Doktorandský den ’04

Ústav informatiky

Akademie věd České republiky

Paseky nad Jizerou, 29. září – 1. říjen 2004

Obsah

Security in mobile environment

doktorand:
ING. ROMAN ŠPÁNEK
Department of Software Engineering, Faculty of Mechatronics,
Technical University of Liberec
roman.spanek@vslib.cz

školitel:
ING. JÚLIUS ŠTULLER CSC.
Ústav informatiky AV ČR, Praha
stuller@cs.cas.cz

obor studia:
Elektrotechnika a informatika
číselné označení: 2612v045

Abstract

Advances in cellular mobile technology have engendered a new paradigm of computing, called mobile computing. New challenges have arisen and solutions are proposed based on various approaches. One of the most important challenges is security and now a day has been found ubiquitous in computing as whole. The paper is intended as a quick survey emphasizing security paradigm and also ad hoc networks are kept in mind and briefly discussed.

1. Introduction

Several challenges are in the mobile environment which is generally divided into a collection of cells which are operated by base stations (BS) located in the center of each cell. Mobile database system is depicted on Figure 1. One or more BSs are connected with a Base Station Controller (BSC), which coordinates BSs using locally stored software and commanded by the Mobile Switching Center (MSC). A fixed host is a set of general purpose computers connected with BSs through a high-speed wired network. Database Servers (DBS) are capable to incorporate data processing without affecting the mobile network. DBS communicate with MUs only through a BS. Every MSC contains Home Location Register (HLR) which keeps user profiles and real-time client location. MSC, in addition, contains also Visitor Location Register (VLR) contains information about users who are actually within the cells responsible by the MSC. When a MU moves out of current cell to another which is operated by different MSC, a new tuple is added into the VLR registry and the HLR is also updated accordingly. This is called two-tier architecture makes user's location transparent to MSCs and therefore MUs. Through the MSCs mobile units can communicate to the Public Switched Telephone Network (PSTN).

Rest of the paper is organized as follows: section 2 summarizes main issues in the mobile computing and some possible solutions are also briefly sketched. Section 3 is dedicated to the security algorithm proposed by us and personalization is also noted as our next research direction. The ad hoc network and related problems are mentioned in section 4. Section 5 concludes the paper and a brief overview on our future research is done.

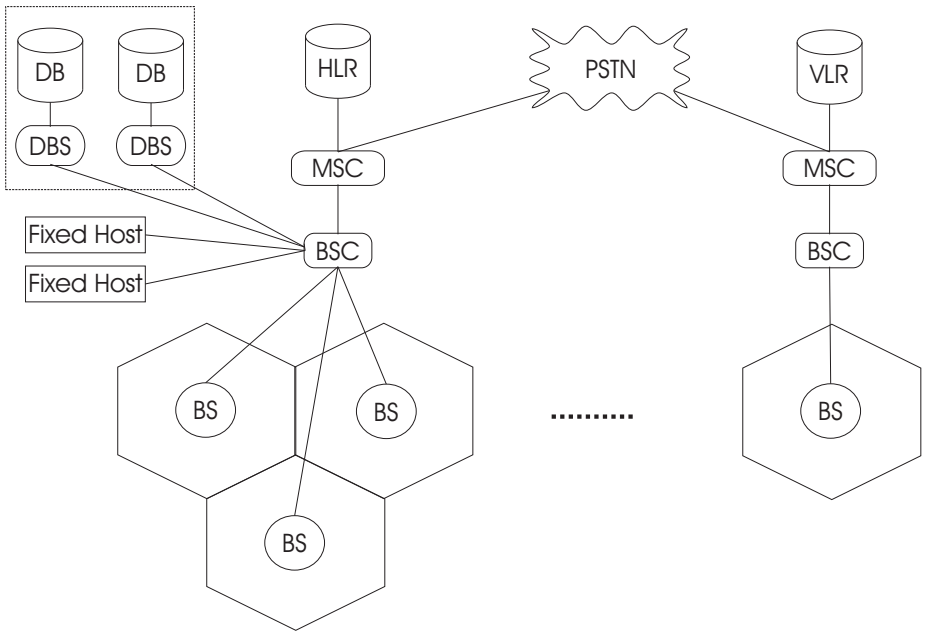

Figure 1: Mobile database system architecture

2. Main issues in mobile computing

2.1. Handoff

A MU freely moving through the cellular network therefore when cross a cell boundary, signal level would decline under minimum threshold and network disconnection would so that occurs, the MU has to switch BS (this is called *Handoff*). The three handoff strategies have been proposed:

