2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops

SP2MS: A MANet-based P2P Service

Marcelo H. Vithoft Altair O. Santin Cinthia O. Freitas Heverson B. Ribeiro
Pontifical Catholic University of Paraná / Graduate Program in Computer Science
R. Imaculada Conceição, 1155, Prado Velho, 80215-901 – Curitiba – PR – Brazil

{vithoft, santin, cinthia, heverson}@ppgia.pucpr.br

Abstract — Applications using P2P as an Overlay network in MANet (P2M) are very unstable in terms of MANet interconnections and P2P churn. MANet-based P2P applications usually create a considerable overhead on the P2P consumer due to the control of the end-to-end communication with the peer that provides the shared content. Moreover, traditional P2P networks offer polluted contents wasting the device´s scarce resources. This paper proposes a service that minimizes the P2M environment instabilities for mobile devices and reduces the probability of downloading corrupt contents. A prototype was developed to show that SP2MS can be easily integrated into the traditional P2P infrastructure.

Index Terms — Mobile Ad Hoc Network; Peer-to-Peer; P2P Content Sharing; Security.

I. INTRODUCTION

Peer-to-peer (P2P) networks can provide shared contents of many types, however its availability is affected by churn (peers frequently joining and leaving the network) [1]. The shared contents available in traditional P2P networks (e.g. Emule, Gnutella, etc.) are usually polluted, fake or corrupted (“P2P garbage”) [2].

MANets (Mobile Ad hoc Networks) are very unstable in their nodes connectivity, despite of its flexibility to be configured [3].

Applications in P2M environments have to deal with both unavailability and instability [3]. Thus, mobile devices can be connected with other peers that may leave the P2P network, provide garbage content, or disconnecting from MANet.

When P2P networks were proposed, an index repository to publish/find shared contents was not predicted. Contents publishing and searching were done through broadcast messages. Nowadays, Distributed Hash Tables (DHTs) are an alternative to broadcast messages. Thus, DHT provides the lookup service to P2P [4], with the advantage that a DHT is distributed and high available.

Based on overlay network, our proposal aims to supply a P2P service that releases the mobile peer (usually playing the role of a consumer in the P2P network) from the task of managing end-to-end connections with the peer providing the contents. This scheme allows hiding the instabilities of the P2P network from the consumer peer, so that the contents are transparently provided.

Moreover, the proposed P2P service intends to minimize the impact of the instability and unavailability, typically experienced by consumers using P2P in MANets. In other words, the shared contents are provided in a secure way, assuring integrity, authenticity and high availability. In this scenario, we also consider a semi-automatic migration of shared contents from the traditional P2P networks to a new approach based on P2M, the service oriented network.

The remainder of this paper is organized as follows. Section II briefly discusses relevant aspects of overlay, mobile and peer-to-peer networks. Our proposal is then introduced in Section III and applied to a scenario in Section IV. The prototype is presented in Section V and it is evaluated in Section VI. Section VII gives an overview of related works. Finally, conclusions are drawn in Section VIII.

II. OVERLAY, MOBILE AD HOC AND PEER-TO-PEER NETWORKS

The overlay network creates an abstraction layer on top of another network, allowing the transposition of the domains of the underlying network [5].

Peer-to-peer network (P2P) provides an end-to-end communication between two computers/devices. P2P networks are mainly characterized by the peer churn, decentralization, self-organization, peer acting as server and client at same time, and scalability. P2P networks are commonly deployed as overlay networks.

The JXTA is independent of programming language and transport protocols and the project aimed to interface P2P systems [6]. However, JXTA for mobile devices is based specifically on the Java 2 Micro Edition (J2ME) framework. JXME is the porting of JXTA for J2ME.

DHTs as overlay networks are organized sparsely as a key space derived from a hash table.

Each node of a DHT is responsible for storing a set of (key, value) pairs, obtained from the execution of a hash function over the key representing a value. At the network layer the DHT maintains a routing table with information about the known neighboring nodes [4].

Currently, DHTs are quite useful as index repositories for contents in P2P networks. The searches become settled when using DHT as opposed to the flooding strategies used in the most aged traditional P2P networks.

A MANet is a network with absence of infrastructure, so all nodes should play the roles of router and host. Thus, a node sometimes routes messages from a neighbor to another and sometimes sends or receives data through their neighbors [7].

