

Connecting Body Sensor Networks to Pervasive Computing Environments

PhD Research Proposal

David Jea
University of California, Los Angeles
Electrical Engineering Department
Networked & Embedded Systems Laboratory

OUTLINE

I. SUMMARY

II. APPROXIMATE DATA COLLECTION

A. INTRODUCTION

B. RELATED WORK

C. PROBLEM STATEMENT

D. PROPOSED RESEARCHES

E. PRELIMINARY ANALYSIS

F. PRELIMINARY EXPERIMENT

III. CONTEXT-BASED USER ACCESS

A. INTRODUCTION

B. RELATED WORK

C. PROBLEM STATEMENT

D. PROPOSED RESEARCHES

E. PRELIMINARY DESIGN

F. PRELIMINARY EXPERIMENT

IV. SCHEDULE

V. REFERENCE

Summary

The purpose of this research is to explore how human interacts with the pervasive computing environments. We specifically focus on the two research topics: approximate data collection and context-based user access. Approximate data collection is the process of collecting reduced information from sensors. The technique is applied in the scenario where energy, bandwidth, or storage is the constraint. In pervasive computing environments, various devices embedded in the surroundings are public and shared among multiple users. Such complicated scenario easily results identity confusion problems. Context-based user access describes the rules of the interaction between a user and a device based on their physical states. This ability enables user access to the designate devices and describes the real usage relationship among these entities.

The approximate data collection is investigated in our earlier work, which shows accurate inference results even with 50% data resolution reduction. Given a context, we reduce the resolution of data samples on low priority sensors while maintaining our confidence to the inferred context. The work presents a preliminary verification that shows how the data samples with different resolution levels (number of bits per sample) collected from two accelerometers attached to a user affects the determination of a ambulatory context.

Continuing our preliminary work, we propose extending approximate data collection in two aspects: resolution reduction based on data features and resolution reduction on multiple sensors. Note that in earlier work, the derivation of resolution lower bound is built on data samples from sensors. However, the inference engine generally takes data features as inputs to classify user contexts. An extended analysis from data samples to data features is required to support resolution reduction algorithm. Also, sensors have different influence factors to an inferred context. While reducing data resolution on sensors, a sensor with higher impact substantially improves accuracy of inferences if the system kept its information. Thus, it is important for the approximate data collection mechanisms to decide not only which sensors to degrade but also their degrading level respectively.

Next, we consider a scenario where multiple devices exist. Selecting a device is confusing to a user if multiple similar devices are near each other and the connection is established through radio. In another scenario where multiple users exist, a device can mistake the physical user (the one who is actually using it) with the connected

user (the one who connects to it) and provide irrelevant information to the connected user. In our preliminary work, we have identified these issues of user access control in a pervasive computing environment and suggest that a context-based user access to a device.

To support the importance of context-based user access in pervasive computing environments, we propose a system implementation to conduct experiments that demonstrates the idea. The system contains different stages for a complete user access process. These stages include login (authentication and secure channel establishing), data collection (context matching), and disconnection. We propose using zero-interaction authentication techniques to maximize usability. We adapt password authentication key exchange mechanisms to verify legal accesses and establish a secure channel between a user and a device. Data collection is activated only when the user is physically using the connected device. This usage relationship is determined through context matching and terminated after disconnection. The system explores and concretizes research possibilities in realizing a seamless interaction of body sensor networks and pervasive computing environment.

We expect to finish the proposed researches within one year. For the extension of approximate data collection algorithms, we expect completing analysis on June, conducting experiments, publishing the work on July and August. We develop the algorithms on September and summarize the proposed researches with a system implementation on October. The system uses the amount of information collected as a control knob to explore trade-off among accuracy, energy cost, and storage. We present and submit the results on November and December. For context-based user access, we are developing the prototype system and anticipate the first version in March. The author conducts the experiment on April. In summer, we investigate the key components of context-based user access mechanisms including context model and access control policies. We submit the final results next fall for publishing. Based on this proposal, the author expects to finish the dissertation next spring.

I. Introduction

The goal of this proposal is to explore the integration of body sensor networks and pervasive computing environments. Body sensor network is the system that wore by a person to monitor his/her physiological information for healthcare purpose. People have imagined a pervasive computing environment where we are surrounded by numerous devices and are able to access all kinds of information from these embedded devices. Wireless sensor network is one of the examples that it is deployed in an environment to monitor the physical phenomenon. To utilize information from these available devices, we consider the use case where a user selects surrounding devices as additional data sources to participate his/her body sensor network. One popular application is the remote healthcare system developed for medical industry.

We focus on two topics: approximate data collection and context-based user access. Approximate data collection is a mechanism that comprises reality and quality while pursuing the everlasting limitation of communication bandwidth and energy cost. The idea is to reduce data resolution on sensors while still maintaining inference results at an acceptable accuracy. We further consider a scenario of multiple users and multiple public shared devices. For a user to access a device, there is no easy way to verify the physical identities of two connected entities if relies solely on wireless connection. To avoid confusion, we employ context-based user access mechanisms for users to select a device and for devices to identify a user. We address the two topics individually in following sections.

II. Approximate Data Collection

A. Introduction

Increasingly richer sensing sources have been incorporated in body sensor networks (BSN) to collect more accurate and detailed physiological information of a person for medical industry. However, the bandwidth of the shared wireless medium is limited and moreover higher data volume have a negative impact on battery life as the system energy consumption is dominated by wireless communication. This has hindered the progress of real-time high data rate monitoring applications in BSN. The situation gets worse when the sensor nodes communicate with each other through a low-power radio, which usually provides lower data rate levels. In-network aggregation is often used to address this issue by reducing communication load through distributing sensor data query operators down to the sensor nodes. The partial results from the different sources are then combined to reduce data redundancy at the intermediate nodes along the path to the base station. Similarly, instead of sending raw sensing data, sensor nodes can perform feature extraction on local data and send feature vectors only. However, in the light of deployment experiences with various sensor network applications, the above approaches are unattractive to domain experts [3], who often want to be able to reconstruct detailed sensor waveforms and not just events and features. Users in BSN research community also often need to communicate back complete sensed information.

To carry detailed sensing information over the resource-limited wireless medium, lossless and lossy compression algorithms may be employed to reduce communication load at the cost of increased encoding complexity. For a highly resource-constrained device, such as a sensor node, a lossless encoding scheme is usually too computationally intensive to be practical. A reasonable compromise to achieve the application fidelity requirements and bandwidth demands is to use lossy data compression schemes that trade information quality for lower computational complexity and higher compression ratio.

Approximate data collection [3] is an in-network lossy compression scheme for collecting data from sensor nodes. Current techniques mostly exploit temporal or spatio-temporal correlations among the measurements of the physical process made by different sensors. It requires domain experts to define the degree of precision (error bound ϵ) required for their queries. The returned answer is guaranteed to be

ε -approximation of the real value with probability ρ . The system continuously adapts the model to approach the physical process and uses the model to reduce communication overheads.

B. Problem Statement

In this research, the approximate data collection is addressed from a different angle. We embrace the idea of "*Based on the current context, the system dynamically adjusts the degree of precision for each sensor. Those sensors of interest provide more detailed information while the rest maintain just enough confidences in an inferred context.*" Indeed, from the viewpoint of a user, the information at different sensors has different significance levels (and hence should be given different priorities) in different contexts.

We believe that the “sensors of different priorities“ concept is especially suitable for BSN. For example, say, when early signs of heart-attack (context) are being detected, the electrocardiogram (ECG) signals will become the highest priority information for diagnosis and should be delivered immediately and with high fidelity. Meanwhile, accelerometers used for classifying the physical context of a user (walking, running, limping, etc.) now become lower priority information sources that can be turned off. In this scenario, however, it is possible to further enhance our confidence in detecting a heart-attack event if the system allows partial accelerometer information to be involved. For example, running could trigger angina while walking might not [16].

