Safe Behaviors by Security Status Table (SST) in Urban Life

Hoon Ko[1], Carlos Ramos[2]

[1 2] *GECAD, Institute of Engineering Polytechnic of Porto, Portugal*

[1]

Abstract

Urban Computing (UrC) which is based on interaction involves all relations of users/space as computing target. That is, UrC can support better results by using user/space information than ubiquitous computing. However, user can't to be safety using without security processing. Although there are many security skills, it is difficult to adapt in dynamic changing of UrC. The most important factors of security are to use encrypt/decrypt algorithm / the number of round of encrypting and decrypting and key size. Encrypting algorithm / the number of round of encrypting and decrypting algorithm and key size has to be changed automatically for mobile devices. In this paper is for making Security Status Matrix (SSM) structure based on UrC as the first version.

1. Introduction

Urban Computing (UrC) usually provides computing environment to between users and space information. That mean users can use on each devices through organically processing of between user environment and space environment. There may be needed security work (authentication/authorization) during users moving. Because there are a lot of companies, which are developing their way security products, so, each company has their encryption algorithm and their key size (Of course, they are almost same). UrC composes many kinds of networks and users, various space information for user's purpose. Therefore, it is very important to arrange suitable information according to security asking. In this paper is for making Security Status Matrix (SSM) structure based on UrC. Section 2 briefly discusses the related work. There are the Urban Computing (UrC), Ambient Intelligence, context classification and some security issues. Section 3 presents our proposed Security Status Matrix (SSM), which describe user scenario, user cyber relationships, and Section 4 discuss our experiments and results include some analysis. At last, we put conclusion in section 5.

2. Related Work

2.1. Urban Life (UrL, include UrC)

Ubiquitous computing had presented in 1990's which involves various networks. It just allows the services only in local area and just provides services according to user request. It means that direction operating to user changes is almost impossible. However Urban Computing is logically on higher layer than ubiquitous computing. It provides organic user moving by users with reference from physical states information of devices. There are various devices and contexts from those devices in urban computing. If users want to get optimized selection with this kind of context, then users usually need to broadcast their information including their devices information and user asking to computing environment near the user. Because Ubiquitous computing only focus to support simple service for user location or fixed space, there is limitations, which use relevant information among space context, social context, time context of UrC has. For example, let's image we are in living room. If there is only family in there, they usually feel living room as rest space, however, if some people in there for public meeting, then that living room would be public space. That is, a space can keep difference context (meaning) or same context (meaning) according to their purpose. UrC provides optimized services to user asking and to resources asking in space with considering of social relation of various user groups, which has multiple-meaning in same space. Surely, securities factors also have to be changed depend on attributes of each location / space. However, because ubiquitous computing just is considering simple context, it cannot solve those asking for global space like urban space.

2.2. Ambient Intelligence

The concept of Ambient Intelligence (AmI), introduced in 2001 by ISTAG (European Commission's IST Advisory Group), who refers to a digital environment that proactively. However, sensibly, assists people in their daily lives [1], is also getting mature mainly because of the overlapping of this concept with others very know and studied topics namely Ubiquitous Computing, Pervasive Computing, Context Awareness, Embedded Systems and Artificial Intelligence techniques[1][2]. We can find examples of Ambient Intelligent (AmI) applications in several environments: smart homes, smart offices, intelligent meeting rooms, ambient healthcare, smart classrooms [2]. These "intelligent" or "smart" environments and systems interact with human beings in a helpful, seamless, adaptive, active, unobtrusive and often invisible way [2]. However mainly in the context of work or education many times this unobtrusive/automation access to the Environment devices must have security concerns like Authentication and Authorization with restrictions for devices and time windows to certain users. However the systems should not lose the capabilities of context aware features such as flexibility of adapt to changes over the time [3][4], in e.g. the task of dynamically add/remove devices and at the same time enable the security policy to those new devices. So being the following study intends to identify security studies in order to understand how we can maintain the philosophy of AmI and context aware and at the same time enable the security on such environments.

