Dynamic Authentication with Sensory Information for the Access Control Systems

Yuanchao Shu, *Student Member*, *IEEE*, Yu (Jason) Gu, *Member*, *IEEE*, and Jiming Chen, *Senior Member*, *IEEE*

Abstract—Access card authentication is critical and essential for many modern access control systems, which have been widely deployed in various government, commercial, and residential environments. However, due to the static identification information exchange among the access cards and access control clients, it is very challenging to fight against access control system breaches due to reasons such as loss, stolen or unauthorized duplications of the access cards. Although advanced biometric authentication methods such as fingerprint and iris identification can further identify the user who is requesting authorization, they incur high system costs and access privileges cannot be transferred among trusted users. In this work, we introduce a dynamic authentication with sensory information for the access control systems. By combining sensory information obtained from onboard sensors on the access cards as well as the original encoded identification information, we are able to effectively tackle the problems such as access card loss, stolen, and duplication. Our solution is backward-compatible with existing access control systems and significantly increases the key spaces for authentication. We theoretically demonstrate the potential key space increases with sensory information of different sensors and empirically demonstrate simple rotations can increase key space by more than 1,000,000 times with an authentication accuracy of 90 percent. We performed extensive simulations under various environment settings and implemented our design on WISP to experimentally verify the system performance.

Index Terms—Authentication, sensory data, access control system, wireless rechargeable sensor

1 Introduction

Access control is a mechanism that enables an authority to control access to restricted areas and resources at a given physical facility or computer-based information system. In general, authentication methods in access control systems can be divided into two broad categories. The first category is based on mechanical matching, such as keys and combination locks. Individuals are authenticated in these access control systems if and only if the blade of the key matches the keyway of the lock or the correct numerical sequence for combination lock has been dialed. Due to the physical constraints of mechanical matching systems, they are insufficient to meet the demanding requirements of access control authentication for critical infrastructures. On the other hand, it is also very hard to frequently change the interior structure of such matching mechanisms for security enhancement.

The other category of authentication for access control systems is electronic authentication including barcode, magnetic stripe, biometrics, and so on. Compared with mechanical matching authentications, the electronic authentications such as RFID-based smart card offer much more convenience and flexibility for both administrators and users of access control systems. However, it still suffers from similar problem of key loss because authentication is only based on the encoded identification data on the card. Anyone who carries the card will be granted the access and the security of the system still can be compromised.

To further enhance the security of access control systems, various biometric authentication mechanisms have been introduced to identify the authorized personnel. Although these biometric authentication methods such as fingerprint, iris, and voice recognitions are able to provide personal identification, they have high infrastructure cost and access privileges cannot be transferred among trusted users.

In this work, we aim at bridging the gap between insufficiency of existing electronic authentication solutions and the increasing demand of high-security guarantee for access control systems. We design a novel electronic proximity authentication framework that enhances the security level of existing RFID-based access control systems with backward compatibility. Specifically, we add dynamic data into the traditional authentication information by using sensors such as accelerometer, gyroscope, and so on. This authentication framework is adaptive to the change of encryption complexity of the access control systems and could be adopted with minor modification of existing infrastructure. In summary, on top of the previous conference paper [1], our contributions in this work are as follows:

- We design and implement a dynamic authentication framework with sensory information for the access

- *Y. Shu and J. Chen are with the State Key Laboratory of Industrial Control Technology, Department of Control Science and Engineering, Zhejiang University, Zheda road 38#, Hangzhou 310027, Zhejiang, China. E-mail: ycshu@zju.edu.cn, jmchen@iipc.zju.edu.cn.*
- *Y.(J.) Gu is with the Pillar of Information System Technology and Design, Singapore University of Technology and Design, 20 Dover Drive, Singapore 138682. E-mail: jasongu@sutd.edu.sg.*

Manuscript received 17 Sept. 2012; revised 25 Apr. 2013; accepted 20 May 2013; published online 29 May 2013.
Recommended for acceptance by X. Li, P. McDaniel, R. Poovendran, and G. Wang.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2012-09-0958.
Digital Object Identifier no. 10.1109/TPDS.2013.153.

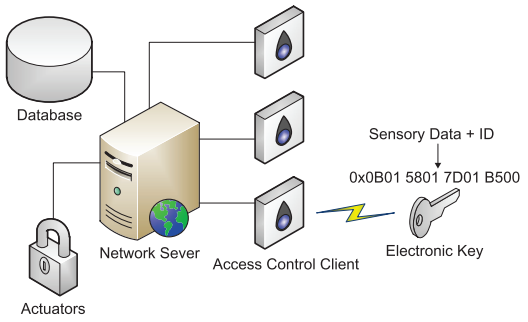


Fig. 1. System function diagram.

control systems. Our design is backward compatible with existing, deployed RFID or access card readers.

