논문 2010-47CI-1-12

이 기종 네트워크에서 퍼지 알고리즘과 MAUT에 기반을 둔 적응적 보안 관리 모델

(Adaptive Security Management Model based on Fuzzy Algorithm and MAUT in the Heterogeneous Networks)

양 석 환*, 정 목 동**

(Seokhwan Yang and Mokdong Chung)

요 약

유비쿼터스 기술의 보편화에 따라 유비쿼터스 환경의 보안 취약성을 해결하기 위한 보안기술의 연구가 주목받고 있다. 그러나 현재의 대다수 보안 시스템은 고정된 규칙을 기반으로 하는 것으로서, 유비쿼터스 기반 사용자의 다양한 상황에 제대로 대응하지 못하는 문제점이 있다. 또한 기존의 상황인식 보안 연구는 ACL (Access Control List) 혹은 RBAC (Role-Based Access Control) 계열의 연구가 많이 수행되고 있으나 보안정책의 관리에 대한 오버헤드가 크고, 또한 예상하지 못한 상황에 대한 대응이 어렵다는 문제점을 보이고 있다. 이에 본 논문에서는 퍼지 알고리즘과 MAUT를 이용하여 다양한 상황을 인식하고 적절한 보안기능을 제공하는 상황인식 보안 서비스를 제안한다.

Abstract

Development of the system which provides services using diverse sensors is expanding due to the widespread use of ubiquitous technology, and the research on the security technologies gaining attention to solve the vulnerability of ubiquitous environment's security. However, there are many instances in which flexible security services should be considered instead of strong only security function depending on the context. This paper used Fuzzy algorithm and MAUT to be aware of the diverse contexts and to propose context-aware security service which provides flexible security function according to the context

Keywords : Context-aware Security (상황인식 정보 보안), RBAC (Role Based Access Control: 역할 기반 접근제어), MAUT (Multi-Attribute Utility Theory: 다중-변수 효용 이론), FCM (Fuzzy C-Means: 퍼지 클러스터링 알고리즘), Fuzzy Decision Tree (퍼지 결정트리)

Ⅰ. Introduction

There are many instances in which flexible security services need to be applied depending on the context when the system handles diverse sensors in the heterogeneous networks. Research on the security technology for solving the vulnerability of ubiquitous environment's security is gaining attention. In particular, there are many instances in which flexible security services should be considered instead of strong only security function depending on the

* 정회원, 부경대학교 정보보호학 협동과정
(Dept of Computer Security, Pukyong National University)
** 정회원, 부경대학교 컴퓨터공학과
(Dept of Computer Eng., Pukyong National University)
※ This research was supported by the Program for the Training of Graduate Students in Regional Innovation which was conducted by the Ministry of Commerce Industry and Energy of the Korean Government and the Brain Busan 21 Project in 2007.
접수일자: 2009년12월16일, 수정완료일: 2010년1월11일

context. Because mechanical security system based on the fixed rules is the main stream in the real world, however, numerous ubiquitous environment systems are not effective counter-measuring. Accordingly, research on the context-aware security that can apply appropriate security system flexibly is strongly required.

Sensor networks, one of the elements that comprise the basis of ubiquitous environment development consist of diverse sensors that provide information such as temperature, humidity level, intensity of illumination, and so on. There is a good possibility that these sensors will infringe upon subject's privacy when it comes to the information on the environment. Accordingly, there is a need to provide strong security function for the access to this information.

However, applying strong only security technology in all contexts can in fact decrease system efficiency and could increase inconvenience. In particular, in case of health care system that manages user's health and life, protection of the user's life should be considered at the first hand instead of the strong security at the time of emergency.

This paper uses sensor's information to be aware of the user's context, and proposes context-aware security service that can apply security technology of the diverse security levels flexibly according to the user's context.

This paper is comprised as follows. Section Ⅱ examines related work. Section Ⅲ introduces context-aware security service model using Fuzzy algorithm and MAUT. Section Ⅳ addresses the result of the experiment and the actual implementation of the proposed Context-Aware Security Service model. Finally, Section Ⅴ suggests conclusion and the further research.

Ⅱ. Related Work

1. GRBAC (Generalized Role-Based Access Control)

GRBAC[1~2] is the model that expanded the existing RBAC[3] model by adding on subject role, object role, and environment role to execute the control for access based on the context. Existing RBAC has the following limitations since it cannot use context information based on the role alone[4~6].

1) The Subject role is based on the role required of individual subjects as members
2) Access right is grouped depending on the role's name
3) Limitation on the use of resources as the role is provided according to the subject's work responsibility and access right

To solve these issues, GRBAC model manifests context-aware application's access policy more than the existing RBAC model, and it provides powerful and flexible method[7]. Since subjects, for example, who use the digital home are likely to be novice when it comes to computer or security, it is very crucial to include a function that would enable them to use with ease by defining the security policy for the application. In this respect, security service that uses GRBAC model that is based on diverse roles can serve as an effective method for building security service for the ubiquitous computing environment.

However, there is also a disadvantage in the GRBAC model that cannot handle unexpected context flexibly since it is based on the fixed rules.

To solve these limitations, it is possible to consider the method that entails renewing classification standard continuously by classifying the context through autonomous classification algorithm. This paper applied FCM (Fuzzy C-Means) clustering algorithm[9] and MFDT (Multivariate Fuzzy Decision Tree)[10] as the classification algorithm. And this paper also focuses on the utility theory[19] and Simple Heuristics[20] to determine the qualified properties such as user's preferences.

