SYD: Building Trust in the Peer to Peer Wireless Network Confederation

Eleftherios C. Stefanis and George C. Polyzos

Mobile Multimedia Laboratory
Department of Computer Science
Athens University of Economics and Business
Athens 104 34, Greece
leste@aueb.gr , polyzos@aueb.gr

***Abstract* – Modern trends in Peer-to-Peer systems lean towards self organized communities based on peer contribution. The inherent difficulty encountered in such systems is that selfish peers that are mutually distrustful of each other are expected to cooperate in order to enjoy the benefit of consuming the resources shared through the p2p system. Furthermore, self organized p2p communities depend on free identities to retain their open nature and privacy requirements. Allowing the ability to change identities at will or to have multiple identities in a given community gives birth to certain attacks (known as Sybil attacks) that allow peers to consume without contributing and further increase distrust in the community. In this report we propose a new strategy - Settle Your Debt (SYD) - for members of the Peer to Peer Wireless Network Confederation (P2PWNC). We show that SYD avoids previous strategies' vulnerability to Sybil attacks and helps to achieve a reasonably stable and thriving community without compromising the assumptions of peer selfishness and mutual distrust.**

I. Introduction

Peer to peer systems are about sharing resources such as files, secondary storage or (in the case of P2PWNC) bandwidth. Opposite to traditional systems where users are assumed to be *obedient* – users who do not stray from a specific protocol, p2p design assumes *rational* peers – peers whose actions aim to maximize their individual utility. In this section we will present the basic characteristics of the Peer to Peer Wireless Network Confederation (P2PWNC) in order to best define the cooperation issue in such systems.

The P2PWNC [7] is a WiFi roaming scheme that aims at providing internet access to pedestrians walking by home Access Points (APs) that are connected to a broadband internet connection (such as DSL or Cable).

Members of the P2PWNC form *teams* that control one or more of such home WiFi hotspots acting as *microproviders* for members of other teams by allowing their traffic to be forwarded through their internet connection.

The peer entities in P2PWNC are teams of users, controlling one or more sites, who have decided to pool their resources together. All members of the same team seem equal to members of another team. In other words, P2PWNC transactions take place between teams.

The P2PWNC design holds the following:

- Identities are *free* and *disposable*, in the form of public-private key pairs issued by the team itself. No personal information is imparted and nothing maps P2PWNC identities to real life identities.
- Peers are mutually distrustful of each other. Members of different teams only trust hard evidence (such as cryptographic proof) of the other's transaction history.
- Peers are selfish**.** They won't engage in any activity unless they expect to gain something out of it.
- There is no form of central control or any entity that acts as an authority that settles disputes. Peers are free to choose their own strategy as to how they behave towards other peers.

These characteristics combined describe what we call an anarchic p2p system. Our interest is to study how peers behave in a community like the P2PWNC.

Essentially, a peer's strategy determines how she responds when another peer requests service (ie to relinquish a share of internet bandwidth). Basic strategies include always contribute (provide service), never contribute, or contribute with some probability. More complex strategies use some kind of decision making algorithm before responding to a request.

The general challenge here is to find suitable strategies that will become popular by the peers of such an anarchic setup and at the same time lead to cooperation and a blooming community.

Our study follows previous work on the cooperation issue in anarchic p2p systems, which relies on the concept of reciprocity: *"I will contribute in order to be able to consume from others like me"*. Reciprocity based strategies try to achieve individual and social optimality by enforcing the rule of reciprocity: *"All peers must contribute as much as they consume.* The absence of authority, however, makes this problem of recognizing non-contributor far from trivial.

In the following sections, we will a) introduce the *Receipt Graph* which is the accounting structure of the P2PWNC and will accommodate our analysis, b) present related work on the cooperation issue in anarchic p2p communities, c) describe Sybil attacks and indicate where a previous solution falls short, d) present the *Settle Your Debt* strategy and e) evalutate the SYD strategy by having it compete with others in an evolutionary game.