- We demonstrate the proposed framework with two case studies and theoretically prove that our dynamic authentication significantly increases the key space for proximity authentication systems with the integration of low-cost sensors.
- We have fully implemented and built a running prototype of the proposed dynamic authentication framework on the Intel Wireless Identification and Sensing Platform (WISP). Based on the running prototype, we have extensively evaluated our design in terms of system accuracy and usability in real-world settings.

The remainder of this paper is organized as follows: First we propose the dynamic authentication framework with sensory information in Section 2. We then provide authentication algorithms of our system in Section 3. System working performance and simulations of the authentication method are shown in Sections 4 and 5. Comparison between the proposed two reference designs is given in Section 6. We discuss related work in Section 7 and conclude in Section 8.

2 Design of the Dynamic Authentication with Sensory Information

The existing electronic proximity authentication of access control systems is mainly based on the exchange of encoded identification information stored on the access card. The security and integrity of such static and passive authentication mechanisms suffer from problems such as access card loss and unauthorized duplications. In this work, we propose to use sensory information obtained from wireless rechargeable sensors on access cards to further enhance the security and robustness of existing electronic proximity authentication systems. The main idea of our system design is shown in Fig. 1. When an access card integrated with wireless rechargeable sensors enters the communication range of an access control client, the access card piggybacks its sensory data to conventional identification information and transmits it (i.e., the electronic key) to the access control client. The information received by the access control client is then forwarded to the network server for authentication. If both sensory data and identification match a valid record in the authentication database, the network server then instruments the actuator and grants the card holder the access to the system. In this way, even an authentic access card is in possession of an unauthorized personnel or has been illegally duplicated, as long as the unauthorized card holder does not know how to generate the correct sensory data, he or she still cannot access the system. Moreover, we successfully remove the system vulnerable period between loss/stolen of access card and the deactivation of the card after users' report. On the contrary, trusted users can share the cards and predefined actions with each other, which is unavailable in biometric authentication systems.

Different from existing authentication methods such as combining RFID and an additional keypad near the reader, we propose an orthogonal design in this paper and the new authentication framework only revises authentication algorithm on the network server without any modification of access clients. In fact, because we piggyback sensory data to ID information before transmitting them to the reader, most existing works on communication encryption for RFID system can be easily adopted into our authentication method [2], [3], [4], and therefore deal with several security vulnerabilities such as replay attack and eavesdropping.

The identification information on access cards normally are static. With the addition of dynamic sensory data from onboard sensors, we are able to significantly increase the security key space P and hence the security level for existing electronic authentication systems. A wide variety of sensors including accelerometer, gyroscope, and so on can be used in our system. To illustrate the basic concept and the resulting security enhancement of our sensory data enhanced access control system design, we use both three-axis accelerometer and gyroscope as examples in the following sections. In particular, we utilize the sensory data generated from the rotation of accelerometer and gyroscope to introduce reference designs for the proposed sensory data enhanced authentication scheme. Through our prototyping system and real-world experiments, we demonstrate such a rotation-based design is a feasible and practical option for the proposed generic dynamic authentication framework.

2.1 Accelerometer-Based Reference Design

2.1.1 Two-Dimensional Rotation

For an accelerometer, if it is being rotated, the static acceleration of gravity on its three axes will change accordingly. For a two-dimensional rotation, we can calculate the tilt angle α of an accelerometer from static acceleration of gravity on its X- and Y-axes to determine the position of the accelerometer in a two-dimensional plane.

In Fig. 2, we illustrate a simple example on how to determine the position of an accelerometer. In Fig. 2, A_x and A_y are acceleration components of gravity on X- and Y-axes, respectively. The tilt angle α can then be calculated by equation $A_x = Gcos\alpha$ and $A_y = Gsin\alpha$, where G is the static acceleration of gravity. We define the most basic rules and parameters for two-dimensional rotations, which can be used to express more complex rotation actions:

- *Basic rotation rules:*
  - For all rotations, they are two dimensional.
  - The basic rotation is omnidirectional, either clockwise or counterclockwise.

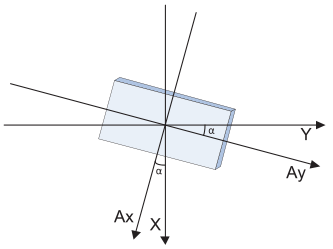


Fig. 2. Accelerometer rotation example.

