Volume 1, No. 2, July-August 2010

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Improved Data Access Method In Ad hoc Networks

Anil Kumar*
Computer Science and Engg.
HCTM
Kaithal, India
akj_jakhar@yahoo.com

Parveen Gupta
Computer Science and Engg.
MIET
Meerut, India
pk223475@yahoo.com

Rakesh Sharma
Information Technology
HCTM
Kaithal, India
rakeshsharma3112@gmail.com

Abstract: Mobile ad hoc network (MANET) makes it possible to dynamic changes in topology and in the availability of resources. For database integrity, Concepts of role-based access and databases are combined to specify separation of duty (on wireless networks) as required. The framework to adapt method based access control models in the MANET environment is discussed. There is an approach where a system developer can design a roll based authorization model for data access and its transfer in an ad-hoc environment.

Keywords: ad hoc; UDDI; Wlan; RBAC; DBMS; DAC

I. INTRODUCTION

These are new emerging wireless technologies such as 802.11 series WLAN [1] and short-range radio technologies such as Bluetooth [2] have opened new possibilities for implementation of the networks which transcend the conventional bounds of fixed physical networks. The network's topology can change rapidly and in unpredictable ways. To address issues related to ad hoc networks, the Internet Engineering Task Force (IETF) [3] is developing MANET specification to enable future applications.

Currently, most of the organizations are interested to accept roles based model rather than conventional, procedural as well as bureaucratic methods [4]. The most important component of access method is how users, groups and roles are associated with access to corporate resources. For example, many organizations provide virtual private network (VPN) access through the corporate perimeter and then since those credentials are not shared with other authorization systems, they segment internal networks with additional firewalls. Unfortunately, as users change location, their Internet protocol (IP) addresses change so the firewall administrator must either create broad access control lists (ACLs) that allow ranges of IP addresses, or method must be updated frequently to accommodate ever changing source IP addresses. The first solution defeats the purpose of segmenting internal networks and the second solution is disruptive to users and unmanageable for an information technology (IT) organization. If a user moves from manufacturing to engineering and gets a promotion to a manager position, a variety of firewall and application policies must be updated to be sure that user's old access rights are deleted from each system and their new access rights are enabled. If the manufacturing firewall allows a block of addresses, application level authorization may be the only logical way to keep that user out of manufacturing systems. These are common situations on most enterprise networks and IT departments simply can't keep up with this constant change for thousands of users and hundreds of applications. With growing compliance concerns caused by regulations like HIPAA and Sarbanes-Oxley, this has become a serious problem that has implications all the way up to the chief executive officer (CEO).

In [5], the author has carried out survey of most recent contribution in the area of data management related to mobile computing. The work surveyed covers areas such as data dissemination, data consistency, location dependent querying, and interfaces. In [6], the authors discuss an application for mobile commerce (*m*-commerce). Specifically, the authors introduce an infrastructure for *m*-commerce in a given geographic area using a multi-channel system. The agents have also been explored in this area of wireless computing, for example in [7]. The authors in [7] address data recovery in wireless environment using mobile agents. The claimed benefit is reduction of overall recovery time by managing system resources and handoffs. To address similar environment, another work is reported in [8], where authors address transaction commit for mobile database systems. The timeout is used to identify the successful end of an activity (commit, abort etc). In order to address buffering and cache issues in mobile databases, a novel approach has been reported in [9], where authors discuss cache retrieval schemes in a mobile computing environment.

There has been a number of access control models discussed in literature for various objectives [10-12]. Most current models are Discretionary Access Control (DAC) model, Mandatory Access Control (MAC) model, and Role-based Access Control (RBAC) model. In RBAC permissions are associated with roles, and users are made members of appropriate roles thereby acquiring the roles' permissions. This greatly simplifies management of permissions. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems

are incorporated, and permissions can be revoked from roles as needed. Not surprisingly DBMSs developers have claimed in taking the lead in providing support for RBAC. The notable contribution related to this work has been reported in [13], where authors compare three (single) commercial database management systems based on RBAC features that have been categorized under three broad areas namely user role assignment, support for role relationships and constraints, and assignable privileges.

This paper is organized as follows: In the next section, we address data access issues in ad hoc networks. Furthermore, infrastructure for such an environment is discussed for role based data access. We highlight method based framework for such an environment. We also propose an access control algorithm to be adopted by individual devices. In section 3, detailed discussion is provided on our proposed approach, followed by conclusions in section 4.

