Location based Authorization Model for Mobile Ad-Hoc Environments

June-Suh Cho*

Abstract

Role-based Access Control (RBAC) became popular because the traditional access control model such as mandatory access control and discretionary access control cannot handle the complicated enterprise-wide access requests. However, it is not suitable for a mobile environment because (i) there is no central trusted authentication entity that activates each user's roles, (ii) there are not many roles involved in such environment, and (iii) access control decisions depend on specific actions to be performed before the decision is taken. In this paper, we introduce a provisional authorization model with location-based predicates embedded in the policy specification languages. It includes three classes of location-based conditions such as position-based, movement-based, and interaction-based conditions. As a result, users can specify their own privacy/security policies in a mobile ad-hoc environment such as mobile auction markets.

Ⅰ. Introduction

Mobile devices with wireless communication capabilities have become part of our lives. In a mobile environment, compared to the static desktop environment, network resources are constantly accessed through these devices while users are still moving. In this new mobile environment, it is easy to form a mobile ad-hoc network where neighboring mobile devices are forming a self-configuring network connected by wireless links. Examples include vehicular ad-hoc networks (VANETs) where neighboring vehicles communicate important information on road conditions or ride-share and also happen in many other applications such as social networks for finding friends,

* College of Business Administration, Hankuk University of Foreign Studies

navigation advice in transportation, asset tracking, and mobile collaborative work. Especially, application to mobile electronic commerce is in our particular interests such as online ad-hoc auction market environment where auctioneers allow bidding from neighboring potential buyers.

In this environment, each mobile user is treated as a peer because one can retrieve data from one's neighboring mobile devices, and at the same time, one can provide the information as the other people request the information that one brings. This local search-and-discover action is performed by each peer without connecting to the centralized server.

In order to protect one's own resources, each peer specifies its own security/privacy policies. In a mobile peer-to-peer environment, access control decision based on these policies depend on (i) specific actions performed before the decision is taken and (ii) also spatio-temporal attributes. First, connection between peers is arbitrary and thus, it would be more appropriate if the access control decision is based on the conditions that the resource holding peer has. For example, in online ad-hoc auction market, an auctioneer allows bidding of only serious users who meet the criteria such as reading and signing the contract beforehand. Second, access control decisions are also based on current locations (i.e., spatial attribute) of neighboring peers within the specific time durations (temporal attribute). For example, in location-based services (LBS) applications, a mobile user wants to receive promotion deals only if current location of the user is within certain distance from the merchant during the evening hours in order not to be overwhelmed by spam mails from merchants.

Role-based access control (RBAC) model is popular because the traditional access control model such as Mandatory Access Control (MAC) and Discretionary Access Control (DAC) cannot handle the complicated enterprise-wide access requests. In RBAC, a role denotes a job function, and permissions to perform certain operations are assigned to specific roles instead of users. Then, each user is assigned to particular roles. Although facilitating resource sharing with enforcing security/privacy policies in static environment has been discussed (Maruoka et al., 2008; Park et al., 2007; Park and Hwang, 2003; Ravichandran and Yoon, 2006; Silva et al., 2005), it is not applicable to a mobile ad-hoc environment due to the following reasons.

First of all, existing RBAC cannot be directly applicable to mobile ad-hoc environment since peers are constantly moving over time and the policies are updated based on time and space. A naïve solution would use a trusted party which authenticates each user and makes an access control decision. However, this is not practical especially for mobile ad-hoc environment where participating peers are not predetermined and do not have capability to connect to the central server. Also, it creates an issue with scalability of the system because the trusted server must be able to deal with all the access control requests and evaluates each peer's security policies. Considering the fact that these policies are based on space and time as well as specific actions that each peer has performed, overheads to the system to enforce these policies would be not be scalable. Also, RBAC is not suitable because in such context, there are not many roles being involved. As the word "peer" represents, in most of the time, each user has the same privileges: for example, for file sharing environment, every user is authorized to access the contents as long as she can access to the system. Finally, in a mobile environment, the connection between peers are arbitrary, and thus, it would be more appropriate if the access control decision is based on the conditions that the resource holding peer has. Usually, the conditions are specific actions that have been performed by the resource-requesting peers, and these specific actions are called as provisions.

Provisional authorization models have been proposed where an access control decision is based on the provisions of requesting peers (Kudo and Hada, 2000; Jajodia et al., 2001). However, the generic provisional authorization model does not address the nature of peer's mobility issues. As we disIn the mobile ad-hoc environment, security/privacy policies are spatio-temporal in nature: a peer is interested in the resources within the specific neighboring region and during a specific time interval without the actual knowledge of peers' identifiers. For example, in mobile electronic commerce, a buyer is interested in sellers in a mall and during the next two hours. In order to properly limit the control of resources, the provisional authorizations must incorporate the spatio-temporal specifications within its model.