- *Mobile-controlled handoff* (MU continuously monitors the signal level and when it decreases under predefined threshold the handoff procedure is initiated);
- *Network-controlled handoff* (BSs measure the signal level and issue handoff process);
- *Mobile-assisted handoff* (MU is responsible for measuring signal level but MSs are responsible to issue handoff procedure).

When the MU's signal level decreases under minimum acceptable level the BS disconnects the MU from the network, send message to BSs in way to found one which will be able to serve the MU while its next movement. The selected BS establishes a new communication channel and the MU continues in the new cell with the new BS serving its requests. This approach is called *HARD HANDOFF* because the MU is disconnected from the mobile network for a while. In spite of the precedent disadvantage this kind of handoff is broadly used in the cellular networks all over the world. The different approach, called *SOFT HANDOFF*, use the different schema how a new link between a MU and a BS can be established. When handoff occurs the MU is in short time connected to the both BSs, to which one has been connected and to which one is being connected. In this approach the MU is all time connected with a BS and is able to continuously broadcast.

2.2. Throughput

The limited wireless line throughput can be addressed as very strict constraint which should be mentioned by all proposals. Proposals have to take in an account MUs' restricted battery power, quite unstable wireless lines with unpredictable handoffs and network disconnections so that the most load and network conduct

ought to be server by wired lines and power BSs. Wired lines between BSs can be treated as sufficient capable and via those lines can be sent more messages without causing any obstacles to the mobile network due to the broad wire line throughput.

2.3. Channel reusing

Number of channels is obviously limited to a quite small number. Because of this limitation a channel reusing is in use. The adjacent BSs use different channels so that no interference can occur. Those channels are reused by BSs located within the sufficient radius so the interference is under acceptable threshold. This schema suffers with inefficient channel utilization because the BSs under heavy traffic require more channels then the idle BSs. To cope with this limitation the Dynamic Channel Assignment (DCA) has been proposed [1], [2]. No channels are initially assigned to the cells and the channels are allocated on a BS's demand when it is necessary. Some additional schemas have been proposed and based on the DCA, like the SCA (*Scheduled Channel Assignment*). The SCA estimated traffic's and movement's peaks and the channels are allocated with respect to these peaks.

Quite different approach has been proposed in [3]-[6]. In this approach each BS has assigned finite number of channels. When BS is becoming to be *hot* (has only few free available channels) the channel borrowing algorithm is triggered. This algorithm takes in account information about the adjacent *hot* BSs and transfers free channels from *cold* (has a plenty of available channels) BS.

The channel reusing is very important from technological viewpoint.

2.4. Data management and location dependent data

The mobile data management as whole poses many obstacles. Some of them are addressed in the next lines.

When a MU issues the request for a data stored on a wired server the BS sends them to the wired network and also receives the reply. But the MU location may be changed so that handoff would occur. Furthermore MU would have been disconnected from the mobile network (e.g. battery failure, line failure, i.e.). Therefore the demanded data have to be sent to appropriate BS if MU has changed location or will be preceded in different way if the MU has been disconnected from the network till be reconnected.

The location dependent data are frequently addressed in the mobile network. Common query like: "City of bird", "Mother's maiden name", etc. usually fetches the same data, independent on the location where has been issued. On the other hand query issued by user through its phone: "Where is nearest hospital?" fetches different data with respect to the MU's location. The first type is referred as "*Location Dependent Data (LDD)*" and the second type as "*Location Free Data (LFD)*". The LDD gives rise to *Location Dependent Query (LDQ)* and *Location Aware Query (LAQ).*

MU location is therefore required to be transparent to data source handling the requested (hospital in our example) information.

