Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Electronic Notes in Theoretical Computer Science 236 (2009) 47–64
Electronic Notes in Theoretical Computer Science
www.elsevier.com/locate/entcs

Design of Architectures for Proximity-aware Services: Experiments in Context-based Authentication with Subjective Logic

Gabriele Lenzini[1]

Telematica Instituut
7523 XC Enschede, The Netherlands

Abstract

This paper addresses the design of architectures for proximity-aware services with unobtrusive and context-based identification and authentication features. A service is "proximity-aware" when it automatically detects the presence of entities in its proximity. A process of authentication is "context-based" when it uses contextual information to discern among different identities and to evaluate whether they are authentic or not. We refer to an existing architecture, available in our institute, where a network of sensors is used to detect the presence users and user devices in various locations in the building. Proximity-aware services are offered at intelligent coffee corners where users are unobtrusively identified and authenticated while approaching. A level of authentication for an approaching identity is calculated as the overall expectation of belief (i.e., trust) that the identity (and not another) is effectively standing at the coffee space. We use the Subjective Logic as a theoretic framework for belief calculations. According to a previous study of ours, we manage each sensors as it was a recommender giving subjective "opinions" over statements concerning the position of users. Informally, an identity has higher level of authentication in a certain place the more sensors-recommenders believe that that identity stands in that place. We present and comment the results from an array of experiments where we show how trust can be used to authenticate an identity in a room. We perform the experiments under different circumstances, namely we change the area of the room and the relative disposition of the sensors. We comment the results and we indicate some guidelines for a design that aims to maximise its benefits from our authentication framework.

Keywords: design of proximity-aware applications, context-based authentication, subjective logic, trust and security

1 Introduction

A service is "proximity-aware" when it is available only to the users that approach the location where the service is offered. The presence of a user is detected by sensors such as, e.g., video cameras, infrared cameras, pressure mats, and counting doors. Actually, the services addressed by this paper are available only to certain users and not to others, or access to resources that are user dependent. For example, a proximity-aware service turns the local PC on with the scheduled presentation ready

[1] Email: Gabriele.Lenzini@telin.nl

doi:10.1016/j.entcs.2009.03.014

for use as soon the speaker enters the meeting room. For this reason, in addition to the presence of users, we have to *identify* who is approaching (e.g., is Alice or Bob approaching?). Some presence-detecting sensors, like video cameras, pressure mats, and so forth, are already able infer the identity of a user with a certain precision. Moreover, users can be identified thanks to portable objects, called *ID-tokens*, that are linked with users and that are assumed to be carried by users. Example of ID-tokens are portable devices (mobile phones, PDAs, laptops) and radio frequency identification (RFID) badges. Because presence-detecting sensors can be deceived (e.g., a picture of Bob can be put in front of a video camera) and ID-tokens might be forgotten, stolen, or used by entities which are not the owner, we also make use of a whole set of contextual information to verify the authenticity of an identity (e.g., is really Bob or is it someone else carrying Bob's mobile phone who tries to access the service?). We address the so called *context-based authentication* [2]. This paper focuses only on two specific types of contextual information, namely location and time.

Section 3 explains our approach in location-based authentication for proximity-aware applications. The basic idea is simple. A sensor can detect the presence of a user in fixed locations and recognise its identity with a certain degree of error; therefore the sensor can express a subjective "opinion" when questioned about statements regarding the position of the user. For example, a video camera recognizes (with a certain probability of error) Bob entering in the building, disbelieves (with the same probability of error) Bob sitting in the meeting room at the third floor. After few minutes, if the camera has not seen Bob exiting the building, the camera has less evidences to disbelieve that Bob is sitting in the meeting room. In fact, Bob might be everywhere in the building. If questioned, the camera can say that it is uncertain about the position of Bob (he might be in the meeting room, he might not). Therefore, a context-aware service can gather the opionions of all the sensors, can resolve possible contradictions, and can estimate the identity and the authenticity of an approaching identity. A few technicalities need to be arranged: how to mathematically define a sensor's opinion, how to calculate it, and how to merge different opinions. As algebra of opinions we use the Subjective Logic [9]. In Subjective Logic it is possible to model an opinion over the truth of an event in terms of belief, disbelief, and uncertainty. Other logic of belief for authentication, like the BAN logic [3], are not appropriate, as we look for quantitative analysis of belief (i.e., our beliefs, disbeliefs and uncertainties are real numbers). We have not investigated the use of fuzzy logic, but according to [14], a fuzzy logic approach is more appropriate for an "objective" analysis of belief, while in our set up we look for "subjective" (of the sensors) analysis of belief. Subjective Logic and its use in our approach are explained in Section 4 and Section 5 respectively.

Actually, sensors are not the autonomous agents able to have opinions as we described so far. To manage sensors, we use a proprietary *context-management framework* [5]. Hiding the technical features of sensors, the context-management framework provides service developers with an abstract (from technological aspects) vision of the sensor network. Section 2 describes the context-management frame-

work and its role in context-based authentication. Section 6 describes our experimental set-up. It illustrates and comments the results of the experiments that we have conducted to measure the reliability of our identification and authentication algorithm. Our test-case scenario has two identities, Bob and Alice, that move from one room to another. Section 7 comments some related work in context-aware authentication and location positioning systems. Section 8 concludes the paper addressing the future work.

2 The Context Management Framework

Our institute employs a hundred workers situated in two connected buildings. Each building has four floors, and the employees that work in different projects are spread (quite randomly) across different office locations. The building is equipped with a high density of sensors allowing for device discovery and human detection by using Bluetooth dongles, RFID readers, WLAN access point bindings, video cameras, and pressure mats. Most employees carry detectable devices (e.g., Bluetooth-enabled mobile phones, PDAs, and WLAN-enabled laptops). All employees also wear a RFID-enabled badge, which is needed to open the doors and to access different floors in the building. The sensor network and the detectable devices used by the employees constitute a rich infrastructure of context sources, which the researchers of our institute utilise for validating the design and for testing the implementation on presence-aware and context-based frameworks and applications. For example, the *Context Management Framework* (CMF) [5], developed the within the Dutch Project Freeband AWARENESS [2], is a software architecture designed to collect and manage raw data from a diversified collection of context sources. The CMF provides interoperability in distributed and context-aware environments: it processes and reasons with low-level information and it can provide context consumers (e.g., applications, distributed services) with a uniform, higher-level and higher-quality, context information. Developers are unloaded from the burden of managing multiple types of low-level sensors data (e.g., hardware signals). One of the application that benefits of the CMF is the *Colleague Radar*, which is offered at *intelligent coffee* places located in each floor of our building. Figure 1 shows how a coffee corner looks like, whilst Figure 2 depicts the user interface of the Colleague Radar application.

The CMF facilitates context-based authentication. In fact, the sensor network is a versatile source of information that can be used to understand the relationship between context (here locations of ID-tokens) and the identity of a user standing at any location of interest (e.g., at a coffee corner). In a wider scenario than that considered in this paper, also the appointments in the MS outlook agenda of users are part of the context [16].