We argue that an energy or bandwidth constrained BSN should not blindly collect maximum fidelity data from all the sensors since different sensors have different significance levels for different inferred contexts. Given a context, the system shall deliver data with high fidelity or fine granularity for sensors of interest (high priority), and reduce information collected from the remaining sensors (low priority). However, it is domain experts who would have the knowledge to assign the significance level of each sensor under different contexts. Therefore, this work does not address how to make such decision. Rather, this work explores the above idea and presents an approach that enables **data resolution** (number of bits per sample) used to represent information from different sensors to be adapted to their priorities, while maintaining desired overall confidence in the inference result.

We formulate the problem below. Consider a BSN consisting of n sensors, whose data resolution settings are described by a vector $R = \{R_1, R_2, \dots, R_n\}$. The overall energy cost is $E(R)$ and the consumed data communication bandwidth is $B(R)$. Given the

available bandwidth B_{phy} , a physical constraint is that $B(\mathbf{R})$ must be less than or equal to B_{phy} . The required confidence to an inferred context is C_{th} , whose value depends on the occurrence probabilities of different contexts. Based on the received data from sensors, the function to determine the confidence to the inferred context is $C(\mathbf{R})$. $C(\mathbf{R})$ is increasing in \mathbf{R} for lower data resolution provides less confident results. Our goal is to find a set of data resolution settings for each sensor that fulfills the required confidence while minimizing $E(\mathbf{R})$. In the cases of weak inferences ($C(\mathbf{R}) < C_{th}$), the \mathbf{R} is set to the setting that maximizes the $C(\mathbf{R})$. We summarize the problem formulation below.

Given:

Available Physical Bandwidth: B_{phy}

The Required Confidence level to the Inferred Context: C_{th}

Define:

The vector of data resolution settings of n sensors: $\mathbf{R} = \{R_1, R_2, \dots, R_n\}$

Required Communication Bandwidth: $B(\mathbf{R})$

Overall Energy Cost: $E(\mathbf{R})$

Confidence level to the Inferred Context: $C(\mathbf{R})$, $C(\cdot)$ is a increasing function of \mathbf{R}

Objective:

$\forall \mathbf{R} : B(\mathbf{R}) \leq B_{phy}$,

$S = \{\mathbf{R} : C(\mathbf{R}) \geq C_{th}\}$,

If $S \neq \emptyset$

Find $\mathbf{R} \in S$ such that $E(\mathbf{R})$ is minimized

Else

Find \mathbf{R} such that $C(\mathbf{R})$ is maximized

C. Related Work

Research communities in different fields have long investigated in monitoring applications. Directed Diffusion [1] is a data-centric protocol for general data collection in sensor networks. Cougar [8] and TinyDB [9] is a database abstraction of sensor networks and provide declarative interfaces. Skordylis et al. conduct a complete survey [2] in approximate data management for sensor networks.

In [3], Chu et al., motivated by existing deployment, attack the "SELECT *" problem for sensor networks. The proposed approach compresses data using replicated

dynamic probabilistic models to guarantee a fixed error bound from the measurement readings. The work is similar to BBQ approach proposed in [4] but pull-based. Both work establish statistic models of real worlds to reduce sensing and communication overheads. Jain et al. [5] explore temporal correlation of a data source and introduce a dual Kalman filter architecture to conserve network bandwidth. The server and the source maintain same copies of a Kalman filter. The server uses the filter to predict data from the source, and the source updates the corresponding filter on server if the prediction is outside of given precision.

Lazaridis and Mehrotra [6] propose the piecewise constant approximation (PCA) approach for data producer to transmit time series to data archiver. The approach represents time series with a sequence of segments (c_i, e_i) , where c_i is a constant value for time in $[e_{i-1}+1, e_i]$.

The Bayesian classifier has been proved to be effective for motion recognition applications. In [17], twelve three-axis accelerometers and a naive Bayesian classifier are used to capture postures and activities of a user. Korpip et al. [18] apply naive Bayesian networks to classify user daily activities based on audio features. Du et al. [19] divide features into global and local classes, and present a dynamic Bayesian network model to recognize interacting activities.

D. Proposed Researches

We propose to investigate the approximate data collection problem in following aspects: (1) How to reduce the resolution of sensors? (2) How to select sensors? (3) How to determine the reduction level of each sensor? (4) What is the accuracy of inference results after reducing resolution on selected sensors? (5) How much energy has been saved?

To answer these questions, we analyze the principle of our Bayesian inference engine and show in preliminary analysis section that how to combine the observations from one sensor. We then show that how multiple sensors affect each other in determining a context. The preliminary analysis shows that, for a given context, selecting different sensors to reduce resolution affects inference accuracy. Continuing the track, we need to determine the reduction level of each sensor so that the inference is most accurate or the energy is most saved. Furthermore, the derived analysis is based on data samples that in general do not directly apply in the inference engine where the features of data streams are the inputs. We need to extend the analysis to relate how reducing data resolution changes the data features and affect inference results.

We propose creating a system that employs data collection algorithms based on the analysis. The system allows the user to set the required confidence of a context. The system provides a user control knob to set the amount of information collected in a body sensor network. The data collection algorithm leverages this requirement and fully explores trade-offs among communication bandwidth, accuracy, and energy cost for a satisfying configuration (greatest confidence or enough confidence with most energy saved). The system achieves approximate data collection through reducing resolution on selected sensors. The sensors then deliver these low-resolution data samples to the base station.

We consider a general one-hop, star topology BSN scenario that consists of one base station and several sensor nodes. The physiological information is constantly collected by sensor nodes and delivered to a base station. An inference engine at the base station takes the features of sensor data as inputs and generates user context as output. Sensor nodes are assigned priorities in each context. The system attempts to collect detailed information from high priority sensor nodes and reduce fidelity information from low priority nodes. A user can setup the lowest acceptable resolution of a sensor to avoid data being degraded too much, yielding an unacceptable distortion level. The features extracted from these samples still allow the inference engine to have desirable confidence level in the current context. In this manner, approximate data collection is achieved based on the context.

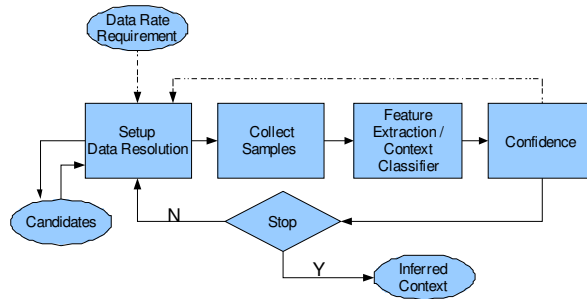


Figure 1: Block Diagram of the Base Station

Figure 1 shows the block diagram of the proposed approximation data collection on the base station. The initial setup is to collect data samples at the highest resolution from all the sensor nodes. The base station extracts features from these samples, and the inference engine classifies the context according to these features. The system imposes data rate constraints to the sensor nodes when it detects a network congestion event, reserves bandwidth for higher priority sensor nodes or simply wants to save energy. Given this data rate constraint, a naive solution is to equally reduce data resolutions and hence the data rate requirements of all nodes. In contrast, in our proposed approach, the base station selects low priority nodes based on the inferred

context, and reduces data resolution of these nodes. The base station then uses the collected data samples to classify current context and possibly adjusts the resolution if it is not confident in the inferred context.

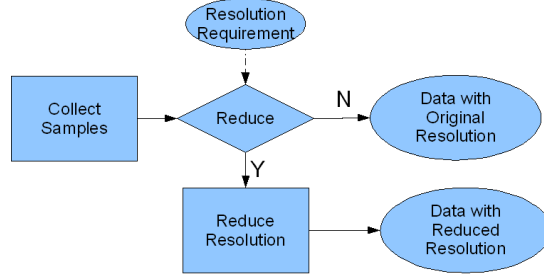


Figure 2: Block Diagram of the BSN Node

Figure 2 depicts that each sensor node controls resolution of the collected samples based on the resolution requirement prescribed by the base station. Note that the finest resolution that a BSN node can provide is the original data without any resolution reduction.

