Wireless LAN Location-based Access Control

I. Lagzdinyte-Budnike[1], R. Petrauskiene[1], N. Sarafiniene[1], G. Vilutis[1], A. Budnikas[2]
[1]Department of Computer Networks, Kaunas University of Technology,
Studentų St. 50, LT-51368 Kaunas, Lithuania, phone: +370 652 19840
[2]Department of Telecommunications, Kaunas University of Technology,
Studentu St. 50, LT-51368 Kaunas, Lithuania, phone: +370 652 21950
ingrida.lagzdinyte@ktu.lt

***Abstract*—Location-based access control model for Wireless LAN is presented. It integrates location-based features and uses the hierarchy of spatial roles. On basis of presented model Wireless LAN location-based access control system was designed and implemented. Location-based access control and policy enforcement algorithms that use location mapping functions and the evaluation of location information confidence were offered and presented. The system is evaluated by testing its operating speed.**

***Index Terms*—Location-based access control, wireless networks, wireless network security.**

I. INTRODUCTION

Wireless networks are a popular alternative to wired networks because of their affordability and flexibility. Unfortunatelly they are more vulnerable and open to various attacks. Authentication and access control are the key elements in ensuring successful use of a wireless network. User authentication can be done by a variety of standard authentication mechanisms, but some of them are still vulnerable [1]. Combining these authentication mechanisms with location information we can achieve better security.

Some researches are made in this field. Ardagna and others offer some studies of how general access control mechanism can be complemented with location-based conditions [2], [3]. I. Ray and M. Kumar [4] offer formalization techniques for location data. They analyse how location-based conditions can be integrated into components of mandatory access control (MAC) mechanism. M. L. Damiani and others [5] describe location-based extensions of role-based access control model (Geo-RBAC). L. Bao and others have described and evaluated a secure location-based access control (LBAC) based on location group and location key concepts [6].

All these studies do not analyse how these models can be adjusted to work in wireless networks. Mapping functions of real user location and role coverage are not discussed also. There is a lack of suggestions and offers for architectural wireless LAN location-based access control solutions and such system‘s design.

The latter questions are discussed in this article. We describe wireless LAN access control model complemented with location information, introduce with most important aspects of spatial features and role-based wireless LAN access control system’s design, and provide some experimental results illustrating implemented system's performance. Afterall some conclusions are made.

II. WIRELESS LAN LOCATION-BASED ACCESS CONTROL MODEL

A general infrastructure of wireless LAN location-based access control system is presented in Fig. 1. Scheme was proposed based on the performed analysis of authentication and access control mechanisms and their facilities to use the location information.

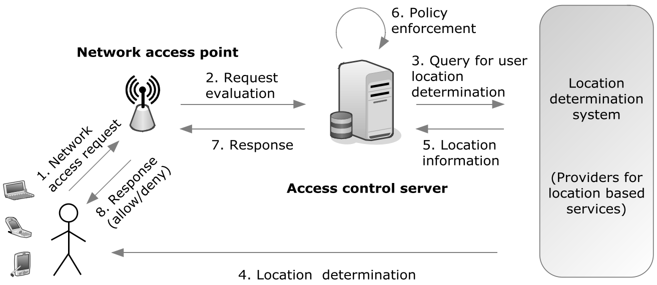
6. Policy enforcement
Network access point
2. Request evaluation
3. Query for user location determination
Location determination system
1. Network access request
7. Response
5. Location information
8. Response (allow/deny)
Access control server
(Providers for location based services)
4. Location determination

Fig. 1. Infrastructure of wireless LAN location-based access control system.

As it can be seen from the picture, wireless LAN location-based access control must be complemented with the location system. In order to access wireless LAN resources users must get confirmation from access control server (ACS). An access point acts only as an intermediary between the user and the server.

ACS has to estimate user’s rights to access wireless LAN resources. To do this task it has to know the location of the user. To get these data it refers to the location determination system. The location determination system analyzes data from sensors, calculates user’s location and returns the answer.

In some cases, ACS can operate in access point. Also it may need to communicate with multiple access points, as suggested in [4] and [5].