The context-based authentication is a quantitative process. The ID-tokens detected in the coffee corner (e.g., Bob's mobile phone) indicate the (potential) presence of an identity (e.g., Bob). But the identity is considered authentic only with a certain probability (e.g., it could be that Charlie uses Bob's phone pretending to be

[2] http://www.freeband.nl

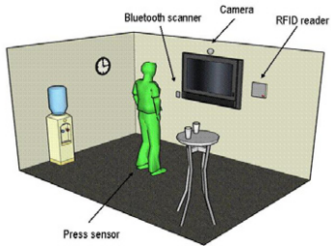


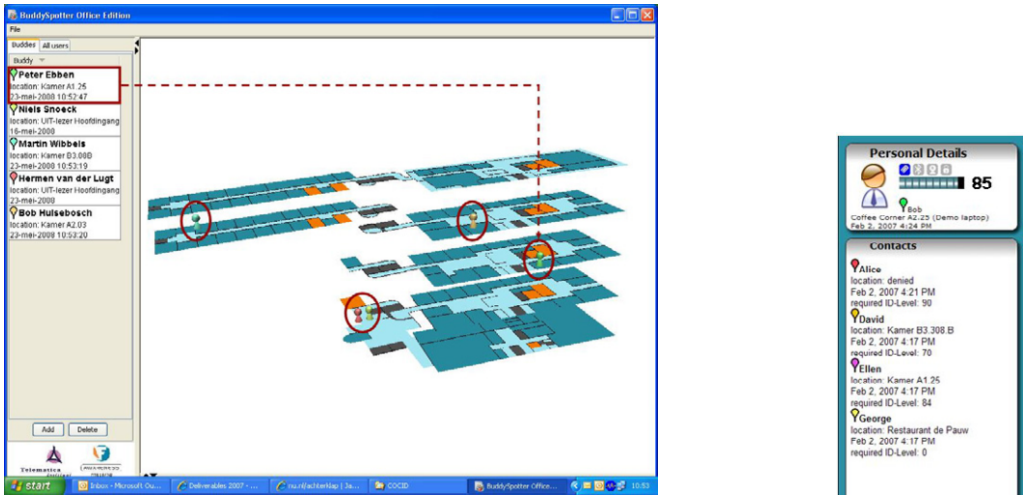
Fig. 1. A coffee corner. Sensors like RFID readers, Bluetooth dongles, and WiFi access points are able to detect the presence of ID-tokens like RFID-equipped badges, smart phones, laptops, and PDAs. Press mats and cameras can recognise the presence of users and, up to a certain probability of error, to deduce their identity.

Bob). The context information that emerges from the sensor network (provided by the CMF) is used to evaluate an overall *level of authentication* of an identity. The higher the level (a real number between 0 and 1), the higher the trustworthiness that the emerging identity is authentic. Because context information is collected continuously (at a certain collecting rate) authentication is a continuous process as well. This means that the user, once authenticated, remains authenticated unless the context changes. A context change occurs, for example, when the user (or one of its ID-token) leaves the space, or when a context datum related to him becomes invalid; for example, the location information detected by a RFID reader becomes old soon because a user can move away after having waved his badge in front the reader. Therefore, our system supports an automatic log-off, which is a desirable characteristic in context-aware authentication solutions (e.g., see [2]).

The design of our context-based authentication solution is not straightforward. First, we want to avoid the use of strongly confidential information like PIN, passwords, or credit cards numbers; coffee corners are social and public spaces and it is easy to eavesdrop personal secrets. Second, an explicit actions of authentication, like typing a PIN, are obtrusive, while we aim to an unobtrusive and seamless identification and authentication. Third, each sensor provides only a partial information, for example, that Bob's mobile phone (and not Bob) is in proximity of the coffee space. Sensors are also not 100% reliable due to their false positive and false negative error rates. Only a overall analysis of all sensors data can bring to a correct estimation of the authentication level.

Our proximity-aware application, the Colleague Radar, allows a coffee taker to visualise in a wall screen the location of his/her colleagues. Privacy policies control the visualisation of the position of an employee. Colleagues who have accepted to have their location traced, allows only specific users (e.g., Bob) to see their position. They can also demand that Bob's identity must be authenticated above a certain threshold before having their locational data disclosed: Alice wants to avoid that someone using Bob's mobile phone and pretending to be Bob can see her position. In a future version of the application, policies will allow Alice to hide her data also when Bob stands not alone at the coffee corner (i.e., when other colleagues accompany Bob).

The success of this kind of presence-aware applications strongly depends on reliability of the authentication methods that protect applications from misuses.



(a) (b)

Fig. 2. (a) A screen-shot of Colleagues Radar interface. The position of the colleagues (here highlighted with arrows and circles, which are not part of the interface) who have allowed Bob to trace them, is visualised onto a three dimensional model of the building. Some colleagues can ask Bob's identity to be certified with an high level as a condition to have their position shown. (b) A screen-shot that shows the authentication level for Bob (the small labels indicate the kind of context information used) and a list of polices with respect to Bob's authentication level. Here, for example, Alice requires Bob to be authenticated with level at least 90 before having her position shown. Being Bob's level 85, her location is not shown and labelled "denied".

The experiments conducted in the research scope of this paper give insights on some related questions.

3 Trust-enhanced Context-based Authentication

We define the level of authentication in terms of trust, namely, "expectation of belief that the authentic identity (and not other) is effectively in a given location". The main idea of a trust-enhanced authentication has been introduced and described in [13]. We use the Subjective Logic (see also Section 4) as an algebra of trust. Subjective Logic is a calculus compatible with the binary logic, probability calculus and classical probabilistic logic [8]. Probabilistic logics combine the capabilities of binary logic and probability to express degrees of trust of certain arguments. The Subjective Logic has the advantage of expressing uncertainty about the probability values themselves. Real situations can be more realistically modelled, and the conclusions reflect more the ignorance and uncertainty about the input arguments.

Our approach is related to the research in recommender networks. At a conceptual level sensors are seen as recommenders. When a sensor is asked for an opinion (about a certain statement to be true) it answers giving a value that expresses the amount of trust it has on the statement to be true from its point of view, that is, from what it has sensed in the environment. The overall evaluation on the belief in the truth of the statement is obtained by merging the opinions of the available sensors.

Considering a sensor as a recommender is an abstraction. The real sensors are

passive objects and mostly without intelligent capabilities. In fact, it is the CMF that collects sensors data over time and calculates opinions on the sensors behalf. The CMF knows the technical features of the sensors and it has access to their logged data. In the following, we stick to considering our sensors as autonomous recommenders, but the reader must be aware that this useful interpretation in indeed justified by the existence of our CMF.