II. The Receipt Graph

The P2PWNC system uses *digital receipts* to record transactions between peers. During a transaction, the P2PWNC software on the server side (the provider's side) periodically requests a digital receipt from the client. These receipts (shown in Fig. 1) contain the providing and consuming teams' public

keys as well as the amount of bytes forwarded so far. The last is referred to as the receipt's *weight***.** The receipt is cryptographically signed by the client in order to remain as undisputable evidence of the transaction. More on the receipt exchange protocol and cryptographic functions can be found in [1].

What is important for our future analysis is that: *Let c be a peer, no peer without c's private key can create a valid P2PWNC receipt in which c is the consumer (fact 1).*

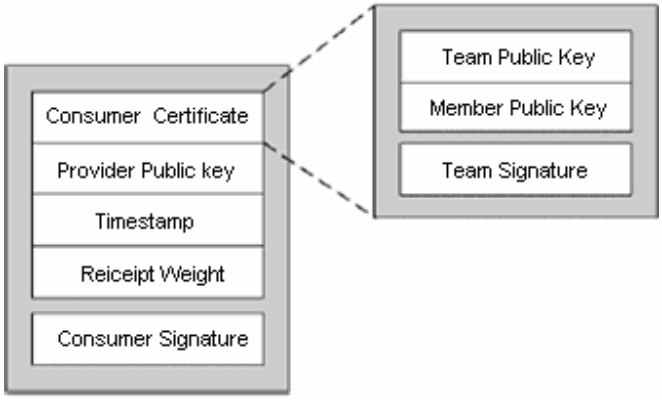


Fig. 1. A P2PWNC receipt

Receipts are stored in a repository where they form the (directed) *receipt graph (G)* thus:

$$G(V,E,W):\forall c,p\in V\ ,\ (c,p)\in E \text{ and } \mathrm{W}(c,p)=w$$

$\Leftrightarrow$ there is a receipt in which c is the consumer, p the provider and w the receipt weight

Fact 1 directly leads to the following: *No peer can create a graph edge where the source node is not controlled by her (fact 2).*

The timestamp value on the receipt makes sure that sessions are properly identified and no double receipts stored.

In our study, we simplify matters by assuming a central receipt repository**,** which remains impartial to any team. This simply means that all peers have a common view of the entire graph and does not conflict any of the design characteristics mentioned in the previous section. Note that both central and distributed repositories are supported in the P2PWNC.

III. Related Work

Feldman et al. [2] uses the maxflow value between two nodes on a transactions graph (similar to the receipt graph described earlier) as a means to calculate contribution and identify non-contributors (*free-riders*) and colluders. The decision making algorithm proposed, uses the formula

$$\min\left\{\frac{\text{maxflow}(P\to C)}{\text{maxflow}(C\to P)},1\right\} \quad (1)\ ^{1}$$

as the probability for peer *P to* offer service to a requesting peer *C.* We will refer to this value as peer C's *reputation score (score (P, C)).* However, the strategy following this basic algorithm is found to be vulnerable to certain *Sybil attacks* (to be described later).

In [9] Sybilproofness is proven to be achieved when asymmetric reputation functions with certain properties are employed. Even though formula (1) belongs to this category, Sybilproofness is defined as preventing peers from increasing their reputation to match or exceed the reputation of other peers. As we will see in the next section being able to consume without having your reputation score decreased is also a way of succeeding at a Sybil attack.

Previous work on the P2PWNC ([3]) uses an extension of Feldman's decision making algorithm, in which the distance between nodes and the average consumption rate in the community are taken into account when calculating maxflow values, in order to detect attackers. While this extension leads to good results, it makes the assumption that most P2PWNC teams are homogeneous in their consumption rates.

In [4] the reputation score is used as a QoS parameter instead of the probability of a successful transaction.

In this study, we make a formal description of the vulnerability encountered in strategies using formula (1), and propose a new strategy – Settle Your Debt (SYD) –which offers robustness against Sybil attacks without requiring any extra assumptions on the consumption rates of P2PWNC teams.

IV. Sybil Attacks

In a fully controlled p2p system, where all peers would be strictly identified, it would be easy to check which peers abide to the reciprocity rule by using some form of accounting (such as the receipt graph described earlier). When peers are allowed to create multiple identities at will, however, the issue of the *Sybil attack* arises [8].