- The new rotation starts from the end position of the previous one.
- Any single basic rotation does not exceed 2π degrees.

- *Basic rotation parameters:*
  - *Granularity of the Rotation Recognition* n. Every two different static positions with their tilt degree gap bigger than $(2\pi/n)$ can be identified and n refers to the maximal number of recognizable rotations within one round. The granularity of recognition indicates the sensing capability of angle degree fluctuation.
  - *The Number of Basic Rotations* k. The number of basic actions performed in one rotation sequence. Basic rotation number reveals the complexity of encryption.

Fig. 3 shows an example of rotation sequence with three basic rotations ($k = 3$) and granularity of the recognition $n = 8$. CW and CCW in Fig. 3 denotes clockwise and counterclockwise, respectively. In Fig. 3, initially the accelerometer is tilted $\frac{\pi}{4}$ degree to the Y-axis. Then, the accelerometer is rotated $\frac{\pi}{2}$ degree clockwise, $\frac{3\pi}{2}$ degrees counterclockwise, and $\frac{5\pi}{4}$ degrees clockwise, respectively. All rotations are in line with basic rotation rules defined above.

Based on definitions above, we can represent the multitude of the key space increase for a two-dimensional rotation by the following equation:

$$P_{acc}^{2D}(n,k) = n[2(n-1)]^k. \quad (1)$$

In (1), n denotes the number of different possible starting positions for the first basic rotation. Then, for the following k rotations, we just need to determine the direction, we can

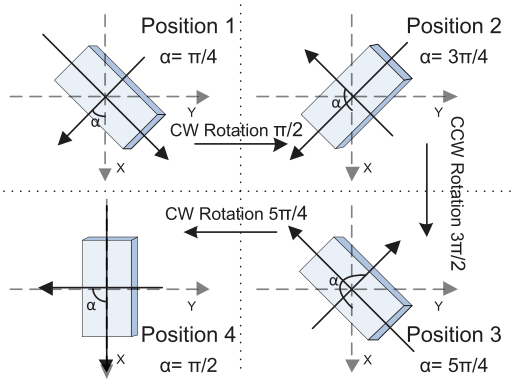
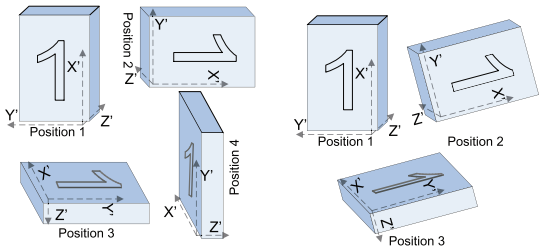


Fig. 3. Rotation sequence diagram (2D).



(a) Valid 3D Rotation (b) Invalid 3D Rotation

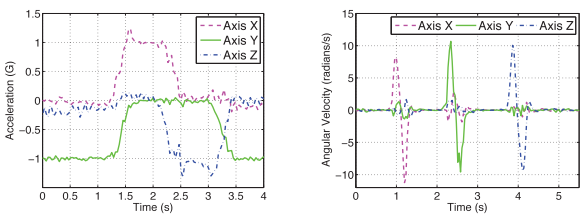
Fig. 4. Rotation sequence diagram (3D).

either clockwise or counterclockwise rotate the accelerometer to all other $n-1$ possible positions.

2.1.2 Three-Dimensional Rotation

In this part, we extend our design to rotations in three-dimensional space. Since determining the attitude of sensor solely based upon static acceleration of gravity is impossible (imagine standing and holding your cell phone face to you, the values of accelerometer at cell phone will not change if you turn from the west to the north). Based on the relative positions of the accelerometer and the ground, we extend the basic two-dimensional rotation rules for three-dimensional rotations: 1) During the whole rotation process, either plane XY, YZ or XZ under the coordinate of accelerometer is perpendicular to the ground 2) Accelerometer only rotates in one plane under its own coordinate (XY, XZ or YZ) during one basic rotation; 3) Rotation in a different plane is allowed if one axis among $\pm X$, $\pm Y$ or $\pm Z$ of the accelerometer is perpendicular to the ground at the end of the previous basic rotation.