In this paper, we introduced the provisional authorization models with location-based predicates embedded in the policy specification languages.

Ⅱ. Background

1. Resource Discovery Process

The resource discovery process in ad-hoc environment defines thee different types of peers in the ad-hoc environment (Nicolacopoulos, 2006).

- Edge peers: An edge peer is a peer that can send and receive messages, but cannot forward the messages. Typically, edge peers start discovery requests to other peers.
- Rendezvous peers: Similar to edge peers, a rendezvous peer can send and receive messages, and start and reply to discovery requests. The main characteristic of the rendezvous peers is that discovery requests are being forwarded. The forwarding characteristic can be achieved because they store other rendezvous peers internally.
- Relay peers: Relay peers hold routing information, and messages are being routed by them. They are important because they can intermediate for communication between peers where in normal circumstances communication with each other cannot be achieved. Thus, although two peers are blocked by firewalls, they can still communicate by using a standard protocol such as HTTP.

Let us take an example to discover resources in ad-hoc environments. The figure 1 shows the discovery process. Peer A is an edge peer making a discovery request. It broadcasts the request to all the peers in its subnet (B, C) including the rendezvous peer (R1). The rendezvous peer searches in its cache in order to detect if the requested information has been published by a peer connected to it. If it is found, the two edge peers will connect and exchange the information. If it does not find in its cache, it will use the list of other rendezvous peers that it has and propagate the request to them (R2 and R3). Each rendezvous peer receiving the request will check its cache and if it cannot find, it will propagate the request again. This will continue until the maximum number of hopes is reached.

2. Requirements for Access Control in Mobile P2P Systems

Fenkam et al. (2002) specifies the requirements for an access control system in mobile ad-hoc systems, which are ineluctably derived from requirements for access control in mobile systems, and access control in ad-hoc systems. Authorization for mobile users is guided by place specific services during their moves. Mobile users are interested in forming ad-hoc networking within a specific region during some time period. Also, another requirement for access control systems in mobile computing environments is the support for various mobile devices. They often lack resources for running conventional security mechanisms themselves. These problems are exacerbated when the number of services is large and services are mobile themselves.

Ad-hoc computing on the other hand principally rejects the concept of central authorization control. In this approach, the client/server scheme has been used for each access request. Each user request needs to connect to the server in order to acquire the access authorization. The main limitation is the feasibility since the server must handle all the access requests, which becomes the bottle neck of the system. The reason for rejecting this concept is that many peers are often responsible for the resources they provide. Also, scalability is often an issue in such environments. The access control mechanism must suitably face the problem of large number of peers.

Ⅲ. Authorization Model for Mobile Ad-hoc Networks

Traditional access control uses the model that a user makes an access request of a system in some context, and the system either authorizes the access request or denies it. However, today’s rapidly expanding environments, such as electronic commerce, make such models that authorize or deny a request overly simplistic and not accommodating (Jajodia and Wijesekera, 2004).

Motivating Example: Suppose a situation of mobile ad-hoc auction market. A mobile seller creates a mobile auction place for mobile customers who are within a shopping mall. Auction models consist of a set of business rules and security policies such as ending conditions and confidentiality of the bidding information (Jajodia et al., 2001). In a sealed-bid auction, submitted bids must be kept secret, and any submission after the closing time must be rejected. The provisional authorization model with support to location-based predicates deals with these security policies in a structured way. Bidders can submit their bids while their stay at the shopping mall. The bidding information is kept secret because the seller encrypts the bidding data with cryptographic key, and the system timestamps the bid. These security policies are properly captured by provisional authorization models. There are two kinds of participants: supplier, and bidders. First, the supplier fills in the item to be auctioned, the closing time of the auction, and the minimum price acceptable. Then, the auction information is published in the mobile ad-hoc networks located within the shopping mall. Any mobile peer who is interested in the item can submit a bid specifying the item and a bidding price. This bidding information is accommodated if the bidding ending time is not reached, and the bidding price is higher than the current bidding price. The seller can fill-in "No Good" in the status field if the current time is after closing time and the maximum price of all the bids is lower than the minimum price.

In this section, first, generic provisional authorizations are presented, and how location-based conditions are embedded in the provisional authorization models (Jajodia et al., 2001) in order to support the mobile P2P systems are presented.

