Dealing with Sporadic Strangers,
or the (Un)Suitability of Trust for Mobile P2P Security

Esther Palomar Juan M.E. Tapiador Julio C. Hernandez-Castro
Arturo Ribagorda
Computer Science Department, Carlos III University of Madrid
Avda. Universidad 30, 28911 – Leganes, Madrid (Spain)
{epalomar, jestevez, jcesar, arturo}@inf.uc3m.es

Abstract

A number of factors, such as the increasing popularity of wireless networks, the opportunities offered by 3G services, and the rapid proliferation of mobile devices, have stimulated a general trend towards extending Peer-to-Peer (P2P) characteristics to wireless environments. As a result, the P2P paradigm has begun to migrate to pervasive computing scenarios. So far, research in this domain has led to some middleware models working over Mobile Ad Hoc Networks (MANETs), which are now viewed as a Mobile-P2P (M-P2P) networks. However, the highly dynamic, decentralized and self-organizing nature of MANETs does not fit well with many approaches developed in the P2P world. In particular, it does not seem easy to deploy security solutions for M-P2P due, among other reasons, to the inherent limitations of the peers' devices and their potentially very sporadic interaction with other peers. Under these assumptions, a significant challenge is how to establish a decentralized trust management system. In this paper, we first summarize the advances in M-P2P security services and point out potential future applications based on opportunistic interactions. Then, we discuss several kind of threats and attacks, and finally analyze the (un)suitability of employing trust-based systems in some of these environments.

Keywords: *Mobile P2P; Security; Trust; Threats and Attacks.*

1 Introduction

M-P2P systems constitute the basis upon which a number of novel applications may be built. They also offer many interesting and challenging research opportunities, such as providing adequate solutions to improvised mobile ad hoc collaboration established on the fly. The perspective suggested in [8] discusses new application domains, e.g. tourists in a trip sharing photos, recommending places to visit, and playing games. Similarly, the proliferation of wireless communications and mobile devices have motivated the interest of migrating common P2P applications (e.g. file sharing and instant messaging) to mobile networks [5].

So far, the straightforward approach consist in mounting an M-P2P system over a MANET –temporary wireless networks where transitory sets of mobile nodes dynamically establish their own network on the fly. Nevertheless, nodes in a MANET are constrained by a limited amount of energy, storage, bandwidth and computational power, among others. Current MANET technology has addressed the efficiency of data search and routing, a major problem since the topology continuously and unpredictably changes due to frequent joins and leaves. Some early works and surveys on MANETs study these fundamental problems (e.g. [3, 7]).

However, it is also necessary to identify vulnerabilities and threats, establish the essential security requirements, and define appropriate mechanisms for M-P2P applications. In this paper, we discuss to what extent trust-based solutions are likely to be a suitable technology upon which some security services are provided.

1.1 Motivation

For our purposes, we assume that the P2P architecture allows peers to collaborate in real time and without relying on central servers. Generally, when the size of the network increases, the probability of a given pair of peers to have repeated interactions with each other tends to vanish. These sporadic participants, to whom we will refer as "strangers" or "chance encounters", need guarantees that they will not run any risk taking part in the network, especially considering they might not have any prior experience and knowledge about any other entity (imagine a M-P2P network deployed in a shopping center or in a rail station, with several thou-

1529-4188/07 $25.00 © 2007 IEEE
DOI 10.1109/DEXA.2007.103

sands of users per day, many of whom will not be join the network again for days.)

Similar interactions carried out in a P2P environment (e.g. forwarding, recommending/accusing, and, according to the service provided, participating) are built around trust, and have to necessarily rely on the cooperation of all the participants. Basically, P2P security schemes show two main characteristics: They are inefficient and, in the absence of central authorities, require nodes to cooperate. In fact, their inefficient performance is currently an obstacle to the acceptance and usage of several cryptographic solutions. For instance, although the foundation of trust has long reached importance for the provision of security in wired distributed networks, the proposed models and metrics may not be considered when designing trust schemes for mobile environments. Particularly, classic recommending protocols based on others' past experiences may be inadequate among strangers. On the other hand, indirect trust are regularly requested to numerous peers, who could be also unknown or, at most, have questionable identity. Furthermore, recommending protocols involve a communication overhead that mobile nodes may not afford.