2.3. Context Classification

There are variously occurred contexts in UrC. To analysis some situation we have to understand each context. The contexts can be not only literal making, special words, and some sentences, but also circumstance, background, and configuration etc. At that same time, we technically define context are partiality, approximation, and perspective. Some definition according to special study is to be Table 1.

Linguistics and Context

The context defined speaking, changing of interpretation, dialog, and presentation depend on context focusing, structures and decision by listener to express all kind of messages by linguistics researcher. In this Linguistics and context, Fetzr [11], Bunt [12] and Connolly [13] defined contexts in linguistics viewpoint. Firstly, the context by Fetzr has three systems, objects, socials, and themes. And, Bunt who defined these contexts is to be among linguistic, semantic, physical, social and cognitive. And lastly, Connolly classified context as relationship between linguistic context and nonlinguistic context.

Table 1. Classification of Contexts

Major	Researcher	Definition for context
Linguistics	Fetzr (1997)	Object, Social, Subject
	Bunt (1997)	Linguistic, semantic, physical, social, cognitive
	Connolly(2001)	Linguistic context, nonlinguistic
Computer Science	Coutaz / Rey	Application, User, Interesting
Psychology	Ziemake(1997)	External context, Internal context

Psychology and Context

The context by psychology was expressed if various recognitions expresses into some kind of aspects of context, ex., sensory perceptions, languages, interpretations, inferences, decisions, problem solving, leanings, memories etc. Therefore, they define that the context is a special characteristic by nature or by effect of the outside. Ziemake [13] had defined context is just as an internal context to internal knowledge and mechanism by external context and human recognition processing involved human circumstances.

Computer Science and Context

This context defined by computer science has more cleaned definition than linguistic and psychology. They had classified an application, a user, an interest the context with computer science views. The application defined the relationship between physical and social in computer devices, user environment factors, circumstance decision state set, etc, then a user sets a user purpose, a task intention, information state of user physical and social to history and sensibility, what do they want to, what do they do etc. An interest essence defined context is contents / material / matter for application / user / device. This item includes the relation between times and user location.