Fig. 4a demonstrates an example of a 3D rotation sequence follows the rules above with $k = 3$ basic rotations. We coplot the coordinate of the accelerometer to illustrate 3D rotations. In Fig. 4a, each action between two consecutive positions is a plane rotation, and rotation plane could changes only when the direction of static acceleration of gravity is consistent with the direction of axes in accelerometer's coordinate. For example, Position 2 rotates to Position 3 in Fig. 4b is prohibited while Position 1 rotates to Position 2 in Fig. 4a is likely to happen if the granularity of the rotation recognition $n = 4$. Corresponding sample data of this three-dimensional rotation are shown in Fig. 5a. In Fig. 5a, it could be found that values at each axis of the accelerometer change in different ways during the rotation process, therefore, offer great opportunities for sensory information-based authentication design.



(a) 3D Rotations of an Accelerometer (b) Standard Rotations of a Gyroscope

Fig. 5. Sample data of rotations of accelerometer and gyroscope.

TABLE 1
Key Space of the Accelerometer-Based Reference Design

	$n=4,\ k=3$	$n=4,\ k=5$	$n=4,\ k=8$	$n=8,\ k=3$	$n=8,\ k=5$	$n=8,\ k=8$
2D Key Space	864	31104	6718464	21952	4302592	1.18×10^{10}
3D Key Space	10368	1492992	2.58×10^{9}	145824	6.25×10^{7}	5.55×10^{11}

On the basis of the rules above, the starting position of each basic rotation can be divided into two types on whether one of axis $\pm X$, $\pm Y$, and $\pm Z$ is perpendicular to the ground at the beginning of the basic rotation. According to the third rule, if one of the axes is consistent with the direction of gravity, the following action can occur in two different planes. However, in the other case, the following basic rotation can only generated within a fixed plane. We define two different series a_k and b_k that equals to key spaces of these two cases, respectively, after k basic rotations with a given granularity of the rotation recognition n. The total key space of rotation in three-dimensional space and the recursive formula of a_k and b_k can be written as

$$P_{acc}^{3D}(n,k) = a_{k+1} + b_{k+1}, \tag{2}$$

where

$$\begin{aligned} a_{k+1} &= 2\cdot 2\cdot 3\cdot a_k + 2\cdot 4\cdot b_k \\ b_{k+1} &= 2\cdot 2\cdot (n-4)\cdot a_k + 2\cdot (n-5)\cdot b_k \\ n &= 4m, m \geq 1 \in \mathbb{N}, \end{aligned} \tag{3}$$

with the initial value $a_0 = 6$ and $b_0 = 3(n-4), n = 4m$, $m \geq 1 \in \mathbb{N}$.

Recursive formulas of both a_k and b_k in (3) consist of two parts that calculate key spaces under different initial positions of the accelerometer. For example, for a_k, $2\cdot 2\cdot 3$ mean two feasible directions, two feasible planes, and three feasible end positions of one basic rotation, respectively.

In Table 1, we summarize key spaces for both two-dimensional and three-dimensional rotations with different numbers of basic rotations k and the granularity of recognition n. From this table, we can see with just such simple rotations, we can significantly increase the key space for access authentication systems and, therefore, increase the security level of the systems. For example, even for two-dimensional rotation, with the number of basic rotations increases from k to $k+1$, the key space will be multiplied by $P_{acc}^{2D}(n,k+1)/P_{acc}^{2D}(n,k) = 2n-2$. If $n=4$, which is a relatively small value, by just adding one simple basic rotation, the key space will increase sixfold. In addition, because we piggyback sensory data to the original underlying identification information on the card, encryption complexity improvement of the conventional identification information will equally increase system security level under our dynamic authentication mechanism.

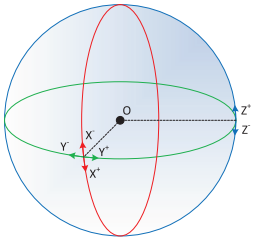


Fig. 6. Standard rotations of a gyroscope.

2.2 Gyroscope-Based Reference Design

Gyroscope is a device for measuring change of orientation. Therefore, it is also possible to utilize the action of rotation of a gyroscope in a three-dimensional space because it returns the angular velocity on each axis simultaneous when rotating. Imaging there is a ball with center of O, Fig. 6 depicts six standard rotations of the ball using vectors. Corresponding sensory data of the six basic rotations of a typical three-axis gyroscope is shown in Fig. 5b.

Different from accelerometer-based design that relies on precise rotations, higher rotation speed of the gyroscope leads to a higher output value that make it easier for authentication. It can be seen in Fig. 5b that different standard rotations of a gyroscope can be easily differentiated from when the gyroscope remains standstill through the amplitude of the angular velocity. In this gyroscope-based reference design, we only use such binary rotation information (whether rotated) at each axis to perform sensory-data-based authentication.

