Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

Fairness and Access Control for Mobile P2P Auctions over MANETs

Hella Kaffel- Ben Ayed[1], Faouzi Jaïdi[2], Inès Doghri[3]

University of Manouba, National School of Computer Science, CRISTAL Laboratory, Tunis, Tunisia,
[1] Hella.kaffel@planet.tn, [3] ines.doghri@gmail.com
[2] University of el Manar, Faculty of Science of Tunis, Tunis, Tunisia, faouzi.jaidi@gmail.com

Received 25 July 2011; received in revised form 17 July 2012; accepted 20 July 2012

Abstract

Mobile ad hoc networks (MANETs) present similarities with Peer to Peer (P2P) systems in terms of decentralization, equality and autonomy. This results in the rise of new collaborative and spontaneous P2P applications over MANETs such as P2P auctions. The deployment of auctions over MANETS should provide new opportunities to the important marketplace created by mobile communities and may be a game changer in local markets when the mobile infrastructures are very pervasive. This business scenario implies multiple advantages such as ubiquity, availability, affordability, opportunity and spontaneity. Nevertheless, it faces various challenges such as fairness and security. In this paper we present a fully distributed architecture and a process designed to support P2P auctions over MANETs. The major goal of this paper is three-fold: i) to propose an estimation model of a fair round duration called Tfair (the bids collection duration) to fulfill fairness, ii) to propose a new scheme for access control and no replay that takes into consideration the unique constraints imposed by the crossing of MANETs, P2P and auctions, and iii) to validate the proposals by simulations. We prove the effectiveness of the proposed Tfair estimation model. We also show that the overhead of the proposed security solution is acceptable for the studied scenarios.

Keywords: Auctions, MANETs, P2P, Fairness, Security.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

1 Introduction

A Mobile ad hoc network (MANET) is a system of wireless mobile nodes that can freely and dynamically get organized into arbitrary and temporary *ad-hoc* network topologies [6]. Such networks are designed to operate in widely varying environments, from military networks to low-power sensor networks and other embedded systems. They allow people and vehicles to be internetworked in areas without a pre-existing communication infrastructure, or when the use of such infrastructure requires wireless extensions. Nodes in MANETs communicate directly or through intermediate nodes which relay the messages hop by hop between the sender and the receiver. Technologies like Bluetooth and Wi-Fi helped to enable commercial deployments of MANETs outside the military domain.

MANETs share the same features as Peer to Peer (P2P) networks i.e.: decentralization, scalability, autonomy and symmetry of peers. Hence, they have been considered to support the deployment of P2P services such as file sharing and e-commerce [17]. Auctions are e-commerce applications that can benefit from these P2P wireless networks. An end user, being in a MANET, has just to open his/her wireless device and expects to easily set up or access an auction event. Interested participants can submit their bids; the process will advance round by round till the best bidder wins the auction. This business scenario would befit the spontaneous markets created temporarily for auction events; for example markets set up in a harbor for the sale of stocks of fish, in a farm for the sale of the whole or a part of a harvest or for spontaneous events such as nomadic exhibitions [33]. The deployment of auctions over MANETs provides new opportunities to the important marketplace created by mobile communities and may be a game changer in local markets particularly in countries where the mobile infrastructures are very pervasive [17]. The real value perceived by the participants would be to use a pervasive auctioning service, with no extra cost and without the necessity to be connected to an infrastructure network. This scenario implies multiple advantages and motivations such as ubiquity, availability, affordability, opportunity and spontaneity.

When an auction is set up over a MANET, bidders are involved in the forwarding of bids without relying on a central entity. The following issues can be identified:

1. Fairness: During the bidding, a bidder may end a given round and starts the next one before receiving all bids sent by the other bidders, especially from the farthest ones. In addition, intermediary bidders can react before the other bidders in competition and may finally win the auction.

2. Security: A dishonest bidder could easily replay or delete bids, access and modify the content of bids while forwarding them on the network. Furthermore, any given node being within the ad hoc network can submit bids without being permitted to perform this task.

In this paper, we present an architecture and an auction process over MANETs. The goal of this paper is three-fold: i) we propose a theoretical model to estimate the fair round duration allowing the bidders to collect all received bids during each round, ii) we propose a new scheme for access control and no replay. This scheme takes into consideration the special constraints imposed by the crossing of MANETs as underlying networks, P2P as architecture and auctions as an application, and iii) we use simulations to show the effectiveness of the proposed model and to evaluate the overhead of the proposed security solution.

The remainder of the paper is structured as follows. Section 2 presents the literature review related to the addressed issues. Section 3 introduces the proposed architecture and process to support P2P auctions over MANETs. In Section 4 we present our estimation model of the fair round duration and the security solution. Section 5 depicts the performance evaluation of the proposals. Finally, in Section 6, we conclude the paper and present ongoing works.

2 Literature Review

Many studies consider the deployment of P2P auctions over the internet [7], [13], [18]. They address the design issues, and/or the economic contributions of P2P auction as well as the trading mechanisms and policies. Most of them focus on the case of double auctions where the choice has influenced the design issues of the proposed systems. In addition, these studies do not address fairness and security.

Few studies address the potential deployment of auctions over MANETs. Lin et al. [22] propose an architecture relying on an auctioneer entity which collects submitted bids. Fairness is fulfilled by the setting of a *Waiting timer*: received bids are saved within the network layer of the auctioneer. When this timer expires, the auctioneer's network layer delivers all received data to the application for evaluation. The best bid is then broadcast to all participants. This approach presents many weaknesses. The presence of a central entity (i.e. the auctioneer) having a vital role during the bidding activity is not suitable for the context of ad hoc networks as it will be explained further. Moreover, the periodic flooding of the current auction information in the network implies messages redundancy and may overload the network. Finally, the introduction of a processing specific to the application embedded within the network layer is not recommended. Frey et al. [15] propose a self-organizing distributed mobile auctioning system over MANETs. Communication is focused on a high density static geographic area, called the marketplace, in order

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

to substantially increase the probability that negotiating peers successfully reach an agreement. To ensure a reliable communication channel between two devices, the proposed solution allows messages duplication and uses acknowledgments. The main drawback of this approach is its overhead in terms of exchanged messages.

The above studies consider design issues to fulfill reliability, efficiency and scalability. Many of them are restricted to a specific auction type while none addressed the security issue.

Various studies propose architectures and mechanisms for access control in the context of P2P environments over the Internet. Winslett [39] introduces an authorization framework for open distributed systems. They consider the specific problem of access to computational resources in a grid environment. This framework helps in reasoning about the behavior of resource owners and their clients. Proofs of authorization are setup on the basis of the local information possessed by peers and their behavior parameters such as query answering, information push/pull, and information release policies. Bertino et al. [3] propose to use XML encryption files to enhance the previous approach with cryptographic access control.

The research community focused widely on controlling access to shared data over P2P systems. Some studies propose approaches using identity based access control to determine the access rules for resources in P2P systems. This kind of access control systems, called Discretionary Access Control (DAC), define protection policies to govern the access to the contents on the basis of the user's identity and the authorizations he/she possesses. They are generally used to limit a user's access to a file. The owner generally controls other users' access to the file. Access control lists are often used to implement the DAC policies [17]. Tran et al. [35] propose a trust-based access control framework extending the DAC model for P2P file-sharing systems. They integrate aspects of trust and recommendation models and define a reputation model that maps two dimensions into rating certificates: trust (a proportion of satisfied transactions) and contribution (measured in megabytes). This approach presents the following drawback: It assumes the existence of a node which classifies users, assigns each user different access rights, and authenticates nodes. This assumption is not suitable to the decentralized nature of MANETs. Gonzalez [17] proposes a scheme to provide authorization capabilities for file sharing over pure P2P networks. She uses public key certificates without relying on a public key infrastructure. Each peer classifies his/her contents according to several security labels, or clearances, stored as certificates attributes. These security clearances can be discretionally issued by the content provider. In order to be allowed to access a given content, a peer must have a security clearance of at least the same level of the content.