What is the advantage of considering sensors as recommenders? The vision of sensors as recommenders provides a highly scalable approach to the design of sensor fusion algorithms. A new kind of sensor can be easily introduced in the architecture whenever we are able to provide a component that calculates an opinion on behalf of the sensor. The algorithm that merges opinions does not need modification. The merging is linear in the number of opinions, then of sensors. Our solution outperforms previous works based on conditional probability whose fusing algorithm is exponential in the number of sensors [7]. Moreover, being the Subjective Logic used in the management of reputation network [10], we see the possibility of interesting extensions. For example, we might extend our framework with a reputation network of sensors. Thus, sensors' opinions can be discounted, or even discarded, depending upon the sensors' reputation in giving honest or accurate feedbacks. The details of such a design are left as future work.

Which kind of recommendation/opinion can give a sensor? A sensor can determine whether an identity becomes noticeable in the zone it controls or it does not. For example, a pressure mat can detect the presence of someone who weights as Bob. An WiFi access point can say that Bob's laptop is in range. A sensor can organise its knowledge to answer a question about Bob's position. For example, if the pressure mat staying in Bob's room detects the presence of Bob, the mat disbelieves that "Bob's is at the coffee corner and not in his room". This amount of disbelieve is affected by the false positive and the false negative probability of error of this specific mat. In summary, if u is an identity and $\ell, \ell', \cdots$ are a locations, each sensor can provide opinions about propositional formula constructed from simple propositions of form $u \in \ell$, $u \in \ell'$, etc.

The next sections describe our theoretical framework, define what a sensor's opinions is, and discuss how to process the opinions originating from the sensor network to obtain an overall authentication level.

4 Subjective Logic

This section reminds the basics of the Subjective Logic (SL). All the definitions are taken from [9,8]. A finite set Θ is called a *frame of discernment*, or simply a *frame*, when its elements are interpreted as possible answers to a certain question. A frame is an epistemic object and its elements are correct relative to a subjective knowledge of an entity, let say s. A *state* is an non-empty subset of elements in Θ. Given a frame of discernment Θ, a *belief mass assignment* in the subjective knowledge of s, is a function $m^s_\Theta : 2^\Theta \to [0,1]$ such that for each $x \in 2^\Theta$, $m^s_\Theta(x) \leq 1$, $m^s_\Theta(\emptyset) = 0$, and $\sum_{x \in 2^\Theta} m^s_\Theta(x) = 1$. Here, 2^Θ is the power-set of Θ. Thus $m^s_\Theta(p)$ expresses

the belief assigned to the state p according to s. It does not express any belief in sub-states of p in particular.

Definition 4.1 [SL Opinion] Given a frame of discernment Θ, a *SL opinion* on a state $p \in 2^\Theta$ is a quadruple $\omega_p = (b(p), d(p), u(p), a(p))$. The items $b(p)$, $d(p)$, and $u(p)$ are called *belief*, *disbelief*, and *uncertainty* respectively. They range over $[0, 1]$, and are such that $b(p) + d(p) + u(p) = 1$. Item $a(p)$ is called the *relative atomicity* and is a function from 2^Θ to $[0, 1]$ that satisfies $a(\emptyset) = 0$ and $\sum_{x \in 2^\Theta} a(p)(x) = 1$.

An SL opinion expresses the belief, the disbelief, and the uncertainty about a state p to be true in the subjective knowledge of s. The atomicity $a(p)$ models an *a priori* probability expectation before any evidence has been received. Given a belief mass assignment m^s_Θ, an SL opinion on p in the knowledge of s $\omega^s_p = (b(p), d(p), u(p), a(p)))$, is calculated as follows (x ranges over 2^Θ):

$$b(p) = \sum_{x \subseteq p} m^s_\Theta(x) \qquad d(p) = \sum_{x \cap p = \emptyset} m^s_\Theta(x) \qquad u(p) = \sum_{x \cap p \neq \emptyset, x \not\subseteq p} m^s_\Theta(x)$$

The choice of $a(p)$ is situational dependent. A common definition is $a(p)(x) = |p \cap x|/|x|$, where $|x|$ is the cardinality of set x. Given an opinion ω^s_p, the *probability of expectation* of p being true, $E(p)$, is calculated as $E(p) = b(p) + a(p)u(p)$. Note that the relative atomicity weights the effect of the uncertainty in the expectation of belief.

The Subjective Logic theory has both basic logic operators and some non-conventional operators for combining SL opinions. We use the following operators of the SL: *Bayesian consensus* ($\oplus$), the *negation* ($\neg$), and the *conjunction* ($\wedge$). The binary operator $\oplus$ is used to used to "merge" independent SL opinions on p. If ω^s_p and $\omega^{s'}_p$ are two SL opinions on p in the subjective viewpoint of the entities s and s' respectively, then $\omega^s_p \oplus \omega^{s'}_p$ is the SL opinion $\omega^{\{s,s'\}}_p$ of the imaginary entity $\{s, s'\}$; it reflects the SL opinions of s and s' both in a fair and equal way. If ω^s_p and $\omega^s_{p'}$ are two SL opinions of the same entity s on p and p' respectively, then $\neg\omega^s_p$ is the SL opinion $\omega^s_{\neg p}$ that s has over $\neg p$ and $\omega^s_p \wedge \omega^s_{p'}$ is the SL opinion $\omega^s_{p \wedge p'}$ that s has on $p \wedge p'$. Another SL operator mentioned in this paper, is the binary operator $\otimes$, which is used to discount an opinion a depending upon the (referral) trust of its source, and the *average consensus* [12], which is used to merge the opinions of dependent sources. All the SL operators are described in [8].

5 Building SL Opinions from Sensor

This section explains how to calculate a sensor's SL opinion. It extends an idea first introduced in [13], where we showed how to build opinions on simple statement like "Bob is in the conference room". In this paper, sensors can give opinions on composite statements like "Bob is in the conference room *and* not in his office". Let $\mathcal{L}$ be the space of all locations. We call "cell" the portion of $\mathcal{L}$ controlled by a sensor. With $\ell_1, \ldots, \ell_n$ we indicate the (not necessarily disjoint) cells controlled by the independent sensors $s_1, \ldots, s_n$, respectively. When a sensor s_i detects an

ID-token related to the identity u (written $s_i(u) = 1$), s_i "believes" $u \in \ell_i$ with probability $P(u \in \ell_i \,|\, s_i(u) = 1)$. The exact location of u within a cell is unknown. It can occupy any position inside the cell with the same probability. When s_i does not detect u (written $s_i(u) = 0$), u can stay anywhere outside ℓ_i (i.e., $u \notin \ell_i$ or equivalently $u \in \mathcal{L} \backslash \ell_i$) with probability $P(u \notin \ell_i \,|\, s_i(u) = 0)$. Probabilities $P(u \notin \ell_i \,|\, s_i(u) = 0)$ and $P(u \in \ell_i \,|\, s_i(u) = 1)$ are calculated by applying the Bayesian theorem to the sensors' false positive and false negative error technical specifications [13]; the sensors are assumed conditional independent. Whenever the sensor s_i is asked for an SL opinion about the statement $u \in \ell$, a frame Θ_i can be defined over the (mutually disjoint) propositions identified by the zones intercepted, over $\mathcal{L}$, by ℓ_i (controlled by the sensor) and by ℓ The frame is defined as follows (we use $p(x)$ as a shortcut for $u \in x$):

$$\Theta_i = \{p(\ell_i \cap \ell), p(\ell_i \setminus \ell), p(\ell \setminus \ell_i), p(\mathcal{L} \setminus (\ell_i \cup \ell))\}$$