This is usually addressed as *Location management*. The different approaches can be used to locate MU in the mobile network and message consuming has to be considered again. The first is called *Deterministic approach* and the MU's location is periodically updated by sending the location message. Choosing the interval and the condition for the location message issuing can be found as the main different between approaches. *Probabilistic approach* on the other hand uses MU's movement patterns and likelihood's algorithms to manage MU's location. This is one of the most important paradigms in the mobile databases.

2.5. Transaction management

Transaction management in the mobile computing is mostly similar with distributed database systems. Each transaction is divided into *Fragments* usually executed on different DBSs and also being location dependent. *Location Mapping* is consequently used to choose the geographic location where the demanded data are stored. A mobile transaction definition follows.

A Mobile Transaction is a triple $\langle F_i, L_i, FLM_i \rangle$ where F_i is a set of execution fragments, L_i a set of location, and FLM_i is a set of fragment location mappings.

Due to Handoff and low wireless line throughput is in the mobile environment very difficult to support transaction with the traditional two or three phase commit protocol broadly in use in stationary database systems. Thereby new transaction methods are found. One solution has been proposed by V. Kumar in [7], solving problem of unstable wireless line with unpredictable handoffs and limited throughput by a time stamp. The time stamp is used so the transaction's participants wait until the time stamp exceeds and only if all transaction's participants have replied than the transaction is committed otherwise is aborted. So the time stamp has to be set very carefully. Too big may cause an unnecessary delay but to short may cause an aborting transaction despite of its correctness.

2.6. Ad hoc network

A network without BSs and stationary units as all is referred as *Ad hoc network*. The network structure without fixed infrastructure is built on freely moving MUs which communicates with its neighbors (MUs in transmission range) and acts also as routers for packages which are not addressed them. In that environment security problems are gained by absence of a certain authority (like a BS in the cellular network) responsible to manage packets and authentication procedures. Capture 3 discussed the ad hoc network in details.

2.7. Security

Security problem can be found in botch environments and is common for mobile and traditional computing. The mobile environment faced us with new obstacles and questions. Sharing information inside a selected group of users in a simple form with respect to the bandwidth utilization is one of the most important clams. The security scheme based on the grouping algorithm has been proposed in [8]. Grouping and personalization are more precisely described in section 3.

3. Grouping and personalization

Some proposals have addressed the security problem and some of them employed the grouping algorithms. Sharing secure information is very difficult to achieve in such unstable environment with threat of tap. Tapping can be partially solved by cryptography algorithms with usually pubic key encryption.

3.1. Grouping algorithm

A grouping algorithm has been proposed in [9] however the member account is limited. A different solution has been mention in [8]. Author found a group as a base unit for the whole humans' society and employs the Hyper Graph theory. The Hyper graphs are used due to semantic which is suggested as solution for groups with huge amount of users, where is inefficient storing complete data about each users by each user. In this approach user stores *secure cookie* (SC) [10] for holding its own information. The SCs are used instead of the traditional cookies because of enhanced security. Note that the traditional cookies are stored in a simple text format and can be easily stolen by malicious users. The SC includes necessary user's information *Group Name, User Name, Cookie Time Stamp, User Trustiness Value, User Group ID, User Password, User IP Address and Seal Cookie* which is made as digital signature of all precedent values using the public key encryption and preventing malicious users to change the SC. The SC is subsequently used for authentication user to the group of which is the member. The semantic given by the hyper graphs has power to store and manage a big group in simple way.

Figure 2 shows a hyper graph structure. Mu1 is the vertex represents particular mobile unit; r_1 is its role in the group and a_1 is the association which is responsible for interconnecting MUs from the same group. Vertex representing MU's *rank (Mu1)* is linked through the *meta-incidence* (i_1), the *meta-edge* (m_1) and the *lift-incidence* (L_1) with connected component built from the vertices N1, N2, N3; the roles r_3, r_4, r_5 and the association a_2 which is again used as interconnection for common vertices. Assume that N1 has the "Sale Manager" value, N2 has the "IT Manager" and their common type N3 has therefore the "Manager" value. Roles for the mentioned vertices can be left blank or can be connected to a connected component.