II. PROPOSED APPROACH

In this section, we address issues that surface after an ad-hoc network of devices is formed. Generally, the data management scheme is very important that is based upon a role based model and uses various techniques to address various issues such as location of database, caching methods, application data logging, service channel etc. Additionally, data management can further be elaborated to include certain access method criteria, as outlined below:

- ***User/Group/Role:*** **Method** can be defined for groups and roles so user access is relevant to their organizational placement.
- ***Application and Application Content:*** Deep packet inspection enables identification of applications regardless of port. Applications using the same port can be distinguished from each other for accurate access control.
- ***Standard ACL (Layer 2, 3, and 4):*** Traditional ACLs can be defined based on source MAC address, source and destination IP Address and protocol, and either type. Groups of addresses and subnets can be combined to define network zones.
- ***Periodic and Absolute Time:*** Policies can be defined as valid only during specified time and day ranges, such as every weeknight between 11pm and 3am.
- ***Location:*** **Access method** can be defined based on the direction of traffic, which is a function of the source and destination locations.

Based on these discussions, the objective of our work summarizes to describe an architectural framework that addresses these issues; and to define easy to manage role based access method.

A. Infrastructure

The ad-hoc network formation requires that at least one architectural component be present (at all times) to initiate forming of an ad-hoc network. The joining of a device is to be authenticated by a central server owned by the organization. It is mostly desired that client device be kept simple and compatible for interoperability. The corresponding software running on a trusted computer, (i.e., central server) preferably at a central location of the organization can be used. Its primary function is to make access control decisions and executing encrypted functions on behalf of the device it represents. Such network architecture is depicted in Figure 1. It consists of a group of devices forming an ad-hoc network through a coordinator device.

Multi-channel model: We propose a multi-channel model for accessing services and information interchange among users, as shown in Figure 2. The universal description, discovery, and integration (UDDI) channel is proposed to include registry information about the groups, given by the central server and propagated by the coordinator device.

Each entry in the UDDI channel is identified by *Key*, and information within the channel is customized to fit wireless environments. The session channel contains the description and executable code of each session. Information within the session channel is indexed with a service key to enable better access performance. The data channel is used transfer among network devices. *Devices:* The device working as Coordinator will have more features in its software component to allow necessary communication with central server for authentication or creating software proxies for network devices. The devices communicate within the network on the data channel and with their proxies through session channel. When device enters a network, its proxy is generated at the central server, and a shared key along with.

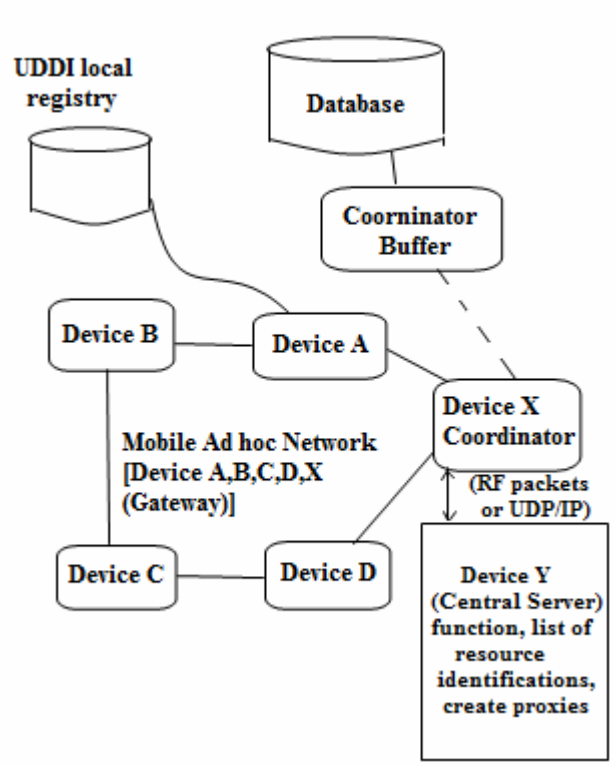

Figure 1: Ad hoc network infrastructure

Resource identifiers corresponding to that specific role are sent back to the device on the session channel Whenever a device enters an ad-hoc network, it downloads UDDI channels content to its device and store it for later use. Caching it avoids frequent access to the channel, and minimizes power consumption of the devices as well. The impact of using a coordinator buffer, as shown in Figure 1, to improve cache retrieval has shown to be useful [14]. At the end of transaction execution, the device has to perform coordinator buffer write to store updated data.

