting system. MoB assumes that both are implemented in a centralized fashion by a third party. In contrast, our proposal takes the MoB concept a step further by applying it to a multi device environment.

In [26, 27] the authors describe a hybrid (e.g. between ad-hoc and infrastructure based) architecture called MobiShare that enables mobile devices to share their data encapsulated in services. MobiShare provides a middleware system and an infrastructure architecture that will act as a service distribution network for the middleware by offering ubiquitous connectivity to mobile devices. The work in [26, 27] focuses on a single device and does not take into account the fact that a WPAN should be regarded as one entity. Also they mainly discuss exchanging information and resources at the application level. [26, 27] also does not address any of the security issues arising in such a system. It requires each mobile device to have a GPS receiver and a Digital Compass for capturing orientation that imposes great restrictions on the devices that could use the system.

Another related project [23] proposes a system to enable sharing of WLAN resources among residential hotspots. The system utilizes a token-based incentive mechanism to prevent free-riding and encourage participation. Its focus is on fixed WLANs and it considers only single devices. As evident from the overview of related work, some of the problems that exist in our proposed framework were addressed in other similar contexts. Currently, there is no complete solution that enables two WPANs to communicate and exchange services in a secure manner.

3. FRAMEWORK COMPONENTS

This section describes some key components of our framework related to security and privacy of users.

3.1 Secure Transactions with Escrowed Anonymity

A key factor in our envisaged framework is the ability of an entity (customer) to verify that the other party (trader) in the transaction is legitimate/authentic, and vice versa. At the same time, entities need to remain anonymous in the course of such transactions. Moreover, in case of a dispute, there must be a means to reveal the identity of one or both parties. This is already the case in a growing number of transactions performed on the Internet [22].

One way to address these requirements is to use an advanced cryptographic construct called "group signatures" [19]. Group signatures are a powerful and versatile tool in the arsenal of privacy-preserving cryptographic techniques. Anonymity provided by group signatures is escrowed since, in exceptional cases, a valid group signature can be ``unlocked'' by a special trusted entity (called a Group Manager) and the identity of the real signer can be obtained.

An important requirement for (and benefit of) using group signatures is that some schemes allow adding new members to the group without any changes to the underlying (common) group public key which is used to verify group signatures. Efficient group signature schemes ([20], [21], [29]) have been proposed recently. In these schemes, the group public key and group signature sizes do not depend on the number of members in the group. We propose using one of these schemes for our system to be scalable and dynamic. Furthermore, some schemes (e.g., [30] and [31]) allow for very efficient revocation of group members.

As pointed out in [32], a number of research challenges remain in the context of group signatures. In particular, there is precious little practical "systems" experience with group signature schemes, especially, when it comes to integrating them with applications. Although group signature schemes gradually become more and more efficient, experience with other advanced cryptographic primitives shows that there is usually a very large gap between claimed "theoretical" performance and actual performance measured in realistic experimental settings. Therefore, one of our goals is to implement and experiment with, several cutting-edge group signature schemes and thoroughly investigate the implications and side-effects of their deployment.

A related issue is that little is known about the inter-operability or co-existence of multiple groups and multiple group signature schemes. With the exception of Idemix [33] (which somewhat addresses the former), there has been no progress in moving group signatures towards real-world acceptance. Since our proposed framework is heterogeneous in nature, multiple groups and multiple group signature schemes are, unavoidably, part and parcel of the overall architecture.

3.3 Authentication, Access Control and Policies

In more practical terms, we expect each WPAN owner (user) to have a smart card or a fob which stores the group public key certificate and the user's group private key. Once attached to any of the WPAN devices, all other WPAN devices are seamlessly able

to use it for authentication purposes. When two users start negotiating connectivity service, the gateway devices in both WPANs exchange their respective group public key certificates (again, recall that these are common for all members of a particular group).

Once a user gets connectivity through another user's (trader's) WPAN, there needs to be some access control to prevent malicious activity inside the trader's WPAN. Also, while service is being provided, we need to support (at least) two traffic classes for the traffic originating from one WPAN. We anticipate having two profiles for each user: a normal profile (for itself) and a guest profile. The guest profile has limited privileges. When a user A negotiates service with another user B, it uses the guest profile in transmitting user B's traffic to the service provider. User A, on the other hand, should be able to use all privileges in his profile. We need a way to distinguish between the traffic from user A and B, which, from the perspective of the service provider's network and beyond, both originate at A.