Similar to the accelerometer-based reference design, a whole rotation process in the gyroscope-based design consists of k basic rotations as well. However, the granularity of the rotation recognition n in Section 2.1 is no longer used as we do not calculate the accurate degree of each rotation. For the sake of simplicity in presentation, we assume that at most values on two axes among axes X, Y, and Z change during each basic rotation. Therefore, the key space increase can be written as

$$P_{gyro}(k) = \left[3\cdot 2 + \binom{2}{3}\cdot 2\cdot 2\right]^k = 18^k. \tag{4}$$

The base of (4) consists of two parts that compute the composition of feasible rotation directions of one basic rotation. Since the gyroscope has three axes and it can rotate on each axis with two directions, there are $3\cdot 2$ feasible rotation directions if the gyroscope rotates on one axis. If values on two axes change during a basic rotation, the total feasible rotation directions can be written as $\binom{2}{3}\cdot 2\cdot 2$.

Key space of the gyroscope-based reference design is summarized in Table 2. It can be seen in Table 2 that even only using the six standard rotation directions, we can significantly increase the key space with increasing

TABLE 2
Key Space of the Gyroscope-Based Reference Design

	$k=2$	$k=4$	$k=6$	$k=8$	$k=10$
Key Space	324	104976	3.4×10^{7}	1.1×10^{10}	3.6×10^{12}

numbers of basic rotations. For example, when the number of basic rotations $k = 8$, key space of the gyroscope-based reference design is larger than 3D rotation of the accelerometer (1.1×10^{10} versus 2.58×10^{9}).

3 Rotation Recognition

In the previous section, we discuss the potential of large key space increase for our dynamic authentication with sensory information design. In this section, we further elaborate on the detailed sensor rotation recognition algorithms.

By comparing the sample data of accelerometer (Fig. 5a) and gyroscope (Fig. 5b), we find that output of the accelerometer exhibits a more complex behavior. This is because gyroscope measures the angular velocity and tends to generate impulses during one single basic rotation, which could be treated as a special case of the output of the accelerometer. Therefore, in this section, we use the sensory data of accelerometer to illustrate the whole rotation recognition algorithms and discuss how to deal with the sensory data of gyroscope in Section 3.4.

One complete dynamic authentication process consists of a sequence of basic rotations. To accurately identify each individual basic rotation from raw accelerometer data, we perform following three operations in the network server.

3.1 Data Preprocessing

The first step of rotation recognition is data preprocessing. The main goals are to separate and filter each individual basic rotation from a series of raw accelerometer data.

To separate the individual basic rotations, we first need to identify the pause between two consecutive rotations. During such pauses, the three-axis readings of an accelerometer would remain relatively stable and unchanged for a short period of time. To accurately recognize such pauses and separate different basic rotations, we adopt a *sliding window* approach. In this approach, the accelerometer readings in the first t_w second are buffered into the sliding window. All data in the sliding window are then fitted by a first-order polynomial function. If the coefficient of first-order polynomial is less than a threshold (one in our implementation), we consider the accelerometer remain stationary within the time frame of this window. Followed by this pause detection in the current window, the window would slide for a step of t_s seconds, with t_s duration of new data appended to the end of the sliding window while the first t_s duration of sensory data are discarded. Empirically, we set $t_w = 1$ s and $t_s = 0.3$ s in our system implementation. In this way, we have achieved accurate separation of basic rotations in one complete authentication. To visualize above data preprocessing step, Fig. 7 shows one authentication with four basic rotations that performed slowly on our prototype implementation. The shaded regions represent sliding windows at three pauses. Clearly from Fig. 7, it can be found that the accelerations on three axes of the accelerometer are rather stable during pauses between different basic rotations.

After identifying pauses between basic rotations, we then use least square estimation to fit the raw readings for each individual basic rotation from the accelerometer.