E. Preliminary Analysis

Our inference engine employs a Bayesian network [11] that combines multiple sensor observations for the purpose of inferring the context of a subject. The assumption is that we are confident in an inferred context if its occurrence probability is greater than T_H and the occurrence probabilities of all the other contexts are less than T_L . The goal is to determine the current context using a reduced resolution version of sensor data.

Denote the n possible observations by O_1, O_2, \dots, O_n and the observation space by O_s , $O_s = \{O_1 \cup O_2 \dots \cup O_n\}$.

The probability of a context C given an arbitrary observation O of a sensor is represented by the conditional probability $P(C|O)$.

We note that for a partial (incomplete) observation O , knowing only the fact that O belongs to the set O_s is sufficient to determine a probability range for context C given O . To be specific, $P(C|O)$ has a lower bound and upper bound given by Eq. (1):

$$\begin{aligned}
& \forall O \in O_s \\
& \exists i, j: P(C/O_i) \leq P(C/O) \leq P(C/O_j), \\
& \text{where } i = \underset{m=1 \dots n}{\operatorname{argmin}} P(C/O_m), \\
& \quad \quad j = \underset{m=1 \dots n}{\operatorname{argmax}} P(C/O_m)
\end{aligned} \tag{1}$$

Moreover, it is also sufficient to upper-bound the occurrence probability of any context other than C (denoted by C') given O , obtained in Eq. (2).

$$\begin{aligned}
& \forall C' \neq C, \\
& \exists k: P(C'/O) \leq P(C'/O_k), \\
& \text{where } k = \underset{m=1 \dots n}{\operatorname{argmax}} P(C'/O_m)
\end{aligned} \tag{2}$$

If we know for a fact that an incomplete observation θ belongs to O_s , we can use the $P(C|O_i)$ in Eq. (1) to lower-bound $P(C|\theta)$. Similarly, $P(C'|O_k)$ in Eq. (2) is used to upper-bound $P(C'|\theta)$. If the lower bound of $P(C|\theta)$ is greater than T_H and the upper bound of $P(C'|\theta)$ is less than T_L , then we are confident that, based on the assumption, the current context is C . Note that a low resolution observation is an incomplete observation, whose rough range instead of real (high-resolution) value is known. By replacing a complete observation by an incomplete (lower resolution) one (θ), Eqs. (1) and (2) can serve to decide the corresponding confidence level in the inferred context. In the case that we are not confident about the inference results, higher resolution or other observations would be required.

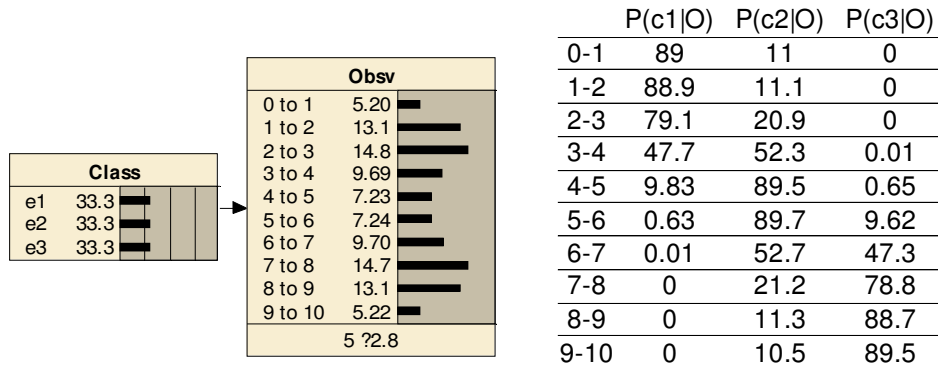


Figure 3: An example Bayesian classifier

In the following we present a simple classifier example for illustration purposes. The example is extended based on a Bayesian belief networks software, Netica [14]. Assume a sensor's observation (ranging from 0 to 10) has a resolution of unit 1. The sensor observations are characterized by a normal distribution, whose mean and

standard deviation values are, respectively, equal to 2 and 1 when context one (c1) occurs, 5 and 2 when context two (c2) occurs, and 8 and 1 when context three (c3) occurs. Assume these three contexts take place with equal probabilities as shown to the left in Fig. 3. After we train the classifier with some random simulated samples, the table to the right in Fig. 3 shows the probability of each context given an observation. Fig. 4 shows the resulting confidence levels in a context based on reduced resolution observation.

Low Resolution Obsv	Lower bound		
	P(c1 O)	P(c2 O)	p(c3 O)
0 – 2	88.90%	11.00%	0.00%
2 – 4	47.70%	20.90%	0.00%
4 – 6	0.63%	89.50%	0.65%
6 – 8	0.00%	21.20%	47.30%
8 – 10	0.00%	10.50%	88.70%

Figure 4: Results of resolution reduction to example classifier

We now extend the discussion to a BSN scenario that contains multiple sensors. In such a scenario, knowing the observation of a sensor will "pull" other sensors to be inclined towards its inference. This means that given that the observation from sensor one is x and the most likely context is C , the distribution of observations on sensor two is now in favor of context C . Note that observations from two sensors (x and y) are conditionally independent given context C in a naive Bayesian network. In this manner, the probability of context C for an observation y at sensor two, conditioned on that x is observed by sensor one, is given by Eq. (3):

$$P(C/y, x) = \frac{P(y/C)P(C/x)}{P(y/x)} \quad (3)$$

Similar to the earlier discussion in the context of single sensor case, we may provide a lower bound of the probability of context C for a low resolution (incomplete) observation Y , $P(C|Y, x)$, $Y=\{y_i \leq y \leq y_k\}$, and also an upper bound of the probability of context C' ($C' \neq C$) given Y , $P(C'|Y, x)$. After replacing an complete observation y by a lower resolution representation Y , the lower bound of $P(C|Y, x)$ and the upper bound of $P(C'|Y, x)$ may determine our confidence level in the inferred context C .

We now extend the example by adding a second sensor, whose observations are also characterized by a normal distribution, with mean and standard deviation values equal to 7 and 2 when context one ($c1$) occurs, 2 and 1 when the second context ($c2$) occurs, and 4 and 2 when context three ($c3$) occurs. Figure 5 shows that if an observation from sensor two (indicated by ObsvY in Fig. 5) ranges from 7 to 8, then the

observations of sensor one is pulled towards the inferred context, $c1$. In that case, given $\text{ObsvY} = 7 \sim 8$, a highly reduced resolution version (0 to 5) of sensor one observation (ObsvX) is able to increase our confidence level in context $c1$ to 98.6% and decrease to 1.35% in other contexts $C' \neq c1$, as shown in the table to the top right of Fig. 5.

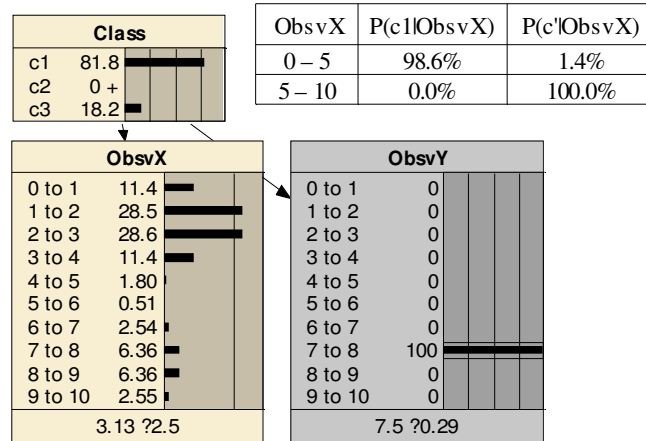


Figure 5: An example with two sensors and shows that the observation from a sensor pulls the other sensor towards its inference. A low resolution of ObsvX can greatly enhance the confidence to inferred context ($c1$)

Note that most practical Bayesian inference engines take data features to classify context rather than plain observations. The paper does not address this gap in depth.