1. Provisional Authorization Models

This section introduces a provisional authorization model proposed in (Jajodia and Wijesekera, 2004). When clients submit an access request, authentication modules is invoked, which verifies if the user is the one that claims to be. Then, the access request is provided to the provision evaluation module, which finds the conditions under which the requested access can be honored. Then, the condition under which the access may be granted is passed to an order specification module that yields a set of ordering constraints on the actions involved. Then, the ordering constraints are handed off to a provision verification module to check if any conditions were previously fulfilled by the requester and, if so, simplifies the condition and waits for reduced conditions to be fulfilled by the requester before final authorization.

Representation of the Policy Rules: The security policy rules are written using a number of predicates, such as cando, do, and dercando (Jajodia and Wijesekera, 2004).

1. A ternary predicate cando (o, s, a), representing grantable or deniable requests where o, s, and a are object, subject, and a signed action term, respectively.
2. A ternary predicate dercando (o, s, a), with the same arguments as cando representing authorizations derived by the system using logical rules of inference.
3. A ternary predicate do, with the same arguments as cando, representing the access control decisions made by the system.
4. A propositional symbol error indicating violation of an integrity constraint.
5. The predicate in (x, y, "hierarchy name") is used to specify properties of subject and object hierarchies.

Representation of Provisions: Provisions are specified with the following form:

$$\oint : \text{Head} \times \text{Body} \qquad (1)$$

where $\oint$ is a predicate for provisions. Jajodia et al. introduce a provisional authorization specification language pASLL. pASLL is based on the declarative, polynomially evaluable authorization specification language ASL proposed by Jajodia et al., The following set of rules model provisional accesses for an online store:

1. register (s, customer): cando (items, s, +buy)×in (contract, Contracts)
2. upgrade (s, perfCust): dercando (item, s, +buy)×cando (item, s, +buy)
3. payFees (s, $100): do (item, s, +buy) ×cando (item, s, +buy)
4. payFees (s, $80): do (item, s, +buy)× dercando (items, s, +buy)

The first two rules allow a customer to purchase by registering and further allow the customer to upgrade her registration to a preferred customer. Next two rules state that the purchase price of an item is $100 for a non-preferred customer and $80 for a preferred customer. Therefore, a customer has the choice of either remaining in the non-preferred category with paying $100, or registering as a preferred customer and paying $80 per item.

2. Supporting Location-based Predicates

The provisional authorization model does not provide the location-based predicates within the model. Thus, it cannot handle the security policies where the location-based predicates are specified. Ardagna et al. (2006) proposed the access control model that supports location-based conditions in access control polices. The main advantage of the proposed model is that the model can be embedded in any currently available access control system to support location-based predicates without the necessity to introduce new specification languages. Also, the proposed model's proposed location-based predicates are well-defined.

The model proposes three main classes of location-based conditions:

- position-based conditions on the location of the user: for instance, to evaluate whether a user is in the proximity of other entities
- movement-based conditions on the mobility of the users such as their velocity, acceleration, or direction where they are headed.
- interaction-based conditions relating multiple users or entities: for instance, the number of users within a given area.

The location-based predicates are expressed as Boolean queries, and their evaluation returns a triple [bool_value, confidence, timeout]. The bool_value is either True or False. If a user access request asks whether a user is located inside a given region. Because none of the current technology fully ensures the exact user location (Horsmanheimo et al., 2004), there exists uncertainty about location information. The confidence expresses the level of reliability that the location information is guaranteed to be accurate within the specified intervals. Also, the assessment (True or False) of the user request has a time validity interval specified by a timeout parameter.

The model includes the following predicates

- A position predicate inarea evaluates whether a user is located within a specific area.
- A position predicate disjoint evaluates whether a user is outside a specific area. Of course, disjoint is the equivalent to the negation of inarea.
- A position predicate distance evaluates whether the user lies within a given distance from the specified entity. The entity involved in the evaluation can be either stable or moving.
- A movement predicate velocity evaluates whether the user speed lies within a given range of velocity.
- An interaction predicate density evaluates whether the number of users currently in an area lies within the interval specified.

<Table 1> shows the example of location-based predicates. The example presents position-type predicates and movement-based conditions.