3. Security Status Matrix (SSM)

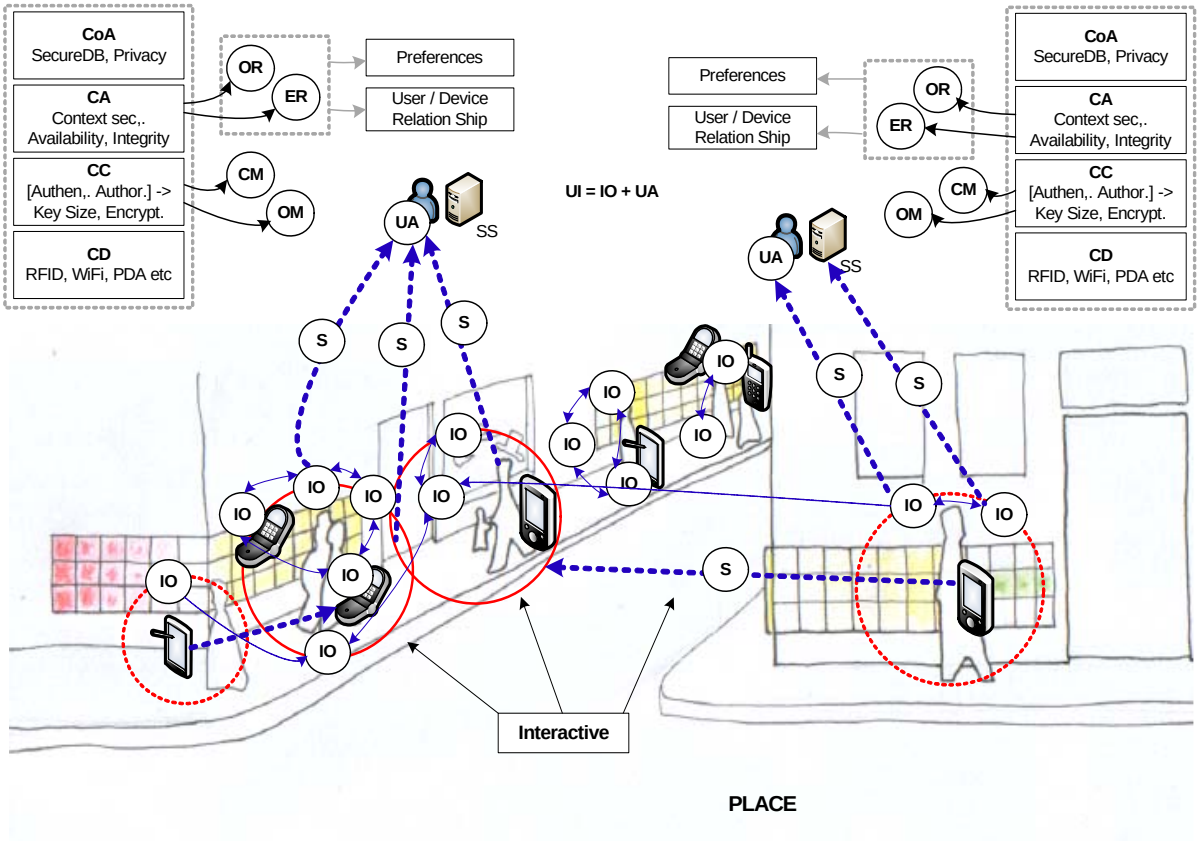

Figure 1. Relation among users (scenario, [3])

3.1. User Scenario

Figure 1 shows us the service steps to users moving. When user's devices enter in service area, they automatically begin to set with devices near users without any user's asking.

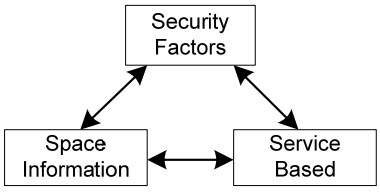

Figure 2. Three factors

There are three factors for proposed Security Status Matrix (SSM) in figure 2, named Security Factors (SF), Space Information (SI), and Service Based (SB). SF defines security factors, which should be processed according to user's location / user's purpose. SI defines the meaning of place for user's purpose.

At last, SB defines the services for place context. Firstly, to set security is the most important. Although, users in the same place may get difference services according to their purpose on UrC. For example, User A want to be there for shopping, User A has to receive some products from shopping center. User A has 'SF [6]' as 'SI [3]', the relevant is 'SB [4]' in figure 3. On the other hand, we suppose User B is a worker in that center, and then User B should get some ordering from their customers. User B has 'SF [2]' as 'SI [4]', the relevant is 'SB [8]' in figure 3. That is, although they are in same place, they get not same processing for why they are there/ what is purpose. Therefore, UrC system has to provide each security module. And, all users can have a service more than one.

3.2. User Social Relation

There may many kind of space information in real location in user's being. Moreover, there may get same service, same security factor, and same service from various users. User can share through same kind of factors like below example [Figure 4]. Security Factors

define EA (Encrypt Algorithm), KS (Key Size), and R (the number of Round).