Studies using digital certificates, as medium for transferring access control data concerning a node, are called certificate based approaches. Digital certificates basically contain the identity (and other information) of their owners. Fenkam et al. [14] develop an access control system for mobile P2P collaborative environments using Authorization Certificates delivered only by specific powerful peers. They consider the specific case of Peer-to-Peer mobile teamwork environments built on the top of a P2P file sharing middleware. Users are requested to present their authorization certificate to the service providers. An authorization certificate conveys the following data: access right, user ID, object ID, expiration date and the issuer signature. Nevertheless, a certificate does not carry any information for the authentication of the owner such as a password. The certificate can then be used by malicious peers to authenticate them. Zhang et al. [40] propose a trusted computing architecture to enforce access control policies in P2P environments based on an abstract layer of trusted hardware. They use identities and certificates to integrate user attributes such as roles into the architecture. The verification of the certificates authenticity requires Public Key Infrastructures (PKI). Such an assumption constitutes a restrictive constraint for the deployment of auctions over MANETs, even if various approaches proposed to setup PKI over such networks [20],

Other studies use Role-Based Access Control (RBAC [32]) mechanisms as an alternative to models based on users' identities [27], [28]. In RBAC policies, permissions are assigned on the base of peer's roles (according to job competencies or responsibilities) rather than to individual users [10]. RBAC simplifies the administration and management of permissions. User membership into roles can be easily revoked. The use of RBAC provides scalability for P2P architectures because there is no need to configure privileges for every user of the system. Park et al. [27] introduce approaches for providing scalable role-based access control (RBAC) in two different architectures: requesting peer-pull (RPP) and ultrapeer-pull (UPP). The RPP architecture uses LightWeight Peer Certificates (LWPC) which include the following: a serial number, the peer's identity, the peer's authentication information, the peer's role information and the validity period. Additional fields can be included in the LWPC to convey application-specific information. All those fields are signed by the LWPC issuer such as the application role server (ARS). However, the decision of access is taken only by super-peers and regular peers have no direct access to resource providers. For this reason, these approaches are not suitable to P2P environment over ad-hoc networks since they assume a double architecture network. This may generate an overhead that affects the scalability of the system. This kind of architecture may also suffer from the sporadic connectivity which characterizes mobile ad hoc networks. Park et al. [28], introduce a controlled P2P computing architecture where access control providers take the decision according to the requesting peer's role. They use Web services through a middleware which retrieves the role information about the requesting peers from the role server and delivers it to the requestor. A policy metadata is then generated and transferred to the access control service provider. The access control decision is based on the policy metadata and the role data presented by the requesting peer. This approach belongs to the RPP architecture presented in [28] and is based on a role server. This feature makes this approach unsuitable for ad-hoc environments for the same reasons as for [27].

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

All these approaches propose mechanisms to provide secure communications and authorization in P2P environments. However, some of them have not considered the deployment of these environments over ad hoc networks [3], [39] and [40]. Approaches that consider mobile P2P environments are designed restrictively for file sharing systems aiming to limit the access to shared resources. For all of these reasons, the proposed solutions are not suitable for the case of P2P auctions over MANETs. Indeed, the superposition of auctions as applications, MANETs as underlying communication network and P2P as a paradigm makes the classical approaches fitted to each of these domains unsuitable for our studied context. To the best of our knowledge, we are not aware of approaches that take into consideration the unique features resulting from the crossing of these three domains.

3 Operation View

Centralized auction systems rely on a central auction server (the auctioneer) which provides the institutional setting for the auction [6]. Several studies have criticized this centralized architecture because of the following issues:

1. It may be restrictive since too many users can overload the server, making the whole auction process less responsive than the sellers and buyers would prefer [11]

2. The auctioneer is a trusted third party that may represent a weak point in the auction process since there are many possibilities for the auctioneer to cheat [36]

3. It may face difficulties while dealing with the autonomy of local markets. National markets may employ their own rules, monetary regulations, payment procedures, etc. [30].

4. It may suffer from the lack of flexibility due to auctions' parameters that are product dependants such as certification, auditing and the treatment of complaints [13]

In addition to these limitations of centralized architectures, auctions over MANETs have to cope with the specific features of these networks such as dynamic and unpredictable topologies, bandwidth constraints and transient connectivity [6]. When a centralized auction system is set up over a MANET, the auctioneer might be disconnected which could result in the inhibition of the auction process.

In a previous work [8], [9], we proposed a distributed architecture to support P2P auctions over MANETs where there is no more need for any moderator or any incentive structure (cf. Figure 1). The auctioneer's activities are carried out by the different participating peers who collaborate with each other. A peer entity can be associated with an auction initiator (Peer intitiator) as well as with a bidder (Peer Bidder) participating to the auction. The auction application processes installed in the peers' mobile devices are the end-users of this architecture.

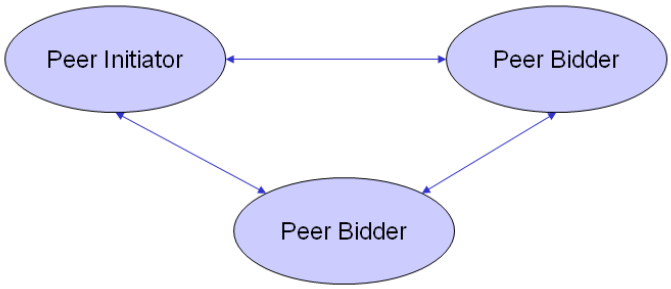

Figure 1: The system Architecture

As for the layered model of our architecture, we define a meta-layer within the TCP/IP stack, named P-auction, under the auction application (cf. Figure 2). This layer is responsible for providing P2P auction applications with required services such as fairness and access control. These services are provided to the auction application on the top and abstracting from the underlying wireless technology and independently from the auction rules and the technology used by the application. These features allow a further widening of our architecture to other underlying networks and other P2P applications.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

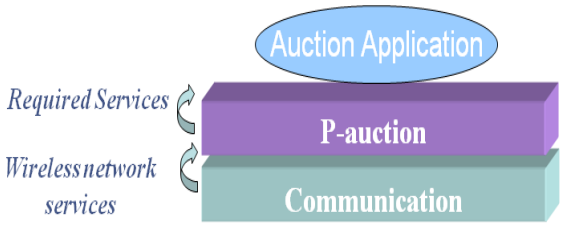

Figure 2: The layered model

As for the auction process, various studies described a typical auction process and identified the following steps: Creation of the auction event, requests for participation (or access), bidding and settlement [20], [21]. The initiator and bidders registration is supposed to occur separately.

We define a dynamic P2P auction process through which the peers have to go without the intervention of any central entity [8], [9]. For the sake of simplicity we consider English auctions as a case study in the rest of the paper. However, our proposal is generic with regards to the auction type. The process is composed of the following steps:

The initialization

a. The advertisement: The initiator **I** announces the auction by broadcasting an Auction_advertise message in order to inform all nodes about the auction event to be set up.

b. The access: Each interested peer sends a request for registration (Register_bidder message) with his/her identifier and personal information to the initiator as soon as he/she receives the advertisement message.

c. The Service creation: The initiator broadcasts a service creation message (Auction_create message) to registered participants.