The Sybil attack is performed by a peer creating multiple identities (called Sybils or shadow identities) that collude with each other in order to create a false image of contribution and thus increase the reputation of her main identity in the community

A simple example of a Sybil attack from a P2PWNC peer is to create an infinite number of nodes with edges pointing towards her "main" identity node, appearing as if she has granted service to all of these (non-existent) teams (see Fig. 2).

It is important to remember that peers seek to acquire receipts that will be useful to them in their future requests (increase their contribution level). Receipts from shadow identities, which will be discarded as soon as the session is over, are obviously useless. This makes it important for our selfish peers to have a way of recognizing false contribution.

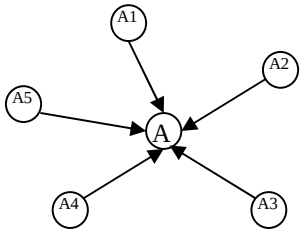


Fig. 2: Peer A creates shadow identities A1-A5 to present false contribution

[1] Note that the formula is reversed to avoid confusion, since the edges of the transaction graph in [2] represent service offered and not service consumed.

Now, let's examine how strategies based on formula (1) respond to Sybil attacks.

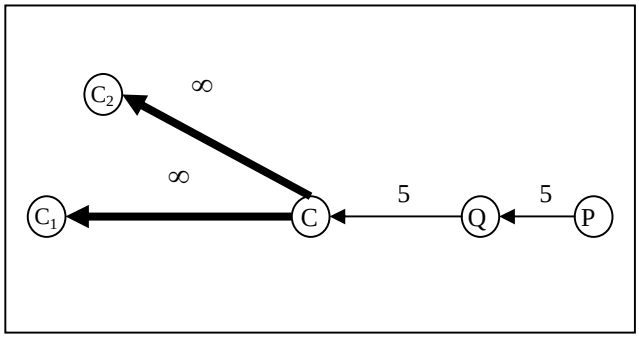
Let $P, C_0, C_1, C_2, ...C_i \in V$ where P is the providing peer and $C_0, C_1, C_2, ...C_i$ are Sybils belonging to the consuming peer C. In order for C to increase her reputation score, she must use her Sybils to either increase the numerator or decrease the denominator in (1).

There are only two possible ways to increase a $\text{maxflow}(x \to y)$ value:

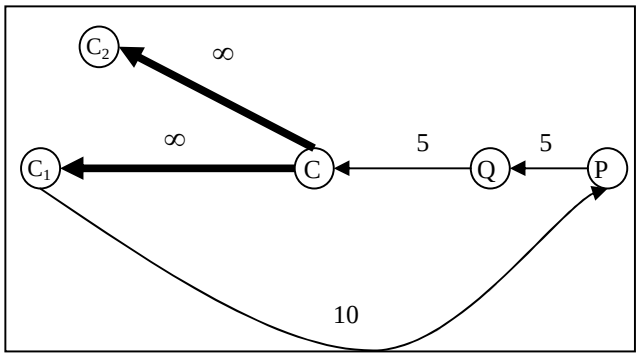
A. Change the weight of edges belonging to a $x \to y$ path. C can only increase the weight of edges originating from a C_i node (see fact 2), loosening the capacity constraint for $\text{maxflow}(C_i \to y)$ and possibly increasing its value. However, the numerator in (1) is in the form of $\text{maxflow}(x \to C_i)$

B. Create new $x \to y$ paths. Again, according to fact 2, C can only create paths where all edges originate from a C_i node. $P \to C_i$ paths do not fall in this category. Simply expanding $P \to C_i$ paths to $P \to C_i \to C_k \to ... \to C_m$ and using $\text{maxflow}(P \to C_m)$ won't help. Due to the capacity constraint quality of a flow, the maximum flow pushed through a $x \to y$ path is equal to or less than the maximum flow pushed through a $x \to y_1 \to ... \to y_i$ path. However, it is a simple task for C to create $P \to C_i \to C_k \to ... \to C_m$ paths that yield the same maxflow results as $P \to C_i$, by making all $C_x \to C_y$ edges of infinite weight. *i.e C can push all of his good reputation to any of his Sybils (fact 3*).