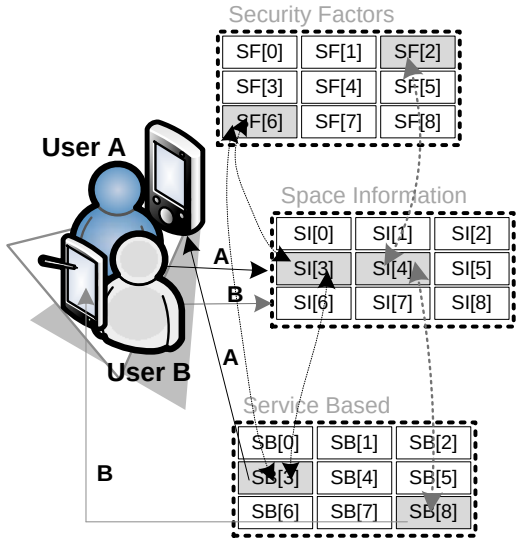

Figure 3. Service of User A and User B

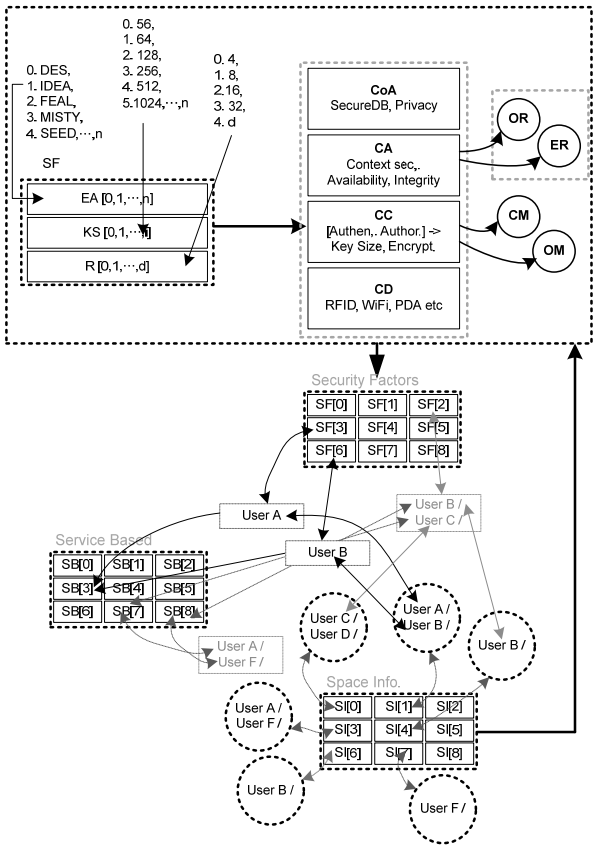

Figure 4. User Social Relation (not pointing fully)

Users, who have same service, can make social relation after reference service information (the purpose of service) of the located place of users. Also, they can share their information with their agreement. Therefore, User A shares 'SB [3]' with User B. However, User A and User B process with each way for security. 'SB [8]' will be shared User B and User F (see Table 2). The result of Table 2 is from figure 4. User A has two SBs; 'SB [3]' and 'SB [7]', each has difference space information for each service. We can define for User A like that, *[User A: SB[3], SI[1], SF[3].0.1.2: SB[7], SI[0], SF[1].1.2.2]*. User A keeps 'SI [1]', then receives the service 'SB [3]' in area of User A. Also, User A takes a service 'SB [4]'. At that time, the security set encrypt algorithm is DES (0), Key size is 64 bits (1), and the number of round is 16 (2). Therefore security factors, SF [#] is (0,1,2). We can understand the rest of them (SF[1].1.2.2) with the same way (see Table 2).

Table 2. Each Definition

Type / User	SB	SI	SF	
			Name	Matrix(Contents)
User A	SB[3]	SI[1]	SF[3]	0, 1, 2
	SB[7]	SI[0]	SF[1]	1, 2, 2
User B	SB[3]	SI[1]	SF[6]	4, 2, 1
	SB[5]	SI[2]	SF[6]	4, 2, 1
	SB[8]	SI[1]	SF[2]	2, 1, 3
User C	SB[7]	SI[0]	SI[0]	0, 0 ,0
User D	SB[6]	SI[3]	SI[0]	0, 0 ,0
User E	SB[0]	SI[3]	SI[3]	0, 2, 2
	SB[2]	SI[5]	SI[6]	4, 2, 1
User F	SB[6]	SI[3]	SI[2]	2, 1, 3
	SB[8]	SI[8]	SI[1]	1, 1 ,1

Also, UrC can dynamically compose the cyber society. Analyzing Table 2, cyber society can be organized by users, who has same configuration / same purpose according 'SB', 'SI', and 'SF', the result are in Table 3. For example, who can get the cyber society by service based [6] are User D and User F.

