

# Fuelling WiFi deployment: A reputation-based solution

Naouel Ben Salem<sup>1</sup>, Jean-Pierre Hubaux<sup>1</sup> and Markus Jakobsson<sup>2</sup>

<sup>1</sup> Laboratory of Computer Communications and Applications (LCA)  
Swiss Federal Institute of Technology Lausanne (EPFL)  
Switzerland\*\*

[naouel.bensalem@epfl.ch](mailto:naouel.bensalem@epfl.ch), [jean-pierre.hubaux@epfl.ch](mailto:jean-pierre.hubaux@epfl.ch)

<sup>2</sup> RSA Laboratories, 174 Middlesex Turnpike, Bedford, MA 01730, USA  
[mjakobsson@rsasecurity.com](mailto:mjakobsson@rsasecurity.com)

**Abstract.** The rapid growth of WiFi over the past two years reveals the willingness of the Wireless Internet Service Providers (WISPs) to develop this technology and the interest of the users in this new service. However, the lack of unified roaming slows down the deployment of this kind of networks. In this paper, we present a simple solution that allows a mobile node to connect to a hot spot managed by a WISP in a secure way while preserving its anonymity. We use a reputation-based system to discourage the WISPs from providing a bad quality of service to the mobile nodes. We will show that all the parties are motivated to behave correctly, that our solution thwarts rational attacks, that it is possible to detect malicious attacks and, in some case, identify the attackers.

## 1 Introduction and problem statement

Wi-Fi networks have a very strong potentiel: They are easy to deploy, they use free spectrum frequencies and they allow the users to have an Internet connection that is several times faster than any cable modem connection. Furthermore, the equipment is inexpensive (typically \$100 for an access point and less than \$50 for a receiver) and the use of the network is very simple (typically plug and play).

Thousands of hot-spots are already deployed in cafes, hotels and airports to attract business travellers and Internet addicts; more and more companies are entering the business (e.g., start-ups like Boingo Wireless[1], Wayport[2], ... or well-established companies like T-Mobile[3]).

However, the lack of interoperability between Wireless Internet Service Providers (WISPs) is an obstacle to the deployment and success of WiFi networks<sup>3</sup>: A client that has an account with a provider *A* cannot connect to a hot spot managed by a provider *B*. This situation is prejudicial to the clients and to the future of WiFi because it particularly discourages small WISPs (i.e., with few hot spots) from entering the business and allows large WiFi companies to monopolize the market and bias the competition.

The goal of the work presented in this paper is to present a simple solution that (i) encourages network usage by mobile nodes; (ii) encourages good quality of service (QoS) provision; (iii) encourages further network deployment; and (iv) minimizes (human) user involvement<sup>4</sup>.

In our solution, we use a reputation mechanism to discourage the WISPs from providing a bad QoS to the mobile nodes. We also use a micropayment scheme to make sure that the mobile nodes pay for the service they received. We can easily show that our solution motivates all the parties to behave correctly (i.e., according to the set of protocols). This work was carried out in the framework of the MISC/Termindes research program [4].

---

\*\* The work presented in this paper was supported (in part) by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005 – 67322

<sup>3</sup> Details about the roaming problem are in Section 2

<sup>4</sup> This involvement should be limited to setting up a few parameters at initialization of the device. Furthermore, roaming should be seamless.

## 2 State of the art

**Reputation-based systems:** Also called feedback or recommendation mechanisms [5], they are mainly used to build trust and foster cooperation among a given community. The efficiency of reputation mechanisms have been widely studied in various fields and with different approaches. Studies such as [6–8] consider the effect of *online* reputation systems [9] on e-marketing and trading communities like e-Bay. Reputation mechanisms are also used to foster cooperation in peer-to-peer networks [10] or in ad hoc networks [11, 12].

But, from all these studies, we cannot draw a clear conclusion about the efficiency of reputation systems; each of these mechanisms should thus be analyzed on a per-case basis.

**Roaming in WISPs:** The deployment and success of WiFi networks is slowed down by the lack of interoperability between WiFi providers (also called *fragmentation* problem [13]): A client that has an account with a WISP  $A$  cannot connect to a hotspot managed by a WISP  $B$ . However, the situation is changing and more and more WISPs are establishing roaming agreements (similar to what is done for GSM). The roaming can be between providers within the same country (e.g., *SFR*, *Orange* and *Bouygue* in France) or international (e.g., between the British *BT* and the American *Airpath*).