F. Preliminary Experiments

We use real data that are collected from testbed experiments for evaluation. The system uses two three-axis accelerometers to collect physiological information of the subject and send back to the base station. We divide the collected data into two sets, training set (75%) and testing set (25%). When running the training set data, conditional probability tables are updated by a supervised learning setting in order to train the classifier to learn the characteristics of each context. The inference engine then extracts features from the testing data set and classifies the subject's context based on learned information. We evaluate the confidence levels in all contexts with different resolution reduction versions of the testing data set. The degree of reduction depends on the number of least significant bits (LSB) being reduced per sample, in which we normalize to ten bits.

We modified a system originally developed for Medical Embedded Device for Individualized Care (MEDIC) in [7]. The system now contains a base station (Nokia 770 [12]) and two sensor nodes (BlueSentry [13]). Each sensor node is equipped with one three-axis accelerometer and uses Bluetooth radio to communicate with the base station. The sensor nodes continuously relay sampled information (a total of six sensing channels) back to base station, and the base station saves received information into files with timestamps. In this experiment, for evaluation purpose, we use an off-line inference engine to perform classification. The prototype system is shown in Figure 6.



Figure 6: The prototype hardware system includes one base station and two sensor nodes. A knee brace is used for emulating limping context.

We investigated four contexts for this evaluation: walking, left leg limping, right leg limping, and stationary. We performed the experiments in the sixth floor hallway of UCLA Engineering IV building. The subject wore two sensor nodes (each with an accelerometer) around his waist, one on the left-hand side, and the other one on the right-hand side. Both accelerometers had the sampling rate set at 100 Hz on each channel (x, y, and z axis). We collected data under each context for approximately 15 to 30 minutes. To emulate limping context, we use a knee brace to enforce a fixed leg. The experiments collect a total of one and a half million samples for these four contexts (walk: ~27.4%, left leg limping: ~26.9%, right leg limping: ~26.6%, stationary: ~19.0%).

To extract features, the base station first converts data from time domain to frequency domain through the fast Fourier Transform (FFT) algorithm. Assume $X(n)$ is the transformed version of the input time-series sensor data and N is its length. It then picks the amplitude of dominant frequency and calculates the integrated spectral energy as shown in Eqs. (4) and (5) as the two features considered in this evaluation

([10]). The inference engine takes these features as inputs and estimates the most probable context.

$$F_{amp} = \max \|X(n)\| \quad (4)$$

$$F_{energy} = \sum_l^N X(n) * X(n) \quad (5)$$

We choose a naive Bayesian classifier as the inference engine in the system. A naive Bayesian classifier often works well in real world and assumes that features are conditionally independent. The classifier is a Bayesian network that contains two types of node: feature nodes and context nodes. Each feature node represents one of the features that are extracted from collected data. Our inference engine employs continuous domain feature nodes and then quantizes the real value into a discrete level state. There are five data levels per "amplitude of dominant frequency" (ADF) feature node and ten data levels per "spectral energy" (SE) feature node. Uniform step-size quantization is applied, with the quantization dynamic range determined by the maximum and minimum value of its training data set. A better setup is possible but beyond the scope of this work. Note that the current setup is shown to be quite sufficient to classify the contexts and to fulfill our evaluation purpose. With the feature nodes being setup, the context node shows the inference result and has the four discrete context states that we consider (walking, left leg limping, right leg limping, and still). Due to space limitation, the result of the trained Bayesian network is presented in [15].

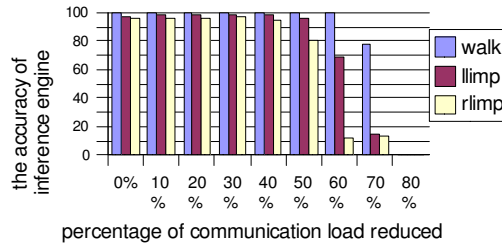


Figure 7: The effects of reducing data resolution in time domain on test data set of every sensing channel.

In this classifier, the inference of stationary context, "still", always has an accuracy of 100%. In addition, irrespective of how much information is being reduced in testing data set, its accuracy still remains at 100%. This is due to its unique characteristics (near zero) in all features, and with reduced data resolution, we actually push the data towards the stationary context. In the highly resolution reduction case, all the inferred results become "still" context. We thus omit its accuracy in following discussion.

We refer the feature space to the union of all level states across all feature nodes in the rest of this paper. For example, in Fig. 5, ObsvX node has 10 discrete states and ObsvY node also has 10 discrete states, the feature space is therefore the 20 states from both nodes. After having learned from the training data set, we find that nearly **50%** of the feature space suggests a confidence level greater than 80% for the "walking" context or a confidence level less than 20% for any of the rest contexts. On the contrary, only 3.3% and 7.8% of the feature space indicates the same confidence level (80%, 20%) for "left leg limping" and "right leg limping" contexts, respectively. In other words, the inference engine can reduce the data resolution of a feature for "walk" context, by combining 50% states of the feature space as discussed in section 3, without losing noticeable confidence, while the "left leg limping" and "right leg limping" contexts are more sensitive to such resolution reduction. In Fig. 7, we show the resulting inference accuracy of the naive solution that equally reduces resolution on all sensing channels. It is noted that "walking" context manages to maintain high accuracy level even with largely reduced data resolution, while the accuracy levels for the other two contexts are significantly degraded as the resolution is reduced beyond a certain level.

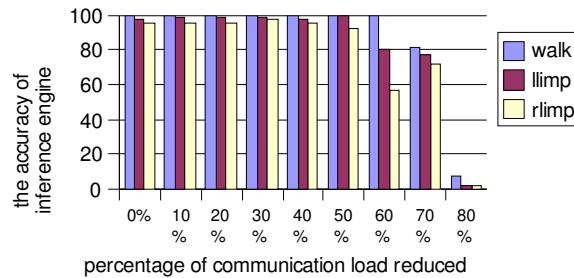


Figure 8: Keeping original resolution on the sensor of interest (the y-axis of accelerometer on left leg). The effects of reducing data resolution in time domain on test data set of the rest sensing channels.

In Figure 8, in contrast to the naive approach used in Fig. 7, the sensing information collected by the y-axis of the accelerometer on the left waist (ACCY_L) is set to high priority and assigned to transmit with complete information. In doing so, we believe that further resolution reduction on other sensors can be performed to provide the same inference accuracy. As described earlier, based on the assumption that ACCY_L is of more importance for the considered context, the other sensing channels are for the large part playing the role of assisting and refining the inference result of ACCY_L. We verified this by comparing the results of Figure 7 to Figure 8 for the cases where sixty or seventy percent of information are discarded on the testing data set. Figure 8 intelligibly achieves more accurate inferences using these highly degrade samples. Figure 9 shows the lowest resolution allowed in both approaches to yield

80% confidence in all inferred contexts. It is thus clearly desirable and necessary to use a more intelligent solution, such as the proposed approach, for adapting the contexts that are sensitive to data resolution reductions to collect data.

III. Context-Based User Access

A. Introduction

People have long envisioned a pervasive computing environment where numerous ambient sensors and actuators are embedded to provide rich experiences of intelligence and interaction. Recent years, Body Sensor Networks (BSN) have employed a similar concept to the human health arena and utilized miniaturized wearable and portable sensor systems to provide remote pervasive health-care monitoring. We imagine in the future that most ambient devices will be shared by the public and can temporarily participate in a user's BSN to provide specific services or data. Such public devices serve as external instruments and are accessible to individuals and can provide private information to authorized users only. Wang et al. [30] suggest four requirements for a secure and flexible access control architecture in ubiquitous computing environments: (1) Access based on contextual information. (2) Easy-to-use access for different users and devices. (3) Collaborative environments. (4) Decentralized administration. This work investigates the first two requirements by looking into different stages of a session.

Basically, there are three main stages involved when a user is trying to access a device. The first action is to log in successfully (authentication) to use the device. The second stage is to maintain a usage session (presence) with the device. The last action is logging out of the device, i.e. a detachment of use. The usage session with a detached device will be invalidated. We believe that it is important, when a user is trying to access multiple public devices among all other devices that can possibly be used by the public, to address all three stages from four aspects: *security*, *selectivity*, *usability*, and *identity*. To access these prevalent public shared devices that can potentially convey private information, the security has been fully investigated in literature. However, considering environments where multiple users are surrounded by pervasive public shared devices, the numerous existing schemes have not fully addressed the remaining three aspects reasonably (Table 1). For example, the traditional authentication techniques such as using account numbers and passwords are straightforward but constitute a substantial usability obstacle to accessing future pervasive computing environments effectively.