This work has been partially supported by Brazilian National Research Council (CNPq), grant no. 550962/2007-7.

978-0-7695-4019-1/10 $26.00 © 2010 IEEE
DOI 10.1109/WAINA.2010.86

IEEE computer society

III. SP2MS Proposal

In our proposal a service peer named *VSP* (*Virtual Secure Service Provider*) intermediates the peer-to-peer connection, between consumers and providers, for a shared content.

The intermediation includes locating the contents providers, as well as managing the end-to-end connection between consumers and providers, maintaining the consumer's connection status, and providing the security (availability, integrity and authenticity) of the contents. As the intermediation is transparent for a consumer peer, it connects to a VSP as a common provider of shared contents. Despite the advantages of connecting to VSP, such option is not a choice for consumers. However, it is desirable for a consumer peer to always achieve a route that leads to VSP.

The VSP is served by an index repository, namely *DSP*, a *DHT-based service provider*, which is organized as a service oriented P2P network in a P2M. Each DHT node in the DSP is a neighbor VSP in the routing table of the overlay network.

The VSPs are implemented as nodes of a DHT overlay network supporting the DSP. That means a DHT node responsible for storing a key instantiates the VSP to manage the aspects related to such content. Therefore, all shared contents regarding a service are stored in the same DHT node. This strategy facilitates the service administration and allows customization when required by the service, without losses to the DHT scheme. Customization of DHT node could be required, when a shared content is highly demanded, for instance. In such case, the combination of hardware and software could be improved to support such requirement.

Additionally, a semi-automatic content migration strategy is proposed in order to obtain content from traditional P2P networks, so that content could also be used in the service oriented P2P network. The main goal of the migration scheme is to allow the acquisition of the content from a traditional P2P network, to get it classified and to make it available in the service network. It is done to assure content integrity (i.e. resources are free from malicious changes) and authenticity (i.e. the guarantee that the shared contents is not fake or polluted).

The classification of contents is based on a heuristic that pre-classifies all of them with a given degree of similarity [8]. Next, the results of classification should be evaluated and certified by a human – the service provider administrator. Thus, the VSP (Fig. 1) can publish itself as a service offer on the DSP, for a given content. When the content is available in the service network (DSP in Fig. 1) no classification will be necessary, since it is intact (consistent) and authentic. Moreover, shared contents from a trustworthy source can be directly published and made available on the service network.

The SP2MS is an overlay layer composed of a traditional and a service oriented P2P network. DIS and P2P providers represent the traditional P2P network, while DSP and Ad hoc were included in the service oriented P2P network (Fig. 1).

A consumer peer may require a shared content from a VSP which is responsible for storing such key – according the DHT node designator. But it may happen that the VSP does not have a service for it. In such a case, the VSP downloads the content, pre-classifies it and replies back to the consumer peer providing the shared content that have been classified with the greater probability of being authentic and unmodified. However, the VSP cannot assure the authenticity and integrity of contents that were not certified by a human and previously announced in the DSP. If the consumer peer agrees with those conditions, the VSP cannot be hold responsible for a possibly inaccurate evaluation of the automatic classification heuristics.

It is important to notice that for the VSP classification, the content must be downloaded from providers and be available in the VSP cache. Thus, the consumer can obtain simultaneous fragments from different offsets of the same content from the VSP cache with a good probability of no corruption in the whole content rebuilding.

When the VSP announces a service on the DSP, it also publishes the whole content hash and a list of fragments and their respective hashes. As fragments have not been yet downloaded, they are kept in the VSP cache until they are completely downloaded. After downloading the content, a consumer can announce itself as a content provider in the DSP, i.e., the consumer peer becomes itself a peer provider.

The VSP administrator is responsible for setting up the time span within which the content will remain in cache and the amount of memory destined to store it. In spite of the importance of such updating policies and caching maintenance techniques, they are out of the scope of this work.

Fault-tolerance of the VSP is obtained directly from the DHT overlay network self-organization. In the case of a failure in one VSP, a neighbor node in the DHT overlay network takes over the service providing, replacing that faulty node. Reconfiguration of overlay routing tables imply in losses of service state. So the node that took over should exchange messages with the consumer in order to recover the connection status (we will not go further here since fault-tolerance is beyond the scope of this work).