Proxy setting: This is a software component running on a central server for each active device on the network. Its

main functions are access control decisions, logging of device actions, role versus access list, generating random key for sharing with device, and interfacing with other proxies. Because of these sophisticated access control and authentication process at proxy, the device remains simple. *Central Server:* This is a powerful computer, and must be able to supervise many ad-hoc network(s), and to create a number of proxies at the same time.

Dynamicity: If the device functioning as Coordinator is relatively stationary during the life of the network, then the level of resources in the network is not seriously low. On the contrary, if device with Coordinator is mobile, then it creates a resource problem. In case, if Coordinator leaves and another joins in, a new mechanism is to be devised to let all devices know that there is a new Coordinator. This can be handled by retransmitting of packets from devices during shorter periods of time. As these packets will reach central server, hence from packet headers, central server can retrieve this information.

Database*:* The objective of coordinator buffer is to share and cache those data frequently used by all mobile users. Roles essentially partition database information into access contexts. Methods (from the object oriented world) associated with a database object, also partition the object interface to provide windowed access to object information. By specifying that all database information is held in database objects and authorizing methods to roles, we achieve object interface distribution across roles. For processing in the commercial world we can design objects and distribute their associated methods to different roles. Our finding is that the products discussed in [13] provide a sound basis for implementing the basic features of RBAC, although there are significant differences but Sybase is the only one to directly support mutual exclusion of roles. The description of the feature in these products is not construed as a complete overview. Rather focus is on significant issues and differences from the point of view of security administrators and developers of applications that have significant security requirements. Because of space limitations in mobile devices (like laptops etc.), data is proposed to be in a single database residing in Coordinator. In case of PDA's or similar devices, the database is proposed to be at the central server, where single or distributed databases can be placed, and then caching of events, registries and other services can be allowed on individual devices.

B. Access control based on roles

At the core of our research on **method** based design of ad-hoc groups is the idea that groups are defined around objects and that objects can be hierarchically combined. All objects are uniquely identified by resource identifiers akin to uniform resource indicators (URIs) and will need to be maintained on central server and on individual devices as needed to provide redundancy when connectivity is unavailable. To develop access control on these objects, we adopt the terminology and concepts of the well-known RBAC96 family of models due to Sandhu et al [11]. Similar to [11], a draft role engineering model [15] proposed by National Institute of Standards and Technology (NIST) in January 2006 is depicted in Fig. 3. The Figure 3 highlights relationships between role groups (basic roles, static roles) work profiles, and functional roles (groups of permissions) consistent with RBAC standard. Role groups (basic roles) place people within an organization's personnel (not necessarily organizational) structure, into categories of personnel warranting differing levels of access control. Role groups allow users to participate in the organization's workflow by job, title, or position but do not specify detailed permissions on specific information objects. As stated before, role groups can allow a user to "connect" to a resource but do not necessarily grant finer-grain authorization on protected information objects. Based on these guidelines, the architecture for access control framework in ad-hoc networks is proposed of four components as shown in Figure 2.

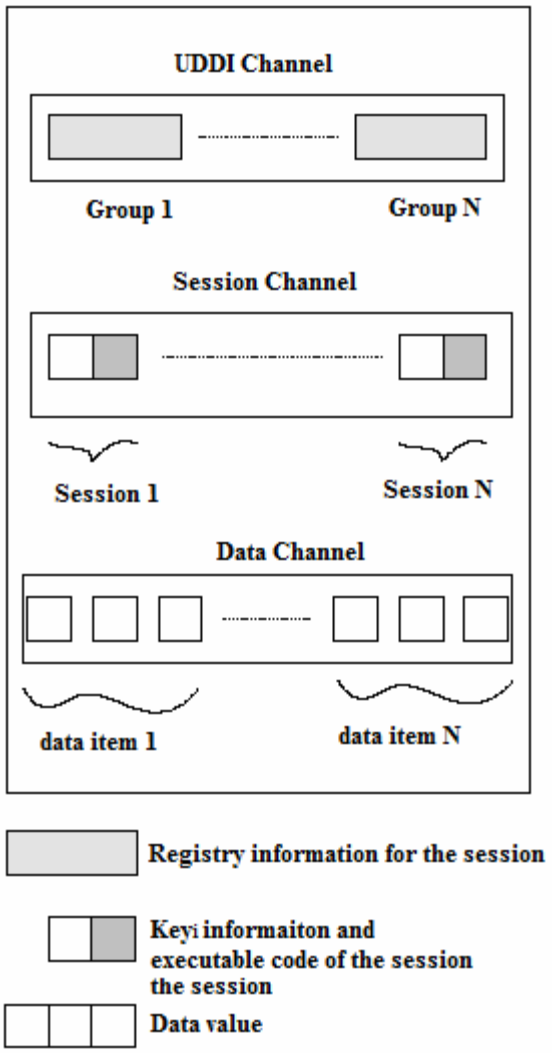

Figure 2: Multi-Channel System for Wireless ad hoc Network

The components are: profile management and membership management (combined as user management), protocol management, method enforcement and an event service. The framework runs on every user's device. The profile management component maintains the user's credentials, such as key certificates and stores, and attributes certificates.