Table 3. Society Composition

Type / Index	SB	SI	SF
[0]	User E	User A User C	User C User D
[1]	-	User A User B * 2 User F	User A User B User F
[2]	User E	User B User F	User F
[3]	User A User B	User E	User A User E
[4]	-	-	-
[5]	User B	-	-
[6]	User D User F	User E	User B * 2 User E
[7]	User A User C	-	-
[8]	User B User F	-	-

In other example, if we reference on Table 3, User A and User C are able to make a cyber society with 'SI [0]' and 'SB [7]'. And, considering 'SF', User A, User B and User F shares 'SF [1]', therefore they can organize a cyber society based on 'SF [1]'.

4. Discussion

4.1. User Profiling using Security Cost

Table 4 is a notation for experiment in this article.

Table 4. Notation (Reference [11] for simulation)

Symbol	Contents
SI	Space Information
SF	Security Factors
SB	Services
$U_{[1,2,3,....Un]}$	Users
ΔJ_{st}	The change from Time *t-1* to *t* in number of jobs in a area *s*
C_{st} or C	Total cost in area *s*
$J_{s(t-1)}$	Set of all jobs in area *s* in Time *t-1*
$F_{s(t-1)}$	Set of jobs in flux in area *s* in Time *t-1*
$CP_{[1,2,3,....CPn]}$	Contents Providers
T_i	Transmission Time (a:ask, r: reply)
P_j	Processing Time
W	Weight
R	Set of jobs

The time for taking a service in present location of user is defined as $User.profile.vector[U.pv] =< SI, SF, SB, CP_{[1,2,..,n]} >$. And we call the expression is as *user. profile*.

$$User.profile.vector[U.pv] =< SI, SF, SB, CP_{[1,2,..,n]} >$$

$$C(si) = T_{si} \cdot (w_{si} \cdot P_{si}) \quad \text{..... (1)}$$

$$C(sf) = T_{sf} \cdot (w_{sf} \cdot P_{sf}) \quad \text{..... (2)}$$

$$C(sb) = T_{sb} \cdot (w_{sb} \cdot P_{sb}) \quad \text{..... (3)}$$

$$C(cp_1) = \{T_{cp1.a} \cdot (w_{cp1} \cdot P_{cp1})\} + T_{cp1.r} \quad \text{..... (4)}$$

Basically, the cost, which be processed in user location, defines like (1) (2) (3), then it will be recognized to user location through processing of (1) (2) (3), and finally users get contents by (4). Variables in each expression are the number of CP, transmission time, the number of user's devices etc [Figure 5]. w_{si}, w_{sf}, w_{sb}, which was defined in each expressing get same value since using by same user. Also, T_{si}, T_{sf}, T_{sb} are able to definition same value for processing by same user and same device (5).

$$C(U) = [\sum_{i=1}^{T_n} f(T_i) + \sum_{j=1}^{P_n} f(P_j) \cdot w] + (\sum_{k=1}^{CP_n} f(CP_k)) \quad \text{..... (5)}$$

4.2. User Modelling

Figure 5 is the experimental model for one user. User has some digitals devices at that same time, each device can receive different contents and can ask to different CP. User usually can use a normal senor (Sensor can be involved each digital device or user can keep as integrated sensor). Generally the current system takes sensor' s task by sending the signal from each digital device of users. When each digital device sends the signal to CP, SF already defined in Table 1, which is security factor for each device, will be transferred in concurrent. And, each job dynamically can be generated and removed (destroyed).

$$\Delta J_{st} = C_{st} - \left| J_{s(t-1)} \right|, \quad \text{..... (6)}$$

We define notation (7) as the set (6) for all tasks. We are able to reference notation (7) with new generated task, or in working task [11].

$$J_{st} = \begin{cases} J_{s(t-1)} \cup F, & if \Delta J_{st} > 0, \\ J_{s(t-1)} & if \Delta J_{st} = 0, \\ J_{s(t-1)} - F_{st}, & if \Delta J_{st} < 0, \end{cases} \quad \text{..... (7)}$$