A main contribution of this work is that we have identified in the user access methods from previous works the common pitfall is that “*the context to gain access control of*

a device is not necessarily the same context to maintain a session and/or the context to release the access control. Moreover, the fact that someone is connected to a device is insufficiently to describe whether the same user is using it.” To explain this issue, we first present the related work in access control in section B, and then discuss the problems of these techniques in section C. We propose in section D a context-based user access solution and describe our system design in section E.

B. Related Work

In recent years, the academic world has started looking into other realms of authentication that could be less demanding on the user, and still maintain the security guaranteed by traditional techniques. Stajano et al. proposed Resurrecting Duckling security model in [24] where a device will recognize as its owner the first entity that sends it a secret key (Imprinting). They suggest that imprinting process as a intuitive physical contact. In [23], Balfanz et al. extends the concept in great detail on the use of location-limited channels to be able to authenticate and use a device. The paper provides concrete pre-authentication details and implementation based on infrared. Another similar solution is the Zero-Interaction Authentication (ZIA) protocol from [20]. The idea involves the user being able to authenticate with a computer with minimal interaction. The ZIA protocol considers a user wears a short-range, wireless authentication token to communicate with the system to determine whether to grant access. However, there is nothing mentioned when dealing with multiple laptops.

There is also a proximity-based authentication technique which explores a new domain of authentication: use of context information. These techniques rely on contextual data to authenticate the user and grant usage. Contextual data refer to information that can be gathered in a pervasive environment. Contextual information such as location of the user (from a nearby camera in the ceiling) can help to determine if the user is still in the session. For instance, Bardram et al. [21] describes a hospital in Denmark where the location of a user is provided by an advanced monitoring system in the hospital. Since it is very cumbersome for users to have to type id and password multiple times throughout the day to gain access to the database, the context of a user (such as "in the surgery room") facilitates the authentication process when a user tries to use computers near his/her vicinity. Gupta et al. [25] point out that proximity based access control potentially allows someone access the resource, when an authorized user is in proximity. To address the problem, they have introduced three different authentication levels and the notation of proximity zone.

Lately, incorporating context information in user access has received attention in

pervasive applications, and different security management models extended from role-based access control (RBAC) [22] has been proposed to explore this issue. The basic concept of RBAC is that users associate with roles, roles associate with permissions to resources, and users grant access authorization by being members of roles. Moyer and Ahamad propose a Generalized Role-Based Access Control (GRBAC) in [28] that extends the role concept to subject (user), object (resource), and environment. The expressiveness of GRBAC allows context information (captured in environment roles), such as business hour or CPU load, to be included in an access decision. Zhang and Parashar [29] describe a Dynamic Role Based Access Control model (DRBAC) that improves security by using context information to dynamically make access control decisions. It addresses two requirements in pervasive applications: (1) A user's access privileges binds with the user's context. Context information includes environment (location, time) of the user accessing the resource. (2) The access permissions of a resource binds with its system information (CPU usage, network bandwidth, etc.). Overall, the role based access control maps naturally to large, structured organizations.

C. Problem Statement

The focal question we pose is *how a user can log in/out of multiple selected devices securely among many others in his/her vicinity and identify him/herself as the person who is using the device, while achieving all of these with little usability issues*. The problems we are trying to solve here can be better illustrated with a scenario. Imagine that Alice enters a public gym for her daily mile on the treadmill. She selects a camera that monitors the treadmills area, selects an electrocardiogram (ECG) sensor (with new electrodes) to wear then starts using one of the treadmills. These public devices (camera, ECG, treadmill) should be able to send her training information or physiological data to her BSN until the exercise is completed and she has left the treadmill.



Figure 9: Questions regarding user access of public shared devices: If there are multiple devices, how to effectively select among these devices? How to maintain sessions to the devices? How to logout these devices when finished? How to keep these sessions secure?

As this paradigm shows in Figure 9, there are many pressing issues to consider. When Alice needs to face multiple publicly accessible devices in her vicinity and only needs to use specific ones within the midst, how can she successfully bind with the devices she intends to use both securely and effectively? How can she also cleanly finish up the usage session when she's done and ready to leave? Moreover, her authentication process or usage session should not disrupt or be disrupted by that of someone next to her who might also be using another treadmill too. Considering the scenario in Figure 10, we expect a public device to be shared by the others, but how can that device verify that the authenticated user, Alice, is the same person who is using it? The purpose of this work is to solve these issues without incurring too much overhead and usability issues. In the following paragraphs, we will first classify the existing techniques into three categories and then elucidate on why they do not make a good solution, before proposing our own.

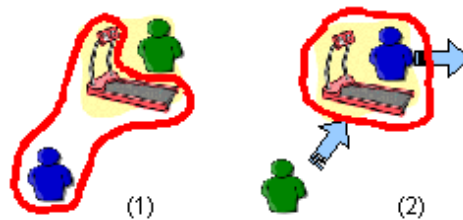


Figure 10: Issues of Identity Confusion: (1) Blue User gains access to the treadmill and the treadmill sends Green User's data to Blue User (2) Blue User is done with the treadmill and leaves. How does the treadmill figure out that the Blue User is gone and identify when the Green User is the new occupant?

For a user to initiate, maintain, or terminate a session with a device, the current state-of-art user access methods can be fundamentally categorized into common wireless technologies (such as GSM, 802.11, Bluetooth, etc.) and location-limited channels (such as physical contact, infrared, short-range RFID, etc.) that exploit the communication medium. The first group is the use of conventional wireless protocols such as 802.11, Zigbee, and Bluetooth. The second group utilizes location-limited channels that are defined in [23] and possess the property where a user can *precisely* control which devices s/he is interacting with. For both categories, a complete session relies on the encrypted information flows on these channels. Additionally, we add a third category that involves user access with the aid of context-based information. We treat this as a separate category due to its intrinsic uniqueness of utilizing context-based information in a session.

Table 1 lists the comparison of different user access methods in the logging in, maintaining a session, and logging out phases. We discuss in detail of each user access method in the following sections to elaborate why a single solution does not fit in pervasive computing environments.

	Existing Wireless Technologies	Location-Limited Channels	Context-Based
Logging In	Low Usability, especially when logging into multiple nodes	Moderate Usability, user must visit nodes one by one	No selectivity among nodes
Maintaining a session	Without explicitly logging out the nodes, a possible identity confusion problem	Either only one node can be used at a time, or the allowed proximity is rather constrained	To continuously detect the context
Logging Out	Receives a command or/and lost signal	Automatically logged out when heartbeat signal lost	Automatically logged out when the context changes

Table 1: Comparison of existing user access techniques.

Furthermore, role-based access control focuses on issues of permissions-role assignment and is generally a layer higher than the access methods discussed here. However, both GRBAC and DRBAC models employ a similar concept to this paper that context information restrains a user's access to a resource in a session. We thus discussed their similarities and differences to this work in a separated subsection.

CONVENTIONAL WIRELESS CHANNELS

Initiating a session through general wireless channels has low usability in pervasive environments. The main issue here is that it is not easy to dynamically set up a connection between devices on the go without much user interaction. Imagine a user, Alice, with three Bluetooth keyboards in front of her. All three keyboards appear on her PDA to be selected for use. Now, with the conventional wireless channel protocol, Alice is confused on mapping id to the keyboard and getting her PDA to figure out which keyboard to be used. It is apparent that we do not want to employ such awkward processes in future device-rich environments.

Moreover, as shown in Figure 10, maintaining sessions to the authenticated public shared devices through wireless channels could lead to identity issues. If the user does not explicitly log out of a device when he or she is done using it, the device needs to detect that itself explicitly (usually done using timeouts). Imagine, in our scenario, where Alice finishes her daily mile and steps off the treadmill. The next person, Bob, who was waiting in line, now steps up the treadmill and starts using it. Alice will keep receiving Bob's information unless she is out the communication range. There is no way for the system to figure out who is using the device if the existing connection to Alice is maintained through mere wireless channels without any more intelligent observations. This is due to conventional wireless solutions do not seek to exploit the use of "context information".