Figure 3 presents the initialization for an auction involving two bidders B1 and B2. Messages between **I** and B2 might go through B1 depending on the network topology.

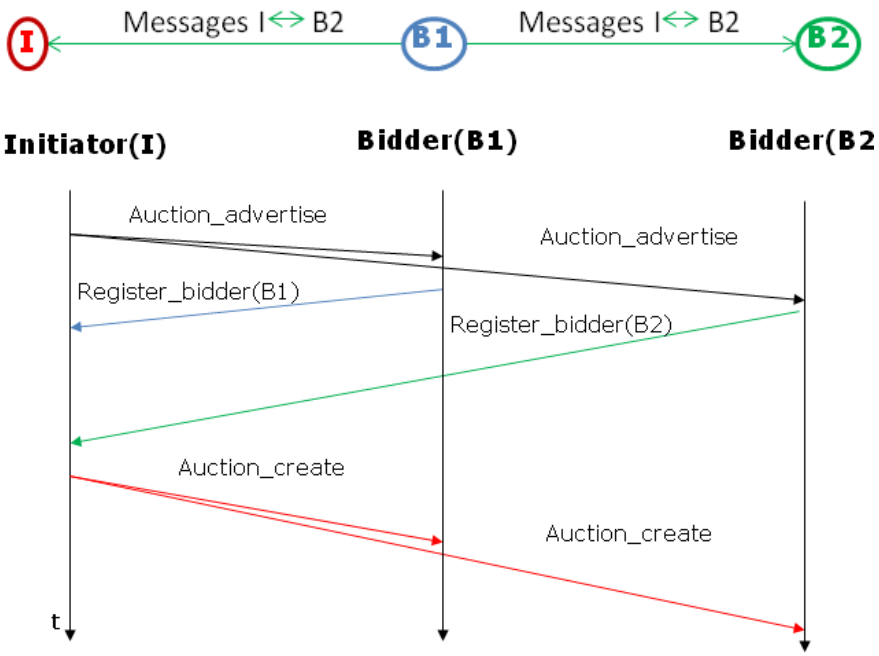

Figure 3: The initialization

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

The bidding

The bidding activity can be organized in rounds. The number and the duration of rounds depend on the auction type. Bidders can bid during each round. Each peer bidder sends a Submit_bid message to the other bidders as soon as he/she receives the Auction_create message and collects the Submit_bid sent by the other peers. For each round j, there is a clearing time during which, each bidder evaluates the collected bids and determines his/her winning bid relative to the round j. If some bids are lost due to wireless communications, they will not be evaluated by all the bidders. A peer bidder can leave the auction by sending an Exit_message to the other bidders as well as to the Initiator of the auction. Figure 4 presents the Bidding for a three rounds auction involving an intiator I and two bidders B1 and B2 for the same network topology as in Figure 3. During each round, a Submit_bid i_j conveys the bid of bidder i during the round j.

The Closing

The decision about the winner (i.e. the bidder having submitted the best bid) of the auction must be taken. If during the very last round one or more Submit_bid messages are lost due to wireless communication, a congestion or bidders disconnection, this might result in a possible inconsistency of the winner determination. To prevent this, we propose that the decision about the auction winner is taken in two steps. We define two clearing times.

i. After the expiration of the very last round, each bidder determines the winner among all collected bids and his/her own bid. If he/she is the winner, he/she sends a 'Winner_notif' message to the initiator.

ii. The second clearing time occurs at the initiator: After having collected all 'Winner_notif' messages, this latter identifies the final winner of the auction (B1 in Figure 4). The transaction settlement occurs between the initiator and the winner and implies a unicast messages exchange (we assume the winner(s) remain connected to the ad hoc network). The settlement is not in the scope of this work. Figure 4 depicts the messages exchanged during the Bidding and the Closing.

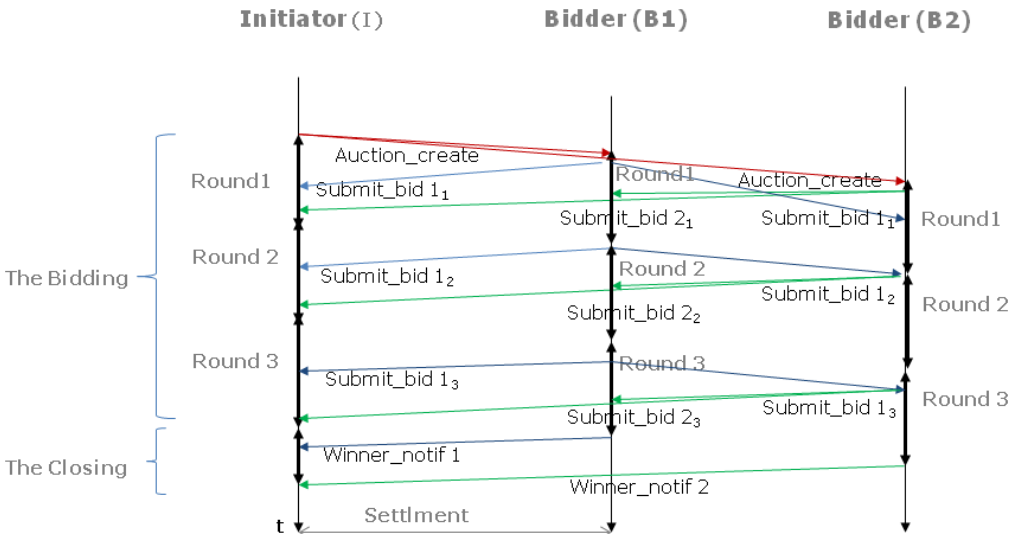

Figure 4: The Bidding and the Closing

4 Fairness, Access Control and No-replay Services

In this section we address the fairness and security problems and depict our approaches toward fair bidding and access control.

4.1 Fairness

Here, we emphasize the requirements of the system as for fairness. We focus on giving every bidder an equally fair chance for submitting a successful bid. To do so, we propose an estimation model of the waiting time allowing each bidder to collect all submitted bids for each round.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

4.1.1 The Requirements

Fairness is a big challenge concerning all auction types [1], [2], [11], [20], [22], [23], [26], [29], [31]. A fair bidding is reached when the following requirements are fulfilled:

- Requirement 1: No bidder should have more information than any other to determine his/her bid
- Requirement 2: All submitted bids during a round should be evaluated during the same round
- Requirement 3: The bidder sending the highest bid should win the auction
- Requirement 4: The auction winner must pay, as determined by the predefined published rules

Although fairness has been considered as optional for Internet auctions, it is not the case for auctions over MANETs for the reasons cited in the Introduction and illustrated in Figure 4. We observe the following:

(i) During the bidding, a bidder may end a given round j and start the round j+1 before receiving all bids sent by the other bidders, especially from the farthest ones. As a result, fairness requirement 2 is not fulfilled.

(ii) At the end of the auction lifespan, the auction initiator I receives the Winner_notif messages of 1-hop distance bidders (B1) before messages from 2-hop distance bidders (B2) or a 3-hop distance bidders or more in the general case. In Figure 4, I receives the winner_notif of B1 and closes the auction before receiving the Winner_notif of B2 even if this message might convey the best bid. B2 would be the winner of the auction instead of B1. When this occurs, fairness requirement 3 is not satisfied.