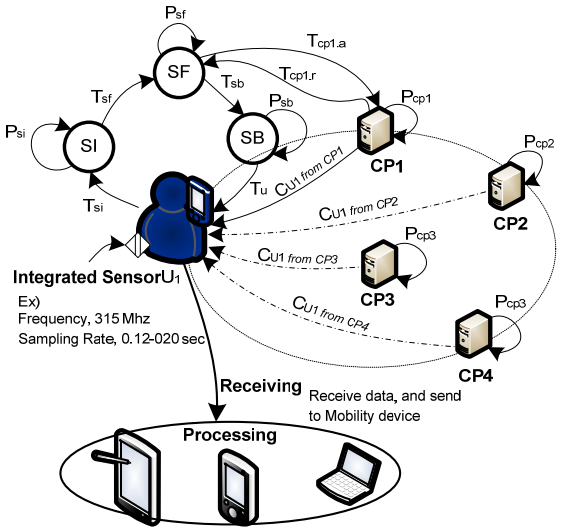

Figure 5. Experiment Model of U1

And, (8) and (9) are defined with processed job in only one device of user [11].

$$F_{s(t-1)} = \{ j \in J_{s(t-1)} \}, \ldots\ldots\ldots\ldots\ldots\ldots\ldots (8)$$

$$\left| F_{s(t-1)} \right| = \left| \Delta J_{ss} \right|, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (9)$$

If there be happened new task, ex, adding or removing, in that model [Figure 5], notation (9) would be changed in real time. However, notation (9) has no security module. Therefore, if we put security module into notation (9), then we get notation (10).

$$\left| F_{s(t-1)} \right| = \left| \Delta J_{ss} \times SF \right| \ldots\ldots\ldots\ldots\ldots\ldots\ldots (10)$$

4.3. Experiment

We took a simulation with MATLAB and set the configuration for experiment (Table 5). And we also set average 2.5 km through 3.5 km for user moving speed, two devices for one user. Each device has three services.

Table 5. Experiment definition

Definition	Value
Experiment Time	300 sec
The number of User	30
Walking Speed	2.5-3.5 km
The number of device a user	2
The number of service a device	3
The number of area in section	4

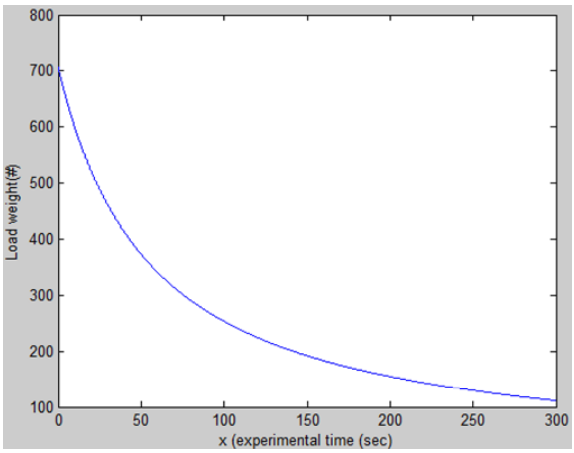

Figure 6. Load Weight of Notation (4)

We are not sure the security definition size, that is, a storing bucket size or key storing module for encryption module, therefore we assume that the size for one processing is 1k. When it begins first simulation, because it has to take a security process for 30 user's devices, approximately the load weight almost reaches 700. However, whenever time passed, the result was decreased step by step. I set all users quit to get service or get to be out of service area depending on time flowing for simulation. Figure 7 shows us the result of utilization. Slight increasing means the result of not taking security processing, sudden increasing means the processing with security. Before, we make an experiment, we set 100 for utilization and that value is to be not using security module.