Another solution would be to use the service of a *WiFi roaming operator* like *Boingo Wireless* [1]. Such an operator tries to solve the roaming problem by having agreements with as many WISPs as possible. Then it aggregates all the hot spots managed by these WISPs into a single (seamless) network. However, the problem remains the same if a Boingo client tries to connect to a hot spot managed by a WISP that has no agreement with Boingo Wireless: This solution thus attenuates the effect of the fragmentation problem but do not solve it.

In [14], Patel and Crowcroft propose a ticket based system that allows mobile users to connect to foreign service providers: The user contacts a *ticket server* to acquire a ticket, requests a service from a *service server* and uses the ticket to pay for that service. However, unlike the solution we present in this paper, the authors do not question the honesty of the service providers i.e., they assume that the service providers provide the users with a good quality of service, which is far from been guaranteed in WiFi networks.

## 3 System model

In this paper, we consider a mobile node  $MN$  that is affiliated with a home network  $H$  and that wants to connect to the Internet via a hot spot managed by a wireless Internet service provider  $W$ .  $MN$  has an account with  $H$ , shares a secret key  $k_{HM}$  with it and fully trusts it for manipulating its account.  $H$  also shares a secret key  $k_{HW}$  with  $W$ .

We assume that all the messages exchanged between  $MN$  and  $H$  go through  $W$  and that the backbone is a commodity; the rewarding of the backbone operator would follow already established practices and techniques, and is not addressed in this paper (a flat rate subscription, probably).

In this paper, we present a reputation based mechanism that encourages the WISPs to behave correctly (i.e., to provide the  $MNs$  with a good QoS). The reputation mechanism is maintained by a trusted central authority we denote by  $TCA$ <sup>5</sup>. The details about the reputation system are in Subsection 3.2.

### 3.1 Adversarial model

In this paper, we assume that:

- $H$  and  $TCA$  are trusted by the other parties for all the actions they perform<sup>6</sup>.
- $W$  is rational and therefore it cheats if there is some gain from misbehaving.
- $MN$  may be malicious and therefore it can cheat even if there is no gain from misbehaving. This implicitly assumes that  $MN$  can also perform rational attacks.

Confidentiality of data is not an issue in our case, so we do not consider passive attacks where the attacker eavesdrops the data exchanges between two parties. Note that this is an orthogonal issue that is easily addressed using standard techniques.

<sup>5</sup> In a “grassroots” vision, the  $TCA$  would be a federation of WISPs, who join forces to centralize a few strategic functions. In a more conventional vision, the  $TCA$  can be under the control of a world-wide organization much as a quality control company (e.g., SGS), a certification company, or a global telecommunications operator.

<sup>6</sup> Even if  $H$  is itself a WISP, it only plays the role of a home network in our model.

We exclusively consider attacks performed against the different phases of our protocols, meaning that we do not consider other arbitrary attacks like DoS attacks based on jamming for example. Several attackers can collude and share information to perform more sophisticated attacks.

In this paper, we want to study the effect of rational and malicious attacks on our set of protocols. Our goal is to make sure that the set of protocols we propose thwarts rational attacks (i.e., an attacker gains nothing from cheating), detects malicious attacks and, if possible, identifies the attacker.

### 3.2 Reputation model

The behavior of each WISP in our model is characterized by what we call a *reputation record*. This record represents an evaluation of the reputation of the WISP and is generated and signed by *TCA*. When a WISP first enters the network, *TCA* provides it with an *initial reputation record* that can afterwards increase (i.e., better reputation) or decrease, depending on the behavior of the WISPs.

If *MN* has two neighboring WISPs that propose equivalent offers, i.e., same QoS and price (see Subsection 4.2), *MN* will choose to connect to the access point managed by the WISP that has the best reputation record.