Users can manage their credentials and device settings through user management interface. In addition, this component also maintains the user's preferences on which communities the device should automatically join. The membership management component exposes the user management interface to the application level, so that applications can initiate the establishment of a new community, search for communities, as well as joining particular com-

munities. Through this interface, the user can register the services that it is providing to other participants. The membership management component is also responsible for checking the authenticity of the doctrines and enforcing them by extracting and distributing the method instances to various enforcement components.

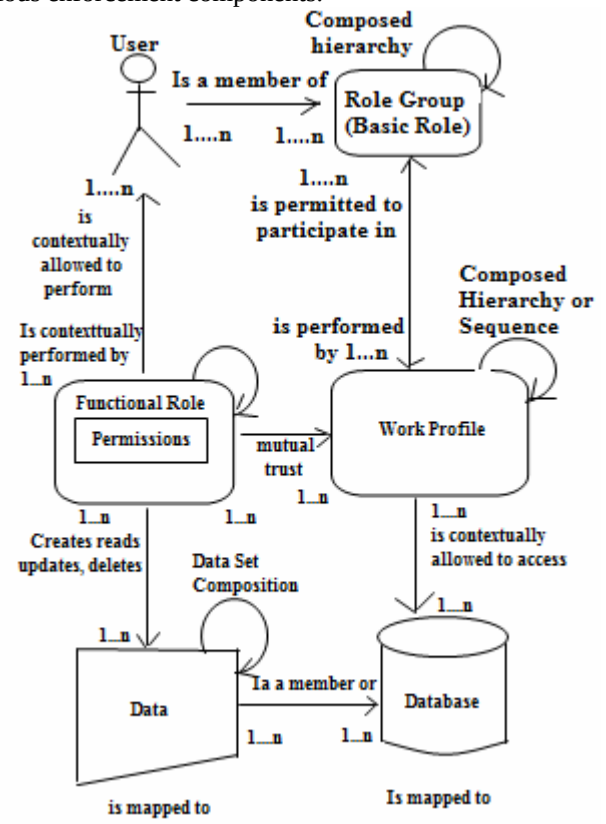

Figure 3: NIST Engineering Model proposed in January, 2006

An optional module, known as coordination service can be dynamically loaded according to the user's device capability in order to enable the device to act as the coordinator. In this case, the membership management will also manage the membership of the specified event and executing the actions specified in the policies when the events occur. Lastly, the event service collects and aggregates events and subsequently forwards them to the method enforcement, e.g. the triggering of the execution of obligation policies. System events are forwarded to the protocol management, so that appropriate protocols can be performed.

C. Access algorithm for devices

Based on our discussions, we present an algorithm below with the steps that need to be performed to execute network access service. Ad hoc users generally start by looking for service on their category and role. The tuning and access to a channel is to be performed by an appropriate access method.

***Algorithm execute-service*:**

/*executed whenever device accesses an ad hoc network*/

Begin:

a. The local UDDI directory is checked for ad hoc service.

b. Select a service and retrieve its service key Key_I and compare with the key stored in the event service.

c. Frequency of the service channel is retrieved

d. The service channel checked.

e. Description is downloaded and code of the service having Key_i as the service key.

f. Based on the service key Key_i, determine input parameters (from user management) for the initiation of access to the network.

g. Proceed to login to the network.

h. After successful login, retrieve the frequency of the data channel

i. Download role specification for the device and store it in event service

j. Execute the service or exchange data with other users on the data channel of the network.