According to the knowledge of s_i and dependent to whether its has or has not detected u at the time t, s_i associates the belief masses $m_{\Theta_i}^{s_i(u)=1}(x)$ or $m_{\Theta_i}^{s_i(u)=0}(x)$, respectively, to the frame Θ_i. These masses are defined as follows:

$$m_{\Theta_i}^{s_i=1}(x) = \begin{cases} P(u \in \ell_i \,|\, s_i(u) = 1), \\ \text{if } x = \{p(\ell_i \backslash \ell), p(\ell_i \cap \ell)\} \\ 1 - P(u \in \ell_i \,|\, s_i(u) = 1), \\ \text{if } x = \{p(\ell \backslash \ell_i), p(\mathcal{L} \backslash (\ell_i \cup \ell))\} \\ 0, \qquad \text{otherwise} \end{cases} \quad m_{\Theta_i}^{s_i=0}(x) = \begin{cases} 1 - P(u \notin \ell_i \,|\, s_i = 0), \\ \text{if } x = \{p(\ell_i \backslash \ell), p(\ell_i \cap \ell)\} \\ P(u \notin \ell_i \,|\, s_i(u) = 0), \\ \text{if } x = \{p(\ell \backslash \ell_i), p(\mathcal{L} \backslash (\ell_i \cup \ell))\} \\ 0, \qquad \text{otherwise} \end{cases}$$

These believe masses represent the knowledge, local to s_i, about the truth of the statements that compose Θ_i. The SL opinion $\omega_{p(\ell)}^{s_i}$ that s_i has in the proposition $p(\ell)$ is calculated according to Definition 4.1. (Here we assume, with a little abuse of notation, that $p(\ell) \subseteq p(\ell')$ iff $\ell \subseteq \ell'$, $p(\ell) \cap p(\ell') = \emptyset$ iff $\ell \cap \ell' = \emptyset$). Figure 3 summarises, in picture, the rational underneath the construction of $\omega_{p(\ell)}^{s_i}$. For example, let us consider the case $\ell_i \cap \ell = \emptyset$ when s_i detects u. In Figure 3 it corresponds to the second square from the left. The sensor has no reason to belief that $u \in \ell$. On the contrary, the sensor has evidence to disbelief that $u \in \ell$ because, according to its knowledge, $u \in \ell_i$, and $\ell_i \cap \ell = \emptyset$. The amount of s_i's disbelief is the probability, $P = P(u \in \ell_i | s_i = 1)$, that $u \in \ell_i$ given that s_i has triggered correctly. The sensor has also an amount of uncertainty, which depends on the probability, $1 - P = P(u \notin \ell_i | s_i = 1)$, that s_i is misbehaving. This latter is a typical case in which uncertainty comes in play; in fact, according to SL, uncertainty arises where there are evidences neither to believe nor to disbelieve. The relative atomicity (not shown in the picture but reported in Algorithm 1) is calculated to weight the impact of this uncertainty in the expectation of belief; in the case we are describing, it depends on the ratio between the size of ℓ and the size of the complement of ℓ_i (i.e., on the probability that the user, not being in ℓ_i is incidentally in ℓ).

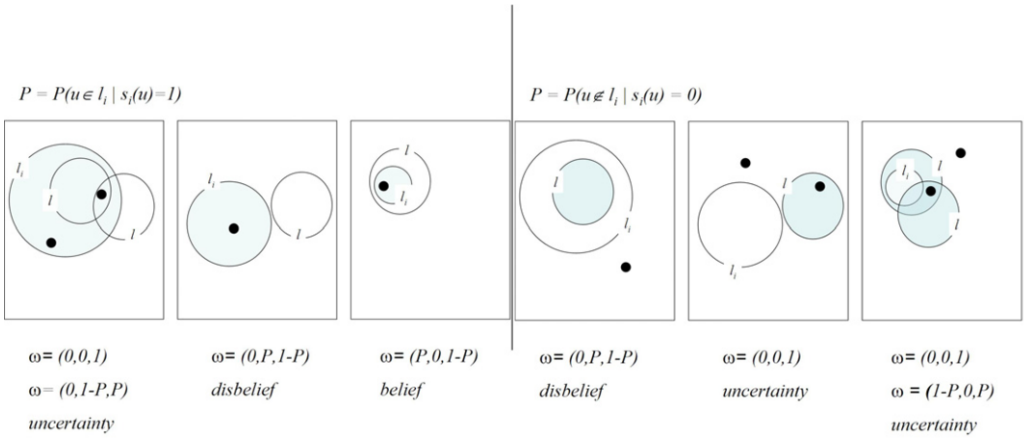


Fig. 3. Depending on the relative position between ℓ and ℓ_i we have different frames of discernment, belief masses and, consequently, SL opinions. On the left, the four cases (the first box on the left summarises two cases) that emerge when the sensor s_i detects the presence of u (u is the black dot) in the cell ℓ_i. A fifth case, omitted, happens when $\ell = \ell_i$. On the right, the four cases (the last box on the right summarises two cases) that occur when the sensor s_i does not detect u (u is the black dot) in the cell ℓ_i. A fifth case, omitted, happens when $\ell = \ell_i$.

There is an additional observation that is worth to be mentioned here. Because not all sensors scan their area at the same time, when s_i is consulted at time t, it may have not fresh observations. We allow s_i to look back at what it has collected at time $t' \leq t$, where t' is the time of the most recent observation. Here we require that the sensor's old observation is meaningful only if it is aged less than a certain t_0 (i.e., $\Delta t = t - t' < t_0$. Moreover, s_i considers that u may have moved during the time interval Δt and that u might be in the wider area $\ell_i + \Delta\ell_i$ at time t; so s_i "adapts" the relative atomicity of its opinion to the wider area. The cell increment $\Delta\ell_i$ is calculated according to a model of movement of user in the space $\mathcal{L}$ along the interval Δt. Note that $\Delta t = 0$ implies $\Delta\ell_i = 0$. Algorithm 1 gives the complete procedure for calculating $\omega^{s_i}_{p(\ell)}$.

An SL opinion $\omega^{s_i}_{p(\ell_1,\cdots,\ell_k)}$ over a propositional statement $p(\ell_1, \cdots, \ell_k)$ is calculated by asking for each single SL opinion $\omega^{s_i}_{\ell_j}$ for all j and later by applying the SL operators $\neg$ and $\wedge$. We remind that $\omega^s_{\neg p} = \neg\omega^s_p$ and $\omega^s_{p\wedge p'} = \omega^s_p \wedge \omega^s_{p'}$. The level of authenticity of an identity in a certain location ℓ is calculated from the SL opinions of all the available sensors in $S = \cup_i\{s_i | s_i$'s most recent data has age at most $t_0\}$. The SL opinions are merged with the $\oplus$ operator to obtain an overall $\omega = \omega^S_{p(\ell_1,\cdots,\ell_k)}$. Then we set the level of authentication to be the expectation of belief $E(\omega)$.