The idea of creating trustworthy communities has attracted considerable attention in the last years. Consequently, there has been a trend in the research community towards the use of trust models to address some security concerns, particularly for ad hoc and self-organized environments. Our contribution in this paper is to introduce potential future applications based on mobile opportunistic interactions and study their applicability in terms of security by means of the use of trust.

The rest of the paper is organized as follows. In Section 2, we provide a brief overview of some related works on security services for M-P2P networks. Section 3 discusses several forms of attack and analyzes the (un)suitability of distributing trust information in M-P2P systems, wherein communities may be sporadic. Finally, Section 4 outlines some future research directions.

2 Challenges for security services in M-P2P

As current mobile devices cannot still store many large files and the network infrastructure have remarkably low capabilities, M-P2P services will differ notably –at least by now– from current P2P applications. Smaller contents, such as games, video and sound clips, photographs and graphics, and even news, to name a few, are more likely to be distributed. There are some future collaboration-based applications in which peers could share data with each other using mobile devices in a P2P fashion. Some works present middleware implementations in Java and SOAP to provide M-P2P services in several wireless technologies, including WLAN, UMTS, GPRS and GSM.

These emergent M-P2P solutions should also consider security and privacy issues. In particular, authentication and access control are fundamental to secure the system from unauthorized actions. In this regard, several works have already shown how to provide authentication, confidentiality, integrity and non-repudiation services in ad-hoc domains, based on identity, reputation and trust, proximity, and also public key cryptography [6]. Traditional cryptographic primitives can be actually used, perhaps with some restrictions, in mobile architectures. However, the low capabilities of wireless nodes have reinforced the use of trust-based solutions rather than the inclusion of regular cryptographic schemes. The main concern with these approaches is that, in most of them, nodes are trusted by default, and therefore they are susceptible to attacks.

2.1 Underlying infrastructure problems

A high transient topology of a MANET's physical network, formed and maintained independently by the peers, can cause significant problems. For example:

- The huge volume of broadcast messages, which implies a constant consumption of bandwidth and processing.

- The existence of an underlying mechanism for providing keys is a problematic issue. Approaches based on the creation and distribution of a common key or on the inference of a strong key from a weak shared password, have some problems with scalability and mobility [3]. Some solutions suggest the combination of centralization and key agreement techniques. In fact, the key agreement protocol is only executed between a subset of nodes, which play a connecting role within the community. Then, the main idea is to cluster nodes in service-oriented communities, generally according to their physical position. Apart from this, problems such as Sybil and pseudo-spoofing attacks –extensively studied in the context of P2P networks– appear whenever authentication protocols use opaque identifiers in favor of anonymity [12]. For this reason, most mobile solutions require the existence of some kind of control, such as a certificate authority or a key sharing mechanism.

- The establishment of a key management service using a CA hierarchy seems unsuitable for the moment, since a naive delegation and replication of the CA's responsibilities makes the service more vulnerable. To solve this problem, some works suggest using trust as a building block to address public key management. Particularly, schemes similar to PGP are fully distributed and self-organized [2]. Nodes can generate their keys, and their distribution can be done without relying on external directories. Nevertheless, this approach presents some inconveniences, e.g. those derived from high transient communities with a high number of strangers. Proposals based on threshold cryptography present a completely different approach –distributing the CA functionality over selected nodes [11]. This scheme is secure if the adversary cannot compromise more than k out of the members in any period of time. These schemes have also a number of drawbacks, mainly related to their communication overhead (any client need to contact at least k different nodes to get a certificate).