IV. Scenario

Multimedia shared contents such as audio, video, and so on are very common in traditional P2P networks. However, no guarantee is given about the content´s authenticity and integrity. The goal of our proposal is to provide these guarantees in a highly available fashion by using a service.

The scenario assumes that a shared content, once downloaded the first time will be fragmented and the integrity of each fragment and the whole contents is assured by a hash function. The digital signature of the VSP providing the service guarantees the authenticity of each fragment and the whole content.

Each fragment of content can be stored by different providers, since the DSP indexes each one of them. In fact, when a consumer searches for some content the VSP looks upon the DSP and gets a list of providers for each fragment making up the desired content.

The VSP obtains and provides one by one the fragments to the consumer, who can check the integrity and authenticity of each fragment individually. The same copy of a fragment can be stored in many different providers. After receiving all the fragments of a given content, the consumer rebuilds the original content joining together the fragments in the correct order. Then, the consumer verifies the whole content's integrity and the VSP signature in order to be sure about its authenticity.

The content is fragmented in order to make it highly available and aiming to provide more than one fragment simultaneously – if the consumer peer has enough bandwidth for it.

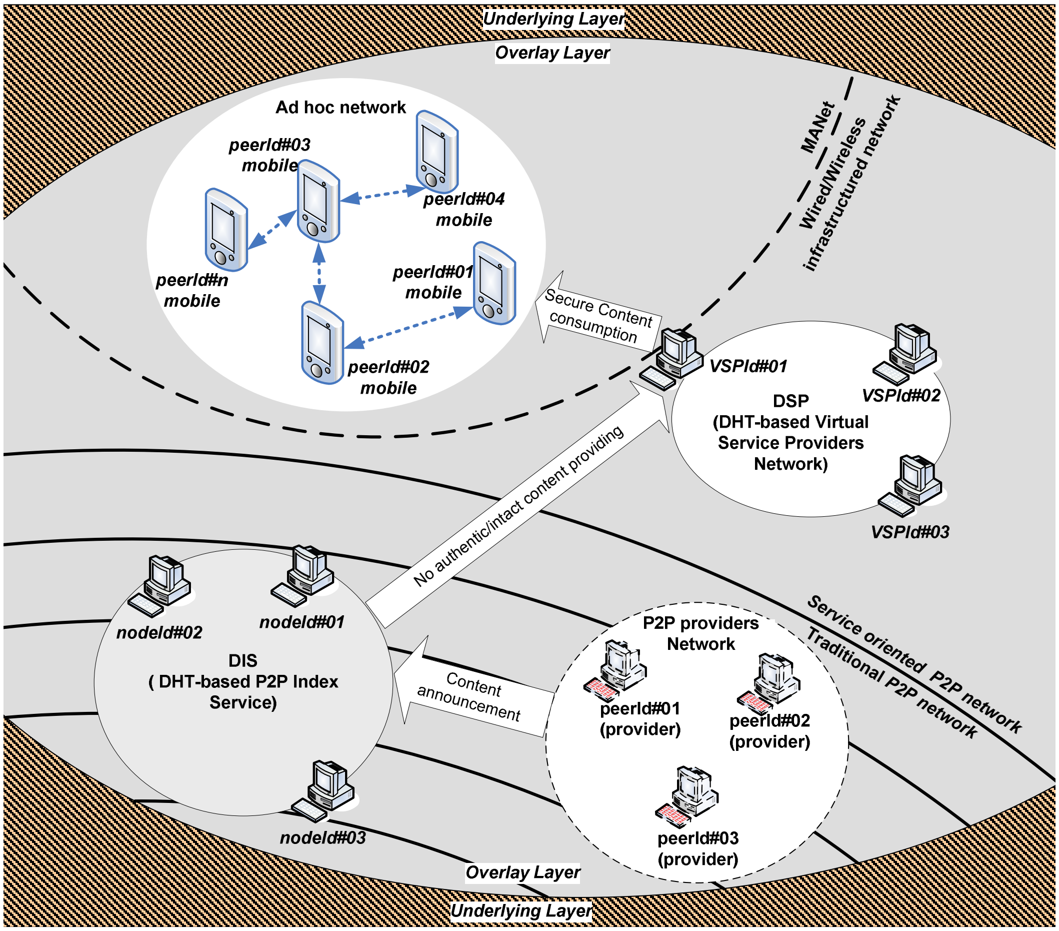

Figure 1: Overview of Proposal Environment

In traditional P2P networks if a consumer obtains different offset fragments from several providers there are no guarantees that all providers share the same content copy. Therefore, content corruption becomes very common in parallel downloads in traditional P2P networks, as the same content offset retrieved from distinct sources could be different.