In Fig. 2 wireless LAN location-based access control model is presented. The main objects that have been added to typical access control model in order to use location information are: 1) location determination system (LDS); 2) location-based features and their types; 3) mapping

Manuscript received March 12, 2012; accepted June 8, 2012.

functions; 4) assurance of location information determination quality; 5) strategy of permits allocation periodicity.

These parts of the model will be discussed in more detail.

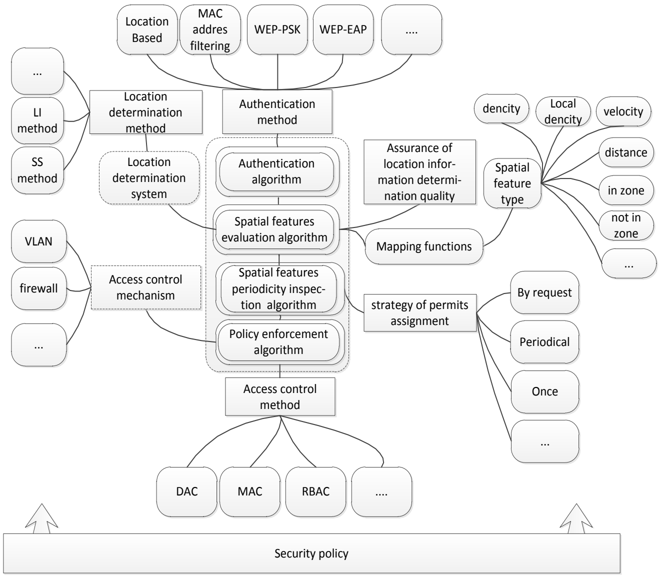

Fig. 2. Wireless LAN location-based access control model.

A. Location determination system

Location information can be calculated using different methods and techniques. The most popular are techniques that: 1) evaluate signal strength; 2) measure the data packet transfer time [7]. LDS is responsible for these functions.

B. Selection of location-based features and their types

The concept of location-based feature describes the location information in access control process. This concept is compatible with one that is used in Geo-RBAC model [5]. Features have application-depended semantics which can be expressed with the term of feature type. Some of location information feature types are described in Table I.

TABLE I. TYPES OF LOCATION INFORMATION FEATURES.

Feature type	Description
in_zone(user, zone)	Estimates if the user is in zone
not_in_zone(user, zone)	Estimates if the user is out of zone.
distance(user, object, min_distance, max_distance)	Estimates if the distance from user to object is in the interval [min_distance; max_distance]
velocity(user, min_velocity, max_velocity)	Estimates if velocity of the user is in the interval [min_velocity, max_velocity]
density(zone, min_amount, max_amount)	Estimates if the quantity of the users in the area is in the interval [min_quantity, max_quantity]
local_dencity(user, zone, min_quantity, max_quantity)	Estimates if the density of users in the area around the user is in the interval [min_quantity, max_quantity]

According to the scope of the entities there can be defined spatial features' and their types' hierarchies. Hierarchies can be used in the wireless LAN location-based access control model. Such types as distance, velocity, dencity and similar are nonspatial. No hierarchy can be defined to nonspatial feature types.

C. Selection of mapping functions

Mapping function binds location information with location-based features. Every feature type can use different mapping function.

D. Assurance of location information determination quality

It is necessary to assure sufficient level of location information determination quality for usage of location information in access control mechanism. This aspect depends on LDS. Before using the location information ACS and LDS can make an agreement on location determination quality level. It is necessary if the LDS provide varying levels of service and required quality is not coordinated in advance.

In addition to the agreement every time when location information is determined LDS can determine its reliability level and uncertainty. Uncertainty shows maximum distance the actual user's location may differ from determined one. Reliability level represents the probability that the terminal is actually in that place. According to reliability value ACS makes a decision if it can use determined location information or it has to query LDS for location information once more again.

E. Strategy of permits allocation periodicity

Typically access control systems authenticate the user only once. If authentication protocol uses location information, at this moment it will check user's location. After successful authentication user has access to all resources for which he is authorized to access. Since users are mobile and location information can change over time access control system should verify users' location periodically. If the location information changes access permitions should be updated as well. Strategy of permits allocation periodicity defines when and how policies will be fulfilled when location information changes. Depending on strategy different algorithms of permits allocation periodicity can be used.