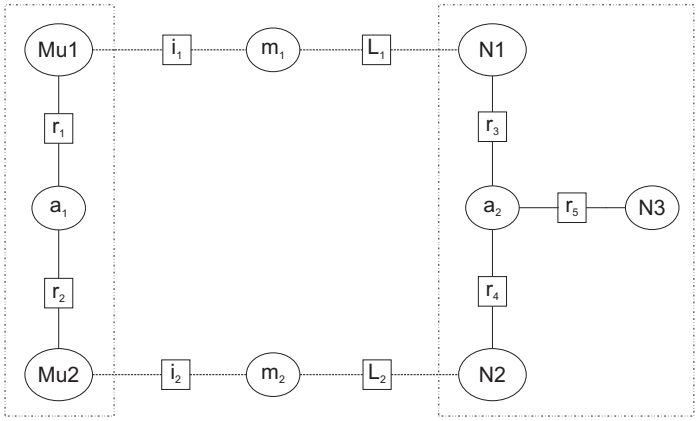

Figure 2: Hyper graph represents the group structure, MU's role and rank in the group

The MU's roles r_1, r_2 have to be linked in similar way with connected components so that appropriate semantic is achieved. The semantic can be easily revealed and reads as follows: The Mobile unit 1 has the nexus "Sale Manager" and its role in the group is "Trusted Member" (note that the value "Trusted member" was assumed for the role r_1 and is achieved through linking it with a connected component). In a similar way the role and the nexus of Mu2 can be achieved. Users simply ask the system if the user demanding data is either trusted or not. This information is derived from the hyper graph structure. So the user issues only yes/no query and system replies with minimum wireless messages optimally including yes/no value. Relations between users are therefore transparent to each.

Meta-incidences and meta-edges are used for interconnecting different connected components and lift-incidences are used for connection as well but have act as a direction manager, so that a server managing a group can easy distinguish which is either vertex represents a MU or vertex represents a nexus.

When a MU is about to built a group, the basic connected component represents basic roles (e.g. "Administrator") and nexuses (e.g. "Group Creator") have to be built. After the precedent steps users are allowed to join the group by connecting its roles and nexuses. User can join a group on invitation issued by trusted user or after completing group's prerequisites (e.g. publishing on valuable conference). Note that the similar process can be found in the human society.

Each group user has its own trustiness value which is used for user behavior validation. The trustiness value is under fluently evolution. When a user behavior is very valued its trustiness value is increased and on this value the user's group nexus and rank can be enhanced. When a new user join the group its trustiness value is set to default (note that quite small) value. With respect to the user's behavior and its group assets is either increased or decreased. Users with sufficient authority (derivate from its nexus and role) can make connected components for its own purposes, manage roles and nexuses of other participants and they can invite a new user.

Important aspect of proposed approach is that the whole structure is built on the hyper graph theory and no additional devices are required.

3.2. Personalization

Personalization is very important research stream. It is also based on the human society behavior; humans need their privacy, their living space; personalization brings those prospects to computing. So that it will be my next research direction and security problems can be narrow addressed with the personalization. The first step was made by grouping algorithm and next step is creating both the living space and the privacy for each user in a group so that its good wouldn't be broken.

On the other hand personalization brings more obstacles because is straightforward opposite to data sharing in simplest form as possible.

4. Ad hoc network

The ad hoc network [11] absents any stationary and trusty structure like a BS in the cellular network. MUs are responsible for packets forwarding, routing and service discovery. From this environment new challenges are raised and have to be solved because of permanently growing amount of such networks and customer demands.

The ad hoc network is permanently changing, because of MU movement and can be imagined as a cellular network where MUs acts instead of BSs. From this specification have risen two different kind of attack:

- active; where a misbehavior node consume some energy to perform harmful operation; nodes acts in this kind of misbehavior are called *malicious*
- passive; consists of lack of cooperation and consequent harmful operations; nodes performing the passive attack to save energy are considered as *selfish*

Malicious nodes can brake down packets forwarding by *modifying routing information*, by *fabricating false routing information* and by *impersonating other nodes* in the network. Recent studies have revealed new attack that is known as *wormhole* attack. In the wormhole attack case the malicious node sends packets via tunnel to another network through a private network and shared them with other malicious nodes. Dangerousness of wormhole attack and its difficult revelation is gained by the routing protocols which try find shortest patch from a packet's source and its destination. From this viewpoint the wormhole nodes acts as shortest patch.