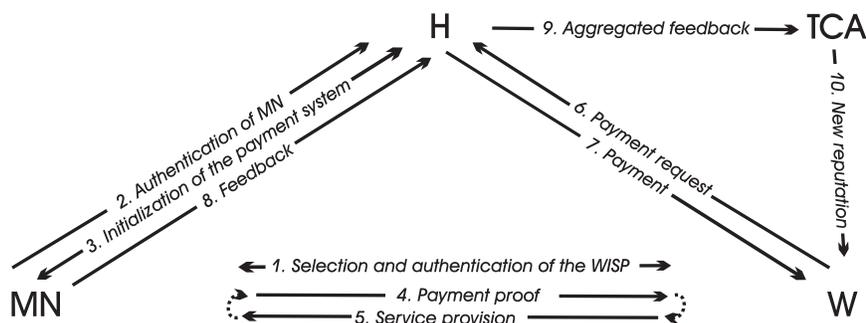
## 4 Proposed solution

### 4.1 Notation

In this paper, we call *Session* the period during which the WISP provides the service and *MN* pays for it. A session is subdivided into *periods*<sup>7</sup>. We also call *Reputation update time* the point in time at which *TCA* stops receiving reputation information from the *Hs* (see Subsection 3.2), updates the reputation records and informs the WISPs about their new records. The new records are valid until the next reputation update time.

### 4.2 Rationale of the solution

In this Subsection, we present the details of our solution (see Figure 1).



**Figure 1.** The proposed solution. The mobile node *MN* wants to connect to the internet via a hot spot managed by the WISP *W*. *H* is a home network with whom *MN* is affiliated. The trusted certification authority *TCA* is in charge of maintaining the reputations of the WISPs.

**Selection and authentication of the WISP:** *MN* scans the spectrum and identifies the different WISPs available in the neighborhood. Each WISP generates an offer containing (at least) its current *reputation record*, the quality of service (QoS) it proposes (e.g., expressed in Mb/s), the price it asks for, its public key and the corresponding certificate. The WISP signs the offer and sends the offer and the signature to *MN*.

Then *MN* collects this information and determines the WISP that proposed the best offer. The decision making should be done by a software agent at the mobile node to automate the process and

<sup>7</sup> This implicitly implies that the payment frequency depends on time, but it can depend also on the amount of information exchanged between *MN* and *W*.

avoid human involvement except if necessary (e.g., setting up parameters like the maximum price  $MN$  is willing to pay for the service, the minimum QoS it would accept, ...). This choice should also depend on the application  $MN$  wants to run (e.g., if  $MN$  wants to chat, it will probably choose the WISP offering the lowest price, whereas it would choose the offer with the best reputation record and QoS for an online payment application). More sophisticated schemes (e.g., auctioning) can be envisioned to select the WISP.

Then,  $MN$  verifies the certificate of the WISP that proposed the best offer. If the verification is incorrect,  $MN$  checks the second best offer and so on. We call  $W$  the so chosen WISP.

**Authentication of  $MN$ :** Before beginning the service provision,  $W$  has to make sure that  $MN$  is a valid mobile node that is registered with a valid and well-established home network  $H$ . As we want to preserve the anonymity of  $MN$ , the verification of the identity of  $MN$  will be done by  $H$ .

We use in this paper the following authentication mechanism that is commonly used in industry (e.g., SecurID [15]): When a mobile node  $MN$  registers with a home network  $H$ , the two parties share a random seed  $s$  that represents the input to a pseudorandom generator. The output is a random number  $tag$  that is 30 to 50 bits long.  $H$  keeps a small window (e.g., 50 entries) of upcoming tags for each mobile node.  $H$  maintains the couples  $(tag; node's\ identity)$  in a sorted database.

Upon reception of a given  $tag$ ,  $H$  searches its database, retrieves the couple  $(tag; identity)$  and identifies  $MN$ . In case of collision (i.e., more than one couple contains the random number  $tag$ ),  $H$  asks  $MN$  to send the next tag value.

$H$  can then identify  $MN$  and respond positively to the identification request of  $W$ . By doing so,  $H$  takes the responsibility of what  $MN$  will do during the session. In case of problems,  $H$  can retrieve the identity of the user and, if needed, sue him.

**Initializing the payment system:** The credit-based micro-payment scheme we use in this paper is highly inspired from the PayWord scheme [16]: During the session setup,  $H$  generates a fresh chain of paywords  $w_1, w_2, \dots, w_n$  by choosing  $w_n$  at random and by computing  $w_i = h(w_{i+1})$  for  $i = n-1, n-2, \dots, 0$ , where  $h$  is a one-way hash function and  $n$  is the maximum number of payments that  $MN$  can send to WISP during the session. The root  $w_0$  of the payword chain is not considered to be a payword itself.