III. SPATIAL FEATURES AND ROLE BASED WIRELESS LAN ACCESS CONTROL SYSTEM

Spatial features and role based wireless LAN access control system was designed and implemented on basis of proposed wireless LAN location-based access control model. Implemented system operates in multi-storey building, uses location-based authentication, spatial features and role based access control, updates access permitions periodically and evaluates feature type "in_zone" (Table I).

The architecture of implemented system corresponds to the architecture of wireless LAN location-based access control system presented in Fig. 1.

ACS in the system is responsible for: 1) Authentication; 2) User disconnection; 3) Policy enforcement. These responsibilities were implemented respectively in Authentication, Disconnection and Policy Enforcement modules. Data flows among ACS modules, location determination system, firewall, wireless LAN and access point are presented in Fig. 3.

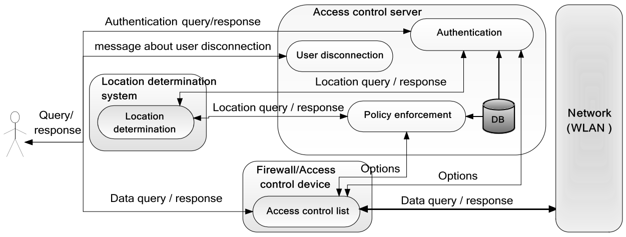

Fig. 3. Data flows in Wireless LAN access control system.

A. Security policy

Security policy creation consists of identification of necessary roles and their schemas, definition of the areas they will work and indication of inheritance between them. The hierarchies of roles and its schemas that were created and included into system implementation are presented in Fig. 4.

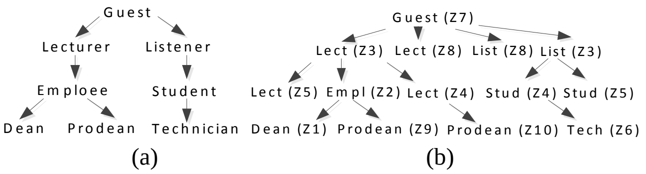

Fig. 4. Hierarchy of role schemas (a) and spatial roles (b).

Permits that are assigned to appropriate role or its schema are defined in Table II. There *Z1, Z2 … Z10* are spatial roles. We can see that there are different spatial features (Kaunas University of Technology (*Z7*), Department of Multimedia (*Z5*) and etc.) to which users are linked to perform a role. *P1, P2 … P16* define user's permits to access appropriate resource.

TABLE II. PERMITS ASSIGNED TO THE ROLES AND ITS SCHEMAS.

Role	**Schema permits**	**Permits assigned to spatial role**									
		Z1	**Z2**	**Z3**	**Z4**	**Z5**	**Z6**	**Z7**	**Z8**	**Z9**	**Z10**
Dean	-	P10	-	-	-	-	-	-	-	-	-
Prodean	P14	-		-	-	-	-	-		P15	P16
Employee	P8	-	P13	-		-	-	-	-	-	-
Lecturer	P3, P9, P11	-	-	P5	P6, P7	P4	-	P12	-	-	-
Student	P2	-	-	-	-	-	-	P6	P4	P7	-
Listener	-	-	-	P3	-	-	-	-	-	-	-
Guest	-	--	-	-	-	-	-	P1	-	-	-
User's permits: P1 – Internet (read), P2 – Lecture material (read), P3 – printer for students (execute), P4 – multimedia labs (execute), P5 – Software for Labs (execute), P6 – Labs of Computer Department (execute), ... , P16 – files for student exchange (write).											

A. Algorithm of authentication

Algorithm of authentication that is used in ACS is presented in Fig. 5. First authentication steps include password, certificate or other login data verification. If data fits, query for location data is sent to LDS. If location data suit the spatial features that are set in the system, authentication process succeeds.