LOCATION-LIMITED CHANNELS

A user can easily initiate a session to a device through location-limited channel (such as physical contact). The location-limited channel is one extreme case of context-based authentication where a user can precisely control which device s/he is interacting with. Unlike initiation through conventional wireless channels, this intuitive selection process avoids confusion. We consider that it has some slight usability issues because a user still has to visit the public shared devices that s/he wants to use one by one. For a user to "precisely" select the device, these location-limited channels are either super-short-range (physical contact) or directional (infrared). Therefore, maintaining sessions through these types of channel limits the number of or the distance between connected public shared devices. Such usability issues of pervasive devices constitute an impetus to creating practically useful pervasive computing environments.

CONTEXT-BASED

In this type approach, a user will access a device if s/he is in a specific context. Proximity-based access control methods are the most popular methods to determine the context of a user and accessibility of a device. Some example contexts in these methods are "the user is inside the room" or "the user is within proximity zone of a device". The session between an authorized user and a connected device is terminated when the defined context changes (such as when the user leaves the room).

Context-based methods address a more general and flexible way in user authentication and are not limited to proximity-based access control. One example is that, in a station, if Alice faints suddenly (the context), her BSN will automatically authenticate with all nearby defibrillators to grant her access. Also, it will authenticate with the public address system and broadcast emergency messages for a doctor.

However, in a scenario of multiple users in the same context (such as they all in the same room) to unoccupied devices [25], depends on the algorithm, these devices are randomly assigned to all users or exclusively to one user. This appears to be a problem in pervasive environments. In our example, Alice only needs one treadmill, the one she selected, at a time, and neither needs nor wants the neighbor treadmills to become part of her BSN. Furthermore, defining the proximity zone of each device is also a challenging task. A small proximity zone causes the same issues we discussed for location-limited channels that either few devices or only one device can be accessed by the user at any one time. A large proximity zone (room) has security risks that it potentially allows someone to access a device if an authorized user is within the proximity but not current using it. Without special considerations, a context-based method generally does not select among devices for use.

ROLE-BASED ACCESS CONTROL

We consider accessing public shared devices in pervasive computing environments as a rather simplified RBAC model (one subject role and one object role). This is a natural result since the public has no clearly structured organizations and thus hard to define roles. However, as discussed earlier and suggested in DRBAC, context information plays the key factor in pervasive applications. Context information in GRBAC or DRBAC captures the environment for use such as time, location, and system information. However, in order to express a user access such as "receiving data from the connected treadmill only if the user is running", we need to apply context information in a more generalized sense that includes the physical state of a subject (user) and an object (device) to describe the usage relationship.

All of these issues constitute the crux of the problem that we want to solve here. We believe that a complete session for a user to access a public shared device within pervasive computing environment should be studied from the different standpoints

D. Proposed Researches

The common pitfall in the user access methods is that **the context to gain access control of a device is not necessarily the context to maintain a session and/or the context to release the access control. Moreover, the fact that someone is connected to a device is insufficiently to describe whether the same user is using it.** Our proposed solution will be as follows. When a user plans to use a device, the device is bound to the user when s/he has established a connection through **initiation-context** (for example, a location-limited channel). When he/she is

successfully authenticated with a device and begins to use it, there should be two context states bound to this session, namely a **session-context** (e.g., user leaves the room) and a **govern-context** (e.g., user is on the treadmill). The session-context defines a specified context state of the connection to this session. The govern-context defines a specified state of the user to this device. A device is connected by the user only when the session-context is valid. Based on formalized and customized rules of how the specific context state changes, the device will determine whether the user has logged out and finished using the system. This will then lead to the system cleaning up this current session. As indicated earlier, the session-context is insufficient to describe whether the user is physically using the device. We thus require govern-contexts to represent this relation. A corollary is that a session-context consists of zero, one or more govern-contexts entities that are collectively used to describe a particular session for the user using a particular device. Although most user access methods treat these contexts as one single session-context, a careful design for pervasive applications shall distinguish them. In addition to select proper contexts from usability perspective, the initiation-context ought to provide selectivity among devices and ability to establish secure channels with selected devices, also, the govern-context should provide a continuously monitoring of the physical identity of current user.

As shown in Table 1, there is no single technique addresses all the issues. Thus, a better design incorporates the strength of these techniques. We propose to create a complete prototype to address issues described earlier. For security related issues, we choose PAKE methods to authenticate trust entities and to establish secure communication channels. We rely on location-limited channels to precisely select a device and use zero-interaction authentication techniques to enhance usability while minimizing user interaction. We then propose an experiment (Figure 12) to unveil the identity confusion problems. In the experiment, a user exercises in gym that has public sensing devices installed on the fitness equipments. A device joins a body sensor network through authentication process, but provides sensing information only when the user is indeed physically using the device. We attach one accelerometer to the user and one accelerometer to the elliptical trainer. The elliptical trainer has another SpO2 sensor to monitor heart rate information. This sensor also connects to the user's BSN but only delivers data to the base station when two accelerometers experience similar phenomenon (context matching). With a different user using the same elliptical trainer, the connected BSN (to the first user) stops receiving data. The purpose of this experiment is to show that a context-based system is smart enough to identify that if a connected device is used by the same user. The result prototype system demonstrates our interpretation to a context-based user access system.

We then propose to explore the two key components in the system: context definition (context model) and context matching (access control policies). Context itself is an abstract concept that used in many ways. Location is one kind of context, and connecting to other entities is a context. Running, limping, walking, etc. are all ambulatory contexts of a human. Therefore, we need to define these contexts concretely to complete a context-based user access to devices. Context matching in govern-context is the core concept of describing the physical usage of a user to a device. For example, if the location of a user overlaps with the location of the device, the system believes that the user is using the device. Other example such as a live connection between the user and the device is the most common way to describe a usage relationship. A complicated context matching example involves both the user and the device experiencing same physical phenomenon. Our research focuses on laying the rules of context matching so that the system accurately captures the user's states and relates to the connected devices. We believe the two issues are the major steps to a context-based user access in pervasive computing environments.

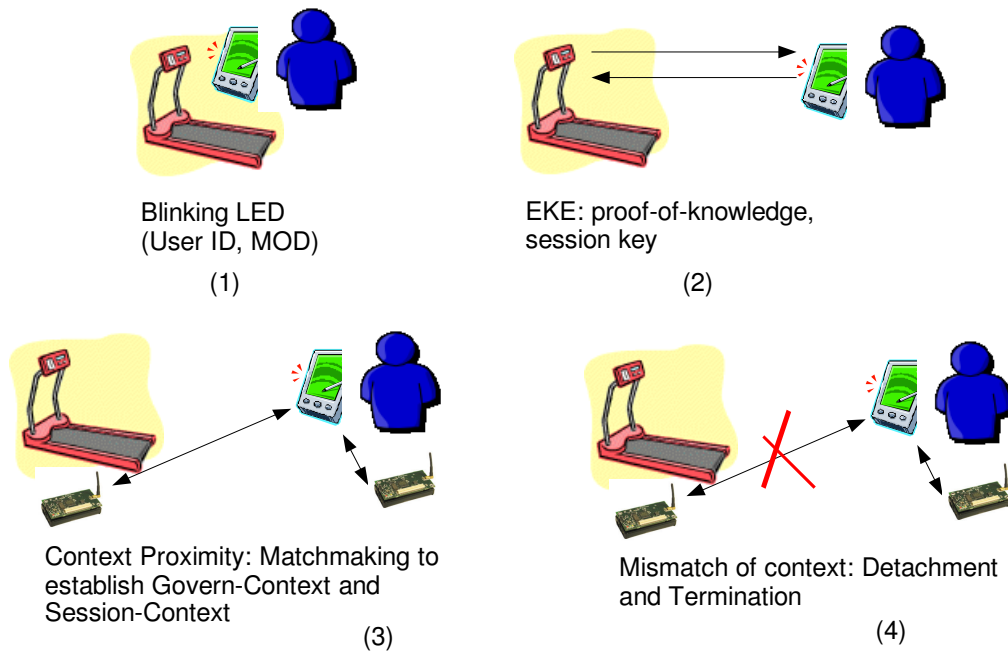


Figure 11: The scenario of proposed experiment

E. Preliminary Design

Figure 12 shows the state diagram of the system. Besides the login, session maintenance, logout states, we have added a data collection state to reflect the physical usage relationship between the user and the device. The BSN enters to the login state once it detects the initiation-context. In the login state, the BSN