End

III. ANALYSIS AND DISCUSSIONS

In the area of user role assignment, we find that in Sybase, the task of assigning roles to users is a centralized activity that can be only performed by the System Security Officer and there is no feature for assigning that right to the role grantee. An important component of security method in many commercial environments is separation of duty. RBAC provides a conceptual framework for implementing this method. Out of the three DBMS products that were reviewed, we found that only Sybase provides features for implementation of this method. Additionally, Sybase maintains tighter control over user-role assignment and more conformant to RBAC framework as it supports static and dynamic separation of duties. Overall our conclusion is that these products provide a sound basis for implementing the basic features of RBAC, although there are significant differences. It should be noted here that our focus in ad hoc networks is limited to single databases, as Oracle 8.0 comes with an add-on security product called Oracle Security Server which allows global users and roles to be defined for use across multiple databases. This security feature was not under our consideration for this work. The total overhead required in terms of functionality on network devices is role based framework and access control algorithm. In case of Coordinator, additional overhead is the data management. As ad-hoc network devices are usually smaller in number, this additional overhead is not expected to be high at any given time. On the other hand, advantages gained are access based on method of the organization, and simplicity at network administration. Thus, this approach provides flexibility in providing additional feature related to security of the network.

IV. CONCLUSIONS

In this paper, an effort is made to define method that dictates three processes initiation, execution and termination of sessions on ad-hoc networks. It requires that mobile devices be simple having various software components including framework for roles. The network support is provided by Coordinator and central server for executing access codes on behalf of the mobile devices. The issues that still remain to be investigated include the maximum number of devices that can be allowed to join a session, and maximum number of sessions that can be initiated by a mobile device itself. Obviously, these together may create a resource constraint problem in an ad-hoc network. Furthermore, rate of mobility is to be seriously looked into, as it may create data manage-

ment issue, specially caching of data during an ongoing session.

V. ACKNOWLEDGEMENT

This paper is based on networking and we completed the work with the help of many experts of networking. We take the help of Networking and Communication Laboratory of HCTM College to perform our task. We thank many of our friends help us in the completion of this work. We also thank Dr. Vikarm Singh (Chairman in Computer Deptt.) and Dr. Dilbag Singh (Reader in Computer Deptt.) in CDLU, Sirsa (India)

VI. REFERENCES

[1] Wireless Ethernet Standards Development, http://www.ieee802.org/11/

[2]. Bluetooth Technology Specification: https://www.bluetooth.org/spec/

[3] Internet Engineering Task Force (IETF) Forum:http://www.ietf.org/

[4] D.F. Ferraiolo, J. Barkley, D.R. Kuhn, "A Role Based Access Control Model and Reference Implementation within a Corporate Intranet", *ACM Transactions on Information and Systems Security*, Vol. 2, No. 1, February 1999, pp. 34-64.

[5] D. Barbara," *Mobile Computing and Databases – A survey"*, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 11, No. 1, January/February 1999, pp. 108-117.

[6] X. Yang, A. Bouguettaya, B. Medjahed, H. Long, and W. He, "Organizing and Accessing Web Services on Air", *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 33, No. 6, November, 2003, pp. 742-757.

[7] S. Gadiraju, and V. Kumar, "Recovery in the Mobile Wireless Environment Using Mobile Agents", *IEEE Transactions on Mobile Computing*, Vol. 3, No. 2, April-June, 2004, pp. 180-191.

[8] V. Kumar, N. Prabhu, M. Dunham, A. Seydim, TCOT-"A Timeout-Based Mobile Transaction Commitment Protocol, *IEEE Transactions on Computers"*, Vol. 51, No. 10, October 2002, pp. 1212-1218.

[9] W. Peng, and M. Chen, "Design and Performance Studies of an Adaptive Cache retrieval Scheme in a Mobile Computing Environment", *IEEE Transactions on Mobile Computing*, Vol. 4, No. 1, January/February 2005, pp. 29-40.

[10] J. Doshi, W. Aref, A. Ghafoor, and E. Spafford, "Security Models for Web-Based Applications", *Communications of the ACM*, Vol. 44, No. 2, February 2001, pp. 38-44.

[11]. R. Sandhu, "Lattice based access control models", *IEEE Computer*, 26, 11, 1993, pp. 9-19.

[12] S. Osborn, R. Sandhu and Q. Munawer, "Configuring Role - Based Access Control to Enforce Mandatory and Discretionary Access Control Policies", *ACM Trans. on Information and System Security*, Vol. 3, No. 2, May 2000, pp. 85-106.

[13] C. Ramaswamy and R. Sandhu, "Role Based Access Control Features in Commercial Database Management Systems", *Proceedings of 21st NIST-NCSC National Conference on Information Systems Security*, October 1998, pp. 503-511.

[14] M. Chen, P. Yu, T. Tang, "On Coupling Multiple Systems with a Global Buffer", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 8, No. 2, April 1996, pp. 339-344.

[15] National Institute of Standards and Technology-RBAC, http://csrc.nist.gov/rbac/