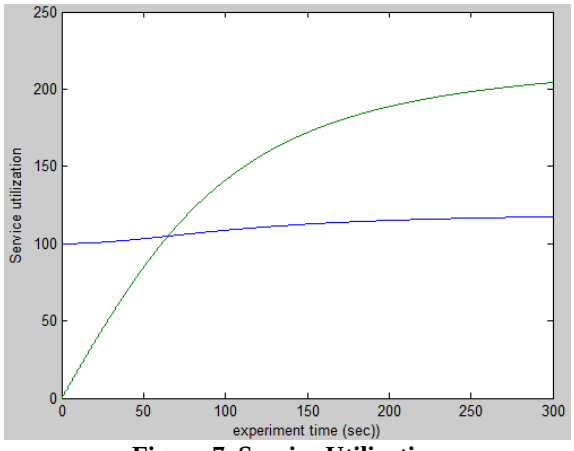

Figure 7. Service Utilization

The reason of rush increasing was for set to make a temporary society, who among users with common purpose, who has to get security processing for society

organization, during experimentation time. In addition, some of the reasons are kind of security factors changing, or real time reacts to context alteration by users changing, etc. All of that make an affection to service utilization.

4.4. Situation in Urban Life (in CSI NY S6, E2)

Scene #1

A driver drives toward his destination. Because it's the first time to visit, he uses GPS. However, GPS give him wrong direction information. (Originally, he is supposed to go Luxury Hotel in midtown.). After notice this strange situation, the driver urgently calls the service center. But, the voice from telephone is strange also, and the strange guy already knows the driver's name. The attacker who has strange voice had hijacked 911, and then he remotely let ring, turn on/off the driver's car. Certainly, the driver exactly put the destination's information to GPS. Nevertheless, he arrived the strange area where is dark and dangerous. Surely there is no problem in his computer, his GPS, and his Car. What happened?

How Attack?

CSI (Crime Scene Investigator) found out the wrong signals from GPS, who operated the GPS to control by attacker, through their analysis. Finally, the illegal operate made the wrong signal. Also, they knew some problem from one of BTS (Base Transceiver Station) before the driver's accident. Also, the attacker already let operate a micro-process beneath bonnet of the car. Finally, the recovery system in car found unauthorized signal. Then the attacker could control the car after using this signal.

Context Analysis

We put all kinds of contexts into Table 6 from Scene #1. As all authors see them, there are various contexts, ex., contexts of user devices, context of car, contexts of networks, contexts of street, context of destination, and all user contexts (see Table 6), around the driver. And they need to be protected among their relations from all attacks. Because the driver didn't process any security module for all contexts during his trip, the put into dangerous situation.

One of Solutions

We usually define Scene#1 is in Ambient Intelligence (AmI). AmI can apply all users take a reaction to dynamic changing in all situations without hesitation. Finally, in this case, all contexts will be recommended to use ISyRAmI SF for security.

Table 6. Context Classification

User	Application	Security
Car	**a.Dest_Car.#1**::=*[Speed:Car.Tem:Distance:Fuel:Remain.Time:]*	**Sec.Policy**::=[Car:Users:Devices:Road:Dest],
User / Devices	**a.Driving.#1** ::=*[User.D:User.Voice]* **a.Device.#1** ::=*[User.Info.#:Meeting.Time:…]*	**Car.Sec.#1**::= *[Auth.T:Author_T:Issued.Date:Key]*
Road	**a.Loc.#1** ::= *[GPS#:Dev.ID.#:Time:Brightness* **a.Traffic.#** ::=*[*	**Devices.Sec.#1**::= *[Auth.T:Author_T:Issued.Date:Key]*. **Devices.Sec.#..**::= *[Auth.T:Author_T:Issued.Date:Key]* **Devices.Sec.#n**::= *[Auth.T:Author_T:Issued.Date:Key] //Same with Users*
Destination	**a.Dest.#1**::=*[GPS#:Temperature:Latitude:Longitude:…]* **a.Dest.#2**::=*[d.name:d.Room#.d.R_conditions…]* **a.Dest.#3**::=*[users.info:..]*	**Road.Sec.#1**::= *[Auth.T:Author_T:Issued.Date:Key]*
Users .1,,,n	**a.User.#1**::=*[::::]* **a.User.#2**::=*[User.a:User.b:User.C…]*	**Destination.Sec.#1**::= *[Auth.T:Author_T:Issued.Date:Key]*