2.2 Trust schemes in M-P2P

There is an extensive amount of research on building, maintaining and using trust. Most of the works focus on presenting a particular concept of trust suitable for being incorporated in processes such as routing, access control or authentication. Some reputation-based solutions have been proposed for a variety of applications in M-P2P, e.g. to measure cooperation of the nodes in forwarding packets. For instance, the work presented in [1] proposes a decentralized trust model based on public key cryptography, which is independent of the security infrastructure and allows the constitution of ad-hoc trust relationships as well. This model suggests the use of certificates for ensuring the integrity of recommendations sent by peers.

So far, M-P2P models are based on proximity approaches and on web-of-trust models, where "trust-your-neighbor" relationships are established. These trust relationships are (1) extremely vulnerable to dishonest actions, and (2) potentially very inaccurate due to the absence of fixed trust infrastructure and the ephemeral nature of the connections. Furthermore, in the presence of adversaries and without any security mechanism deployed, we cannot assume that all friendly nodes will be reachable –malicious users may have rendered a small or big part of the network unreachable [10]). This is particularly critical when a decision has to be made about an unknown entity who does not have proper recommendations. For example, currently on-demand computing is being applied in close research areas such as Grid computing [9]. Similarly, it seems realistic to anticipate some kind of *on-demand* security over M-P2P, perhaps based on trust, and very application- or service-dependent.

3 Dealing with strangers in M-P2P

In this section, we discuss about the suitability of establishing trust schemes in M-P2P using a particular application scenario.

3.1 An M-P2P scenario

A blog party or a discussion forum are clear examples of future M-P2P applications. The only distinction here is that participants are mobile, such as people in a shopping mall, who can read and publish advertisements, send recommendations about the favorite restaurant around, or announce news about special offers in real time without requiring a single point of access. Such a temporary peer community can be set up either on a wireless local/metropolitan area network (e.g. IEEE 802.11g/IEEE 802.16a) or over a 3G platform such as UMTS, or even through other types of direct connections such as Bluetooth. The network access provider has control over the traffic of the mobile terminals, and the user has to trust the pervasive environment, including the resources and services available. As a result, this scenario can adopt an hybrid approach where some special nodes, mainly static and located in shops, agencies or restaurants, play an special role in the authentication, access control, and accounting processes.

We identify some working assumptions for the following main operations.

3.1.1 Identification and join

When a mobile node wants to join the community or wants to send a message but does not have a route to the group, it broadcasts a join request packet. According to the topology management service, e.g. On-demand Multicast Routing Protocols, a node receiving the request stores the upstream node ID and rebroadcasts the packet, and usually a *join table* is periodically broadcasted. We can consider different possibilities for authentication, using either a Trusted Third Party (TTP), a web-of-trust, or a location-limited mechanism. Some works have recently point out other mechanisms, such as Zero Knowledge Proofs and Byzantine agreements [4]. These are especially interesting in one-to-one interactions –a portal which presents information from diverse sources in a unified way often requires to have a centralized application; in that case, a single server may manage the credentials.

3.1.2 Trust metric

When transaction rating and user rating cannot be properly weighted, two straightforward strategies are to generously trust all strangers, or pessimistically refuse the interaction. Some works propose an adaptive strategy to deal with strangers, where first-time interactions with any unknown node are aggregated together. Later, a trust metric estimates the probability of being cheated by the next stranger and decides whether to trust the next stranger using that. Nodes thus decide whether to cooperate or not by using a probabilistic strategy. Note, however, that participants

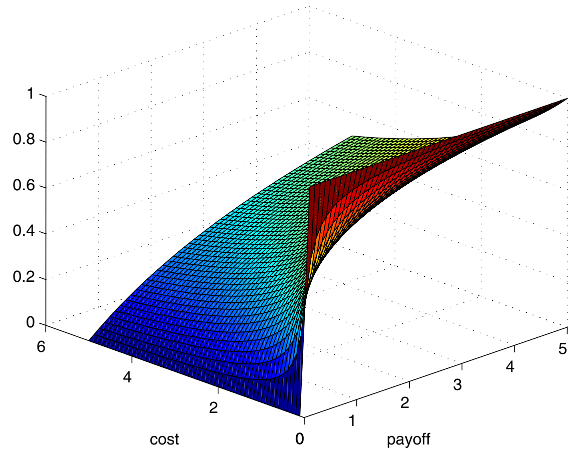

Figure 1. Nodes will collaborate when cost is less than payoff (maximum payoff and cost are 5 units.)

observe each other's actions, but not their strategies, which evolve over time. Furthermore, game-theoretic experiments have demonstrated that trust is close to rationality, since neither party has much to gain by deviating from the protocol, e.g in Internet auctions such as `eBay`.