2. FCM clustering and Fuzzy Decision Tree

FCM (Fuzzy C-Means) is the data classification algorithm that classifies each data point that belongs

to the single cluster with the degree of membership. FCM clustering uses Fuzzy division technique and the membership function U may have value between 0 and 1. The sum of the value of membership function for the data set is always 1 as shown below[11].

$$\sum_{i=1}^{c} u_{ik} = 1, \quad \forall k = 1, \cdots, n \quad 0 < \sum_{k=1}^{n} u_{ik} < n$$

Cost function for the FCM clustering may have the following formula.

$$J(uik, vi) = \sum_{i=1}^{c} \sum_{k=1}^{n} u_{ik}^{m} (d_{ik})^2$$

$$v_i = \{v_{i1}, v_{i2}, \cdots, v_{ij}, \cdots, v_{iL}\}$$

$$d_{ik} = d(x_k - v_i) = \left[\sum_{f=1}^{1} (x_{kj} - v_{ij})^2 \right]$$

$$vi_j = \frac{\sum_{k=1}^{n} (u_{ik})^m x_{kj}}{\sum_{k=1}^{n} (u_{ik}) m}, \quad u_{ik} = \frac{1}{\sum_{f=1}^{c} \left(\frac{d_{ik}}{d_{jk}} \right)^{\frac{2}{m-1}}}$$

u_{ik} : Degree of membership of the k-th data of the X_k that belongs to the i-th cluster

v_i : i-th cluster's centroid

m ($1 \leq m < \infty$): Parameter that controls the volume of the Fuzzy characteristics in the classification process. m=2 in general.

d_{ik}: Distance between k-th data x_k that belongs to the cluster and i-th cluster's centroid v_i

$J(u_{ik}, v_i)$: Cost function for the FCM clustering

Decision tree[12] is the tree that expresses classification rule. Non-terminal node specifies the characteristics of the data that is compared for the classification. In the link, conditions for comparison or value of the characteristics are endowed. In the terminal node, value of the class whose data satisfies all the conditions and is on the route up to the applicable node from the root node, is allocated. Decision tree divides up the characteristic space using the clear value as the standard. Thus, two data that are subtly different can be classified into different classes, respectively. Accordingly, concept of Fuzzy function is introduced in the decision tree, and research is underway on the Fuzzy Decision Tree that divides into the Fuzzy boundary side using membership function[13].

3. MAUT and Simple Heuristics

MAUT (Multi-Attribute Utility Theory) is a systematic method that identifies and analyzes multiple variables in order to provide a common basis for arriving at a decision. As a decision making tool to predict security levels depending on the security context (network state, the resource's and user's environments, etc), MAUT suggests how a decision maker should think systematically about identifying and structuring objectives, about vexing value tradeoffs, and about balancing various risks. The decision maker assigns utility values to consequences associated with the paths through the decision tree. This measurement not only reflects the decision maker's ordinal rankings for different consequences, but also indicates him relative preferences for lotteries over these consequences[11].

According to MAUT, the overall evaluation $v(x)$ of an object x is defined as a weighted addition of its evaluation with respect to its relevant value dimensions. The common denominator of all these dimensions is the utility for the evaluator. The utility quantifies the personal degree of satisfaction of an outcome.

The MAUT algorithm allows us to maximize the expected utility in order to become the appropriate criterion for the decision maker's optimal action.

The Center for Adaptive Behavior and Cognition is an interdisciplinary research group founded in 1995 to study the psychology of bounded rationality and how good decisions can be made in an uncertain world[20]. This group studies Simple Heuristics. The first reason why we use Simple Heuristics is that security level can be decided without user's detailed preference. And the second reason is that it is difficult to predict the preferences of users concerning

the attributes of the security level. It is also difficult for even users to determine their preferences quantitatively which is related to the attributes of the security level.

By the way, different environments can have different specific heuristics. But specificity can also be a danger if a different heuristic were required for every slightly different environment, we would need an unworkable multitude of heuristics. Fast and frugal heuristics avoid this trap by their simplicity and enable them to generalize well to new situations. One of fast and frugal heuristics is Take The Best which tries cues in order, searching for a cue that discriminates between the two objects. It serves as the basis for an inference, and all other cues are ignored. Take The Best outperforms multiple regression, especially when the training set is small[20].

III. Context-Aware Security Service Model based on Fuzzy Algorithm and MAUT

Among existing context-aware security models, many models are based on the RBAC (Role-Based Access Control) model. However, disadvantage of those models is that they cannot control appropriately unexpected context. To solve this problem, this paper proposed a context-aware security service model that applied FCM clustering algorithm and Multivariate Fuzzy Decision Tree (MFDT: Multivariate Fuzzy Decision Tree). We also use MAUT and Simple Heuristics to adjust the result of Fuzzy algorithm.