4.1.2 The Mechanism

Our goal is to provide the auction application with an estimation of the waiting time allowing each participant to collect all submitted (and received) bids for each round [8], [9]. We call this duration Tfair. This estimation would be a tool provided to the application to inform it about the waiting period for the different peers in order to determine the clearing time for each round. We contribute this way to give every bidder an equally fair chance for submitting a successful bid and fulfill this way the fairness requirement 2. Moreover, the design of the Closing combined with Tfair allows satisfying the requirement 3.

In a previous work [16], we proposed a static estimation of Tfair. In this paper, we define a model for the estimation of Tfair while taking into account: 1) the dynamic parameters of the networks such as the end-to-end delay and 2) parameters from the applications: in Internet auctions, the number of bidders increases very fast during the last few minutes of the auction lifespan. More than thirty percent of the bids are submitted during the last five minutes. of the auction process. This process may close before a number of important bids arrive [23], [25], [37]. In some auction Web sites, the auction time may consist in a main part and an extension part, which can be extended (i.e. starting from 3 minutes as an initial extension down to a few seconds at the very end) whenever a bid arrives shortly before the auction ends [29], [38]. Hence, to take into consideration this phenomenon, Tfair should increase with the round number.

For our estimation model, we rely on the Initialization step of the P2P auction process. We consider the two farthest peers from the initiator (farthest and penultimate peers in Figure 5).

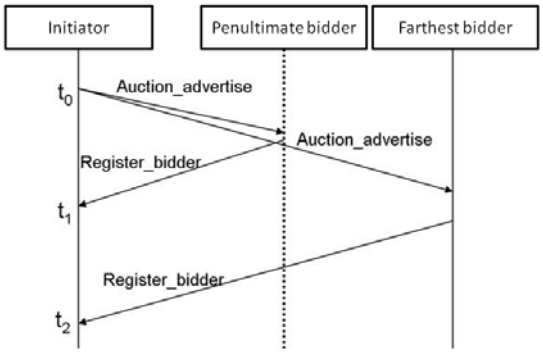

Figure 5: Registration of the farthest and penultimate bidders

As shown in Figure 5, during the Initialization the initiator sends the Auction_advertise message at t_0. He/she receives the register message from the penultimate peer at t1 and from the farthest peer at t_2.
We assume:

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

1. K: the number of hops between the farthest peer bidder and the initiator during the initialization phase.

2. $D(t) = t_2 – t_0$

3. $D'(t) = t_1 – t_0$

Taking into account the dynamic topology of the ad hoc network supporting P2P auctions as well as the increasing of the number of bids at the very end of the auction lifespan, we note f(i) as the additional number of hops at a given round i of an auction. Asymptotic function for f(i) has been revealed reasonable for ad hoc networks (f(i)=log(i)) [24]. As a result, we propose the following estimation model of the minimal Tfair for each round i:

$$Tfair(R_i) = \frac{1}{2} * \left(D(t) + D'(t) + f(i) * \frac{D(t)}{K} \right) + T(submit) \quad (1)$$

With:

- (D(t)+D'(t))/2 is considered as the worst Tfair during the initialization phase. The factor 1/2 divides the estimated RTT (Round Trip Time) to have the one way delay.

- D(t)/K is the transmission delay over one hop during the initialization.

- f(i)*D(t)/K corresponds to the additional transmission delay for the round i.

- T(submit) is the transmission time of Submit_bid message for a given round. If we assume N the number of peer bidders (N= number of registered bidders), every bidder sends each bid to the other (N-1) bidders and collects (N-1) bids. So, the transmission delay of $(N-1)^2$ messages is computed as follows:

$$T(submit) = K * (N-1)^2 * \frac{size(submit\_bid)}{throughput} \quad (2)$$

In the proposed model, Tfair has a slow growth with the number of rounds. At the end of the auction, the last round has the most important Tfair. This permits to consider the increasing of the number of bids during the very last minutes of an auction lifespan. Furthermore, this model is dynamic similarly to the basic features of MANETs.

4.2 Access Control and No-replay

In this section, we identify the vulnerabilities and the security problems that the considered system faces. Then, we focus on access control and no replay services. We present the mechanisms and the design of the proposed security approach. We try to be as generic as possible with regard to the auction type.

4.2.1 The System Vulnerabilities

Ad hoc networks have to cope with the same kinds of threats as their wired counterparts, as well as with new vulnerabilities specific to the ad hoc context such as wireless vulnerabilities, limited physical security and dynamic network topology [6], [34]. On the other hand, several threats have been identified and can occur during an auction process [4], [36]. P2P auctions over MANETs are subject to general communication threats linked to the mobile ad hoc environment and to specific threats related to the nature of the application. Some of these threats are increased due to the ad hoc environment such as attacks against the integrity of bids, illegal access to auctions and replay attack. In a previous work [16], we addressed the bids integrity issue. In this paper, we focus on illegal access to auctions and replay attacks. The replay consists in intercepting messages and playing them again in the same or a further round/auction. The access to auctions by malicious peers as well as messages replay can disturb the bidding process.

4.2.2 The Requirements

Our goal here is to define an appropriate access control mechanism, which limits the activity of legitimate bidders and serves as an obstacle to dishonest ones. This mechanism aims to determine if the peer attempting to submit a bid is actually authorized to participate in the bidding. The requirements for an access control system in mobile P2P auctions systems are derived from requirements for access control in mobile ad hoc systems, access control in P2P systems and access control in auction systems.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

For Internet auctions, access control mechanisms are usually centralized and controlled by a central entity i.e. the auctioneer. They operate under the assumption that all principals (bidders) are known (registered) by the auctioneer which gives all registered bidders the same rights during the bidding.

Many specific features of ad hoc networks introduce new requirements for access control: i) working offline from any central point of administration, ii) mobile computing in area without infrastructure, iii) using various mobile devices that often lack resources for running conventional security mechanisms, iv) a sporadic connectivity and v) a dynamically changing topology. These features present a challenge from the point of view of the security mechanisms that should be applied to provide access control.

Access control in P2P systems principally rejects the concept of central authorization control for many reasons: 1) many peers are often responsible for the resources they provide; 2) scalability is often an issue in P2P networks.

P2P auctions over MANETs introduce the following requirements for access control:

- Decentralization during the bidding
- Off line working from any central point of administration during the whole lifespan of the auction process,
- Dynamicity of the group during the bidding.
- Involvement of bidders in more than one auction
- The transient connectivity makes that peers may be temporarily disconnected from the MANET.

4.2.3 The Proposed Mechanisms

To superpose the features of ad hoc networks, mobile P2P systems and auction systems, we consider each P2P auction over a MANET as a group of bidders who are allowed to participate to the bidding. We propose a hybrid access control scheme:

- A centralized access control performed by the initiator of the auction during the Initialization. All authorized bidders are then known by the initiator. An Access Control List (ACL), containing the list of registered bidders is set up by the initiator and delivered to registered bidders after the creation of the auctioning service (conveyed in the Auction_create message). This list is updated at the end of each round when peers join or leave the service.
- A distributed bid admission control is performed by each bidder during the Bidding while using the received ACL. This control prevents unauthorized bidding from peers that are not registered.