Assuming the accelerometer readings for one basic rotation on one of the three axes is

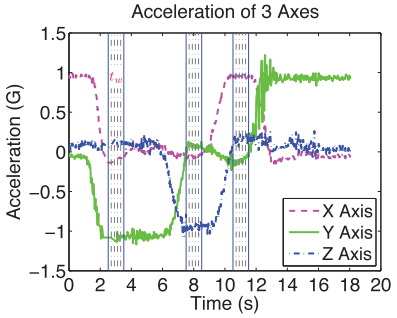


Fig. 7. Example sensory data of a 3D rotation.

$$p_i = (x_i, y_i), i = 0, 1, 2, \ldots, m.$$

Then, the least square estimation tries to build a polynomial function below:

$$y = f(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_{m-1} x + b, \tag{5}$$

such that

$$\begin{aligned} min(F(\boldsymbol{a}_k, b)) &= min\left(\sum (f(x_i) - p_i)^2\right) \\ &= min\left(\sum_{i=0}^{m} (f(x_i) - p_i)^2\right) \\ k &= 0, \ldots, m-1. \end{aligned} \tag{6}$$

In Section 4, we discuss fitting effect in detail and make the decision of m through prototype experiments.

3.2 Feature Vector Extraction

After separating basic rotations for one single authentication, we match them with standard feature vectors. As feature-based classification of time-series data has a simple model and lower computation, we choose this method for rotation recognitions. First, feature vectors (F-vectors) for each individual basic rotations are extracted based on their fitting functions created in the previous section. Specifically, we extract the start and end sensory data, the maximal and minimal sensor readings, and the corresponding time of these events within one basic rotation. Then, for a three-axis accelerometer, we can represent their feature vectors using the following set of equations:

$$\begin{aligned} \boldsymbol{T}_x &= \{\boldsymbol{v}_x\} = \{\boldsymbol{v}_{x\_start}, \boldsymbol{v}_{x\_end}, \boldsymbol{v}_{x\_max}, \boldsymbol{v}_{x\_min}\}, \\ \boldsymbol{T}_y &= \{\boldsymbol{v}_y\} = \{\boldsymbol{v}_{y\_start}, \boldsymbol{v}_{y\_end}, \boldsymbol{v}_{y\_max}, \boldsymbol{v}_{y\_min}\}, \\ \boldsymbol{T}_z &= \{\boldsymbol{v}_z\} = \{\boldsymbol{v}_{z\_start}, \boldsymbol{v}_{z\_end}, \boldsymbol{v}_{z\_max}, \boldsymbol{v}_{z\_min}\}, \\ \boldsymbol{v} &\in \mathbb{R}^2, \end{aligned}$$

where $\boldsymbol{v} = (value, time)$ is a vector consisting of fitted acceleration value and its relative time within one basic rotation.

3.3 F-Vectors Matching

After extracting feature vectors, we then try to match them with standard feature vectors in the database to recognize a specific basic rotation. Standard feature vectors with given n could be mathematically calculated and automatically generated since the acceleration components on three axes represent a trigonometric relationship with acceleration of gravity. Taking the rotation in Fig. 2 as an example, after the

accelerometer clockwise rotates π degrees, the acceleration components A_x and A_y during such rotation can be calculated as $A_x = Gcos\theta$ and $A_y = Gsin\theta$ ($\theta \in [\alpha, \alpha + \pi]$). Therefore, it is easy for users to reset their keys without any modification on access cards.

To match extracted F-vectors of a basic rotation to standard ones in database, we use euclidean distance to measure the closeness of these two vectors. Specifically, we use following set of equations for three axes:

$$d_x = |\boldsymbol{T}_x - \boldsymbol{S}_x|,$$
$$d_y = |\boldsymbol{T}_y - \boldsymbol{S}_y|,$$
$$d_z = |\boldsymbol{T}_z - \boldsymbol{S}_z|,$$

where

$$\boldsymbol{S}_x = \{\bar{\boldsymbol{v}}_x\} = \{\bar{\boldsymbol{v}}_{x\_start}, \bar{\boldsymbol{v}}_{x\_end}, \bar{\boldsymbol{v}}_{x\_max}, \bar{\boldsymbol{v}}_{x\_min}\},$$
$$\boldsymbol{S}_y = \{\bar{\boldsymbol{v}}_y\} = \{\bar{\boldsymbol{v}}_{y\_start}, \bar{\boldsymbol{v}}_{y\_end}, \bar{\boldsymbol{v}}_{y\_max}, \bar{\boldsymbol{v}}_{y\_min}\},$$
$$\boldsymbol{S}_z = \{\bar{\boldsymbol{v}}_z\} = \{\bar{\boldsymbol{v}}_{z\_start}, \bar{\boldsymbol{v}}_{z\_end}, \bar{\boldsymbol{v}}_{z\_max}, \bar{\boldsymbol{v}}_{z\_min}\}.$$

The closeness between the extracted feature vector and a standard feature vector then can be expressed as

$$R = \max\left(\frac{1}{d_x + d_y + d_z}\right).$$

To identify a basic rotation from the extracted feature vector, we choose the one that has the maximal R value for a corresponding standard feature vector.