6 Experiments

We have organised our experimental set-up around four scenarios, numbered from 1 to 4. All the scenarios share a simple geometry, which consists of a certain number of sensors (each controlling a cell) and two spaces called, respectively, room 1 and room 2. Room 1 is the location of our proximity-aware application. Two identities, Bob and Alice, stay initially at room 1 and room 2, respectively. Figure 4 illustrates the four scenarios. In scenario 1, the rooms are bigger than the sensors' cells. In

Data: s_i and, at time t, a request for opinion on $p(\ell) = u \in \ell$
Result: An SL opinion $\omega^{s_i}_{p(l)}$
if $s_i(u) = 1$ *at time* t', *and* $t - t' < t_0$ **then**
  $P \leftarrow P(u \in \ell_i \,|\, s_i(u) = 1)$;
  $E \leftarrow P \cdot (\frac{|\ell \cap (\ell_i + \Delta\ell_i)|}{|(\ell_i + \Delta\ell_i)|}) + (1 - P) \cdot (\frac{|\ell \cap (\mathcal{L} \setminus (\ell_i + \Delta\ell_i))|}{|\mathcal{L} \setminus (\ell_i + \Delta\ell_i)|})$;
  if $\ell = (\ell_i + \Delta\ell_i)$ **then** $\omega^{s_i}_{p(\ell)} \leftarrow (P, 1 - P, 0, 0.5)$;
  if $\ell \subset (\ell_i + \Delta\ell_i)$ **then** $\omega^{s_i}_{p(\ell)} \leftarrow (0, 1 - P, P, \frac{E}{P})$;
  if $\ell \cap (\ell_i + \Delta\ell_i) = \emptyset$ **then** $\omega^{s_i}_{p(\ell)} \leftarrow (0, P, 1 - P, \frac{E}{P})$;
  if $\ell \supset (\ell_i + \Delta\ell_i)$ **then** $\omega^{s_i}_{p(\ell)} \leftarrow (P, 0, 1 - P, \frac{E-P}{1-P})$;
  if $\ell \cap (\ell_i + \Delta\ell_i) \neq \emptyset$ **then** $\omega^{s_i}_{p(\ell)} \leftarrow (0, 0, 1, E)$;
end
if $s_i(u) = 0$ *at time* t', *and* $t - t' < t_0$ **then**
  $P \leftarrow P(u \notin \ell_i \,|\, s_i(u) = 0)$;
  $E \leftarrow (1 - P) \cdot (\frac{|\ell \cap \ell_i|}{|\ell_i|}) + P \cdot (\frac{|\ell \cap (\mathcal{L} \setminus \ell_i|)}{(|\mathcal{L} \setminus \ell_i)|})$;
  if $\ell = \ell_i$ **then** $\omega^{s_i}_{p(\ell)} \leftarrow (1 - P, P, 0, 0.5)$;
  if $\ell \subset \ell_i$ **then** $\omega^{s_i}_{p(\ell)} \leftarrow (0, P, 1 - P, \frac{E}{1-P})$;
  if $\ell \cap \ell_i = \emptyset$ **then** $\omega^{s_i}_{p(\ell)} \leftarrow (0, 1 - P, P, \frac{E}{P})$;
  if $\ell \supset \ell_i$ **then** $\omega^{s_i}_{p(\ell)} \leftarrow (1 - P, 0, P, \frac{E-(1-P)}{P})$;
  if $\ell \cap \ell_i \neq \emptyset$ **then** $\omega^{s_i}_{p(\ell)} \leftarrow (0, 0, 1, E)$;
end

Algorithm 1: SL opinion for sensor s_i on $p(\ell)$

scenario 2, we increase the number of sensors from six to ten. In scenario 3, each room is smaller than a cell. In scenario 4, the rooms are closer and no sensor covers entirely and exactly a room. The sensors are assumed to be able to detect one type of device, let say a Bluetooth mobile phone. We assume that all the sensors have the same technical features, namely, the same frequency of scanning, and the same 1% of false positive and false negative rates. The algorithms for calculation, collection, and fusing of opinions are written in Objective Caml[3].

In each scenario we perform the following three experiments: (A) Bob and Alice move without exiting from the room they are; (B) Alice goes from room 2 to room 1; (C) Alice goes from room 2 to room 1 and back. Figure 5 illustrates, in reference to scenario 1, the three movement patterns. In the figure, the exact position of Alice and Bob is only sketched (for the details, see next subsection). Finally, we run the twelve experiments (1.A, 1.B, $\cdots$, 4.C) asking for opinions about the following statements: "what about Bob (resp. Alice) staying in room 1?", and "what Bob (resp. Alice) staying in room 1 and not in room 2?".

[3] http://caml.inria.fr

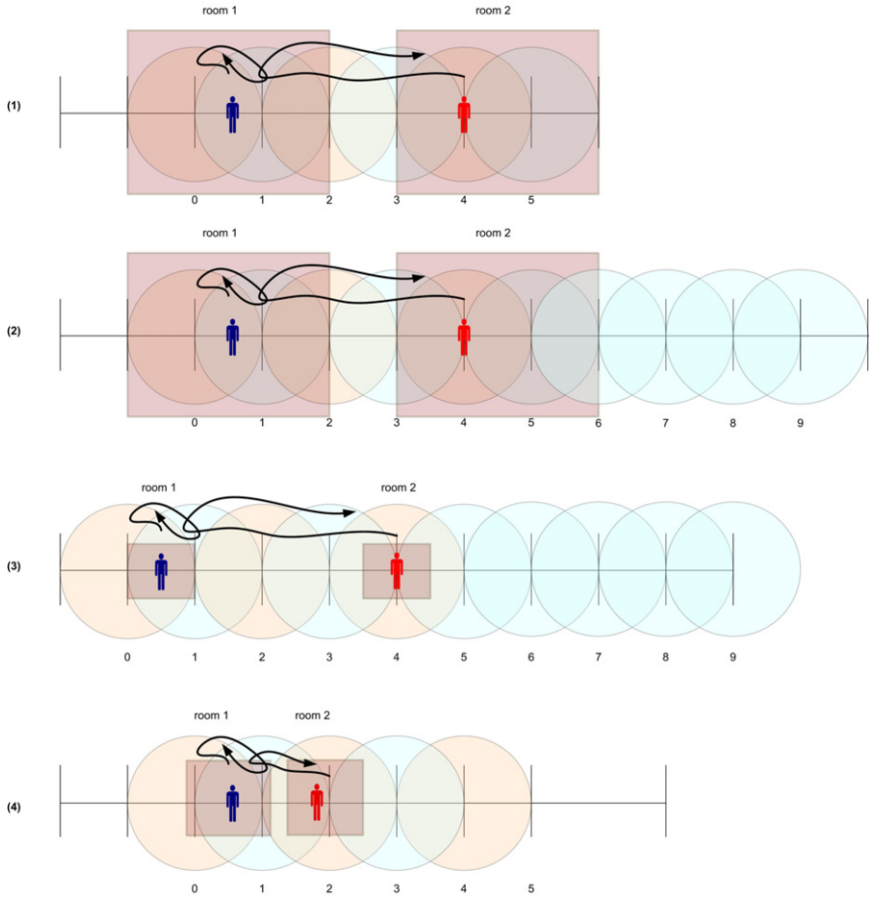


Fig. 4. A pictorial representation of the four scenarios. (1): the rooms are bigger than the cells. (2): as (1), but with more sensors. (3): the rooms are smaller than the cells. (4): as (3), but none of the cells include completely and solely one room.