As for the medium for transferring the access control information on authorized bidders, this can be achieved through the use of authorization certificates. However, the absence of infrastructure and the decentralized nature of the system make approaches based on certification authorities inapplicable here. Hence, we rely on authorization tickets which are generated and delivered by the initiator to the different peer bidders during the Initialization. Tickets prove bidders' rights to participate to the bidding. An authorization ticket is composed of the following fields:

- Ticket Identifier: a unique value to identify the ticket such as serial number.
- Auction Identifier: a unique value to identify the auction.
- Peer bidder's Identifier: a unique value to identify the bidder.
- Peer bidder's Public Key: We assume that each bidder has a key pair (public and private). The public key of the bidder is conveyed in his authorization ticket.
- Peer bidder's Authentication Information: a password used to verify the link between the ticket and his owner. In order to prove that he/she is the owner of a ticket he/she sends, a given peer must provide a correct password that matches with the password included in the ticket. There are two ways to secure the password :
    - To encrypt the password: This requires a cryptographic keys management and more processing than the previous way.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

- To hash the password: simple to use since it does not require cryptographic keys management and reduces data processing within nodes. We choose to use this solution considering the limitations of nodes' capacities and the features of mobile P2P environments.

- Extra field: reserved to a future use. It could be the Ticket Validity Period. For the present case of auctions, the ticket remains valid during the bidding process. This field can also be used to store auction dependant data.

- Initiator Signature: this allows checking the ticket validity and integrity.

The ACL contains the identifier and the ticket of each registered bidder. This list contributes to prevent unauthorized access and to detect malicious peers whose goals are to disrupt normal bidding process. For example, peers who left the service are removed from the ACL. However, one of them, peer Bi, can try to participate to the bidding while using his/her ticket, which might remain valid. This will be detected by the other bidders as a malicious access to the bidding since Bi is no longer in the ACL.

In order to prevent the replay of exchanged bids, we propose to include a nonce in each message. It is unique for each message and easy to check by peers for a quick bid admission control. We propose to calculate the nonce as follows: the identifier of the current round *ID_Round* encrypted using the private key of the sender.

$$Nonce = P_E^- (ID\_Round) \quad (3)$$

where P_E^- is the private key of peer E and ID_Round is the current round identifier.

4.2.4 The Design of the Security Solution

In this section, we present the additional messages, header fields and processing generated by the security mechanisms.

For the Initialization phase:

- The public key of the initiator (I.pubkey in Figure 6) is conveyed in the Auction_advertise to allow the nodes to check the received tickets. The Register_bidder conveys the public key (Srce.pubkey) and the hashed password (H(pwd)) of the peer bidder.

- Cryptographic processing is performed by the initiator in order to sign authorization tickets.

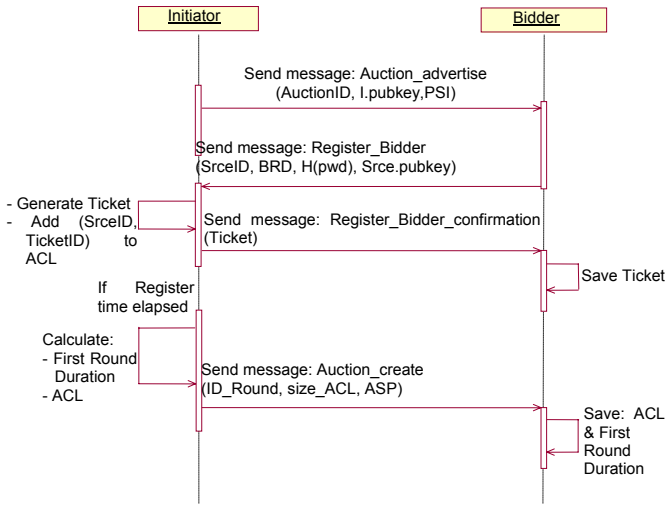

Figure 6: The Initialization

For the Bidding phase:

- We incorporate the ticket, the hashed password and the nonce in the structures of the Submit_bid and the Exit_message.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

- Cryptographic processing is also performed by the different bidders in order to verify the ticket, the password and the nonce or each received message.

Figure 7 describes the activity of bidders during the bidding: A given bidder starts the bidding when he/she receives the Auction_create. He/she calculates his/her bid and sends it in a Submit_bid message. He/she also collects the received bid during Tfair. For each received bid the peer bidder checks the nonce, the authorization ticket and the password. At the expiration of the Tfair period, he/she computes the next bid value and takes a decision about continuing the bidding activity or leaving the auction.

For the Closing phase:

- We include the ticket and the hashed password in the structure of the Winner_notif message.

- Cryptographic processing is performed by the initiator in order to check the ticket and the password of the sender.

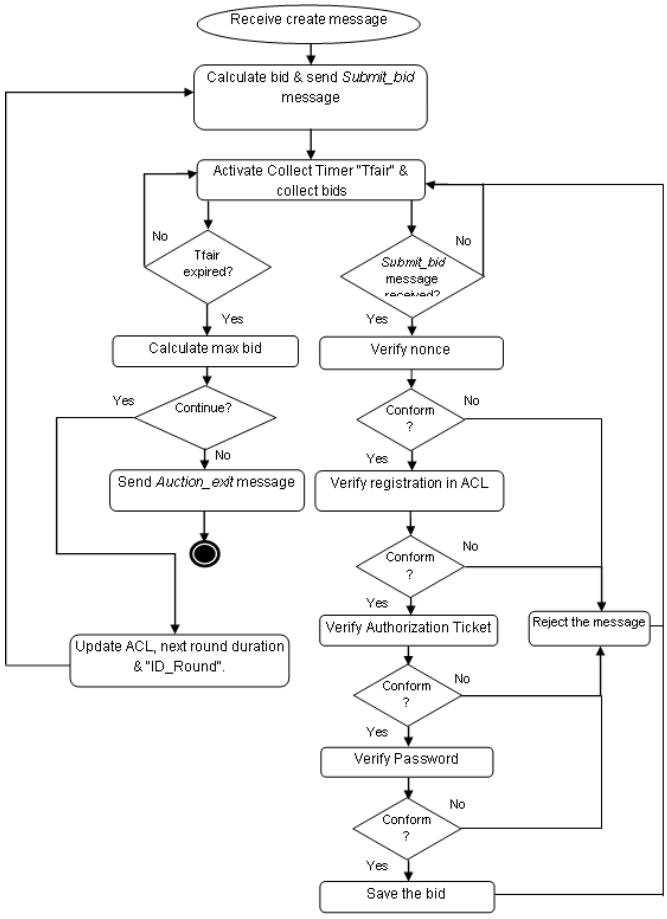

Figure 7: The bidder activity during the Bidding

5 The Performance Evaluation

The use of simulation techniques in the performance evaluation of communication networks is a consolidated research area. Hence, to evaluate the performances of our proposals, we used NS-2 simulator with CMU extensions to support MANETs [12]. We implemented the P2P auction system and the proposed mechanisms for Tfair, access control and no reply. We defined the following simulations scenario:

- Nodes' speed equal to 1 meter per second.

- A pause time equal to 5 seconds.

- Random waypoint mobility model [5] and AODV as a routing protocol.

- We varied the node Population from 10 to 70 nodes.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

- The considered simulation areas of the network were 183m x 183m, 258m x 258m, 408mx 408m, 483m x 483m and 578m x 578m for the 10, 20, 50 and 70 node networks respectively (ensuring the network density of around 300 nodes=km2).

We performed 30 runs for each simulation and computed the 95% confidence interval for all simulations' results. We assume that the initiator remains connected to the ad hoc network during the whole auction service life cycle.