Using policies to govern access control decisions is not a new concept. For example, some similar issues were considered in the early 90-s in Internet Policy Routing research [34]. Nevertheless, our environment exhibits a much greater diversity of devices and users (e.g., Policy Routing considered policies expressed by organizations) that will very likely translate into a commensurately greater diversity of policies. The Personal Router project [5] addressed similar issues, but, due to the differences in approach, we need to extend this work to capture new requirements imposed by our framework. Some concrete policy-related issues that must be addressed are as follows:

- How does the user formulate and enter the policy for a device? Locally, on each device, or, should the user have a "master device" that manages all policies for the entire WPAN?
- How do policies get transmitted to different devices and how does a change or malfunction in a device affect the policy and the overall operation of the WPAN?
- What factors should policies be based on? Services, application, network or devices?
- What are the different requirements that users will need to specify in their policy and what are the factors that will affect these requirements?
- Should user policies be static or dynamically adaptable to the changing environment and the current status of the devices in the WPAN?

3.4 Billing and Reputation Management

The problem considered in our proposal has different requirements than the traditional case of peer-to-peer systems in where peers exist (persist) for a relatively long time in the network and, once they are "up", establish relatively long-term relationships with their neighboring peers. Our case is significantly different, because we are considering the existence of a peer in an unfamiliar environment for short periods of time, due to mobility and intermittent connectivity. Peers need to be able to establish trust relations with the neighbors in a distributed manner, as fast and as efficiently, as possible. Such issues have not been addressed so far, and, we believe that they are much more challenging than those in traditional peer-to-peer systems.

Another issue arising in the context of our framework is billing. Several questions have to be answered in order to design a scalable and efficient billing scheme, which is cheat-proof and provides cooperation incentives for users. We anticipate using micro-payments – in conjunction with group signatures, which is something that has not been attempted before – among users exchanging connectivity services. The use of micro-payments would allow the users to avoid fraud and misbehaving traders (who fail to provide promised service) while minimizing "monetary" losses. Having micro-payments collectable from the service provider, would also give an incentive for users to engage in our system and offer connectivity to other users. Of course, the service providers would also have to be somehow involved in the whole system to allow (and perhaps even encourage) their customers to re-sell connectivity. This could increase the revenue and utilization of service providers, because visiting users who did not have the chance to use its network before will now be able to use it indirectly through regular customers. This translates into greater service penetration for the service providers.

4. CONCLUSION

With the increased mobility of users and their personal gadgets and the plethora of access technologies, we will see a move to peer to peer style communication sharing. Users will be given incentives to share their local resources and access links to allow for an "always" connected universe, one in which no one will be left stranded due to interface/technology mismatch or unavailability of service. In this paper we outlined a framework that would provide a secure and reliable environment for the sharing and bartering of access services and computing resources.

REFERENCES

1. R. Kravets, "Moving from Mobile Hosts to Mobile Networks," Department of Computer Science, University of Illinois, Urbana Champaign, Technical Report UIUCDCS-R-2000-2166, 2000.
2. R. Kravets, C. Carter and L. Magalhaes, "A Cooperative Approach to User Mobility," ACM Computer Communications Review, vol. 31, 2001.
3. C. Carter and R. Kravets, "User Devices Cooperating to Support Resource Aggregation," 4th IEEE Workshop on Mobile Computing Systems & Apps (WMCSA02), 2002.
4. C. Carter and R. Kravets, "Contact Networking: A Localized Mobility System," ACM MobiSys 2003.
5. David D. Clark and John T. Wroclawski, "The Personal Router Whitepaper," MIT Laboratory For Computer Science, Technical Report, March 2001.
6. V. Typpö, J. Eisl, J. Höller, R. Aguero Calvo and H. Karl, "Research Challenges in Mobility and Moving Networks: An Ambient Networks View," Workshop on Challenges of Mobility 2004, Toulouse, France.
7. C. Kappler, P. Mendes, C. Prehofer, P. Pöyhönen, Di Zhou, ``A Framework for Self-organized Network Composition,'' IFIP Workshop on Autonomic Communication, 2004, Berlin, Germany.