Additionally, in our proposal the fragmentation is used to minimize the negative effect of bandwidth consumption experienced with traditional approaches. In other words, in traditional P2P networks it is only possible to find out that a content is fake or corrupted after it is completely downloaded. In our proposal after downloading the first fragment the consumer can verify its integrity.

V. Prototype

The prototype (Fig. 2) employs the *JXTA infrastructure* as a framework for P2P development and the Bamboo as *DHT* implementation [9]. NetBeans IDE 5.5 together with the toolkit for wireless communication [10] – emulates a mobile device – so that *JXME* is supported in the prototype.

In Fig. 2, all blocks identified as *APP* correspond to modules used to support the proposed architecture. The service network (*DSP*) which is composed of VSPs gets integrated into the Bamboo DHT as nodes of it.

The *administration GUI* module allows the management of the VSP, including setup of features and contents handling. The *history* keeps track of all unauthentic and corrupted contents, as well as those contents accessed by consumer peers and selected by automatic classification for human approval. It also helps the classifier heuristics on defining which contents are the most likely to be authentic. The history acts as a log file for the VSP service manager; it is updated by the content manager.

Integrity and *authenticity management* are performed by executing hash functions and digital signature, respectively, in order to make sure that some contents actually have such properties. These modules are invoked in order to verify the signature and integrity, and they allow the Service Manager to assure integrity and authenticity of content announcements.

The *classifier* uses a clustering technique to group contents by similarity. Then, based on similarity of contents and on the number of occurrences, the one most likely to be authentic is estimated.

The *content Manager* module is the core of the VSP, responsible for storing the contents of VSP cache and for offering an interface to handle the contents provided by the VSP as a service. The content manager searches for the provider, updates the *list of content providers*, manages downloads and *content cache* and invokes other necessary modules. The configuration parameters for content cached are configured through an administration GUI.

The *DSP Catalog* module records all authentic and unmodified contents available in the DSP. This module uses history as source of information. The Service Manager uses the DSP Catalog to announce content service on the service oriented network.

The *Service Manager* is the front-end of the VSP. It enables searches and downloads of contents, migration of contents from a traditional P2P network to DSP, management of the service status, management of downloading, management of content providers list, and integration of all VSP modules.