The model proposed by this paper is comprised of USN (Ubiquitous Sensor Networks), the input part that collects and transmits information on the context, Context-Aware Engine that obtains results of classification by executing learning using input information, and Access Control Lists (ACL) that manages access permission list due to the applicable security level, and the security service engine that provides diverse security functions. In the learning module, FCM algorithm, which is one of the

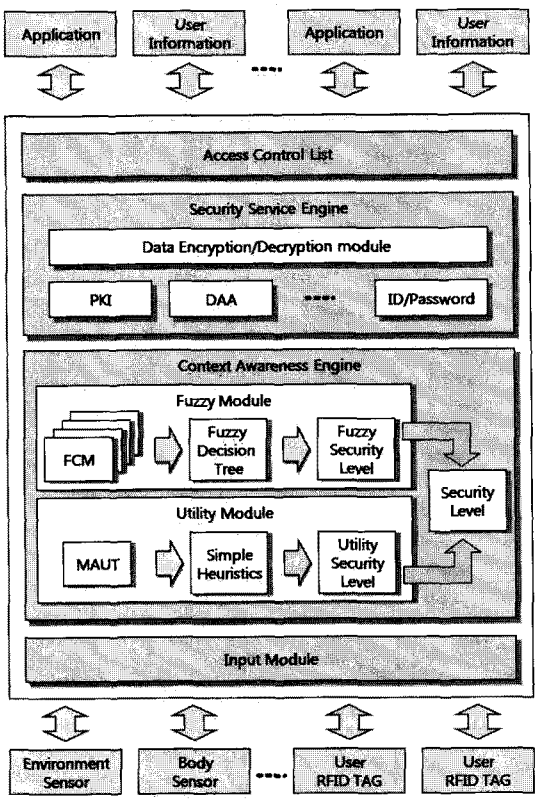

그림 1. 제안된 보안 모델
Fig. 1. Proposed Security Model.

autonomous learning algorithms, to execute pattern classification for the data input from the USN module, and the results are used to decide on the Fuzzy Security Level. The proposed model utilizes MAUT and Simple Heuristics to produce Utility Security Level. Finally, two Security Levels are merged into the Security Level. Figure 1 shows the proposed security model.

1. Input module

Input module collects the context information that is provided by the various sensors. Sensor network is comprised of the diverse sensors such as environment information sensor including temperature, humidity level and intensity of illumination, sensor for human body such as body temperature, blood pressure, and number of pulse and so on. Data collected in the input module is transmitted to the context aware engine. Figures 2, 3 and 4 demonstrate examples on the structure of the context information that can be obtained through diverse sensors.

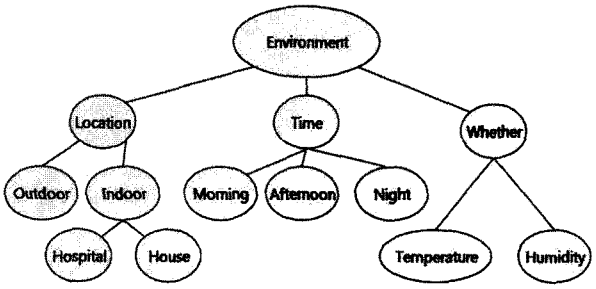

그림 2. 환경 상황 정보의 예
Fig. 2. Example of the Environment Context.

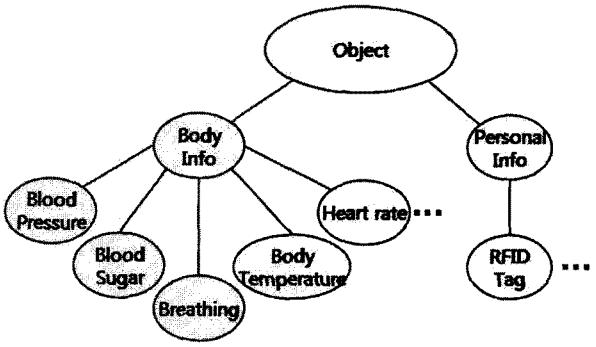

그림 3. 대상 상황 정보의 예
Fig. 3. Example of the Object Context.

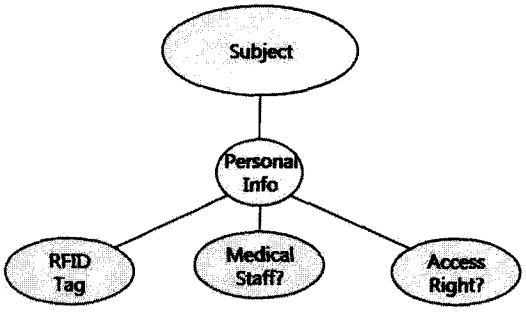

그림 4. 주체 상황 정보의 예
Fig. 4. Example of the Subject Context.

2. Context Aware Engine

Context aware engine is comprised of Fuzzy module and Utility module. Fuzzy module consists of FCM clustering module and Fuzzy Decision Tree module. And the Utility module consists of MAUT module and Simple Heuristics module. In the FCM clustering module, membership function is calculated according to the standard information for the environment that is the most appropriate for the patients depending on the level of importance. Calculated value of membership function is used to draw out the Fuzzy security level according to the environment information and information on the human body. Utility security level may be calculated by the function of MAUT and Simple Heuristics modules.

가. FCM clustering algorithm

Clustering is the technique for comparing the given data with the class that is already determined, and discerning it into the closest class, which is one of the key works in the pattern recognition, decision-making, data analysis, and so on. As the amount of information processed by computer becomes vast, intelligent system extracts information through learning, and requires adaptation function that handles similar context in an appropriate level, and this creates diverse neural network structure and learning algorithm.