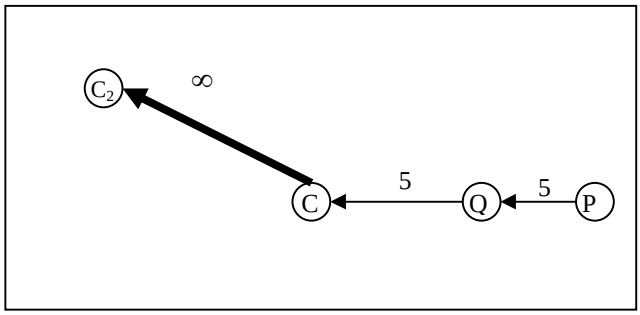
Decreasing the denominator in formula 1 is a simple matter. C can just use a Sybil C_z with no outgoing edges (she can create them on the fly), and therefore, no debt: $\text{maxflow}(P \to C_z) = 0$. Combining this with fact 3 we arrive at the conclusion that, even though C can't raise her reputation score, she can preserve a good reputation score while having a disproportional contribution to consumption ratio: She can contribute once and consume an infinite amount of times using a different Sybil each time. Fig. 3 depicts this form of Sybil attack.



(a) C pushes all of her good reputation to Sybils C_1 and C_2



(b) C introduces herself as C_1 to P



(c) C_1 won't be used again: consumption vanishes! Next time C will introduce herself as C_2

Fig. 3. Taking advantage of single – use Sybils to avoid bad reputation

V. The "Settle Your Debt" Strategy

In this section we present our reciprocal strategy, which is shown to be invulnerable to the Sybil attack presented in the previous section.

A. Purging Cycles

We continue to use maxflow values as a measurement of contribution and in this context we refer to $\text{maxflow}(x \to y)$ as x's debt to y (or y's contribution to x)**.** For instance, in the graph in Fig. 4a, peer P owes peer C a debt of 5 units (the value of $\text{maxflow}(P \to C)$). Indeed, the receipts that form the path between P and C represent indirect contribution from C to P. Using formula (1), $\text{score}(P \to C) = 1$.

(a) Starting graph (b) A new edge forms a cycle

Fig. 4. A 3-party debt example

Now, lets assume peer Q gets some service from peer P ($\text{score}(P \to Q) = 1$), the edge Q→P is created, say with a weight of 10. We observe that although C's good reputation to P comes through Q, this new edge does nothing to affect it and $\text{score}(P \to C)$ is still 1. To use our new terminology: *P owed 6 units to Q. Q owed 5 units to C. i.e P could repay some of her debt to Q directly to C (hence C's good reputation). P pays 10 units to C. P still thinks that she owes (indirectly) to C.*

The above anti-intuitive result prompts us to use a more real – life solution: erasing debt that is settled**.** Indeed, in a real life situation where C, Q and P are people, the result of the previous transaction would be: *Q owes 5 units to C, Q owes 4 to P.* This is easily implemented on the receipt graph by finding the cycle Q-P-Q and deleting the weight of the lightest edge from all edges in the cycle, effectively breaking the cycle (see Fig. 5). Cycles in the receipt graph represent *dept settlement* and *purging* them in this way makes sure that redundant edge weights are deleted from the graph.

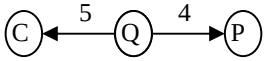


Fig. 5. The cycle is purged

Erasing settled debts from the receipt graphs enables us to eliminate the reason the aforementioned Sybil attack was successful: reusing contribution over and over, each time by a different Sybil**.** Fig. 6 shows how C's contribution can be used just once no matter which Sybil she assumes.