Another kind of harmful behavior is *spoofing* when a malicious node impersonates a legitimate node. *Integrity attack* should be also kept in mind. In this kind of attack malicious nodes altering protocols fields in order to deny communication with legitimate nodes (it is also known as denial of service).

Several proposals have been aimed to solve precedent security problems [12] and most of them solved active attacks with successfulness but passive attack remains as a half solved.

5. Conclusions

The mobile computing and mobile databases are quickly growing and evolving area with quickly increasing number of users. This part of computing brings new possibilities and obstacles indeed.

The entire paper is dedicated to the mobile computing and brings an overview on the obstacles and their solutions as have been proposed in the recent years. The security part is emphasized and solution based on the paper proposed by author is described more precisely. The ad hoc networks are also briefly taken in account and the problems raised from the specific environment are sketch with the possible solutions.

Next research will be dedicated to enhance security schema based on the grouping algorithm and also the implementation task will be considered. For that purpose some other mathematical theories will be taken in account to propose the one with the simplest and most efficient implementation task. The ad hoc network and it security tasks will be kept in consideration as well.

Next turn will be personalization task. It is a very important part mutual for the human society and computing as whole.

References

[1] S. Nanda, D.J. Goodman, "Dynamic Resource Acquisition in Distributed Carrier Allocation for TDMA Cellular Systems", *Proceedings GLOBECOM*, pp. 883–888, 1991.

[2] E. Re, R. Fantacci, G. Giambene, "Handover and Dynamic Channel Allocation Techniques in Mobile Cellular Networks", *Transactions on Vehicular Technology*, vol. 44, 1995.

[3] S.K. Das, S.K. Sen, R. Jayaram, "A Novel Load Balancing Scheme for the Tele-Traffic Hot Spot Problem in Cellular Networks", *ACM/Baltzer Journal on Wireless Networks*, vol. 4, 4, pp. 325–340, 1998.

[4] S. Mitra, S. DasBit, "Load Balancing Strategy Using Dynamic Channel Assignment and Channel Borrowing in Cellular Mobile Environment", *Proceedings, International Conference, ICPWC*, pp. 278–282, 2000 (December). Architechture and Protocols, 1991 October.

[5] S.K. Sen, P. Agrawal, S.K. Das, R. Jayaram, "An Efficient Distributed Channel Management Algorithm for Cellular Mobile Network", *IEEE International Conference ICUPC*, 646–650, 1997 October.

[6] I.I. Jiang, S.S. Rappaport, "Cbwl: a New Channel Assignment and Sharing Method for Cellular Communication Systems", *IEEE Transactions on Vehicular Technology*, vol. 43, 1994 May.

[7] V. Kumar, N. Prabhu, M. Dunham, Y.A. Seydim, "TCOT - A Timeout-Based Mobile Transaction Commitment Protocol", *Special Issue of IEEE Transaction on Computers*, vol. 51, No. 10, pp. 1212–1218, 2002.

[8] R. Spanek, "Security in Mobile Environment base on Grouping Algorithm", in preparation.

[9] P.K. Behera, P.K. Meher, "Prospects of Group-Based Communication in Mobile Ad hoc Networks", *Springer-Verlag Berlin Heidelberg*, 2002.

[10] J. Park, R. Sandhu, S. Ghanta, "RBAC on the Web by Secure Cookies", *Database Security XIII: Status and Prospects*, Kluwer 2000.

[11] Basagni, "Remarks on Ad Hoc Networking", *Springer-Verlag Berlin Heidelberg*, 2002.

[12] Molva R., Michiardi P., "Security in Ad Hoc Networks", *Springer-Verlag Berlin Heidelberg*, 2003.