Research on the neural network is the representative method that entails classification

[Stage 1] Number of clusters decision c ($2 \le c \le n$)
Index' weighted value m ($1<m<\infty$) selection
Initial membership functions initialization $U^{(0)}$
Frequency of algorithm repetitions.
Set as r ($r = 0, 1, 2, \ldots$)

[Stage 2] Calculate center of the Fuzzy cluster

$$\{v_i \mid i = 1,2,\cdots,c\}, \quad v_{ij} = \frac{\sum_{k=1}^{n} (u_{ik})^m x_{kj}}{\sum_{k=1}^{n} (u_{ik})^m}$$

[Stage 3] Calculate new membership function $U^{(r+1)}$

$$u_{ik}^{(r+1)} = \frac{1}{\sum_{j=1}^{c} \left(\frac{d_{ik}^r}{d_{jk}^r}\right)^{\frac{2}{m-1}}} \quad , \quad for\ I_k = \Phi, \quad or$$

$$u_{ik}^{(r+1)} = 0 \quad , \quad for\ all\ classes\ i, \quad i \in \overline{I_k}$$

$$I_k = \{i \mid 2 \le c < n;\ d_{ik}^{(r)} = 0\}, \quad \overline{I_k} = \{1,2,\cdots,c\} - I_k$$

$$\sum_{i \in I_k} u_{ik}^{(r+1)} = 1$$

[Stage 4] Calculate Formula Δ. If $\Delta > \varepsilon$, set as $r = r+1$, and repeat from [Stage 2], If$\Delta \le \varepsilon$, then end algorithm. (ε is critical value)

$$\Delta = \left\| U^{(r+1)} - U^{(r)} \right\| = \max_{i,k} \left| u_{ik}^{(r+1)} - u_{ik}^{(r)} \right|$$

그림 5. FCM 클러스터링 알고리즘
Fig. 5. FCM Clustering Algorithm.

through learning. FCM is one of the representative cluster analysis methods and it has been applied to the various applications, but it is still being assessed for astringency, optimization, and generalization[15].

Context-aware security service model using FCM clustering algorithm applies the result of the closest classification using the distance with the center of each classified cluster. Thus, it can draw out the most appropriate result for the unexpected context, which is not registered in the security policy. Figure 5 demonstrates FCM clustering algorithm[11].

나. Multivariate Fuzzy Decision Tree

Ultimately, the proposed model requires the most appropriate single security level. Accordingly, each security level drawn out from FCM clustering uses Multivariate Fuzzy Decision Tree to get an integrated single security level.

Decision tree is the method for extracting standard pattern from the data expressed as the value of specific attribute for the classification and the decision-making. As for the method for extracting standard pattern automatically, there are decision tree, neural network, probability based model, Genetic Algorithms technique, and so on. In decision tree, there is an advantage that the subject can understand the critical causes easily, and that it guarantees easy implementation.

However, while numerous data used in the real world might be given in the form of ambiguous status due to the surveillance error, uncertainty, subjective judgment and so forth, the decision tree could classify the similar two data into different classes due to its characteristics of exact value classification. Due to this issue, research on the fuzzy decision tree is underway which divides up the fuzzy boundary side defined by using membership function[13, 16].

In the proposed model, each sensor information that comprises the input data may have different level of importance depending on the sensor types. For example, when there are blood pressure and a number of heart beatings in the patients of high blood pressure's physical information, information on the blood pressure appears to be more important than the information on the heart beat. Accordingly, the proposed model uses the value that multiplies the weight factor to each security level drawn out through the FCM clustering as Fuzzy Decision Tree's input data.

[Stage 1] Calculate T-norm using membership function and attribute vector starting from the root node to the terminal node.

(1) Project input data x into the direction of each node's attribute vector w_i.

$$z_i = w_i^T x$$

(2) Calculate T-norm up to the n-th terminal node starting from the root node.

$$T_n = \prod_{i=\sqrt{node}}^{n_{th} \le af\ node} \mu^i_{S_{i|\alpha}}(z_i)$$

When the above mentioned process is repeated for all terminal nodes, each terminal node may have T-norm between 0 to 1.

[Stage 2] Calculate average of T-norm of terminal nodes that apply to each class among the terminal nodes, and classify the input data with the largest average value.

A_i : Average of the T-norm of the terminal nodes that have *i-th* class

$$class\ C = arg_i\ max\ A_i$$

그림 6. MFDT를 이용한 분류 프로세스
Fig. 6. Classification Process using MFDT.

Because the proposed model uses information on the diverse sensors, input data extracted from the FCM clustering may be applied as diverse variables as well. Therefore, this model uses the Multivariate Fuzzy Decision Tree (Multivariate Fuzzy Decision Tree: MFDT)[10] that applied the multivariate concept to the fuzzy decision tree to draw out the final security level. Figure 6 demonstrates classification process using MFDT.

다. *Utility Module Algorithm*

The overall algorithms of the Utility Module for determining adaptive security level are shown in Table 1 to Table 5.