5.1 Validation of the Tfair Estimation Model

Our goal here is to show how the theoretical estimation of Tfair is realistic. To do so, we first estimate Tfair via simulations than we compare the values obtained by simulations with those computed according to our proposed model (1). To determine the values of Tfair via simulations, we varied the following simulation timer: The Round timeout, e.g. the end of the bids collection duration for each round. To measure the rate of bids that are missed by each bidder after the round timeout, we define a metric named Bid-out-rnd (4).

$$\text{Bids-out-rnd} = \frac{\sum_{j=1..\text{Size-ACL}} \text{Bids-out-rnd/bidder}_j}{\text{Size-ACL}} \quad (4)$$

With:
Bid-out-rnd/bidder: The rate of bids out of round for each peer bidder. These are bids received by each peer bidder after the round timeout has elapsed. Bid-out-¡rnd/bidder is computed while considering the total number of rounds for each auction set up as well as the total number of received bids during each round.

Size_ACL = the number of registered peer bidders.

Tfair is the collect duration that corresponds to a bids-out-rnd/bidder equal to zero.

In order to compare the estimated values with values obtained by simulation for the same scenario, we have implemented the estimation model (formula (1)) and also used simulations. Figure 8 shows that the curves of estimated Tfair according to the proposed model (theoretical Tfair) and Tfair computed by simulations (simulation Tfair) are close for networks with 30 and 40 nodes. For a network with 70 nodes the values of Tfair in the two curves belong to the same time interval [20 sec, 30 sec]. We also see that the theoretical Tfair curve is lower than the simulation Tfair curve. This can be explained by the fact that during the simulations, the round timeout was varied intuitively (5sec, 6sec, 8sec, 10sec, 20sec and 30sec) in order to obtain Tfair. The accurate values of theoretical Tfair correspond to the interval [5sec, 6sec] and [20sec, 30sec] where the Bid-out-rnd is equal to 0. These results prove that the proposed estimation model of Tfair is realistic and efficient for the considered simulation scenario.

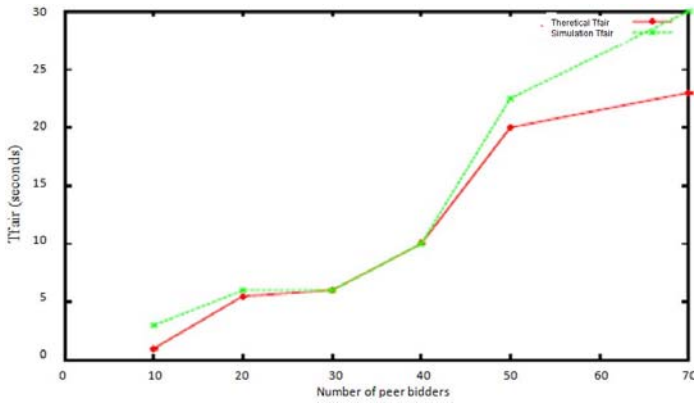

Figure 8: Theoretical Tfair vs. simulation Tfair

5.2 Performances Evaluation of the Security Solution

Security services of any kind have usually significant performance overhead. Our goal here is to evaluate the overhead of the security solution. For that, we used the same simulations' environment and scenario as previously. For the implementation of the cryptographic processing, we included the OpenSSL library (Site 1), SHA (Secure Hash Algorithm) to hash passwords, RSA for nonce encryption and combined both of them for the tickets signature.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

5.2.1 Overhead on the Initialization

For the Initialization we define Tregister as the duration that gives the chance to all mobile nodes to join the auction event. This is a waiting period that permits the initiator to collect all Register_bidder messages. For the system without access control, Tregister is the total time from the instant the initiator broadcasts the Auction_advertise until he/she receives the last Register_bidder. For the system with Access controls, Tregister is the period of time from the instant the initiator sends the Auction_advertise until he/she sends the last Register_bidder_confirmation. The overhead of the security solution is measured as the variation between the two values of Tregister.

To determine the values of Tregister, we varied the following simulation timer: Register timeout, e.g. the end of the *Register_bidder* collection duration. To measure the rate of messages that are missed by the initiator after the register timeout, we define a metric named Register-out. Tregister is equal to the register timeout for Register_out equal to zero (see Figure 10).

For simulations of the system . *w*ithout security, Register_out is computed according to the formula (5) and corresponds to *Tregister without access control* in Figure 9. For simulations of the secured solution, it is computed as in formula (6) and corresponds to *Tregister with access control* in Figure 9.

$$\text{Register - out} = \frac{\text{Register - Nb - out}}{\text{RegNb}} \tag{5}$$

With *Register-Nb-out* = the number of Register_bidder messages received out the register timeout.

$$\text{Register - out} = \frac{\text{Register - Confirmation - Nb - out}}{\text{RegNb}} \tag{6}$$

With:

- *Register-out* = Rate of registrations out the register timeout.
- *Register-Confirmation-Nb-out* = Number of Register_bidder_confirmation received out the register timeout.
- *RegNb* = Total number of registrations.

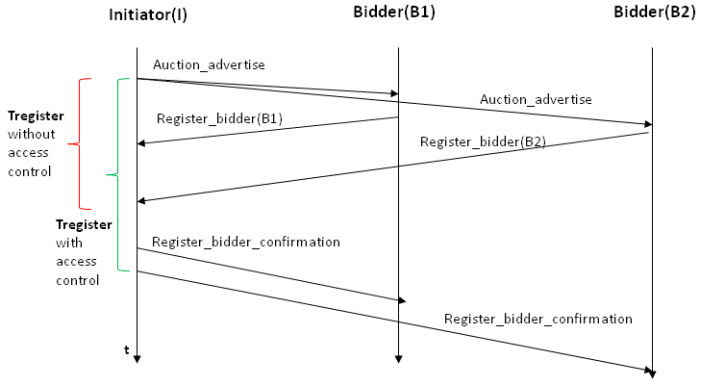

Figure 9: Tregister estimation

Figure 10 plots the comparison of Tregister values for secure and non secure systems. In these simulations, we evaluated the Register_out rate for different values of Register timeout. This rate is equal to zero when the Register timeout reached 11.04 seconds for the system without access control and 11.68 seconds for the system with access control. The curve shows an increase of Tregister in the secured system with 0.64 seconds compared to the unsecure system.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

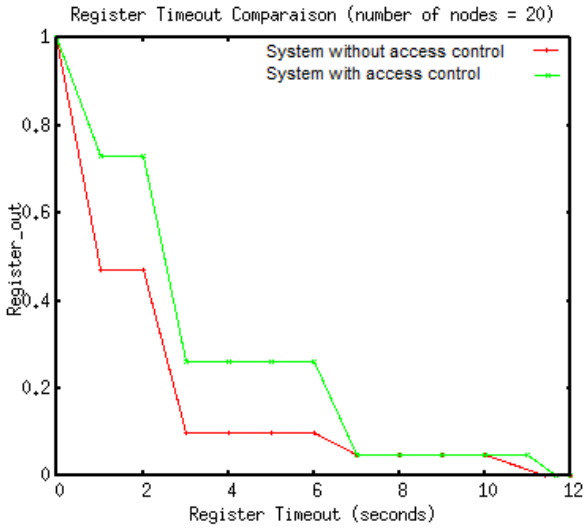

Figure 10: Initialization phase: Register timeout vs. Register_out Rate

In Figure 11, we evaluate the Tregister values while varying the number of nodes in the ad hoc network. We can see that Tregister increases when the number of bidders becomes important. For instance, Tregister for the two systems are close for 10 nodes. For a 90 nodes network, Tregister of the secured system increases by 2 seconds higher than the unsecured system. This is explained by the fact that a new message (Register_bidder_confirmation) is defined for the secured system. This message is delivered to peers during the registration. Furthermore, the security solution introduces cryptographic processing at the initiator's side. However, since the registration phase is occurring just once in the whole auction's lifespan, this raise of Tregister measured in seconds can be tolerated.