6.1 Results and Comments

We comment the results of the forth experiments only, namely experiments 1.C, 2.C, 3.C and 4.C in Figure 4; these are the experiments conducted with the third movement pattern, which is the most general and includes the others. We comment only the outcomes related to the statement "Bob (resp. Alice) staying in room 1 and not in room 2" (Figure 6). The outcomes obtained with this statement are substantially the same as those we had with the statement "Bob (resp. Alice) staying in room 1".

From Figure 6 it is clearly evident that, in all the experiments, Bob is (correctly) recognised in room 1 and Alice is (correctly) recognised in room 1 when she actually enters the room. This result implies that, if someone pretending to be Alice brings an Alice's ID-token (e.g., the Alice's Bluetooth mobile phone) in the room 1, only the sensors able to detect Bluetooth mobile phones recognise Alice as the identity staying in room 1. The sensors detecting other type of ID-tokens (e.g., a WiFi laptop) recognise Alice outside room 1, if actually Alice carries those tokens outside. Such a contradiction denotes a conflict. Conflicts can be detected by checking the

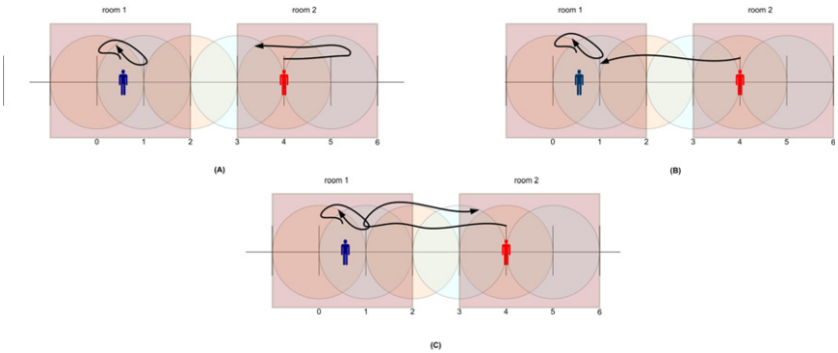


Fig. 5. A graphical representation of the three movement patterns (here illustrated in reference to the experiment 1). (A) Bob moves but stays in room1 and Alice moves but stays in room2; (B) Alice moves from room1 to room 2; (C) Alice moves from room1 to room2 and back.

coexistence of one SL opinion satisfying $b \geq d + u$ and another satisfying $d \geq b + u$. In case of conflict, to understand the real position of Alice, we need to consult a third type of sensor.

The outcomes of experiments 1.C and 2.C are identical. Experiment 2.C differs from 1.C because it has more sensors (sensors 6 to 9 in Figure 4 case (2)). When Bob or Alice are in room 1, these sensors do not have evidences either in favour or against the statement regarding the position of Bob and Alice. Their opinions do not bring meaningful information, because they have not detected any ID-token and most of them do not even intersect the location of interest. It follows that we can safely exclude from the list of useful recommenders. In the next paragraph we identify another reason which makes this exclusion even advisable.

The outcomes of experiments 3.C and 4.C are more critical. Despite correct, the maximal expectation does not go higher than 0.39. One explanation for such a low value resides in the size of room 1, smaller than the size of any sensor cell. The sensors that detect the Bob's ID-token (e.g., sensors 0 and 1, in Figure 4 case (3)) are uncertain about whether Bob is in room 1 or inside their controlled cell but not in room 1. Despite they can not disbelieve that Bob is in room 1 they cannot believe it either. This is consistent with what we expect from the Subjective Logic theory, where the conclusions more correctly reflect the ignorance and uncertainties about the input arguments [8].

Referring to experiment 3.C, a typical SL opinion given by sensors 0 and 1 is $(b = 0.01; d = 0.08; u = 0.92; a = 0.50)$. If no other sensor were taken into account, it would bring to an expectation of 0.46, the best value we can get from this disposition from rooms and cells. However, the nature of uncertainty of sensors 0 and 1 (Figure 4 case (3)) has a different nature from the uncertainty that emerges from the sensors that have *not* detected Bob's ID-token (i.e., sensors 2 to 9 in Figure 4 case (3)). The first set of sensors are uncertain about Bob being in room 1 or outside it, but they know he is within the boundary of their cell. The second set of sensors are uncertain about Bob's position at all, because Bob can be everywhere but not in their cell. A typical SL opinions that emerges from this second set of sensors is $(b = 0.01; d = 0.01; u = 0.98; a = 0.05)$. Note the relative atomicity's