표 1. 접근 제어 알고리즘
Table 1. Access Control Algorithm.

```
AccessControl (AccessProblem)
// AccessProblem: Grant or deny access for the protected resources according to Access Policy(AP);
// Search Role that related Resource
search Role by using context about User's Request
// Determine Security Level using Security Policy(SP)
SL = SecurityLevel (securityProblem) ;
// Grant or deny access by calculating Role, AP, and SP.
calculate Role, AP, and SP by using Constraints, Role, AP, and SP;
if true return grant;
else return deny;
```

표 2. 보안 등급 알고리즘
Table 2. Security Level Algorithm.

```
SecurityLevel (securityProblem)
// Determining security level using Security Policy (constraint, utility function, user preference)
// Utilization of domain independent properties
calculate SL by I end;
   if SL = 0 then return; SL // No security system
// Utilization of domain dependent properties
// select a strategy between MAUT and S. Heuristics
if MAUT then SL= MAUT(X);
if Simple Heuristics then SL = TakeTheBest(X);
returnSL
end;
```

표 3. MAUT 알고리즘
Table 3. MAUT Algorithm.

```
MAUT (X) // Determine total utility function by the interaction
                // with the user according to MAUT
u(x1,x2,...,xn) = k1u1(x1)+k2u2(x2)+... +knun(xn)
        // ki: set of positive scaling constants for all i
        // xi: domain dependent variable, where
ui(x°i)=0,ui(x*i)=1
ask the user's preference and decide ki
for i = 1 to n        do ui(xi) = GetUtilFunction(xi);    end
return u(x1,x2,...xn) end
```

표 4. GetUtil 함수 알고리즘
Table 4. GetUtil Function Algorithm.

```
GetUtilFunction (xi)
// Determine utility function due to users' preferences
// xi is one of domain dependent variables
   uRiskProne : user is risk prone for xi // convex
   uRiskNeutral : user is risk neutral for xi // linear
   uRiskAverse : user is risk averse for xi //concave
   x: arbitrary chosen from xi
   h: arbitrary chosen amount
   <x+h, x-h> : lottery from x+h to x-h
// where the lottery (x*, p, x°) yields a p chance at x*
// and a (1-p) chance at xo
ask user to prefer <x+h, x-h> or x // interaction
if user prefer <x+h, x-h> then
   return uRiskProne;        // e.g. u = b(2^cx-1)
else if user prefer x then
   return uRiskAverse;       // e.g. u = blog2(x+1)
else
return uRiskNeutral;
end;// e.g. u = b
```

표 5. Take The Best 알고리즘
Table 5. Take The Best Algorithm.

```
TakeTheBest (u(x1,x2,,xn))
// Take the best, ignore the rest u(x1,x2,,xn): user's basic preferences
// if the most important preference is xi, then only xi
// is considered to calculate SL
// The other properties except xi are ignored
   u(x1,x2,,xn) is calculated by only considering xi
   SL is calculated by the value of u(x1,x2,..,xn)
return SL;
end;
```

3. Security Service Engine

Security service engine is comprised of certification module for the certification of the subject's identity and diverse data encryption/decryption module for maintaining the confidentiality of the information. In the data encryption/decryption module, symmetrical and asymmetrical keys support encryption/decryption module. In the certification module, diverse certification modules including simple ID/Password module and PKI (Public Key Infrastructure) module and DAA (Direct Anonymous Attestation)[17~18] module is supported. Appropriate security service is provided using this module according to the drawn out security level.

가. A. DAA(Direct Anonymous Attestation) Protocol

DAA is one of group signature scheme designed by TCG. DAA protect privacy for platform user. And DAA is signature scheme providing remote authentication of TPM hardware. DAA propose group signature based on group signature of Fiat-Shamir. But DAA delete open function for protecting privacy. Features of DAA are as follows[17~18].

1) DAA authorizes without TTP(Trusted Third Party)
2) It provides anonymous
3) It can find rogue TPM
4) It is safe in random oracle model using Strong RSA and Decisional Diffie Hellman Assumption.

DAA protocol constructs with TPM user, Issuer and Verifier. TPM user is person who needs

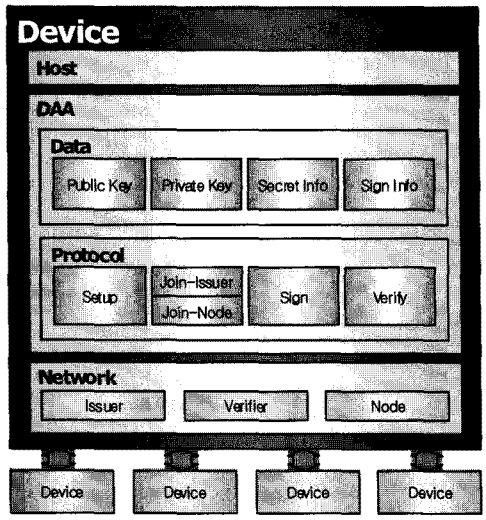

그림 7. DAA 모듈을 가진 단말기의 구조
Fig. 7. Structure of a Device with DAA module.

authentication. Issuer have function that issued certification. Verifier will check TPM users.

Each step is as follows.

1) *Setup* : Public key and Private key of Issuer are made by using Fiat-Shamir heuristics.
2) *Join* : TPM forwards the information of N_f type to DAA issuer. And it provides its own secret information(f) after verifying users' own secret data (f_0, F_1, v).
3) *Sign* : TPM signs message using certification and N_2f from verifier.
4) *Verify* : Check validate of the signature from DAA verifier.

We implemented software TPM version to test the features of TPM chip in the heterogeneous networks as shown in Figure 7.

4. Access Control Lists

The proposed system executes diverse security functions that are provided by the security service engine according to the final security level, and accesses the information depending on the access right provided by the ACL (Access Control Lists).