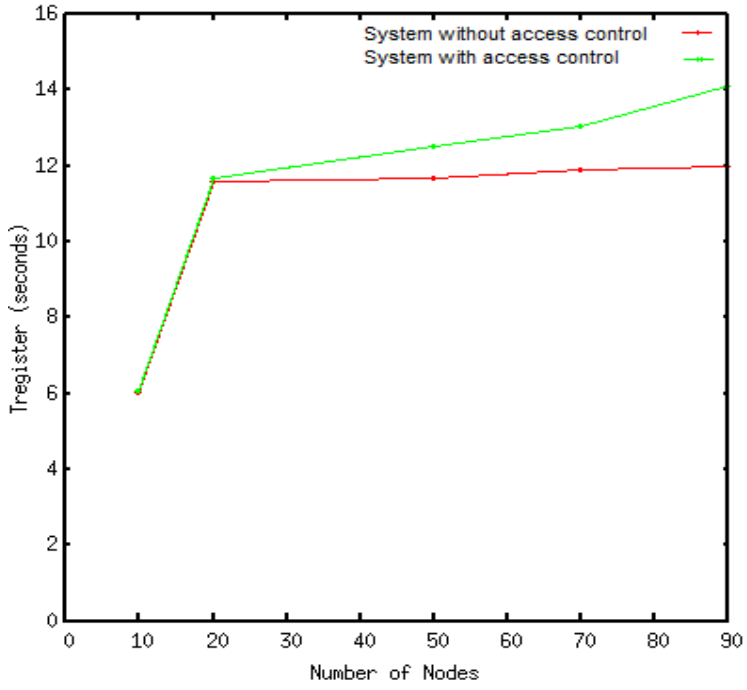

Figure 11: Initialization phase: Tregister vs. Nodes Number

5.2.2 Overhead on the Bidding

The overhead of the security solution is measured as the increase of Tfair. Figure 12 shows that the curves of Tfair without access control and Tfair with access control are close. Hence, we can say that the impact of our security solution on Tfair is less important than on Tregister. This is explained by the fact that we introduce new cryptographic processing during the bidding but no new additional messages. This raise of Tfair, measured in few seconds, can be considered insignificant compared to the round duration that can be measured in minutes or more.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 7 / ISSUE 3 / DECEMBER 2012 / 11-27

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

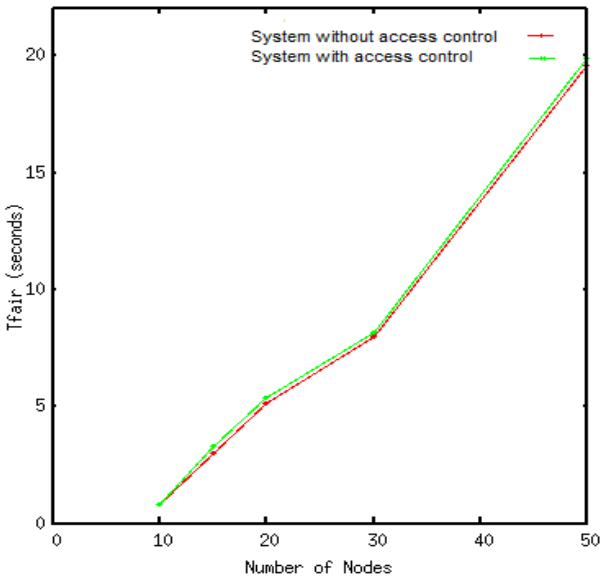

Figure 12: Bidding phase: Tfair vs. Node Number

6 Conclusion and Future Work

In this paper we explore the deployment of P2P auctions over mobile ad hoc networks. This scenario presents many advantages such as ubiquity, availability, affordability, opportunity and spontaneity. Spontaneous markets created temporarily for auction events can then be setup in situations where the mobile infrastructures are very pervasive. We identify the fairness and security problems that these systems face. We first address fairness and define a fair round duration (called Tfair). Tfair is the waiting time period, allowing each participant to collect all submitted bids for each round. We propose a new theoretical model for the estimation of Tfair. This model is aware of the network conditions (the number of hops between the farthest peer bidder and the initiator and the number of peer bidders) as well as of the features of the application (the number of rounds and the bidding activity). For the validation of this proposal, we use simulations to show that this estimation is realistic. Indeed, Tfair values computed according to this estimation are close to Tfair obtained by simulations in the conditions of considered scenarios. We provide a tool toward a fair bidding service which can be invoked by the auction application at the auction starting time.

As for security, we propose a new approach for access control and no replay that takes into consideration the unique features of P2P auctions over MANETs. We define a hybrid access control scheme that is undertaken in two phases: During the Initialization, each Initiator controls the access to the auction he/she sets up. During the Bidding, a bid admission control is decentralized over the bidders. We use ACLs and authorization tickets for the implementation of this access control. We evaluate by simulations the overhead of our security approach. We define new metrics in order to compute the additional time incurred by the security mechanisms during the Initialization and the Bidding. The simulations show that during the Initialization the overhead is measured in seconds and increases with the number of nodes in the MANET. However, since the Initialization phase is occurring just once in the whole auction's lifespan, this overhead can be tolerated. During the Bidding, the raise of Tfair can be considered negligible considering the round duration that can be measured in minutes or more.

A fundamental aspect of our contribution is concerned with the original combination of simulation techniques and mathematical tools contributing to the resolution of the fairness and security problems while considering the unique constraints and vulnerabilities implied in the special context of P2P auctions over MANETs

Ongoing work addresses the genericity of the estimation of Tfair with regards to the application and its validation on other simulations scenarios. We also plan to study the feasibility of our proposed security solution in the context of other P2P systems while moving towards a more general wireless communication environment.

Websites List

Site 1: OpenSSL Project
http://www.openssl.org

References

[1] N. Asokan, Fairness in Electronic Commerce, Ph.D dissertation, University of waterloo, Waterloo, Canada, 1998.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