8. R. Campos, C. Pinho, M. Ricardo, J. Ruela, P.i Pöyhönen, C. Kappler ``Dynamic and Automatic Interworking between Personal Area Networks using Composition,'' The 16th Annual IEEE Int'l Symp. on Personal Indoor and Mobile Radio Communications, Berlin, Germany.
9. F. Berggren, A. Bria, L. Badia, I. Karla, R. Litjens, P. Magnusson, F. Meago, H. Tang, R. Veronesi , ``Multi-Radio Resource Management for Ambient Networks,'' The 16th Annual IEEE Int'l Symp. on Personal Indoor and Mobile Radio Communications, Berlin, Germany.
10. H.Lach, C.Janneteau and A.Petrescu, ``Network Mobility in. Beyond-3G Systems,'' IEEE Communication Magazine, pp.52-57,. July 2003.
11. N. Niebert, A. Schieder, H. Abramowicz, G. Malmgren, J. Sachs, U. Horn, C. Prehofer, H. Karl, ``Ambient Networks – An Architecture for Communication Networks Beyond 3G,'' IEEE Wireless Comm. (Special Issue on 4G Mobile Communications – Towards Open Wireless Architecture).
12. Norbert Niebert, Hannu Flinck, Robert Hancock, Holger Karl, Christian Prehofer, ``Ambient Networks–Res. for Comm. Nets Beyond 3G,'' IST Mob. Summit, June 2004.
13. David D. Clark , Karen Sollins , John Wroclawski , Ted Faber, ``Addressing reality: an architectural response to real-world demands on the evolving Internet,'' Proc. of the ACM SIGCOMM workshop on Future directions in network architecture, 2003.
14. Rajiv Chakravorty, Suman Banerjee, Sulabh Agarwal, Ian Pratt, ``MoB: A Mobile Bazaar for Wide-area Wireless Services,'' ACM Mobicom, 2005.
15. D. Chaum and E. van Heyst,``Group signatures,'' In D. W. Davies, editor, Advances in Cryptology — EUROCRYPT '91, volume 547 of Lecture Notes in Computer Science, pages 257–265. Springer-Verlag.
16. Giuseppe Ateniese, Jan Camenisch, Marc Joye, and G. Tsudik, ``A practical and provably secure coalition-resistant group signature scheme.'' In Mihir Bellare, editor, Advances in Cryptology – CRYPTO 2000, vol 1880 of Lec. Notes in Comp Sci, Springer, 2000.
17. Dan Boneh, Xavier Boyen, Hovav Shacham, ``Short Group Signatures,'' CRYPTO 2004.
18. M. S. Blumenthal and D. D. Clark, ``Rethinking the design of the Internet: The end-to-end arguments versus the brave new world,'' ACM Trans. Internet Techn, vol. 1, no. 1, Aug. 2001.
19. E.C. Efstathiou and G.C. Polyzos, ``Designing a Peer-to-Peer Wireless Network Confederation,'' Proc. IEEE Workshop on Wireless Local Networks (WLN 2003), Bonn, Germany, Oct. 2003.
20. E. C. Efstathiou, P. A. Frangoudis and G. C. Polyzos, ``Stimulating Participation in Wireless Community Networks,'' IEEE INFOCOM 2005.
21. E. C. Efstathiou and G. C. Polyzos, ``Fully Self-Organized Fair Peering of Wireless Hotspots,".
22. C. Ververidis, S. Valavanis, M. Vazirgiannis, and G.C. Polyzos, ``An Architecture for Sharing, Discovering and Accessing Mobile Data and Services: Locations and Mobility Issues,'' Proc. LBS Workshop, Mykonos Island, Greece, Oct. 2002.
23. E. Valavanis, C. Ververidis, M. Vazirgianis, G.C. Polyzos, and K. Nørvåg, ``MobiShare: Sharing Context-Dependent Data and Services from Mobile Sources,'' Proc. IEEE/WIC Int'l Conference on Web Intelligence (WI 2003), Halifax, Canada, Oct. 2003.
24. M. Weiser, ``Ubiquitous Computing", IEEE Computer "Hot Topics", October 1993.
25. A. Kiayias and M. Yung,``Group Signatures with Efficient Concurrent Join,'' IACR EuroCrypt'05, 2005.
26. J. Camenisch and A. Lysyanskaya, ``Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credential,'' IACR Crypto'02, 2002.
27. G. Tsudik and S. Xu, ``Accumulating Composites and Improved Group Signing,'' IACR AsiaCrypt'03, 2003.
28. G. Ateniese and G. Tsudik., ``Group Signatures,'' Contributed Chapter in: "Cryptographic Protocols: Techniques for Secure Protocol Design.'' February 2006. Prentice Hall.
29. J. Camenisch and E. Van Herreweghen, ``Design and Implementation of the Idemix Anonymous Credential System,'' In ACM CCS 2002, November 2002.
30. D. Estrin, M. Steenstrup and G. Tsudik ``A Protocol for Route Establishment and Packet Forwarding Across Multidomain Internets.'' IEEE/ACM Transactions on Networking 1(1): 56-70 (1993).