authenticates with the device bounded by initiation-context and establishes a secure channel based on generated session key. The authenticated device becomes a member of BSN and the system then determines the necessary session-context and govern-context involved between the user and the authenticated device. The BSN continuously maintains the session to the device if it detects a valid session-context. When the govern-context is true (attachment), this means that a user is using the device. Otherwise, the device is detached from the user (detachment). And the user's BSN only takes the data of a connected device when the user is actually using the device. The system terminates a connection when the session-context is invalidated.

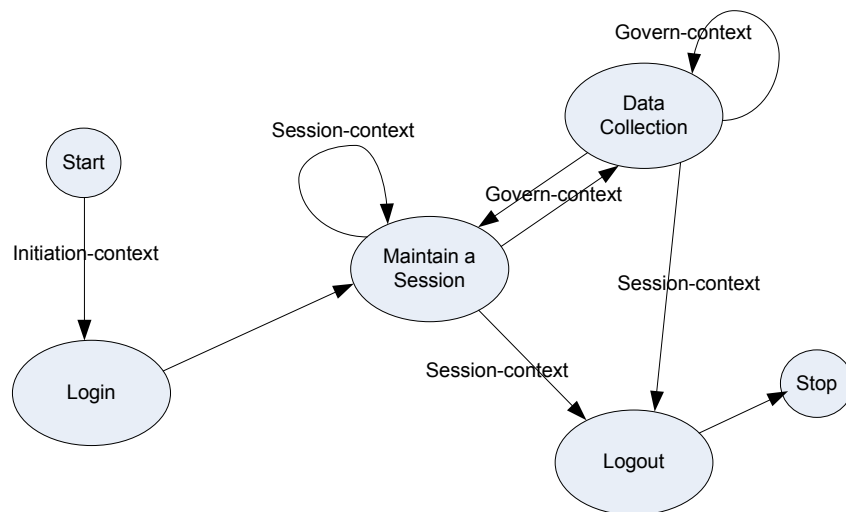


Figure 12: State diagram of the system

We divide the connection procedure between a user and a device into four phases: authentication, context establishment, attachment/detachment, and termination. In the authentication phase, the secret information exchanges on location-limited channels and is later used for subsequent authentication over wireless. In context establishment phase, the system determines the necessary session-context and govern-context involved between the user and the authenticated device. When the govern-context(s) is(are) true (attachment), this means that a user is using the device. Otherwise, the device is detached from the user (detachment). And the user's BSN only takes the data of a connected device when the user is actually using the device. The system terminates a connection when the session-context is invalidated. We explain the four phases below in detail.

AUTHENTICATION

Authentication is the first step in establishing a secure communication channel between the user and the device. When using a location-limited channel, a user can

easily and precisely select the device s/he wants to authenticate with by first approaching it intuitively. The basic assumption here is that *at least one location limited channel* (LED, Infrad, RFID, sound, physical contact, etc.) is available between a BSN and a public sensor node. After selecting the device, we break down the issue of authentication into two problems that need to be addressed: trust and privacy.

Between two parties, how can the user and the device acknowledge and trust each other? We suggest the use of the password-authenticated key exchange methods (PAKE). Encrypted Key Exchange is the first PAKE protocol that published in [26]. The idea is that the user and the device have common knowledge of a secret and when the user authenticates with the device, they challenge each other on the knowledge of the secret without revealing it. The user and the device only trust each other if both parties prove their knowledge of the secret. To reduce security risks, we suggest a use of hybrid keying model where each BSN has a unique key that is shared by BSN members, and a separate global key to access all public shared devices.

The second major issue is privacy. During the process of verifying trust among two parties, PAKE methods such as EKE protocol automatically generate a unique session key based on Diffie-Hellman key exchange algorithm. The method is capable of producing a key that is non-reproducible and is conducive to the current session of interaction. To prevent external cryptographic attacks, security protocols rely on the produced session key to encrypt/authenticate the exchanged messages and allow the user to communicate securely with a trusted device.

CONTEXT ESTABLISHMENT

Context establishment is the next phase where the user needs to establish some form of connection based on the state of using the device. A govern-context describes that if a user is physically attaching to (using) a device, and a session-context is the description of the context for the user's current usage session. After authentication and connecting to a user (meaning that the overall session-context is valid), the device has joined the user's BSN and become one of the BSN nodes. The BSN then decides from a list of contexts the session-context and govern-context of this connection and continuously monitors the two contexts. The system now enters a state of detachment, and if the govern-context is true and session-context is valid, then the system enters the attachment phase. The connection terminates if the system detects the invalidate session-context. Both session-context and govern-context track specific observed states of the physical controlled objects. There are three main types which we discuss.

The first form of the context is the god view, where a central context server that monitors all entities and their behavior in its controlled environment. A govern-context example is the location of a user and the public shared devices. When a user is in proximity of a device, then the system assumes that the user is attaching to the device. Likewise, there are also many possibilities for a session-context. Examples from our treadmill-usage paradigm could be the camera detecting a user leaving the treadmill, or the user waving goodbye at some interpretation device.

The second case is one based on local decision, the context that is determined by the BSN that a user is wearing. The BSN detects current context of the user and the decision is based on this context. For example, if the inferred context of a user is running and a treadmill has been connected to his/her BSN, then the system considers that the user is attaching to the device.

There is the special case where the context can rely on *context proximity* among devices as epitomized in [26]. Their work proposes a scenario where small devices are connected when two persons handshake, the two artifacts connect with each other if both experience similar context. We extend similar idea to search matchmaking context among a user and devices. for example, in our treadmill scenario, a user can only attach to a treadmill if similar accelerometer contexts are found on both entities.

ATTACHMENT AND DETACHMENT

Attachment refers to when the user has connected to and is using a particular device (session-context is valid and govern-context is true). Detachment is the scenario where the user is temporarily not using the device (session-context is valid and govern-context is false). A reasonable assumption is that when a user *attaches* to a sensor, it describes the user is using that sensor and no other people (with less or equal access right) can override that relationship physically or virtually. And the sensor believes that all the sampled information belongs to the attached user (exclusive).

After establishing contexts, the device constantly check if all the govern-contexts involved are true (attachment). If it is, the attachment state is activated and the BSN treats the device as being used by the user and allows information flow from the device to the user's BSN. However, if any of the govern-context fails, the device will be considered detached temporarily from the user and stops taking information from the device.

TERMINATION

The BSN continuously monitors all session-contexts of each connected device and terminates the connection if any of its session-contexts is invalidated. The invalidation of a session-context could occur actively if receives a user command or detects a specific context. It could also occur passively if the detached state holds on for too long or when communication has broken down between the user and device.

F. Preliminary Experiments

We build a prototype system to investigate the importance of context-based user access. The BSN platform consists of one PDA-class device as base station, one dual-radio node as gateway, and one accelerometer as wearable sensor. The public shared device is emulated by mounting three wireless sensor nodes (LED, SpO2, and Accelerometer) on an elliptical trainer. Both Bluetooth and IEEE802.15.4/Zigbee radios are used in the system to demonstrate the access between two popular technologies. Cellular phones with Bluetooth capability are the prevalent devices a user may possess. Sensor nodes with IEEE802.15.4/Zigbee radio are the popular candidates for wearable devices due to their low-power design. The system architecture is shown in Figure 14.