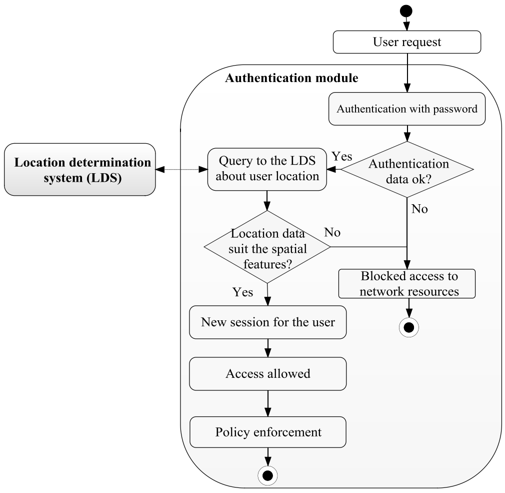
User request
Authentication module
Authentication with password
Location determination system (LDS)
Query to the LDS about user location
Yes
Authentication data ok?
No
Location data suit the spatial features?
No
Yes
Blocked access to network resources
New session for the user
Access allowed
Policy enforcement

Fig. 5. Algorithm of user authentication.

B. Sequence of policy enforcement

Policy enforcement algorithm is presented in Fig. 6. Algorithm is executed periodically. Before update process of user permits, system checks if the user is still in the building. This feature is checked first. Otherwise no one of spatial roles will be executed.

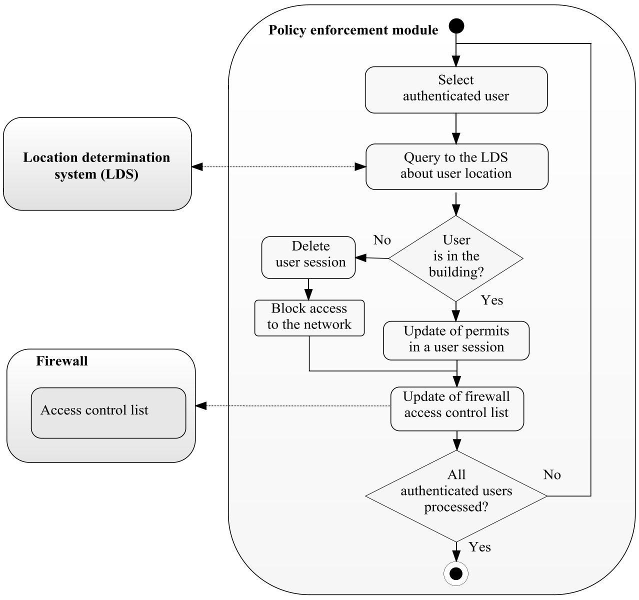
Policy enforcement module
Select authenticated user
Location determination system (LDS)
Query to the LDS about user location
Delete user session
No
User is in the building?
Yes
Block access to the network
Update of permits in a user session
Firewall
Access control list
Update of firewall access control list
All authenticated users processed?
No
Yes

Fig. 6. Algorithm of policy enforcement.

Some more important actions must be made before policy enforcement starts. These actions include granted permits identification and assignment to user according to roles that are defined for him.

IV. SYSTEM TESTING AND EXPERIMENTAL RESULTS

ACS was designed and implemented on Linux Ubuntu OS. Server and client were implemented in C. Data about users, roles, and spatial features were stored in MySQL. Experiments were performed on Pentium (R Dual-Core) 2 GHz CPU, 512 MB RAM.

A. Experimental environment

30 users with different spatial roles were included into DB. LDS was simulated creating file that contains location data records. Users' activity to get or refuse WLAN resources was simulated also.

B. Experimental results

There were performed two experiments. During the first one service time of user authentication queries was analysed. During the second experiment dependency of average service time and user authentication queries intensity was analysed.

All experiments were performed on system using multi-threaded query service model. 1 thread was used to demonstrate the case, when the queries are processed in sequential way.

The first experiment (Fig. 7) showed that implemented system with one operating thread can sequentially process up to 15 queries with service time <1s. If in the same moment there are more queries, service time grows up to 10s. If we have multi-threaded service model, all user queries are serviced in acceptable time (approximately 0,1s).