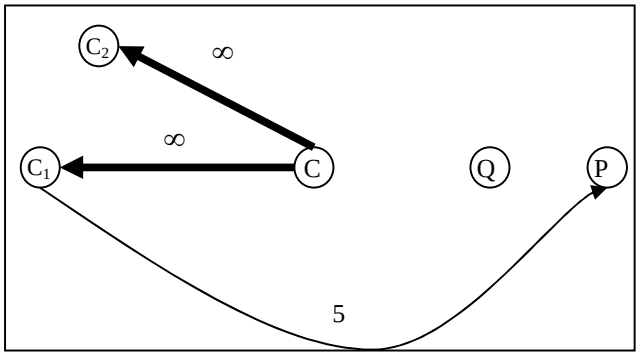


Fig. 6. The Sybil attack fails when debt settlements are erased from the receipt graph.

Since having no cycles in the receipt graph means that for any two peers A, B at most one of the values maxflow(A→B) and maxflow(B→A) is non-zero, we use a new formula to measure reputation:

$$score(P,C) = \text{maxflow}(P \to C) - \text{maxflow}(C \to P) \quad (2)$$

A positive score represents P's debt to C, which she should repay if she expects to get service from peers involved in the debt. Note that since the score value is not in the [0, 1] range anymore, peers should keep an average score in order to normalize this value and use it as a QoS parameter.

A negative score means that C is already indebted to P so she will not grant her service in order to comply with the rule of reciprocity

A score of zero means that neither C nor P is indebted to each other. P still doesn't grant service to C to make sure that he has *"paid his dues"*. This mistreatment of newcomers is proven in [5] to be required in order to prevent whitewashing (introducing oneself as a new peer every time and enjoying the benefits of a clean history).

B. Credit Windows

Even though this seems like a step in right direction, there is a new problem that arises. Deleting edges may prohibit attackers from succeeding, but also prohibits well behaving peers from retaining a good reputation in the community.

It is easily shown that: *After all peers bootstrap, existing edge weights in the receipt graph can only decrease (fact 4).* (Bootstrappers are new peers in the system, who contribute to everyone in order to build a starting reputation [3]):

Lets assume that there exists an edge *(u. v)* whose weight can increase ➔ there can be a transaction between *u* and *v* where *v* is the provider. ➔ $score(v,u) > 0$ ➔ $\text{maxflow}(v \to u) > 0$ ➔ there exists at least one $v \to u$ path. This is impossible since such a path would create a cycle by adding edge *(u, v)* and the receipt graph is acyclic (all cycles are purged).

Members of a community using this cycle purging strategy, in their efforts to remain strict, fail to build sufficient trust between them and are condemned to meagerness and a low overall community benefit. To resolve this issue we introduce another concept: *credit windows***.**

Each peer keeps a list of all peers he has interacted with along with a credit window value (initially 0). When a debt is settled each peer involved in the debt (in the graph cycle) increases the credit window for the previous peer in the cycle, by the amount of debt settled (the weight of the lightest edge in the cycle). Peers increase the credit window for the previous peer in the cycle because she is the one that got (or had got) service from her and repaid it though the settlement the cycle purge represents.

These credit windows represent the *"amount of trust"* peers have for one another. The insight here is that when two peers A, B have a settlement of debt they are content, having participated in transactions beneficial for both of them. When A visits B again it is only logical that B should remember these previous transactions and expect them to be repeated. Thus, even though she doesn't owe A anything, she might grant her access trusting that A will return the favor. Of course, this can't happen indefinitely or we would have the same problem as in the Sybil attack described in the previous section: A could settle a debt once and then consume an infinite number of times from

those involved in the debt. This is where credit windows come into play; to show B exactly how much credit she should allow A. This effectively makes our formula:

$$\text{maxflow}(P \to C) - \text{maxflow}(C \to P) + crWin(P,C) \quad (3)$$

The SYD strategy tries to simulate the behavior of real life merchants and their suppliers. A supplier will require a first time customer to pay up front[2], since she has no guarantees that the merchant isn't a phony. However, after some successful transactions the supplier starts letting the merchant buy with credit[3]. She knows now that the merchant understands that it is in her best interest to pay up (in order to continue having successful transactions with this supplier) and trusts that she will behave rational[4]. If the supplier remained strict he runs the risk of missing out on future beneficial transactions[5] (just because the merchant had cash problems). We can call this kind of trust *rational trust* and find that it is the only kind of trust possible for our selfish, distrustful peers.