3.4 Discussion of Gyroscope-Based Design

Since a rotation process in gyroscope-based design also consists of several basic rotations, the first operation of data pre-processing presented in Section 3.1 can be used without any modification. In feature vector extraction, we only need to extract the maximal sensor readings on each axis because there is only one impulse during a basic rotation. After constructing the standard feature vectors of limited rotations of the gyroscope (e.g., six standard rotations), F-vector matching can be accomplished identically to the accelerometer-based design.

Note that methodology of rotation recognition is not limited to the feature-based classification. For example, one can calculate distance between sensory measurements and sensory data of standard rotations through dynamic time warping to recognize basic rotations, and online learning of the timing parameters in the data preprocessing step could also use to improve the recognition performance. In addition, methodologies used in gesture recognition can also be borrowed [5], [6], [7], [8]. Although they may have higher computation complexity, they will not affect the essence of the dynamic authentication framework.

4 Testbed Evaluation

To evaluate the proposed dynamic authentication method, a prototype system is built based on the Intel Wireless Identification and Sensing Platform [9]. WISP is a fully passive ultrahigh-frequency (UHF) RFID tag that integrates an ultralow-power processor and several low-power sensors such as temperature sensor and accelerometer. Through WISP's antenna, the signal from standard UHF RFID readers can be used for both communication and powering the entire WISP [10].

Fig. 8. Antenna-reshaped WISP tag and reader.

In the prototype system, an antenna-reshaped WISP tag equipped with an accelerometer is integrated onto a standard access card. WISP tags we use are backward-compatible with existing RFID standards and hardware. Therefore, they can be powered and read by any unmodified, commercially available UHF RFID readers. We use Impinj Speedway Reader IPJ-R1000 as RFID access control client, which provides network connectivity between WISP tags and back-end authentication computer servers. Fig. 8 is a picture of our prototype system. Further insights of the system are presented in Appendix, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.153.

Since the current WISP does not have an embedded gyroscope, we test the accelerometer-based design exclusively on the prototype system. However, by modifying the hardware, gyroscope can be integrated onto WISP as well. In this paper, we conduct experiments on an iPhone 4 to evaluate the gyroscope-based design and summarize the authentication results in Appendix B, available in the online supplemental material.

4.1 Evaluation of the Accelerometer-Based Design

Both authentication accuracy and delay are two most essential factors for practical access control systems. In this section, we comprehensively study the accuracy of our rotation recognition algorithm on identifying a series of basic rotations performed by users for system authentication with one single accelerometer. Specifically, we define accuracy rate of the system authentication as the percentage of complex rotations that have been correctly recognized for system authentication algorithm. During the experiment, we also record rotation delay which refers to the duration of a complete action and the accuracy rate of authentication with varying number of basic rotations k under two different granularity of recognition n. In experiments, predefined rotations are randomly generated by the computer and then performed by users. Due to the space constraint, we only present two-dimensional authentication evaluation and analysis in the main file. Experimental results of three-dimensional rotations can be found in Appendix C, available in the online supplemental material.

4.1.1 Accuracy Rate of the System Authentication

First, a total of 600 basic rotations are performed by one user. The experiment results are summarized in Table 3.

TABLE 3
Accuracy Rate versus Different k and n

	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
$n=4$	100%	93.3%	91.7%	90.0%	86.7%
$n=8$	100%	91.7%	90.0%	90.0%	83.3%
Delay	1.9s	4.7s	7.7s	10.5s	13.3s

It can be found in Table 3 that as the number of basic rotations k and the granularity of rotation recognition n increase, the accuracy rate decreases. This is because when the granularity of recognition increases, the likelihood of mismatching two different basic rotations also increases. In addition, as the number of basic rotations increases, the false negative rate will sum up and lead to a lower accuracy rate. From the last line of Table 3, it can be found that the delay of rotation grows almost linearly but even when the number of basic rotations $k=5$, delay including breaks in between each basic rotations is no more than 15 s. By improving hardware design and optimizing authentication algorithm, delay could be further reduced.

To evaluate the practicability of our design for daily usage, we also conduct experiments among different users. The results can be found in Section 4.1.3.