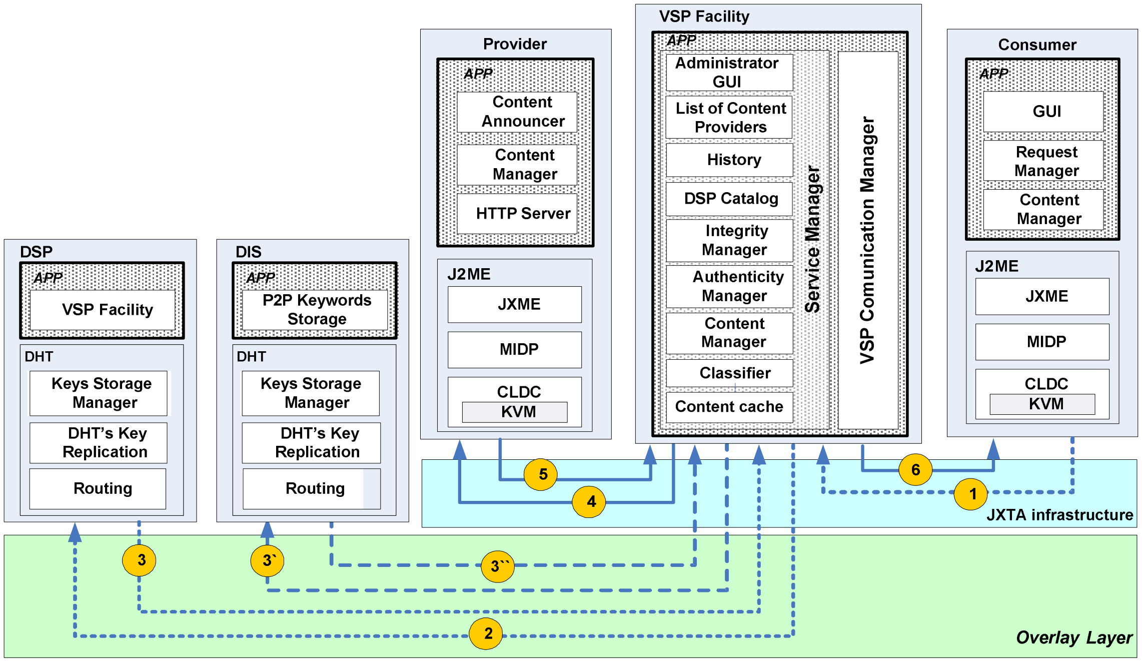

Fig. 2: Prototype Architecture Overview

The DSP instantiates the *VSP Facility* module whose goal is to support the network of VSPs, in addition to the typical DHT functions as routing, key (words) storage management and key replication.

The access to traditional P2P networks is implemented by a Emule client accessing Kademlia DHT. Kademlia represents DHT based P2P Index Service (DIS) that is used as *storage* for *P2P keywords* and therefore a resource for consumers to make searches through it.

Although provider and consumer entities are detailed separately for didactic purposes, in practice, each peer plays both roles according to its current needs.

The Provider *Content Announcer* module is employed on our prototype to publish on the DSP the availability of an intact and authentic fragment of some content. The Provider *Content Manager* module deals with local storage of contents announced and it offers an interface to handle the content maintained locally; it includes features to assure the integrity and authenticity of an announced content.

The *HTTP Server* implemented on the P2P server side, provides the contents to be downloaded through JXTA by the consumer peer.

Consumer *GUI* enables access to the resources on the consumer side. *Request Manager* offers an interface to the VSP for searching contents and manages the requests sent to the provider. The Consumer *Content Manager* handles download requests, rebuilds whole content from their fragments – after the download is complete, and verifies integrity and authenticity of the rebuilt content.

Fig. 2 shows the prototype overview. We assume that providers in the traditional P2P network have announced some contents in the DIS (DHT-based P2P Index Service).

The consumer initialization comprehends starting the CLDC (Connected Limited Device Configuration**)** and JXME in order to initialize the peer, which involves loading a configuration file with network information (host IP address, JXTA Proxy IP and TCP Port, JXTA relay IP, etc.). Then a peerID (associated to a groupID) and an input pipe are created and announced in the DSP. Additionally, when the peer stores content, acting as provider, it creates an output pipe that announces in the DSP all contents available.

In fact, the VSP initialization requires the bamboo node initialization, which in its turn loads the JXTA application to act as a P2P service provider. Moreover, all the service manager modules are loaded.

After the consumer initialization (bootstrap), the user may choose one of the following options: search a peer, send an announcement, search for content, or download the searched content. Event 1 (Fig. 2) represents a mobile peer requesting the service manager to search contents, even though it is unaware of the service infrastructure. The VSP, in its turn inquires the DSP invoking the *get function* of the DHT through the content manager. This causes the hash function to be applied to the searched content (key) and the overlay network routing the request to a VSP – the node responsible for that DHT key space.

The VSP pointed by the overlay network (event 2) is instantiated as a Bamboo node. VSPs are virtual nodes of the Bamboo DHT overlay network supporting the DSP. This means that a DHT node stores all information regarding a service provided by a VSP. To achieve such behavior on a distributed hash table, all the information concerning a content is stored with the same key, generating the same hash on the key space. Therefore, a single DHT node stores all key records and thus facilitates the management of information about a content, which is viewed as a service in our proposal.

If the searched contents have already been approved (certified) by a human and therefore published in DSP, the DSP returns the list of providers for those contents to the service manager (event 3).

The service manager, by means of the content manager, connects the active providers and starts the download of the required content via the http protocol (event 4). Each provider implements a basic http server to provide contents.

Information about the *http server* like the IP address, the TCP port and URL (relative path in the peer provider) are included in the content announcement, which is published in the DSP during the provider initialization.