ACL provides the list of the access rights that can be accessed by the subject according to the security level drawn out through the access right

```
<ACL>
  <POLICY>
    <SECURITY_LEVEL>1</SECURITY_LEVEL>
    <SUBJECT_LEVEL>1</SUBJECT_LEVEL>
    <OPERATION>Read</OPERATION>
    <LIST>
      <INFORMATION>Blood Pressure</INFORMATION>
      <INFORMATION>Heart Rate</INFORMATION>
      <INFORMATION>History of a Patient</INFORMATION>
      <INFORMATION>Clinical History</INFORMATION>
      <INFORMATION>Case History</INFORMATION>
      <INFORMATION>Special Attention</INFORMATION>
    </LIST>
  </POLICY>

  <POLICY>
    <SECURITY_LEVEL>1</SECURITY_LEVEL>
    <SUBJECT_LEVEL>1</SUBJECT_LEVEL>
    <OPERATION>Read</OPERATION>
    <LIST>
      <INFORMATION>Blood Pressure</INFORMATION>
      <INFORMATION>Heart Rate</INFORMATION>
      <INFORMATION>Case History</INFORMATION>
      <INFORMATION>Special Attention</INFORMATION>
    </LIST>
  </POLICY>
</ACL>
```

그림 8. 접근 제어 목록 (ACL)의 예
Fig. 8. Example of the access control list.

```
function ContextAwareSecurityService(){
  x = count of sensor class;
  set sensor_weight[x];
  data[x] = inputMethod(); // input sensor information
  sl[x] = FCM(data[x]);
  for(i=0;i<x;i++) sl[x] = sensor_weight[x] * sl[x];
  security_level = MFDT(sl[x]);
  executeSecurityService(security_level);
  adaptAccessControlList(security_level);
}
function FCM(data[x]){
  set count_cluster();
  set exp_weight();
  set membership_function();
  set count_repeat();
  while(i < x){  // execute up to the number of sensor types
    res[i] = getCenterOfCluster(data[x]);
    membership_function = getNewMembershipFunction(res[x]);
    if(delta <= e) break;
    else repeat++;
  }
  return res[x];
}
function MFDT(sl[x]){
  calculate Tnorm[x];
  Ai = sum(Tnorm[x])/x;
  class = arg(max(Ai));
}
.....
```

그림 9. 제안된 퍼지 모델 알고리즘
Fig. 9. Algorithm for the Proposed Fuzzy Model.

classification module. In general, role based access control techniques such as GRBAC are used, but the role based access control technique may not be able to maintain integrity due to the conflict of the access right under the diverse contexts.

In the proposed model, Context-Aware module is leveraged to conclude the single security level by virtue of the FCM clustering, MFDT algorithm, and MAUT utility module. Thus, this conflict of access right does not occur. Figure 8 demonstrates the example of the access control lists. Figure 9 shows algorithm for the proposed Fuzzy model.

IV. Implementation and Evaluation

To identify the learning effect and the performance of the proposed model, we implemented the proposed one by using JDK5.0 on the IBM compatible PC with the Intel Pentium-IV 3.0GHz CPU and 1GB Ram. We used UBee430/UBee430-AP-Kit as for the sensor equipment based on the TinyOS 2.x to input context information.

As for the experiment, 300 virtual data pertaining to the variations in the high blood pressure of the patients were used to execute clustering. After clustering was completed, we have checked the variation on the security level according to the changes in the input blood pressures. Moreover, we try to compare the result from GRBAC model and that of FCM clustering model. Table 6 demonstrates access right policy to apply to the GRBAC.

Security level is classified into five levels, and security service of lower level is applied when the level is lower. In the proposed model, security level is decided depending on the context faced by subject. When the current context faced by subject is poorer, lower level is granted. That is we provide full information in case of emergency context in order to protect the subject's life by modifying the level of

표 6. 다양한 상황정보에 대한 권한 정책
Table 6. Access right policy for diverse contexts.

Environment information		Work	Subject	Object of behavior	Blood pressure	Level
Time	Place					
All times	All locations	Information inquiry	Medical clinic	Patient information	156/100~	1
					155/99~151/98	2
					150/97~146/96	3
					145/95~141/94	4
					~140/93	5

표 7. 다양한 상황정보에 대한 권한 정책
Table 7. Access right policy for diverse contexts.

Blood pressure	GRBAC model	FCM model	Expected Level
152.5 / 98.8	2	3	3
155.6 / 97.8	Unknown	2	2
153.2 / 100.3	Unknown	3	3
151.8 / 99.8	2	3	3
167.7 / 109.5	1	1	1
157.3 / 105.3	1	2	2
120.8 / 82.5	5	4	5
141.5 / 87.4	Unknown	3	4
137.3 / 85.3	5	4	4

security to the minimum level. In other words, when the context faced by subject is relatively favorable, security service of high level that can impeccably protect personal information is provided. In case of emergency context, this means that the protection of the subject is critical above all.

Table 7 shows the calculations of the security level which were applied to GRBAC model and FCM clustering algorithm, respectively. In Table 7, the expected level is the level decided by the distance between the normal blood pressure and the measured blood pressure.