To understand the inter-workings of the SYD strategy, we take another look at our example (Fig. 3a) and assume that peers P and Q follow the SYD strategy while C attempts the same Sybil attack. After the transaction, P's (indirect) debt to C is settled (Fig. 6) and now C and C_1 are the ones owing units to P. All peers involved in the settlement (i.e. C, C_1, Q, P) have their credit windows updated as shown in Fig. 7 (non SYD followers are omitted).We make the following observations:

1. C has now less incentive to switch identities. Sure, C_2 is clear of debt but on the other hand, C_1 has established some recognition in the community and is now entitled to credit. In our example $score(P,C_1) = score(P,C_2) = 0$. Peers are less eager to dump indebted identities out of concern of losing possible credit rights.
2. If credit windows weren't used, P and Q would now view each other as strangers, whose receipts they can't trust to be useful. Now, $score(Q,P) = 5$, giving them the opportunity to repeat their previous successful interaction.

TABLE I: CREDIT WINDOW EXAMPLE

Credit Windows	C	P	Q	C_1	C_2
P	0	∞	0	5	0
Q	0	5	∞	0	0

Fig. 7. When a cycle is purged credit windows are updated according to the amount of debt settled.

[2] Just as SYD providing peers won't offer service to consumers with 0 score

[3] Debt may be 0 or less but credit windows lead to a positive score

[4] A consumer will want to repay the debt in order to increase her score and gain service again from that provider or peers in debt to that provider

[5] Like the trust issue we saw in fact 4

A peer can take maximum advantage of credit windows by using the following strategy dubbed "*The lazy ant attack*"**:**

1. Behave as a SYD follower until you have accumulated a total credit of *m* units and your total debt is 0.
2. Behave as a free-rider until your total credit reaches 0.
3. Change identity and start over

During the first step, the attacking peer contributes and consumes *m* units (no other way to accumulate *m* credit). During the second step, she consumes additional m units. Consequently, peers using this strategy will get to consume two times the amount they have contributed (regardless of the value of *m*). However, the reader should not forget that starting over comes with the price of bootstrapping. So if an attacker chooses a small value for *m* she must often go through periods of time when she will be unable to consume. On the other hand, a large *m* value means that she may not get to spend all her credit on step 2 due to the short term history nature of the system (old receipts are discarded from the graph as fresh ones are inserted). So we judge that this bounded unfairness is not particularly dangerous.

To sum up, SYD consists of the following characteristics:

- **Cycle purging**. When a cycle is formed in the receipt graph, the weight of that cycle's lightest edge is subtracted from all the edges in the cycle – thus removing settled debts.
- **Credit Windows.** When a cycle is purged each peer which took part in the cycle updates the credit window value for the previous peers in the cycle (the peer who settled her debt to her) by adding the weight of the lightest edge (the amount of debt settled).
- The decision making formula used is: $\text{maxflow}(P \to C) - \text{maxflow}(C \to P) + crWin(P,C)$ where *P* is the provider and *C* the consumer.

VI. EVALUATION

In this section we try to evaluate the SYD strategy in a simulated P2PWNC community, using an evolutionary game theoretic perspective [6]. In an evolutionary game, players choose from a set of strategies and interact with each other competing for a resource. During the game they may change strategies through either *mutation* or *evolution*.

A. Definitions

A peer's **benefit (b)** from participating in a P2PWNC community is a value representing money saved in mobile phone bills, enjoying better bandwidth, internet access where there is no other (commercial) network coverage etc. Benefit is increased each time a peer participates in a transaction as the consumer.

A peer's **cost (c)** from participating in the community is a value representing extra money spent in metered DSL bills, losing part of her bandwidth, exposing herself to possible security threats etc. Cost is increased each time a peer participates in a transaction as the provider.

The value: *benefit – cost* represents the **profit (p)** a peer has earned through his activities in the community.

A **round** is defined by *n* transactions (successful or not) where *n* is the size of the population.