After downloading the content, verified its integrity and authenticity, the VSP forwards it to the consumer (event 6).

If during event 3 the service manager does not find the desired contents in the corresponding DSP, the DIS is inquired (event 3'). So, DIS returns the list of providers on the traditional P2P network (event 3''), the classifier is activated and the aforementioned sequence is executed.

VI. Prototype Evaluation and Considerations

In order to evaluate the scenario described in Section IV, we developed the prototype presented in Section V and evaluated it in a controlled laboratory environment.

The main goal of the evaluation was to measure the impact that the introduction of a VSP causes to the response time for the consumer.

The instabilities of MANet were not taken into account since they do not concern our evaluation goal. The number of possible topologies that can produce conclusive evaluation results are countless. However, we chose to use a hybrid network scenario – composed of an infrastructure-based DSP network and a MANet for consumers and providers, because according to [11] the behavior of a DHT over MANet is unpredictable.

The MANet is composed of *N* laptops connected to each other forming the ad hoc network. In fact, *N/2* laptops act as providers and *N/2* as consumers and all the *N* laptops are interconnected. Each laptop may have a different signal range, but only one provider laptop and one consumer laptop are connected to the DSP.

The DSP network, based on an access point, instantiates a few VSPs, all of them having access to the Internet, i.e., the VSP can connect to Kademlia network directly, through the access point.

We distributed the content across the providers so that, in average, we had *N/2* hops between a provider and a consumer on the MANet. In order to a message to flow from a node and its neighbor we assume a time *t*, which is constant. Thus, the consumer total time, dt_M, to download a content directly from a provider on MANet is given by $dt_M = N/2*t$.

In our measures we observed that the VSP processing time introduce an overhead of *t* in the response time for the consumer, for both searches and downloads. Therefore, when a consumer requests some content to the VSP and it is on cache, the download time is $dt_C = dt_M + t$. However, if the content is not in cache and it should be retrieved from the provider on the MANet the delay is about 2*t, thus, $dt_P = dt_M + t + 2t$.

When a content is not found on the VSP and it should be obtained from DIS, the overhead to make it available for the consumer on the VSP cache is equivalent to 5*t, thus the $dt_D = dt_M + t + 5t$.

In our scenario, the time *t* represents 10% of the time to connect a consumer to a provider traversing *N/2* hops on the MANet, dt_M . In the following, we compare the acquisition of a content using the VSP with the same acquisition but now directly from a provider on MANet.

Summarizing, when a consumer gets content from DIS, a delay of 60% ($dt_D = dt_M + 6t$) is imposed. If it is done by provider on the MANet the delay is 30% ($dt_P = dt_M + 3t$), while from the VSP cache it is 10% ($dt_C = dt_M + t$).

If the consumer has enough bandwidth available, it can download more than one fragment in parallel from the VSP. In such a case, the download delay can be reduced significantly, because it is dependent only on the downloading route itself.

All the aforementioned measures were obtained by computing the average results of a hundred experiments and the variation coefficient observed was under 5%.

The main advantages of our proposal do not lie in the quantitative, but in qualitative point of view. The proposed service guarantees that the contents downloaded by a mobile application are intact and authentic. That is, the P2P application will not waste time downloading corrupt or unexpected content over the MANet. Therefore, we suppose the undesirable P2P traffic (junk content) will decrease significantly.

In regard to multiple providers, the service makes sure to their consumer that each fragment downloaded is not corrupt, independently of the provider. In other words, at the end of the download operation the consumer is able to concatenate all intact fragments in correct order to rebuild the original content.

The DHT natively replicates the P2P index keywords. Therefore, if a VSP becomes unavailable, one of its neighbors will assume its role. Moreover, VSP maintains the connection status with a consumer peer, allowing the transparent recovery in case of disconnection. The VSP hides the content providers, transparently replacing those that are unavailable to consumers.

The consumer does not need to manage each connection with each provider, since the VSP does this in a reliable way. From the consumer's point of view the VSP assumes the place of a regular provider, meaning the proposal was developed taking into account its compatibly with the current P2P technology; it works with no changes in the consumer side.

The VSP accelerates considerably the download of popular contents by using its cache in parallel downloads.