Then,  $H$  generates a commitment to this payword chain, which contains (at least)  $w_0$  and  $w_n$ , encrypts it using the key  $k_{HM}$  it shares with  $MN$ , and sends it to  $MN$ .  $MN$  can then regenerate the payword chain and use it during the session (see Subsection 4.2).  $H$  also encrypts  $w_0$  using the key  $k_{HW}$  it shares with  $W$ , and sends it to  $W$ .

**Service provision and payment:** First of all,  $MN$  and  $W$  agree on a symmetric session key  $k_{MW}$ . They will use that key to secure all the messages they exchange during the session (e.g., compute a MAC on these messages).

The session is subdivided into *periods*. During the  $t$ -th period,  $MN$  sends to WISP the  $t$ -th PayWord  $w_t$  encrypted with the symmetric key  $k_{MW}$ .  $w_t$  represents the  $t$ -th payment and WISP can verify its the validity by checking that  $h(w_t) = w_{t-1}$ , where  $h$  is the one-way hash function used by  $H$  to generate the chain. If the verification of the payment is correct,  $W$  provides  $MN$  with the  $t$ -th part of the service.

In our protocols, we use a payword system to allow the off-line verification of the payments by WISP. The paywords are payment authorizations that  $W$  will later send<sup>8</sup> to  $H$  to get paid for the service it provided. If  $MN$  stops sending the payment authorizations,  $W$  will also stop the service provision and the session is ended. If there is a packet loss the payment or the service is just resent.

**Sending the payment request:** At the end of the session,  $W$  sends to  $H$  the latest hash value  $w_\ell$  it received from  $MN$  and the number  $\ell$  of provided services.

Then,  $H$  verifies the validity<sup>9</sup> of  $w_\ell$ , rewards  $W$  for the  $\ell$  parts of the service, and charges  $MN$  for them.

<sup>8</sup> In the PayWord scheme, only the latest payword is sent to  $H$ . Details are in Subsection 4.2

<sup>9</sup> This verification can be optimized by using techniques like [17]

**Sending the satisfaction level to  $H$ :** At the end of the session,  $MN$  sends<sup>10</sup> to  $H$  (via  $W$ ) a report on its satisfaction level. For the sake of simplicity, we assume that this report is a binary variable that corresponds to 1 if the QoS received from  $W$  corresponds to what  $MN$  and  $W$  agreed on, and to 0 otherwise. The absence of feedback counts as bad feedback: Since  $H$  knows that a session was started (due to the account verification) it would know if the feedback is missing. This is to avoid that  $W$  drops a feedback it suspects would not benefit its reputation.

When  $H$  receives the satisfaction level, it refunds  $MN$  a small amount  $\varepsilon$ . The reward  $\varepsilon$  is meant to encourage the mobile nodes to report their satisfaction levels: It covers the cost  $c$  of sending the report ( $\varepsilon > c$ ).

**Aggregation and sending of the feedback to  $TCA$ :**  $H$  aggregates all the satisfaction levels of the  $MNs$  affiliated with it by generating, for each WISP, a couple  $(g, b)$  where  $g$  is the number of good feedbacks and  $b$  is the number of bad feedbacks.  $H$  sends this information to  $TCA$  (e.g., right before the reputation update time) and resets its counters.

**Updating the reputation record:**  $TCA$  collects the information about the satisfaction levels from the  $Hs$ . Then, at *reputation update time*,  $TCA$  processes this information, updates and signs the reputation record of each WISP and informs the WISPs about their new records.

### 4.3 Design model

During these different phases, we use symmetric key and public key cryptography primitives to secure the message exchange and to correctly authenticate the different parties involved in the communication. We minimize however the use of public key cryptography to reduce the computation cost of our solution.

Hence, public key operations are used (by  $MN$  and the neighboring WISPs) only during the verification the identity of the selected WISP (see Subsection 4.2).

Symmetric key primitives are used for all the message exchanges in our solution. Indeed, when two interacting parties need to verify the integrity of the data they exchange, they use a Message Authentication Code (MAC). They use symmetric key encryption and decryption operations when they need to preserve the confidentiality of the messages, e.g., the data sent by  $MN$  to  $H$  during the verification of the identity of the mobile node (see Subsection 4.2).