We define a **strategy rating** as the average profit per round of all peers following it. w_i denotes the number of rounds peer *i* has been using his current strategy. In our experiments we also weigh this average using the number of rounds each peer been has followed his current strategy:

$$rating(s) = \frac{\sum_{i \in F(s)} \frac{p_i}{w_i} w_i}{\sum_{i \in F(s)} w_i} = \frac{\sum_{i \in F(s)} p_i}{\sum_{i \in F(s)} w_i} \quad (2)$$

Experiences of veteran followers are much more accurate than those of novice followers whose profit is affected greatly by the chance factor.

Mutation occurs randomly and results in the mutated peer uniformly selecting a new strategy from the set of available strategies (could be his current one).

Evolution also occurs randomly and results in the evolving peer to uniformly select a new strategy from the set of available strategies and compare his current strategy rating with it. The evolving peer will then either follow the new strategy or remain a follower of his current one with a probability depending on this comparison. In our experiments we use the formula:

$$p_{jump} = 1 - \frac{rating(oldstrategy)}{rating(newstrategy)} \quad (3)$$

So, a peer only evolves to the new strategy if it has a better rating than his current one.

We use two alternative strategies: *altruism (ALTR)* (always provide) and *free-riding (FREE)* (never provide), and test whether the SYD strategy succeeds in providing sufficient incentive for peers to choose it in favor of the other two.

B. Simulation Results

In the following results we plot the followers of the three different strategies as a percentage of the total population (Y axis) in relation to simulation time measured in the number of rounds (X axis). The evolution mechanics described in the previous section make sure that the most (individually) rewarding strategy dominates over time.

Even with the addition of credit windows, we find that the SYD strategy remains strict enough to make it ill suited in a large P2PWNC community where peer matching is uniform (for each transaction the provider and the consumer are chosen randomly from the set of peers) (Fig. 8).

Nevertheless, in many communities, it is reasonable to assume that there is significant correlation between consumer and provider peers. i.e peers often visit the same P2PWNC sites over and over again. To model this behavior, we use the following correlation model:

In each transaction, the consumer peer *c* is chosen randomly. The provider peer is chosen from a small group of familiar peers (*neighborhood*) with a probability *r*, or randomly (with a probability 1-*r*).

Using this model we get much better results regarding the popularity of the SYD strategy. Peers within a familiarity group benefit from the continually increasing credit window values and build lasting relationships based on rational trust. In Fig 9 we see that the SYD strategy dominates in the long run when 30% of a peer's consumptions take place in a neighborhood the size of 5% of the total population.

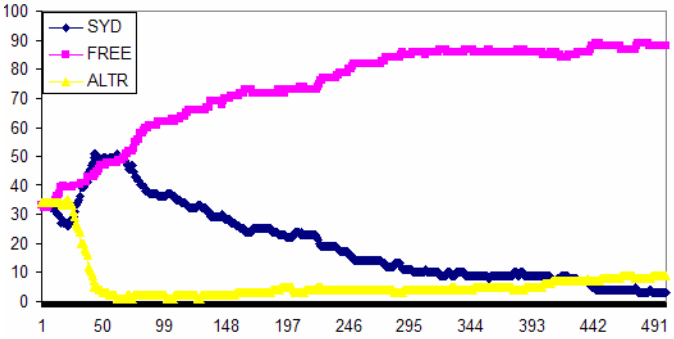


Fig. 8. Uniform peer matchings (Experiment A).

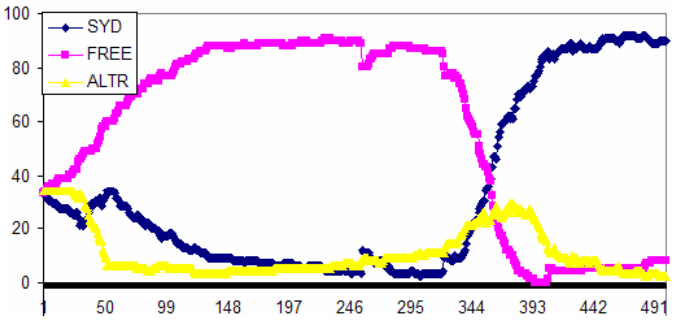


Fig. 9. Correlated peer matchings (Experiment B)