Briefly, the system dynamics depends upon the conjecture that node P makes on the type of target T's behavior, and computes the ratio (cost over profit). P will adjust her threshold according to the interaction's evaluation. Fig. 1 shows the relationship between the ratio cost over profit and the threshold computed.

3.2 Deploying trust over M-P2P networks

The notions of trust and peers' reputation have been quite relevant in heterogeneous environments wherein no symmetry concerning nodes' collaboration, capabilities and trust exists. However, peers can misbehave in a number of ways, and anonymity incurs an additional challenge. Moreover, strangers –peers who have not interacted with others and, therefore, no trust information is available– constitute an interesting challenge for trust. Furthermore, some malicious peers may behave properly for a period of time and then, after reaching a good reputation, begin misbehaving. Therefore, the proportion of peers that are dishonest has too an impact in the design. Byzantine protocols, for example, assume that less than a third part of the peers will misbehave. This kind of approaches can tolerate a fraction of faulty or dishonest nodes, whenever a group of trusted peers collaborate.

We have identified several attack scenarios against trust in M-P2P, maninly some forms of cheating (fake accusations, and whitewashers, among others), DoS attacks, anonymity and the use of pseudonyms, and collusion attacks. Next, we briefly discuss some considerations and desired properties that should be considered when dealing with strangers in trust-dependent operations in M-P2P:

- **Naming and authentication.** The goal of these processes is to exclude attackers and unauthorized nodes from participating in main operational tasks such as routing, authentication, access and recommendation protocols. Malicious nodes and whitewashers may impersonate others and use the spoofed identities to launch false accusations and purify the bad reputation accumulated under their previous identity. Most accurate trust metrics have the property of increasing slowly with positive interactions, while decreasing very quickly when there is malicious behavior. Furthermore, the utilization of public key certificates (similar to PGP) and the infrastructure provided by some kind of authentication protocol based on signatures prevent from them. Finally, collusion is one of the most dangerous threats, since dishonest peers act together in efforts to impact honest's decisions. For instance, Sybil attack involves a stream of colluding recommenders boosting the trust of one badly behaved principal. These are also limited by the identity certification. Thus, peers need to be sure that the other party (especially the source, or the recommender) is really who she claims to be. On the contrary, anonymity has been an important consideration in the earlier P2P designs. In terms of trust schemes, and especially in mobile environments, anonymity incurs an unacceptable overhead of flooding and uncertainty about the credibility of the potential participant. One solution considers the existence of a self-organized public key infrastructure, such as the proposed in [2], or a hybrid architecture.

- **Routing and forwarding.** MANETs perform physical broadcast, and the efficiency of routes often depends on the honest collaboration among nodes, who may serve also as routers. Generally, the trustworthiness of routes is kept in order to exchange them among different peers. This raises a scalability problem. An encrypted channel can be created if nodes share a key. If the common key can be stored and shared by devices, the problem would have an easy solution. Otherwise, a pair-wise shared key has to be established on the fly, without requiring the use of any on-line key distribution center. Current solutions envisage probabilistic key sharing and threshold secret sharing.