## 5 Assessment

### 5.1 Reputation system

In our solution, the different players are motivated to participate in the reputation mechanisms. Indeed:

- $W$  is motivated to provide  $MN$  with a good QoS because otherwise the feedback of  $MN$  will be negative (see the analysis of the *Selective misbehavior* attack in Subsection 5.3).
- $MN$  is motivated to report on its interaction with  $W$  because it receives a refund  $\varepsilon$ .
- $W$  is motivated to forward the report (see the analysis of the *Report dropping* attack in Subsection 5.3).

All the entities involved in the maintenance of the reputation system are therefore motivated to behave correctly (i.e., according to the proposed solution).

### 5.2 Attacks

In this Subsection, we present some attacks that an attacker may want to perform against our solution:

- *Selective misbehavior* attack:  $W$  misbehaves (i.e.,  $W$  intentionally provides a bad QoS) with a specific mobile node to whom it is supposed to provide the service.
- *Denigration* attack:  $MN$  receives a good QoS from  $W$  but pretends the contrary by sending a negative report on the satisfaction level or by not sending the report at all. A more sophisticated attack would be for several mobile nodes to collude and perform this attack.
- *Report dropping* attack:  $MN$  sends the report but  $W$  does not transmit it to  $H$ .
- *Denial of service* attack:  $W$  receives the  $t$ -th payment from  $MN$  but refuses to provide the corresponding service.
- *Refusal to pay* attack:  $MN$  does not send the  $t$ -th payment to  $W$ .

<sup>10</sup> If  $MN$  moves, the report is sent via another WISP.

### 5.3 Security analysis

In this Subsection, we analyse the robustness of our solution against the attacks listed in Subsection 5.2. We show that none of these attacks is rational, that we can detect malicious attacks and that it is possible, in some cases, to identify the attackers.

**Selective misbehavior attack:** If  $W$  misbehaves with a given  $MN$  it provides service to,  $MN$  will send a negative report to its home network  $H$  and  $H$  will inform  $TCA$  about this feedback.

If this attack is repeated, the cumulation of the negative reports will affect the future reputation records of  $W$ . If on the contrary, this attack is performed rarely, it will not affect much the reputation of  $W$  but  $W$  will still gain nothing from performing this attack; as  $W$  is rational, it will not perform this attack.

**Denigration attack:** If  $MN$  does not send the report on the satisfaction level,  $H$  will not give it the  $\varepsilon$  reward and will consider the absence of feedback as negative feedback. Therefore, this attack is not rational for  $MN$ .

So it is more interesting for  $MN$  to send a negative feedback instead of not sending the report at all: The effect of the attack is the same and at least  $MN$  will get paid for the sending. But this attack is still not rational. Indeed,  $MN$  gains nothing from sending a negative feedback instead of a positive one (the cost of the sending remains the same). Such behavior is thus purely malicious.

$H$  can statistically detect this attack. Indeed,  $H$  keeps track of all that is happening between the nodes affiliated with it and the different WISPs. It will then consider  $MN$  as a misbehaving node if the following events happen frequently<sup>11</sup>:

- $MN$  always pretends that it received a bad QoS from a given WISP, whereas many other  $MNs$  report on a good QoS on that very WISP (as the selective misbehavior attack is not possible, this situation is suspect), or
- $H$  never receives reports from  $MN$  about the sessions it established with  $W$ , or
- $MN$  pretends that the QoS was bad but at the same time the duration of the session and the amount of data exchanged prove that the QoS was good.

If several  $MNs$  collude and perform this attack,  $H$  is still able to identify them as long as the number of colluders does not represent an important fraction of the nodes interacting with  $W$ .

Please note that this colluding attack comes with an important cost: if an attacker  $\mathcal{A}$  wants to alter the reputation of  $W$  by parking misbehaving nodes close to the hot spots managed by  $W$ ,  $\mathcal{A}$  should own many devices and for each of them, it should register with a valid home network  $H$  (and pay a registration fee). Note also that this colluding attack may harm very small WISPs (with few number of hot spots) - if the attacker pays the price - but it is much too costly against WISPs with hundreds or thousands hot spots.

**Report dropping attack:** If  $W$  expects a negative feedback, it may want to drop the report on the satisfaction level instead of transmitting it to  $H$ . But as the absence of feedback counts as negative feedback, this dropping does not help  $W$ . Furthermore, the report may be positive, in which case  $W$  would lose a good feedback. This attack is therefore not rational for  $W$ .