3. Representation of Location-based Provisions

Location-based provisions are specified in the same way that non-location-based provisions do, which is shown in (1). It is important to observe that confidence plays a role for accuracy of user locations. Therefore, threshold of reasonable range of values for confidence may needs to be set up. Ardagna et al. (2006) introduce the concept of an Extended True Table (ETT) for custom confidence thresholds for each predicate. For example, suppose the confidence threshold for the inarea predicate is [0.1, 0.9]. If the confidence is less than 0.1, the returned Boolean value is not confirmed, and the location-based condition is set to false. If the confidence level is above 0.9, then returned Boolean value is confirmed. If

<Table 1> Examples of Location-based Predicates

Location-based Predicates	Evaluation Result	Description
inarea (Alice, Newark)	[True, 0.9, 2010-11-09_11:10am]	Alice is located in Newark with a confidence of 90%. Such an assessment is to be considered valid until 11:10am of November 9, 2010.
velocity (Alice, 70, 90)	[True, 0.8, 2010-11-03_03:00pm]	Alice is traveling at a speed included in the range [70, 90] with a confidence of 70%.

the threshold level is between 0.1 and 0.9, predicate re-evaluation is triggered because under the current threshold level, the returned value is not confirmed. The maximum number of tries is specified in order to prevent the deadlock situation.

Now, we have all the capabilities to specify the access control policies for mobile ad-hoc auction market.

1. cando (supplier_info, X, +rw) ∮ in (X, supplier)
2. cando (supplier_info, X, +r) ∮ in (X, bidder)^inarea (X, ShoppingMall)
3. cando (bid, A1, +r) ∮ owner (bid, A1)^uid (A1)
4. encrypt (Price, key1)^timestamp (Price, tsa1): cando(bidder_info, A1, +w (Price)) ∮ ×not (done (bidder_info, A1, +w (Price’)))^uid (A1)^time (T)^ field (closing_time, A2)^T < A2.
5. write (winning_price, -1): cando(status, supplier, +w (“No Good”)) ∮ current_top (A1)^field (minimum_ price, A2)^A1 < A2^time (T)^field (closing_time, A3)^T >= A3
6. write (winning_price, A1): cando (status, auctioneer, +w (“Completed”)) ∮ current_top (A1)^field (minimum_ price, A2)^A1 >= A2^time (T)^field (closing_time, A3)^T >= A3

The first two rules specify that the suppler can read and write any fields in supplier_info node, and the bidder who is in the shopping mall can read any fields in supplier_info. The third rule specifies that the bidder who submitted bid data can read her data. The forth rule specifies that if the bidder has not submitted a bid before the closing time of auction is not reached, a bidder can submit a bid, if price is encrypted with time release key key1 and timestamp from tsa1 authority is recorded. The fifth rule specifies that if the maximum price of submitted bids is lower than the minimum price and the current time is after the closing time, the seller writes “no good” in the status field in the system_ info section, if error code is written in winning_price field. The last rule specifies that if the maximum price of submitted bids is equal or greater than the minimum price and the current time is after the closing price, the supplier writes “completed” in the status field in the system_info section, provided the highest price is written in the winning_price field.

Ⅳ. Discussions

We assume that the identification of a peer (user) is properly authenticated. In the traditional static client/server architecture, the authentication procedure is rather standardized. However, in the mobile ad-hoc environment, it raises some issues with authentication. It mainly comes from the limited resources of mobile devices. Due to the mobile nature, the mobile devices do not necessarily be on-line to other networks except the mobile ad-hoc network. Therefore, in a typical case, a peer with resources does not have any prior knowledge about the peer who asks an access request. Thus, authentication process is rather problematic.

Fenkam et al. (2002) discuss an interesting idea of authentication procedure, called DUMAS (Dynamic User Management and Access Control System). There are two types of mobile peers: L1 peers (Peers of Level 1) and L2 peers. L1 peers are peers that maintain a security infrastructure. This includes the complete intelligence for assigning permissions, revoke permissions, and provides authentication. To use a service protected by a L1 peer, a user must present his authorization certificates including his authentication information. L2 peers are devices lacking the resources for instantiating the full DUMAS engine. L2 peers utilize the power of L1 peers to verify authorization certificates related to the service it provides. Obviously, the main disadvantage of this architecture is that if an ad-hoc mobile network does not include L1 peers, authentication of consisting peers cannot be processed. However, with the reasonable number of L1 peers, the security of system can actually work file because at least one L1 peer in the ad-hoc network can provide the security environment for participating peers.

In the motivating example, due to the limited memory capacity of mobile devices, in some cases, all the bidding history cannot be stored in the supplier's device. In this case, the auctioneer can start truncating the bidding records of oldest records because these biddings with lower bidding prices are less likely to be the winner of the auction.