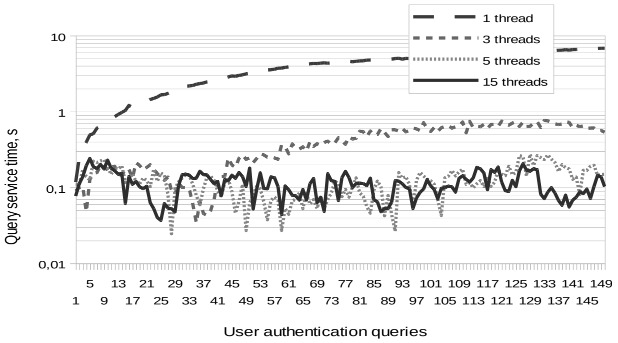

Fig. 7. User queries service times.

The results of second experiment (Fig. 8) showed that ACS with multi-threaded service model can process queries which come to server in various intensity. When queries intensity grows, average query service time grows in 1, 2 or 3 threaded system as well. More than 5 parallel operating threads query service models let us keep average query service time in 0,1±0,06s range.

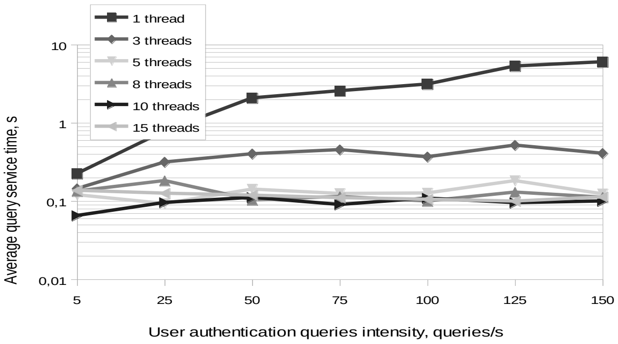

Fig. 8. Average user queries service times under different user queries intensity.

V. CONCLUSIONS

Presented wireless LAN location-based access control model propose to use location information obtained from a variety of wireless LAN positioning techniques and to combine it with a different wireless network authentication protocols. Model-based systems can be designed to expand and control access to enterprise wireless LAN resources. Presented spatial features and role based wireless LAN access control system is an example of such design.

Experimental studies of the designed system operating characteristics showed that user requests were served less than in 1 second using: 1) multi-threaded service model under different user queries intensities; 2) one-thread service model if the intensity of user queries have not exceeded the value of 15 q/s. It shows that during such systems design it is important to estimate system load and to choose the most appropriate query service model.

REFERENCES

[1] Y. Xiao, Ch. Bandela, X. Du, Y. Pan, E. Dass, "Security mechanisms, attacks and security enhancements for the IEEE 802.11 WLANs", *International Journal of Wireless and Mobile Computing*, vol. 1, no. 3, pp. 276–288, 2006. [Online]. Available: http://dx.doi.org/10.1504/IJWMC.2006.012562

[2] C. A. Ardagna, M. Cremonini, P. Samarati, "Access Control in Location-Based Services" *Privacy in Location-Bas ed Applications: Research Issues and Emerging Trends*, pp. 106–126, 2009.

[3] C. A. Ardagna, M. Cremonini, P. Samarati, *Privacy-enhanced Location-based Access Control, The Hand-book of Database Security: Applications and Trends,* Springer-Verlag, 2007, pp. 531–552.

[4] I. Ray, M. Kumar, "Towards a Location-Based Mandatory Access Control Model" *Computers & Security*, vol. 25, no. 1, pp. 36–44, 2006. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2005.06.007

[5] M. L. Damiani, E. Bertino, B. Catania, P. Perlasca. "GEO-RBAC: A Spatially Aware RBAC", in *Proc. of the SACMAT 05. ACM*, 2005, pp. 29–37.

[6] S. Cho, L. Bao, "Secure Access Control for Location-Based Applications in WLAN Systems", in *Proc. of the MASS 2006*, 2006 pp. 852–857.

[7] H. Liu, H. Darabi, P. Banerjee, J. Liu, "Survey of Wireless Indoor Positioning Techniques and Systems", *IEEE Transactions on Systems, MAN, and Cybernetics*, vol. 37, no. 6, pp. 1067–1080, 2007. [Online]. Available: http://dx.doi.org/10.1109/TSMCC.2007.905750