**Denial of service attack:** If  $W$  refuses to provide the  $t$ -th service,  $MN$  will keep asking for it (by sending again the  $t$ -th payment). After a predefined number of retransmission requests,  $MN$  will end the session, which prevents  $W$  from providing more services and thus earning more money.

In order to prevent  $W$  from receiving the payment for the  $t$ -th service (which it did not provide), we can use the payment system presented in [18].

**Refusal to pay attack:** If  $MN$  does not send the  $t$ -th payment,  $W$  will not provide the  $t$ -th service and the session will end (after a predefined number of retransmission requests). This attack is then not rational: It prevents  $MN$  from receiving the service but does not harm  $W$ .

<sup>11</sup> The higher the number of events is, the more accurate the detection is.

## 6 Conclusion

In this work, we present a simple solution that encourages the use and the deployment of WiFi networks. We propose a reputation mechanism that encourages the WISPs to behave correctly and to provide all *MNs* with a good QoS. We also use a micropayment scheme to make sure that *MNs* will pay for the service they received. Our solution leads to a seamless roaming that makes the use of the WiFi network more attractive to *MNs*.

By using symmetric key and public key cryptography primitives, we can secure the message exchange and correctly authenticate the different parties involved in the communication. We minimize however the use of public key cryptography to reduce the computation cost of our solution.

Our solution thwarts rational attacks, detects malicious attacks and, in some cases, identifies the attacker while keeping the communication and computation costs very moderate for the mobile node *MN*.

As future work, we intend to implement our solution and to verify, by means of simulations, the efficiency of the reputation mechanism and the robustness of the protocols against various rational and malicious attacks.

## References

1. <http://www.boingo.com/>.
2. <http://www.wayport.com/>.
3. <http://www.t-mobile.com/>.
4. J.-P. Hubaux, Th. Gross, J.-Y. Le Boudec, and M. Vetterli. Towards Self-Organizing Mobile Ad-Hoc Networks: the Terminodes Project. *IEEE Communications Magazine*, 39(1):118–124, January 2001.
5. M. Jakobsson. Financial Instruments in Recommendation Mechanisms. In *Proceedings of Financial Cryptography*, 2002.
6. D. Houser and J. Wooders. Reputation in Auctions: Theory, and Evidence from eBay. Working Paper 00-01, University of Arizona, 2001.
7. P. Resnick and R. Zeckhauser. Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. In *NBER workshop on empirical studies of electronic commerce*, January.
8. P. Resnick, R. Zeckhauser, J. Swanson, and K. Lockwood. The Value of Reputation on eBay: A Controlled Experiment. In *ESA Conference*, June.
9. C. Dellacrocas and P. Resnick. Online Reputation Mechanisms - A Roadmap for Future Research. In *1st Interdisciplinary Symposium on Online Reputation Mechanism*, 2003.
10. Z. Despotovic and K. Aberer. Trust and Reputation in P2P networks. In *1st Interdisciplinary Symposium on Online Reputation Mechanism*, 2003.
11. S. Buchegger and J.-Y. Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Distributed Ad Hoc NeTworks. In *Proceedings of MobiHOC*, Lausanne, CH, June 2002.
12. P. Michiardi and R. Molva. Core: A Collaborative Reputation Mechanism To Enforce Node Cooperation In Mobile AD HOC Networks. In *Proceedings of The 6th IFIP Communications and Multimedia Security Conference*, Portoroz, Slovenia, September 2002.
13. Boingo Wi-Fi Industry White Paper. Towards Ubiquitous Wireless Broadband. [http://www.boingo.com/wi-fi\\_industry\\_basics.pdf](http://www.boingo.com/wi-fi_industry_basics.pdf), September 2003.
14. B. Patel and J. Crowcroft. Ticket based Service Access for the Mobile User. In *Proceedings of MobiCom*, 1997.
15. <http://www.rsasecurity.com/products/securid/>.
16. R. Rivest and A. Shamir. PayWord and MicroMint: Two simple micro-payment schemes. Technical report, MIT Laboratory for Computer Science, 1996.
17. D. Coppersmith and M. Jakobsson. Almost Optimal Hash Sequence Traversal. In *Proceedings of Financial Cryptography*, 2002.
18. L. Buttyán. Removing the Financial Incentive to Cheat in Micropayment Schemes. *IEE Electronics Letters*, January 2000.