VII. Related Work

The performance of a P2P network based on DHT over MANet was evaluated by Cramer and Fuhrmann [11]. The evaluation through simulation highlights that the ability of the Chord DHT to perform consistent queries was badly affected by the MANet environment. The authors observe that happened due to the pessimistic strategy adopted by the simulator algorithm when a node leaves the network. In such a case, the algorithm simply terminates the pending queries by time-out. The results were nevertheless inconclusive.

Bisignano and his colleagues proposed an implementation framework whose goal is to hide connection instability from P2P application developers [12]. The implementation requires changes at the core of the JXTA in order to include functionalities like management of intermittent connections and multiple physical interfaces.

Availability, integrity, confidentiality and reputation along with their cost from the viewpoint of both development and processing are addressed by Campadello [13]. However, the focus of the work is authenticity, which is guaranteed by reputation mechanisms. It means, the peer trusts in the authenticity of some contents based on the reputation of its providing peer.

VIII. Conclusion

This paper presented a proposal to minimize the impact of the instability and churn of P2P networks over MANets in a context where security properties for shared contents are important.

The proposed scenario considered the semi-automatic migration of contents from traditional P2P networks to P2P service-oriented networks.

The *VSP* as a front-end that intermediates the connections between consumers and providers, maintains the compatibility with current consumer P2P applications.

The VSP enables: (a) searches and downloads of content, (b) announcements of content, (c) migration of content from traditional P2P network to DSP, (d) management of the service status, (e) secure provision of content whose origin is the service network, (f) management of the active providers transparently to the consumer, and (g) parallel downloads without the content integrity corruption.

The prototype developed showed viability and easy integration with traditional P2P networks over MANets as described in Section VI.

Our proposal took into account a case of P2P content coming from traditional P2P network. We only considered such source of content to show the proposal's real application, because we did not identify a better one. However, we do not approve illegal flow of content over any kind of network.

References

[1] Schollmeier, R., A definition of peer-to-peer networking towards a delimitation against classical client-server concepts. In Proc. of the 7th EUNICE Open European Summer School and the IFIP Workshop on IP and ATM traffic management, 2001, pages 131-138.

[2] Kumar, R., Yao, D., Bagchi, A., Ross, K., Rubenstein, D. Fluid Modeling of Pollution Proliferation in P2P Networks, In: Proc. of ACM Sigmetrics, 2006, pages 335-346.

[3] Perkins, C. E., Ad Hoc Networking. Addison-Wesley, Boston, USA, 2001.

[4] Stoica, I., Morris, R., Karger, D. R., Kaashock, M. Frans et Balakrishman, H., Chord: A scalable peer-to-peer lookup protocol for internet applications. In Proc. of the ACM SIGCOMM, 2001, pages 149-160.

[5] Andersen, D., Balakrishman, H., Kaashoek, F. & Morris, R., Resilient Overlay Networks. In Proc. of 18th ACM Symposium on Operating Systems Principles, 2001, pages 131-145.

[6] Oaks, S., Traversat, B., Gong, L., JXTA in a Nutshell, O'Reilly Press, 2002.

[7] Van Der Merwe, J., Dawoud, D., and McDonald, S. 2007. A survey on Peer-to-Peer Key Management for Mobile Ad Hoc Networks. *ACM Comput. Surv. Vol. 39*, no. 1, 2007, page 1.

[8] Oliveira, L. S., Morita, M, Sabourin, R., Feature Selection for Ensemble using the Multi-objective Optimization Approach. In Studies in Computational Intelligence (SCI), Springer-Verlag, 16, 2006, pages 49-74.

[9] PlanetLab: Home, available: http://www.planet-lab.org/, 2010.

[10] Sun Java Wireless Toolkit for CLDC Home, available: http://java.sun.com/products/sjwtoolkit/, 2010.

[11] Cramer, C., Fuhrmann, T., Performance Evaluation of Chord in Mobile Ad Hoc Networks, In Proceedings of ACM MobiShare'06, 2006, pages 48-53 .

[12] Bisignano, M., Calvagna, A., Di Modica, G., Tomarchio, O., Expeerience: a JXTA middleware for mobile ad-hoc networks, In Proc. of IEEE P2P, 2003, pages: 214- 215.

[13] Campadello, S., Peer-to-Peer Security in Mobile Devices: a user Perspective, In Proc. of IEEE 4th P2P, 2004, pages 252-257.