TABLE II: SIMULATION PARAMETERS

	Experiment A	**Experiment B**
# of teams	100	100
# of transactions	50000	50000
correlation probability	0 (uniform matchings)	0.3
neighborhood size in % of total population	N/A	5
benefit per successful consumsion	10	10
cost per successful provision	1	1
evolutions %	20	20
mutations %	0.1	0.1

VII. CONCLUSION AND FUTURE WORK

In this report we have studied the Peer to Peer Wireless Network Confederation as a community consisting of selfish and distrustful peers. We introduced a new reciprocal strategy that overcomes Sybil attack vulnerabilities of previous strategies using the technique we dubbed *cycle purging* and

encourages peers to build foundations of trust in order to achieve individual optimality, by introducing *credit windows*.

We showed that the SYD strategy is suited for communities where peer interactions are not uniform but correlated with the identities of the peers. In order for the SYD strategy to provide acceptable results, peers should perform at least 30% of their transactions within a small group of familiar peers.

An extension to the SYD strategy is currently being considered, which makes use of super peers -dubbed *paragon peers*. Paragon peers are peers known to the whole community and whose receipts can be used as if issued by any provider that suits the holder. In effect, if peer C is the consumer peer, peer P the provider peer and peer R is a paragon peer, peer P would consider both $score(P,C)$ and $score(R,C)$ before deciding whether to grant access to C. The paragon peer extension is yet to be formally analyzed and evaluated but may lead to better results as well as resolve possible partitioning issues in the receipt graph. The matter of having a P2PWNC community agree on who the paragon peers are (remember that there is no central authority) should also be considered.

Lastly, we assumed in our analysis that all peers share a common view of the entire receipt graph. However, in a P2PWNC system such a global receipt repository may not exist leaving peers with a partial view of the graph pieced together by receipts gained through the gossiping protocol described in [3]. Future work on the SYD strategy would include investigating whether it can function with this distributed version of the receipt graph.

The SYD strategy has been implemented for the Receipt repository module of the P2PWNC system architecture and will be available at [7].

VIII. Aknowledgements

We thank the rest of the P2PWNC team: Elias C. Efstathiou, Fotios A. Elianos, Pantelis A. Frangoudis, Vasileios P. Kemerlis and Dimitrios C. Paraskevaidis for their invaluable help and support, as well as the anonymous reviewers whose comments helped improve the quality of this paper.

References

[1]. P.A. Frangoudis, *The Peer-to-Peer Wireless Network Confederation Protocol: Design Specification and Performance Analysis*, Technical Report, 2005-MMLAB-TR-02, June 2005.

[2]. M. Feldman, K. Lai, I. Stoica and J. Chuang, "Robust Incentive Techniques for Peer-to-Peer Networks," Proc. 5th ACM Conference on Electronic Commerce, 2004.

[3]. E.C. Efstathiou, P.A. Frangoudis, G.C. Polyzos, "Stimulating Participation in Wireless Community Networks," Proc. IEEE INFOCOM 2006, Barcelona, Spain, April 2006.

[4]. E.C. Efstathiou, F. Elianos, P.A. Frangoudis, V.P. Kemerlis, D. Paraskevaidis, E.C. Stefanis, and G.C. Polyzos, "Public Infrastructures for Internet Access in Metropolitan Areas," Proc. 1st International Conference on Access Networks (AccessNets 2006), Athens, Greece, September 2006.

[5]. E. Friedman and P. Resnick, "The Social Cost of Free Pseudonyms," *Journal of Economics & Management Strategy*, 2001

[6]. http://plato.stanford.edu/entries/game-evolutionary/, *Introduction to Evolutionary Game Theory*.

[7]. http://mm.aueb.gr/research/P2PWNC/ (the P2PWNC project site).

[8]. J.R. Douceur, "The Sybil Attack," Proc. 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), Cambridge, MA, March 2002.

[9]. Alice Cheng, Eric Friedman, "Sybilproof Reputation Mechanisms," Proc. ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems (P2PECON-05), August 2005.