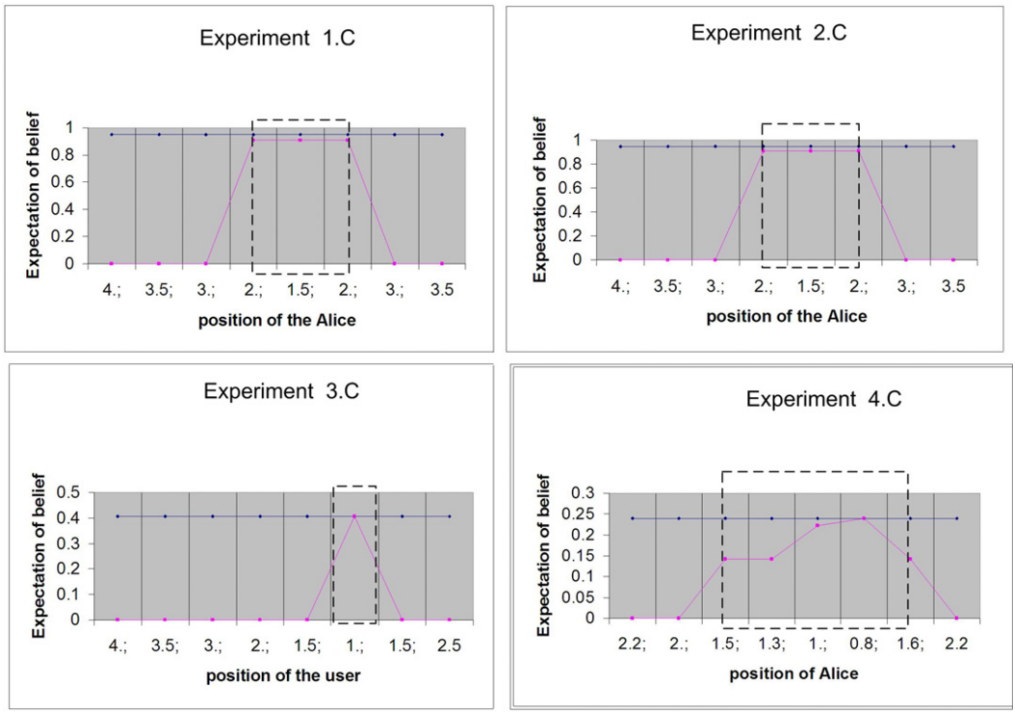


Fig. 6. Results from experiments 1.C, 2.C, 3.C and 4.C. In each graphic, on the x-coordinate stands the position of Alice along time, whilst on the y-coordinate stands the expectation of belief. The dark curve is the expectation of belief of Bob being in room 1 and not in room 2. The light curve, is Alice's. The dashed boxes indicate the boundaries of room 1 in each scenario.

value, which is very low. In experiment like 3.C, where all the sensors' opinions bring mostly uncertainty, this low relative atomicity in one of the opinion reduces significantly the relative atomicity in the merged opinion. Consequently, the overall expectation of belief, obtained with $E = b + au$, results low too.

A similar situation occurs in experiment 4.C. Here, the expectation of belief is even smaller. Again, the uncertainty is the main factor of evidence even for the sensors who detect the ID-token (sensors 0, 1, and 2 in Figure 4 case (4)). But here, even the relative atomicity in the SL opinion of the sensor 2 (considered a useful recommender) is small; in fact, the intersected area between room 1 and the cell controlled by sensor 2 is, in fact, minimal and the sensor "weights" its uncertainty in dependence on that small area. Two observations follow from experiments 3.C and 4.C.

First, when the cells are larger than the location of interest, the threshold for a positive authentication level must be around 0.45. There is no way of getting higher values. Moreover, the disposition of the sensor network must be carefully design so that to avoid sensor cells that intersect only very partially a space of interest (like sensor 2 in 4.C). In a real set-up, this means a time-consuming task in finding the right disposition of the sensors; in fact, sensor cells have not such a sharp geometry as we assumed in our scenarios and it is not easy to understand whether they intersect or not with the location of interest. For example, a Bluetooth dongle has usually a range of about 10mt with a grey zone, where ID-token may or may not

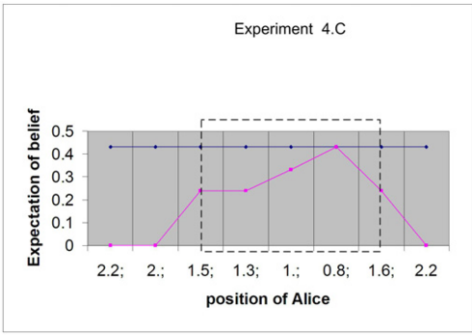


Fig. 7. The improved outcomes obtained from experiment 4.C when the sensors that do not detect the presence of an ID-token and that do not intersect with room 1 are averaged before being merged.

be detected depending on external factors like the density of people, the presence of metal shelves or metal objects, and the weather. A good news, in this context, is that with Bluetooth 2.1 dongles is it possible to tune the power of the signal and thus the sensors cells can be adjusted by sofware instead of by positioning the dongles.

Second, the information coming from sensors that have *not* detected any ID-token and that do not intersect with the area of interest cause an (excessive) low the expectation of belief. The SL opinions originating from these sensors should be either excluded or treated as "dependent" and merged with another operator called *average consensus* [12] before being merged (with the Bayesian consensus) with the others. This idea is promising as Figure 7 shows with respect to experiment 4.C: the overall authentication level is now close to 0.46, the maximum in this kind of scenario. We leave the task of performing more experiments in this directions as future work.

We are also considering to extend our framework with a reputation network of sensors. In this way, the opinions originating from sensors can be discounted, or even discarded, depending upon the reputation of the sensors in giving honest or accurate feedbacks. An algorithm that copes with sensors reputation can be easily obtained with the use of the discount operator of the Subjective Logic. The design of a sensors reputation management system and its integration in our CMF, instead, is left as future work.

7 Related Work

The research conducted in this paper is strictly related to what our group has been researching and implementing in term of CMF and context-aware authentication. The CMF has developed as part of the Dutch project Freeband AWARENESS. Its design is related to the research on ontologies done in the EU-project Amigo, and it was used in the ITEA-EU Trust4All to implement a context-aware trust evaluation demo. It will be used in EU-project INem4U to enhance the multi-media experience of users, which requires the use of special wearable sensors for in-situ measurement of social feelings during moment of sharing experiences between related users. The

latest version of the CMF is described in [5].

We started to investigate in context-aware authentication in [7], where the level of authentication was calculated in term of conditional probability. That approach was not scalable and the algorithm exponential in the number of sensors. The use of the Subjective Logic in our CMF was first studied in [13]. The present paper is the natural extension of that work, with a more stable algorithm and a simulation set-up which has allowed us to conduct an intensive series of different experiments.

The work presented in this paper is also related with the research in context-aware authentication. In [2], Bardram *et al.* have presented a complete overview of methods and principles for context-aware authentication in a pervasive computing environment (an Hospital), included a description of typical ID-tokens. They also introduce the concept of *proximity-based login* to indicate the automatic authentication of a user on a device by simply approaching it. The authors identify four key principles to be fulfilled in context-aware authentication: (a) a physical token must be used to active gesturing and to initiate a cryptographic basic authentication, (b) a context-awareness system is required to verify the location of the user, (c) a fall-back mechanism must allow to switch between authentication methods when one of them is not available and, (c) the automatic log-out must support users. Our solution complies with three of these principals, with the exception of the first one, because of our goal of achieving an unobtrusive authentication. Contextual information and different authentication mechanisms are managed at level of the CMF. Automatic log out happens naturally when the user leaves the space where the service is offered.

Our approach is also connected with studies on the prediction of the user position indoor. A survey, with a description of several types of algorithm used for location prediction can be found in [4]. We claim that the use of users behaviour as a fingerprint for identification is an emerging strategy in positioning users indoor. In this direction, [1] has proposed a neural network-based prediction of the position of mobile users from their habits and repeated behaviours as it is captured by a wireless network. Dedicated neural networks are used in the prediction after a learning phase on user's mobility profiles.

Finally, our work is related to the use of belief theories in sensor fusing. In one of the first work in this area, Wu *et al.* use Dempster-Shafer theory to fuse video data coming from independent sensors, which monitor the user's face, to deduce if the user is paying attention during a meeting [17]. The Subjective Logic approach improves the Dempster-Shafer approach as explained in [11]. Subjective Logic has been used in intrusion detection to fuse alerts coming from multiple detectors [15]. Alerts, which are opinions on different anomalies, are merged to calculate the expectation of belief that an attack has occurred. Alerts coming from not completely trusted sensors are discounted before being processed.