We can see that the system recognizes emergency when the blood pressure is 167.7 / 109 in Table 7, and decides that the security level is 1. Moreover, we can find that the system selects level 2 to level 3 when the blood pressure is relatively high, and applies level 4 to level 5 when the blood pressure is normal.

However, the system shows '*Unknown*' as the result of the security level by applying the GRBAC model when the blood pressures are 155.6 / 97.8, 153.2 / 100.3, and 141.5 / 87.4. This is the case in which patient's state of blood pressure is not classified normally. Instead, conditions are intersected with at least two conditions. If we set the authority policy of the GRBAC in more detail, then it is possible to calculate more appropriate security level. However it is nearly impossible to set an appropriate policy for each authority for all contexts in the real world. In addition, as the number of

classifications for the authority policy increases, it is expected to take much time to draw the results.

Unlike the GRBAC model, the FCM clustering applied model demonstrates the appropriate results for all contexts in general. That is because the FCM clustering applied model presents more appropriate level using the distance between each cluster's central value and the input vector after processing the autonomous clustering. As a result, compared to the GRBAC model that is based on the fixed rule sets, the proposed FCM clustering applied model can show more flexible and appropriate result.

Moreover, the proposed model executes context-awareness based on the diverse information that is input from the sensor network of the RFID/USN environment. Thus, the model uses the extensive sensing information such as blood pressure, heart rate, body temperature, temperature at the vicinity and humidity level to classifying each security level. Accordingly, we need to integrate all differently calculated security levels for the analysis of the diverse criteria. To do this, data from the result obtained through FCM clustering could be applied to the Fuzzy Decision Tree once again to draw out the result of the context aware for the diverse environments. Diverse information is integrated by generating Fuzzy Decision Tree, to select the most appropriate security level.

In case of the patients of high blood pressure, the most important one is the blood pressure information. But it is also significantly affected by the information such as heart rate, body temperature, temperature at the vicinity etc. Moreover, because the weight of each sensor information is different, the result from multiplying the weight value of the importance level by the result of the FCM clustering is the input value of the Fuzzy Decision Tree.

Table 8 demonstrates security level using FCM clustering and Fuzzy Decision Tree, where FCM clustering is applied as the input value of the Fuzzy Decision Tree. Table 8 shows how the change in the blood pressure and heart rate are applied to the Fuzzy Decision Tree and thus to calculate the final security level.

표 8. FCM 클러스터링과 FDT를 이용한 보안 등급
Table 8. Security level using FCM clustering and FDT.

Blood pressure	FCM Level	No. of heart beats	FCM Level	FDT Level
152.5 / 98.8	3	117	4	3
155.6 / 97.8	2	189	2	2
153.2 / 100.3	3	95	5	3
151.8 / 99.8	3	86	5	3
167.7 / 109.5	1	122	4	1
157.3 / 105.3	2	78	5	2
120.8 / 82.5	4	73	5	4
141.5 / 87.4	3	160	3	3
137.3 / 85.3	4	201	1	2

When the blood pressure is 137.3/85.3 in Table 8, security level by the change in blood pressure is level 4, but the security level by the change in the heart rate is calculated as level 1. Thus, level 2 is presented for the final security level. This shows that the patient's current blood pressure is normal, but that the possibility of blood pressure aggravating is factored into the blood pressure state due to the high heart rate. In other words, the proposed model is aware of the patients' context, and suggests the most appropriate security level.

When we compare the proposed model and the existing GRBAC based context-aware system, the results are as follows.

First, since FCM clustering is not based on fixed rule and uses autonomous clustering method, it could draw out appropriate classified results even for unexpected context.

Second, because it is possible to suggest appropriate security level without managing numerous rules directly, it is possible to solve the managerial overhead.

Third, since it can use the FDT with the weighting factor to integrate the results of classification for diverse contexts, it might apply the security level in the more realistic way.

Finally, we can adjust the Fuzzy Security Level by

표 9. 퍼지모델과 제안모델을 이용한 보안등급
Table 9. Security level using Fuzzy and Proposed model.

Blood pressure	No. of heart beats	Fuzzy Model	Fuzzy+MAUT Model		
			Prone	Averse	Neutral
152.5 / 98.8	117	3	3	2	3
155.6 / 97.8	189	2	3	2	2
153.2 / 100.3	95	3	3	2	2
151.8 / 99.8	86	3	3	2	3
167.7 / 109.5	122	1	1	1	1
157.3 / 105.3	78	2	2	2	2
120.8 / 82.5	73	4	5	3	3
141.5 / 87.4	160	3	4	2	3
137.3 / 85.3	201	2	3	2	2

표 10. GRBAC 모델과 제안 모델 비교
Table 10. GRBAC model vs. Proposed model.

Category	GRBAC model	Proposed model (Fuzzy + MAUT)
Autonomy	Aware of the context by using fixed rule input in advance	Aware of the context by using autonomous clustering and Fuzzy decision-making tree
Handling ability	Impossible to handle context that is not registered due to the fixed rules	Can handle unexpected context by using the distance with the center of cluster.
Ease of management	Overhead due to the direct management of rules and policies.	No need to manage rules and policies directly
Integration	Policy structure might be increasingly complex for the diverse contexts.	Integrates diverse contexts to suggest appropriate result due to the Fuzzy and MAUT

the help of MAUT and Simple Heuristics. Table 9 illustrates this comparison

In conclusion, Context-Aware Security Service system that uses FCM clustering algorithm and Fuzzy Decision Tree decreases the management overhead and provides the more appropriate security service for the various contexts including unexpected context. Table 10 illustrates the comparison between GRBAC model and the proposed model.