- **Trust evaluations.** The lack of a central repository re-

Trust requirements	**P2P solutions**	**M-P2P applicability**
Node stability Node identity	Overlay mechanism for ad-hoc P2P	Persistent identifiers Hybrid architectures
Scalability	Decentralized trust	Mobile agents
Verifiable encryption	Secure trust models	Lightweight models
Authentication Key Management	Self-organized Public Key Infrast.	Hybrid architectures Credentials
Fairness	Incentives-based trust schemes	Hybrid architectures
Reliability Privacy	Decentralized data mngmt.	Storage resources Encryption
Stranger policy	Selection threshold Peer selection	Probabilistic strategies

Table 1. Trust requirements and M-P2P.

sponsible for the computation and distribution of recommendations makes difficult to form trust relationships in mobile networks. Firstly, heavy trust computation deals with nodes' limitations, e.g. its battery will be depleted faster. Secondly, distributed trust models must allow to compute weighted values locally, and rely on allied nodes for recommendations over a target as well. Here it is unrealistic to assume that every integrating node will behave honestly, even if they have systematically done so in the past. For instance, the main goals of the adversaries are, on the one hand, to disrupt the trust system by mounting degradation attacks and, on the other hand, isolate the well-behaving nodes.

Table 1 briefly summarizes the main requirements of trust systems, their classical solution in wired P2P networks, and how these may be addressed in M-P2P systems. For example, an efficient node identification may need an hybrid approach with some kind of super-nodes. Encryption demands concrete computational and communication requirements which must be taken into account. Moreover, each node may apply a local, individual stranger policy according to its security display, its history, or even its trust threshold. In summary, as mobile devices such as 3G cellular phones, PDAs and wearable computers, have become increasingly powerful, we believe that more robust security solutions should be deployed, particularly in service-oriented frameworks which have to react to a constantly changing context. Hence, we predict that security-related decisions will have a significant impact on the developments of M-P2P applications and their implantations.

4 Conclusions and research directions

Currently, MANETs and M-P2P applications can only exist and operate if nodes demonstrate a collaborative behavior. However, there may always exist dishonest nodes aimed at disrupting or corrupting the network. In this paper, we have discussed different challenges for M-P2P security and some of the problems concerning their deployment. Finally, a formalization of a certain scheme and some experimental results are needed to evaluate to what extend trust-enhanced security schemes may suffice to provide, for example, a basic authentication protocol.

References

[1] F. Almenrez, A. Marn, C. Campo, and C. G. R. Ptm: A pervasive trust management model for dynamic open environments. In *Proceedings of the First Workshop on Pervasive Security and Trust at MobiQuitous*, Boston, USA, August 2004.

[2] S. Capkun, L. Buttyán, and J.-P. Hubaux. Self-organized public key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 2(1):52–64, Jan-Mar 2003.

[3] D. Djenouri, L. Khelladi, and A. Badache. A survey of security issues in mobile ad hoc and sensor networks. *Communications Surveys and Tutorials*, 7(4):2–28, 2005.

[4] U. Fiege, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. In *Proceedings of the 19th annual ACM conference on Theory of computing*, pages 210–217, New York, USA, 1987. ACM Press.

[5] D. Grigoras. Challenges to the design of mobile middleware systems. In *Proceedings of the 1st Int. Symp. on Parallel Computing in Electrical Engineering*, pages 14–19, Sept. 2006.

[6] M. Haque and S. Ahamed. Security in pervasive computing: Current status and open issues. *International Journal of Network Security*, 3(3):203–214, 2006.

[7] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. In *Proceedings of the 9th International Conference on Network Protocols*, pages 251–260, California, USA, November 2001. IEEE.

[8] A. Mondal and M. Kitsuregawa. Privacy, security and trust in p2p environments: A perspective. In *Proceedings of the 3th International Workshop on P2P Data Management, Security and Trust*, pages 682–686, Krakow, Poland, September 2006. IEEE.

[9] M. Smith, T. Friese, M. Engel, and B. Freisleben. Countering security threats in service-oriented on-demand grid computing using sandboxing and trusted computing techniques. 66(9):1189–1204, 2006.

[10] Y. L. Sun, W. Yu, Z. Han, and K. Liu. Information theoretic framework of trust modeling and evaluation for ad hoc networks. 24(2):305–317, 2006.

[11] L. Zhou and Z. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, 1999.

[12] B. Zhu, S. Jajodia, and M. Kankanhalli. Building trust in peer-to-peer systems: a review. *International Journal of Security and Networks*, 1(1/2):103–112, 2006.