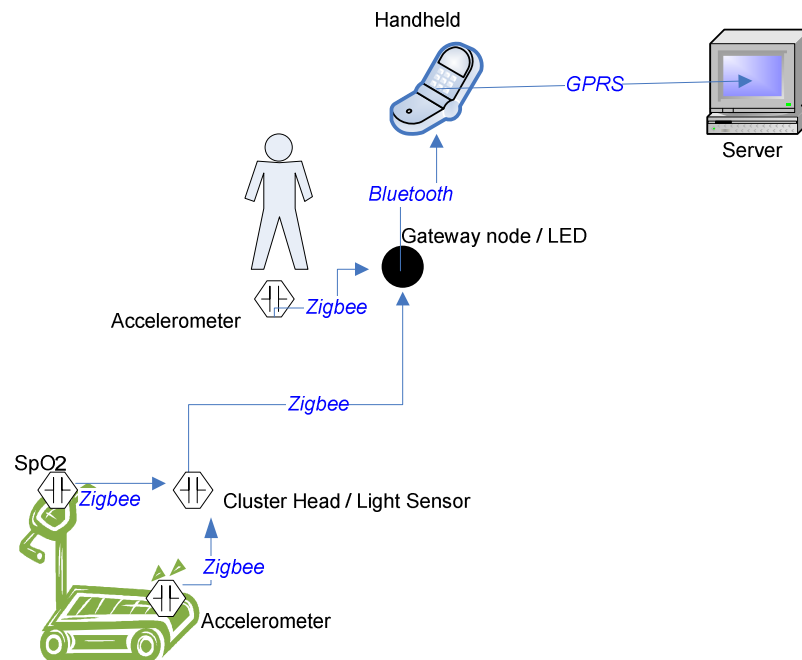


Figure 14: The Architecture of Prototype System

Schedules

The author expects to finish the proposed researches within one year. For the extension of approximate data collection algorithms, we expect completing analysis on June, conducting experiments, publishing the work on July and August. The author develops the algorithms on September and summarizes the proposed researches with an implementation of the system on October. The system uses the amount of information collected as a control knob to explore trade-off among accuracy, energy cost, and storage. We present and submit the results on November and December. For context-based user access, we are developing the prototype system and anticipate the first version in March. The author conducts the experiment on April. In summer, we investigate the key components of context-based user access mechanisms including defining contexts and context matching rules. We submit the final results next fall for publishing. Based on this proposal, the author expects to finish the dissertation next spring.

References

1. C. Intanagonwiwat, R. Govindan, and D. Estrin., "Directed diffusion: A scalable and robust communication paradigm for sensor networks," *Proc of ACM MOBICOM*, 2000.
2. A. Skordylis, N. Trigoni and A. Guitton, "A Study of Approximate Data Management Techniques for Sensor Networks," *Proc of the 4th Workshop on Intelligent Solutions in Embedded Systems*, 2006.
3. D. Chu, A. Deshpande, J. M. Hellerstein, and W. Hong, "Approximate Data Collection in Sensor Networks using Probabilistic Models," *Proceedings of the 22nd International Conf. on Data Engineering (ICDE)*, 2006.
4. A. Deshpande, C. Guestrin, S. Madden, J. Hellerstein, and W. Hong. "Model-driven data acquisition in sensor networks," *In the 30th International Conf on Very Large Data Bases (VLDB)*, 2004.
5. A. Jain, E. Chang, and Y.-F.Wang. "Adaptive stream resource management using Kalman Filters," *Proceedings of the 2004 ACM SIGMOD international conference on Management of data*, 2004.
6. I. Lazaridis and S. Mehrotra. "Capturing sensor-generated time series with quality guarantees," *Proceedings of the 19th International Conf. on Data Engineering (ICDE)*, 2003.
7. W.H. Wu, A.A.T. Bui, M.A. Batalin, L.K. Au, J.D. Binney, and W.J. Kaiser, "MEDIC: Medical Embedded Device for Individualized Care," *Artificial Intelligence in Medicine* (2006 submitted).
8. Y. Yao and J. Gehrke. "The Cougar approach to in-network query processing in sensor networks," *ACM SIGMOD record*, 2002.
9. S. Madden, M. J. Franklin, J. M. Hellerstein, W. Hong. "TinyDB: an acquisitional query processing system for sensor networks," *ACM Transactions on Database Systems (TODS)*, 2005.
10. W.H. Wu, A.A.T. Bui, M.A. Batalin, D. Liu, and W.J. Kaiser, "Incremental Diagnosis Method for Intelligent Wearable Sensor Systems," *IEEE Trans Info Technol Biomed* (2006 accepted).
11. Richard E. Neapolitan, "*Learning Bayesian Networks*", Prentice Hall, 2004.
12. Nokia 770, <http://www.nokiausa.com/770>
13. BlueSentry, <http://www.gridenabled.com/bluesentry.html>
14. Netica, <http://www.norsys.com/>

15. Trained Bayesian Network,
<http://www.ee.ucla.edu/~dcjea/researches/drc/TrainedBayesNet.jpg>
16. American Heart Association,
<http://www.americanheart.org/presenter.jhtml?identifier=4472>
17. N. Kern, B. Schiele, and A. Schmidt, "Multi-sensor activity context detection for wearable computing," *Proc. of Eur. Symp. on Ambient Intelligence (EUSAI)*, pp. 220-232, November 2003.
18. P. Korpip, M. Koskinen, J. Peltola, S. Mkel, and T. Seppnen, "Bayesian approach to sensor-based context awareness," *Personal and Ubiquitous Comp. J*, vol. 7, pp. 113-124, February 2003.
19. Y. Du, F. Chen, W. Xu, and Y. Li, "Recognizing Interaction Activities using Dynamic Bayesian Network," *Proceedings of the 18th International Conference on Pattern Recognition (ICPR'06)*, 2006.
20. M. D. Corner, and B. D. Noble, "Zero-Interaction Authentication," *Proceedings of Eighth Annual International Conference on Mobile Computing and Networking (Mobicom)*, 2002, pp. 23-28.
21. J. E. Bardram, R. E. Kjær, and M. Pedersen. "Context-Aware User Authentication – Supporting Proximity-Based Login in Pervasive Computing," *Proceedings of Fifth International Conference on Ubiquitous Computing (UbiComp)*, LNCS 2864, Springer, 2003, pp. 107-123.
22. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," *IEEE Computer 29(2)*, IEEE Press, 1996, pp. 38-47.
23. D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to Strangers: Authentication in Ad-Hoc Wireless Networks," *Proceedings of Network and Distributed System Security Symposium (NDSS)*, Internet Society, 2002, pp. 23-35.
24. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," *Proceedings of the 7th International Workshop on Security Protocols*, LNCS 1796, Springer, 1999, pp. 172-194.
25. S. K. S. Gupta, T. Mukherjee, K. Venkatasubramanian, and T. Taylor, "Proximity Based Access Control in Smart-Emergency Departments," *Proceedings of 4th IEEE Conference on Pervasive Computing Workshops, First Workshop On Ubiquitous & Pervasive Health Care (UbiCare)*, 2006, pp. 512-516.
26. L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. W. Gellersen, "Smart-Its Friends: A Technique for Users to Easily Establish Connections between Artefacts," *Proceedings of Third International*

- Conference on Ubiquitous Computing (Ubicomp)*, LNCS 2201, Springer, 2001, pp.116-122.
27. S. M. Bellare and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," *Proceedings of the IEEE Symposium on Security and Privacy*, 1992, pp. 72-84.
 28. MJ Moyer, M Ahamad, "Generalized Role-Based Access Control," *Proceedings of the 21st IEEE International Conference on Distributed Computing System*, 2001, pp. 391-398.
 29. G. Zhang and M. Parashar, "Context-Aware Dynamic Access Control for Pervasive Applications," *Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, 2004, pp. 219-225.
 30. H. Wang, Y. Zhang, J. Cao, "Ubiquitous Computing Environments and Its Usage Access Control," *Proceedings of the 1st international conference on Scalable information systems*, 2006, Article No. 6.