V. Conclusion and Further Research

This paper proposed the Context-Aware Security Service using Fuzzy algorithm and MAUT for the appropriate security service in the diverse contexts. We also demonstrate the case study for the patients who have high blood pressure.

When we compare the proposed model and the existing GRBAC based context-aware system, the results are as follows.

First, since FCM clustering is not based on fixed rule and uses autonomous clustering method, it could draw out appropriate classified results even for unexpected context.

Second, because it is possible to suggest appropriate security level without managing numerous rules directly, it is possible to solve the managerial overhead.

Third, since it can use the Fuzzy Decision Tree with the weighting factor to integrate the results of classification for diverse contexts, it might apply the security level in the more realistic way.

Finally, we can adjust the Fuzzy Security Level by the help of MAUT and Simple Heuristics.

As for the future the research, it is necessary to develop the system into the general system that can be applied to the general domains as well as to the security domain.

References

[1] M. J. Convington, et al., "Generalized Role-Based Access Control for Securing Future Applications," Proc of the 23th National Information Systems Security Conference, Baltimore, 2000, pp.115-125.

[2] M. J. Moyer and M. Ahamad, "Generalized Role- Based Access Control," Proc of IEEE International Conference on Distributed Computing Systems, 2001, pp.391-398.

[3] David F. Ferraiolo and D. Richard Kuhn, "Role-Based Access Controls," Proc of the 15th National Computer Security Conf, Baltimore MD, 1992, pp.554-563.

[4] Seung-Jwa Nam and Seog Park, "Context Conflicts of Role-Based Access Control in Ubiquitous Computing Environment," Journal of the Korea Institute of Information Security and Cryptology, 15(2), 2005, pp.37-52.

[5] R. S. Sandhu, et al., "Role-based Access Control Models," IEEE Computer, 29(2), February 1996, pp. 38-47.
[6] http://csrc.nist.gov/rbac/NIST.
[7] M. J. Convington, et al., "A Context-Aware Security Architecture for Emerging Applications," Proc of the 18th Annual Computer Security Applications Conferences, 2002, pp.249-258.
[8] Hyun-Soo Im et al., "The Model of Conflict Detection between Permission Assignment Constraints inRole-Based Access Control," Proc. of 2005 fall The Korea Society for Simulation Conference, 2005, pp.51-55.
[9] J. Bezdek, "A convergence theorem for the fuzzy ISODATA clustering algorithm," IEEE Trans. Pattern Anal. Machine Intelligence, PAMI2(1), 1980, pp.1-8.
[10] Moonjin Jeon et al., "Hand Gesture Recognition using Multivariate Fuzzy Decision Tree and User Adaptation," J. of Korea Robotics Society, 3(2), 2008, pp.81-90.
[11] Sung-Kwun Oh, Computational Intelligence by Programming focused on Fuzzy, Neural Networks, and Genetic Algorithms, Naeha Publishing Co., 2002.
[12] R.L.P Chang, T. Pavlidis, "Fuzzy Decision Tree Algorithms," Systems, Man and Cybernetics, IEEE Transactions, 7(1), 1977, pp.28-35.
[13] Woo-Hang Lee, Keon-Myung Lee, "Fuzzy Decision Tree Induction to Obliquely Partitioning a Feature Space," Journal of KIISE : software and applications, Vol.29, No.3, 2002, pp.156-166.
[14] Teuvo Kohonen, Self-Organizing Maps (3rd), Springer, 2001.
[15] Rhee Hyunsook, "An Adaptive Classification Model Using Incremental Training Fuzzy Neural Networks," Journal of Fuzzy Logic and Intelligent Systems, Vol.16, No.6, 2006, pp.736-741.
[16] Keon-Myung Lee, "Classification Rule Mining from Fuzzy Data based on Fuzzy Decision Tree," J. of KIISE : software and applications, 28(1), 2001, pp.64-72.
[17] E. Brickell, et al., "Direct Anonymous Attestation," In Proc of 11th ACM Conference on Computer and Communications Security, ACM Press, 2004 Practical Solutions to Identification and Signature Problems, ACPC 86, LNCS, 1987.
[18] TCG, TCG Specification Architecture Overview Specification Revision 1.3, 2007.
[19] R.L. Keeney and H. Raiffa, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, John Wiley & Sons, New York, NY, 1976.
[20] L. Martignon and U. Hoffrage, *Why Does One-Reason Decision Making Work? In Simple Heuristics That Make Us Smart*, Oxford University Press, New York, 1999, pp. 119-140.

저 자 소 개

양 석 환(정회원)

He received a B.S degree from Dong-Seo University in 2007 and received an M.S degree from Pukyong National University in 2009. He has interests in artificial intelligence and context-aware technology.

정 목 동(정회원)

He received a BS in computer engineering from Kyungpook National University, in 1981. And he received an MS and a Ph.D. in computer engineering from Seoul National University, in 1983, 1990, respectively. He was a professor at Pusan University of Foreign Studies from 1985 to 1996. And he has been a professor at Pukyong National University since 1996. His research interests are OOP technology, computer security for application, intelligent agent, and context aware computing. He is a member of KIISE, IEEK, KIPS, KIISC, and KMMS.