[2] J.P.Banatre, M.Banatre, G.Lapalme, and F.Ployette, The design and building of Enchère, a distributed electronic marketing system, Communications of the ACM, vol. 29, no. 1, pp.19-29, 1986.
[3] E. Bertino, E. Ferrari, and A.C. Squicciarini, Trust-X: a peer-to-peer framework for trust establishment, IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 827-842, 2004.
[4] C.Boyd and W.Mao. (2000, July). Security Issues for Electronic Auctions. HP Trusted E-Services Laboratory. [Online]. Available: http://www.hpl.hp.com/techreports/2000/HPL-2000-90.pdf.
[5] T. Camp, J. Boleng, and V. Davies, A survey of mobility models for ad hoc network research, Wireless Communications Mobile Computing (WCMC): Special Issue on Mobile Ad hoc Networking Research, Trends and Application, vol. 2, no. 5, pp. 483-502, 2002.
[6] I. Chlamtac, M. Conti, and J.N. Liu, Mobile Ad hoc Networking: Imperatives and Challenges, Ad Hoc Networks, vol.1, no. 1, pp. 13-64, 2003.
[7] Z. Despotovic, J. C. Usunier, and K. Aberer, Towards Peer-To-Peer Double Auctioning, in Proceedings of the 37th Hawaii International Conference on System Sciences, Waikoloa, 2004, pp. 8.
[8] I. Doghri and H. Kaffel-Ben Ayed, Towards Fair P2P auctions over MANETs, in Proceedings of IEEE Computer and Information Technology, Sydney, 2008, pp. 658-663.
[9] I. Doghri and H. Kaffel-Ben Ayed, Performance Evaluation of a Protocol for Fair P2P Auctions over MANETs, IFIP Advances in Ad hoc Networking, in Proceedings of the 7th Annual Mediterranean Ad Hoc Networking Workshop, 2008, pp. 85-97.
[10] W. K. Edwards, Policies and Roles in Collaborative Applications, in Proceedings of the ACM Conference on Computer Supported Cooperative Work, ACM Press, Boston, Massachusetts, 1996, pp. 11-20.
[11] P. Ezhilchelvan and G. Morgan, A Dependable Distributed Auction System: Architecture and an Implementation Framework, in Proceedings of 5th IEEE International Symposium on Autonomous De-centralized Systems, 2001, pp. 3-10.
[12] K. Fall and K. Varadhan. (2011, November). The NS Manual. The VINT Project. [Online]. Available: http://www.isi.edu/nsnam/ns/ns-documentation.html.
[13] M. Fantoura, M. Ionescu, and N. Minsky, Decentralized Peer-to-Peer Auctions, Electronic Commerce, vol. 5, no. 1, pp. 7-24, 2005.
[14] P.Fenkam, S. Dustdar, E. Kirda, G. Reif, and H. Gall, Towards an Access Control System for Mobile Peer-to-Peer Collaborative Environments, in Proceedings of the 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), 2002, pp. 95-100.
[15] H. Frey, D. Gorgen, J.K. Lehnert, and P. Sturm, Auctions In Mobile Multihop Ad-Hoc Networks Following the Marketplace Communication Pattern, in Proceedings of 6th International Conference on Enterprise Information Systems (ICEIS'04). Porto, Portugal, 2004, pp. 161-169.
[16] A. Fourati, K. Al Agha, and H. Kaffel-Ben Ayed, Secure and Fair Auctions over Ad Hoc Networks, International Journal of Electronic Business, vol. 5, no. 3, pp. 276-293, 2007.
[17] E. P. Gonzalez, Content Authentication and Access Control in Pure Peer-to-Peer Networks, Ph.D dissertation, Computer Science Department, Universidad Carlos III De Madrid, Leganés, 2008.
[18] D. Hausheer and B. Stiller, PeerMart: The Technology for a Distributed Auction-based Market for Peer-to-Peer Services, in Proceedings of IEEE International Conference on Communications, 2005, pp.16-20.
[19] H. Kaffel-Ben Ayed and A. Belkhiri. (2011, March). Toward a Peer-to-Peer PKI for Mobile Ad-Hoc Networks, Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), [Online]. Available: http://www.cyberjournals.com/Papers/Mar2011/09.pdf.
[20] H. Kaffel-Ben Ayed and S. Kaabi Chihi, Un Protocole de Communication pour Enchères Temps-réel, in Proceedings of Colloque Francophone sur l'Ingénierie des Protocoles, Tozeur, 2006, pp. 1-12.
[21] P. Klemperer, The economic Theory of Auctions, Edward Elgar Publishing, 2000.
[22] N. Lin, and S. Shrivastava. System support for small scale auctions, in Proceedings of IFIP Med-Hoc-Net, Mahdia, 2003, pp. 143-149.
[23] D. A. Menascé and V. Akula, Towards Workload Characterization of Auction Sites, in Proceedings of 6th IEEE Workshop on Workload Characterization, Austin TX, 2003, pp. 12–20.
[24] J. & S. Milgram, An Experimental Study of the Small World Problem, Sociometry, vol. 32, no. 4, pp. 425-443, 1969.
[25] A. Ockenfels and A.E. Roth, Last Minute Bidding and the Rules for Ending Second Price Auctions: Evidence from Ebay and Amazon Auctions on the Internet, American Economic Review, vol. 92, no. 4, pp. 1093-1103, 2002.
[26] F. Panzieri and S. K. Shrivastava, On The Provision of Replicated Internet Auction Services, in Proceeding of the 18th IEEE International Symposium On Reliable Distributed Systems, Lausanne, 1999, pp. 390-395.
[27] J. S. Park and J. Hwang, Role-Based Access Control for Collaborative Enterprise in Peer-To-Peer Computing Environment, in Proceedings of the 8th ACM Symposium on Access Control Models and Technologies, Como, Italy, 2003, pp. 93 - 99.
[28] J. S. Park, G. An, and D. Chandra, Trusted P2P Computing Environments with Role Based Access Control, IEEE, IET Information Security, vol. 1, no. 1, pp. 27-35, 2007.
[29] C. S. Peng, J. M. Pulido, K. J. Lin, and D. M. Blough, The Design of an Internet-based Real-Time Auction System, in Proceedings of the 1st IEEE workshop on dependable and realtime e-commerce systems (DARE-98), 1998, pp. 70-78.
[30] B. Rachlevsky-Reich, I. Ben-Shaul, N.T. Chan, A. Lo, and T. Poggio, GEM: A Global Electronic Market System, Information Systems, vol. 2, no. 6 ,pp. 495-518, 1999.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762012000300003

[31] B. Rumpe and G. Wimmel, A Framework for Realtime Online Auctions, Proceeding of IRMA International Conference, Toronto, 2001, pp. 208-912.
[32] R. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, Role Based Access Control Models, Computer, vol. 29, no. 2, pp. 38-47, 1996.
[33] P. Shubert and J. F. Hampe, Mobile Communities; How Viable are their Business Models? An Exemplary Investigation of The Leisure Industry, Electronic Commerce Research, vol. 6, no. 1, pp. 103-121, 2006.
[34] V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. Rao, Cooperation in Wireless Ad Hoc Networks, in Proceedings of IEEE Infocom, 2003, pp. 808-817.
[35] H. Tran, M. Hitchens, V. Varadharajan, and P. A. Watters, A Trust Based Access Control Framework for P2P File-Sharing Systems, in Proceedings of the 38th IEEE Hawaii International Conference on System Sciences, 2005, pp. 302c-302c.
[36] J. Trevathan, H. Ghodosi, and W. Read, Design Issues for Electronic auctions, in Proceedings of 2nd International Conference on E-Business and Telecommunication Networks (ICETE'05), 2005, pp. 340-347.
[37] Y. Vakrat and A. Seidmann, Implications of the Bidders' Arrival Process on the Design of Online Auctions, in Proceedings of the 33rd Hawaii International Conference on System Sciences, Los Alamitos, CA, IEEE computer Society Press, CD-ROM, 2000, vol. 1, pp. 7.
[38] M. P. Wellman, P. R Wurman, and W. E. Walsh, The Michigan Internet AuctionBot: A Configurable Auction Server for Human And Software Agents, in Proceeding of the 2nd ACM International Conference on Autonomous Agents, 1998, pp. 301-308.
[39] M. Winslett, PeerAccess: A Logic for Distributed Authorization, in Proceedings of the 12th ACM Conference on Computer and Communications Security, 2005, pp. 168-179.
[40] Y. Zhang, L. Xianxian, J. Huai, and L. Yunhao, Access Control in Peer-To-Peer Collaborative Systems, in Proceedings 25th International Conference on Distributed Computing Systems, Workshop on Mobility of Peer-to-Peer Systems, Columbus, 2005, pp. 835-840.