Ⅴ. Related Work

In the security literature, there are limited numbers of research on RBAC model in the ad-hoc environment as follows:

- Role-based access control with centralized components: In this approach, the client/server scheme has been used for each access request. Each user request needs to connect to the server in order to acquire the access authorization. The main limitation is the feasibility since the server must handle all the access requests, which becomes the bottle neck of the system.
- Role-based trust model: This model is built in the context of digital libraries by Khambatti et al. (2004). Each peer keeps its own list of book profile that she want to share with others. If this profile matches with someone who keeps the book, the information is used for sharing their books. However, the usage of role is limited because a role simply denotes the trustworthiness, which is different from the perspective of this paper since different roles may specify different policies.
- Trust based access control: This model is developed in the context of P2P file sharing network. A peer has the right to download files from other peers, but a resource holding peer can control the prospective downloads of its file. However, the access control is determined by the trustworthiness and performance of peers instead of their roles. Thus, the model cannot classify peers with different functionalities.

However, our work is orthogonal to above work because they are not applicable to a mobile ad-hoc environment, as they cannot support location-based conditions, and access control decisions depend on specific actions to be performed before the decision is taken rather than roles.

Ⅵ. Conclusion

Mobile ad-hoc environments are characterized by its local ad-hoc network formation which can be used for searching for local resources of the users' interests. In most of cases, the local resources are available during a limited duration of time and proximately located with the user. For example, the local search-and-discover, for example, can happen in many applications such as social networks for finding friends, navigation advice in transportation, mobile electronic commerce, asset tracking, and mobile collaborative work.

The main purpose of this paper is to

develop an access control system for mobile ad-hoc environments. In this setting, each peer has its own security/privacy policies for protecting its resources. In the access control research literature, facilitating resource sharing with enforcing these policies in the static ad-hoc environment has been discussed. However, a number of challenges are brought into attention in the mobile ad-hoc environment because peers are constantly moving over time and the policies are updated based on time and space.

In this paper, we introduced the provisional authorization models with location-based predicates embedded in the policy specification languages. It includes three classes of location-based conditions such as position-based, movement-based, and interaction-based conditions. The mobile ad-hoc auction markets are used as a motivating example to explain the concept of the provisional authorizations.

References

[1] Ardagna, C.A., M. Cremonini, E. Damiani, S.D. di Vimercati, and P. Samarati, "Supporting location-based conditions in access control policies," In Proceedings of the 2006 ACM Symposium on information, Computer and Communications Security, 2006.

[2] Braun, T. and H. Kim, "Efficient Authentication and Authorization of Mobile Users Based on Peer-to-Peer Network Mechanisms," HICSS, 2005.

[3] Fenkam, P., S. Dustdar, E. Kirda, G. Reif, and H. Gall, "Towards an Access Control System for Mobile Peer-to-Peer Collaborative Environments, WETICE, 2002.

[4] Horsmanheimo, S., H. Jormakka, and J. Lahteenmaki, "Location-aided planning in mobile network trial results," *Wireless Personal Communications: An International Journal*, Vol.30, No.2-4(2004), pp.207-216.

[5] Khambatti, M., P. Dasgupta, and K. Ryu, "A Role-Based Trust Model for Peer-to-Peer Communities and Dynamic Coalitions," *Second IEEE International Information Assurance Workshop*, Charlotte, NC, 2004.

[6] Nicolacopoulos, K., "Role-based P2P Access Control" M.S. thesis, Lancaster university, Lancaster, U.K, 2006.

[7] Kudo, M. and S. Hada, "Xml document security based on provisional authorizations," In Proceedings of

the 7th ACM Conference on Computer and Communications Security, (2000), pp.87-96.

[8] Jajodia, S., M. Kudo, and V.S. Subrahmanian, Provisional authorizations, In Recent Advances in Secure and Private E-Commerce, A. Ghosh, Ed. Kluwer Academic Publishers, Boston, 2001.

[9] Jajodia, A. and D. Wijesekera, "A Flexible Authorization Framework for E-Commerce," ICDCIT, 2004.

[10] Maruoka, M., A. Nemati, V. Barolli, T. Enokido, and M. Takizawa, "Role-Based Access Control in Peer-to-Peer (P2P) Societies," Proceedings of the 22nd International Conference on Advanced Information Networking and Applications Workshops, 2000.

[11] Park, J., G. An, and D. Chandra, "Trusted P2P computing environments with role-based access control (RBAC)," *IET (The Institution of Engineering and Technology, formerly IEE) Information Security*, Vol.1, No.1(2007), pp.27-35.

[12] Park, J. and J. Hwang, "Role-based access control for collaborative enterprise in peer-to-peer computing environments," SACMAT, 2003.

[13] Ravichandran, A. and J. Yoon, "Trust management with delegation in grouped peer-to-peer communities," SACMAT, 2006.

[14] Silva, J., L. Gaspary, M. Barcellos, and A. Detsch, "Policy-based access control in peer-to-peer grid systems," The 6th IEEE/ACM International Workshop on, Vol.7(2005), pp.13-14.