8 Conclusion and Future Work

We have described an architecture for proximity-aware services, and conducted and commented a series of experiments on context-based authentication with it. We have used a context management framework (CMF) to collect, arrange, and elaborate the contextual information that is processed to identify and authenticate users approaching a service. We assume a sensor network of RFID readers, WiFi access points, Bluetooth dongles, pressure mats, video camera, and similar sensors. Such a sensor network is actually available in our institute. Our CMF makes it possible to abstract from any technical features of the sensors, and to see each sensor as a recommender. When a proximity-aware application is in the need of identifying and of authenticating an approaching user (e.g., Bob), it asks the sensors-recommenders for their opinions about a location-related statement that sounds like "is Bob in proximity of the application and not in his office?". Each sensor composes a Subjective Logic opinion from what it subjectively has seen in the environment, then the opinions are merged using a Subjective Logic operator. The authentication level, expressed in term of the overall expectation of belief, is calculated from the overal opinion on the truth of the location-related statement.

Our experiments consist in calculating the authentication level of two identities, Bob and Alice, when they move back and forth between two specific locations. We set up a set of different scenarios, created by varying the number of cells controlled by the sensors and the disposition and the size of two location of interest.

The results of our experiments confirm what we were expecting from our context-based authentication solution: identities are correctly recognised and authenticated in a place, when they are actually in that place. The relative disposition of the sensors and the location where the proximity service is being offered have a visible impact on the maximal expectation of belief (a real number) we can obtain. This phenomenon is observed in most of our experiments. In words, if all the sensors intersect minimally with the location of the service, the opinions that those sensors can give on a user being in that location are mainly composed of uncertainty. Moreover, the use of opinions originating from the sensors that do not detect the presence of a user is critical. If not treated properly, the uncertainty brought by the opinions originating from those sensors can override the believes brought by the opinions of the sensors that, instead, have detected the user in the location of the service.

We have implemented our algorithm in the context management framework of our institute. A first run of tests has shown results that are consistent or identical to what we have obtained in the simplified experimental set-up described in this paper. We plan to integrate the implementation with our colleague radar application, and to have a demo where users are authenticated by using the theory presented in this paper.

We are also planning an extension of our approach where it is possible to ask opinion such as e.g., "Bob is moving from his office to the meeting place". This requires an extension of approach, reasonably by using a temporal extension of

Subjective Logic (cf. [6]) so that to cope with time-related trust relationship.

Acknowledgement

This research has been supported by the Dutch Freeband Communication Research Program (AWARENESS project) under contract BSIK 03025. The author thanks B. Hulsebosh, M. S. Bargh, and P. Ebben for the implementation of the approach in the context management framework. The author also thanks the anonymous reviewers for their helpful comments.

References

[1] Akoush, S. and A. Sameh, *Bayesian learning of neural networks for mobile user position prediction*, in: *Proc. of 16th Int. Conf. on Computer Communications and Networks (ICCCN 2007)*, 2007, pp. 1234–1239.

[2] Bardram, J. E., R. E. Kjær and M. Ø. Pederson, *Context-aware user authentication - supporting proximity-based login in pervasive computing.*, in: *Proc. of the Int. Conference on Ubiquitous Computing (Ubicomp 2003)*, 2003, pp. 107–123.

[3] Burrows, M., M. Abadi and R. Needham, *A logic of authentication*, ACM Trans. on Computer Systems (TOCS) **8** (1990), pp. 18–36.

[4] Cheng, C., R. Jain and E. van den Berg, "Location prediction algorithms for mobile wireless systems," CRC Press, Inc., 2003 pp. 245–263.

[5] Hesselman, C., H. Eertink, M. Wibbels, K. Sheikh and A. Tokmakoff, *Controlled disclosure of context information across ubiquitous computing domains*, in: *Proc. IEEE Int. Conf. on Sensor Networks Ubiquitous, and Trustworthy Computing (STUC 2008)*, 2008, pp. 98–105.

[6] Huang, C., H. Hua-Ping and Z. Wang, *Modeling time-related trust*, in: *Proc. of the Int. Work. Grid and Cooperative Computing (GCC 2004)*, LNCS **3252**, 2004, pp. 382–389.

[7] Hulsebosch, R. J., M. S. Bargh, G. Lenzini, P. W. G. Ebben and S. M. Jacob, *Context sensitive adaptive authentication*, in: *Proc. of the 2nd European Conference on Smart Sensing and Context*, LNCS **4793**, 2007, pp. 93–109.

[8] Jøsang, A., *Probabilistic logic under uncertainty*, in: *Proc. of the 13th Australian Symposium on Theory of Computing (CATS 2007)*, ACM Int. Conf. Proc. Series **65**, pp. 101–110.

[9] Jøsang, A., *A logic for uncertain probabilities*, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems **9** (2001), pp. 279–312.

[10] Jøsang, A., L. Gray and M. Kinateder, *Simplification and analysis of transitive trust networks*, Web Intelligence and Agent Systems Journal **4** (2006), pp. 139–161.

[11] Jøsang, A., S. Pope, J. Diaz and B. Bouchon-Meunier, *Dempster's rule as seen by little coloured balls* (2005), manuscript, submitted to Information Fusion Journal.

[12] Jøsang, A., S. Pope and S. Marsh, *Exploring different types of trust propagation*, in: K. Stølen, W. H. Winsborough, F. Martinelli and F. Massacci, editors, *Proc. of the 4th Int. Conf. on Trust Management (iTrust 2006)*, LNCS **3986**, 2006, pp. 179–192.

[13] Lenzini, G., R. J. Hulsebosch and M. S. Bargh, *Trust-enhanced security in location-based adaptive authentication*, in: *Proc. of the ESORICS 3rd International Workshop on Security and Trust Management (STM 2007)*, number 197 in Electronic Notes in Theoretical Computer Science, 2008, pp. 105–119.

[14] Nefti, S., F. Meziane and K. Kasiran, *A fuzzy trust model for e-commerce*, in: *Proc. of the 7th EEE Int. Conf. on E-commerce Techonolgoy (CEC 2005)*, 2006, pp. 401–404.

[15] Svensson, H. and A. Jøsang, *Correlation of Intrusion Alarms with Subjective Logic*, Technical Report IMM-TR-2001-14, Informatics and Mathematical Modelling, Technical University of Denmark, DTU (2001).

[16] van Kranenburg, H., M. S. Barg, S. Iacob and A. Paddemors, *A context management framework for supporting context aware distributed applications*, IEEE Communications Magazine **44** (2006), pp. 67–74.

[17] Wu, H., M. Siegel and S. Ablay, *Sensor Fusion using Dempster-Shafer Theory ii: Static Weighting and Kalman Filter-like Dynamic Weighting*, in: *Proc. of 20th IEEE Instrumentation and Measurement Technology Conference (IMTC 2003)*, 2003, pp. 907–912.