5. Conclusion

We studied how use this kind of context with safe by users and by user devices in urban environment. To use them in urban space, we also researched the security factors changing, that is, the way to react in real time against whenever context changing. Also, this character belongs to urban space. In this paper, we studied the react way for an authentication of real time services and for user with real-time including service changing, security factors changing. Those can by objects changing which is organized in urban environment, users object (user, user devices) etc, in future. As we see figure 6 and figure 7, there give some affection to utilization and load weight according to security processing. Above all, it is the most important to make a light security module or light security factors for users safe using. UrC offers more dynamic environment than Ubiquitous Computing. Therefore, In future, we need to study more to make light security module, for example, light encryption algorithm and light key size etc.

Acknowledgments

This work is partially supported by the Portuguese Foundation for Science and Technology (FCT) in the aims of Ciência 2007 program for the hiring of Post-PhD researchers.

References

[1] Carlos Ramos, Juan Carlos Augusto, and Daniel Shapiro, "Ambient intelligence the next step for artificial intelligence," *IEEE Intelligent Systems*, Vol. 23, No. 2, Nov. 2008, pp. 15–18.

[2] Carlos Ramos, "Ambient Intelligence – A State of the Art from Artificial Intelligence Perspective" in Progress in *Artificial Intelligence from Lecture Notes in Computer Science*, 2007, pp. 285-295.

[3] Karmen Franinovic and Yon Visell, "Modulating Urban Atmospheres: Opportunity, Flow, and Adaptation," *Urban Computing Conference, Metapolis and Urban Life Workshop Proceeding*, 2005, pp. 82-87.

[4] Mingchao Ma, "Authorization delegation for u-City in subscription-based," *Computers & Security*, 2006, pp. 371-378.

[5] IST Advisory Group, *Scenarios for Ambient Intelligence in 2010*, European Commission, 2001.

[6] Eiko Yoneki, "Evolution of Ubiquitous computing with Sensor Networks in Urban Environments," *Ubiquitous Computing Conference, Metapolis and Urban Life Workshop Proceedings*, September, 2005, pp. 56-59.

[7] Stephen J. H. Yang, "Context-Aware Ubiquitous Learning Environments for Peer-to-Peer Collaborative Learning," *Educational Technology & Society, Security*, 2006, pp. 188-201.

[8] David Hawking nad Paul Thomas, "Server Selection Methods in Hybrid Portal Search," *WSIGIR'05*, August 15-19, 2005, pp. 75-80.

[9] Andy Ward, Alan Jones, and Andy Hopper, "A new location technique for the active office," *IEEE Personal Communications*, Vol. 4, No. 5, 1997, pp. 42-47.

[10] Guanling Chen, and David Kotz, A Survey of Context-Aware Mobile Computing Research, Technical Report: TR2000-381 Dartmouth College, Hanover, NH, USA.

[11] Fetzer, A., "Recontextualizing context," *Proceedings of Context Organiser workshop*, April 9-11, Manchester, UK, 1997.

[12] Bunt, H., "Context and aialogue control," *Proceedings of CONTEXT97*, 1997.

[13] Connolly, J. H, "Context in the study of human languages and computer programming languages: A comparison," *Proceedings of CONTEXT2001*, Berlin Germany, 2001.

[14] Coutaz, J., & Rey, G, "Recovering foundations for a theory of contextors," *Presentation delivered at the 4th International Conference on Computer-Aided Design of User Interfaces*, May, Valenciennes, France, 2002.

[15] Ziemake, "Embodiment of context," *Proceedings of ECCS*. April 9–11, Manchester, UK, 1997.

[16] Hoon Ko and Carlos Ramos, "A Survey of Context Classification for Intelligent Systems Research for Ambient Intelligence," *Fourth International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing (IMIS2010)*, February 15–18, 2010, pp. 746-751, Krakow, Poland.

[17] Hoon Ko and Carlos Ramos, "A Study on Security Framework for Ambient Intelligent Environment (ISyRAmI SF: ISyRAmI Security Framework)," *ICWMC2009*, August 23–29, 2009, pp. 93-98, Cannes, France.