4.1.2 System Performance with Dual Accelerometers

During single-sensor experiments, we observed there exists severe sensory data loss between the WISP and reader. This is because quality of energy harvesting and communication between WISP and reader cannot be always guaranteed during rotation process. Particularly, we call continuous data loss in a period of time as the data fracture. To reduce the impact of data loss, we orthogonally placed two WISPs onto one smart card. In this way, two different orientated antennae ensure a more stable power supply and data transmission within the entire space. Data from two different accelerometers are complementary and consolidated for authentication. Same set of experiments for single sensor have been done with dual accelerometers. Results are shown in Table 4 (line of delay is omitted as there is no difference with single accelerometers).

From Table 4, compared with single sensor experiments, it can be found that authentication accuracy rate increased effectively in dual-sensor situation where two accelerometers work at the same time. Specifically, compare Table 4 with Table 3, when the granularity of recognition $n=4$, accuracy rates are all higher than 95 percent with dual accelerometers while 80 percent under single accelerometer situation is below 95 percent.

4.1.3 System Performance among Different Users

In the first experiment, 50 complex rotations under each number of basic rotations k are designated to five users.

TABLE 4
Accuracy Rate versus Different k and n with Dual Accelerometers

	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
$n=4$	100%	100%	95%	95.0%	95.0%
$n=8$	100%	95.0%	90.0%	90.0%	90.0%

TABLE 5
Accuracy Rate versus Different Users ($n=4$)

	k=1	k=2	k=3	k=4	k=5
User #1	100%	100%	90.0%	86.0%	78.0%
User #2	94.0%	92.0%	84.0%	72.0%	74.0%
User #3	98.0%	92.0%	82.0%	82.0%	70.0%
User #4	100%	98.0%	92.0%	84.0%	80.0%
User #5	98.0%	88.0%	76.0%	82.0%	72.0%

Experiments with both single and dual accelerometers are conducted.

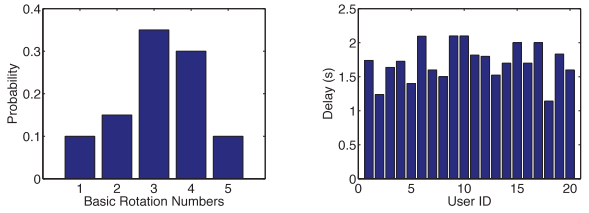
Accuracy rates of authentication with single accelerometer for each users are reported in Table 5. From Table 5, we can see individual accuracy rate varies. When $k=1$ and $k=2$, average accuracy rate are higher than 90 percent (98 and 94 percent, respectively), while most of accuracy rates when $k>4$ are below 80 percent, which means an error exists in every five certification processes. Among different users, when $k=3$, the variance of accuracy rate $\sigma=32.96$, which is the highest among five columns. However, variances of accuracy rate are below 20 when $k<3$. From results shown in Table 5, system achieves high security level on both average accuracy rate and variance when $k\leq 2$ if $n=4$.

Experimental results with dual accelerometers are shown in Table 6. In Table 6, average accuracy rates of all five columns are higher than 95 percent while in single accelerometer experiment, accuracy rates in 14 of 25 cases are below 90 percent and the worst case of accuracy rate is as low as 70 percent, which is occurred when user 3 performs a five basic-rotation authentication. Experimental results shown in Table 1 demonstrate our proposed method could increase the key space by more than 30,000 times with a high enough accuracy rate of authentication. Besides, accuracy rates among different users are much more stable in Table 6. With dual accelerometers, all accuracy rate variances among five distinct k are below 7.5 and average variance of different k is 71.8 percent less than that of single sensor (5.312 versus 18.816).

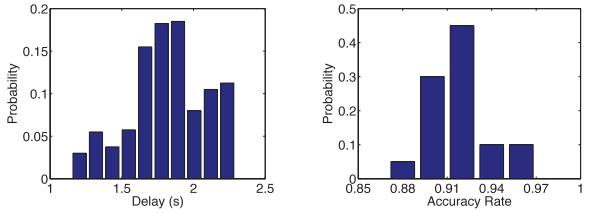
To further verify the practicability of our system, we conduct experiments among 20 nontechnical users. First in this experiment, each user-defined rotation (i.e., private key) is performed once and added into the database. Then, for each user, he/she repeats rotating the card for more than 20 times. Fig. 9a shows the distribution of basic rotation numbers k among 20 users. It can be found that the majority of users pick actions with 3-4 basic rotations. Refer to Table 1, key space can be multiplied by thousands of times naturally. Figs. 9b and 9c show the average delay

TABLE 6
Accuracy Rate versus Different Users with Dual Accelerometers ($n=4$)

	k=1	k=2	k=3	k=4	k=5
User #1	100%	100%	94.0%	94.0%	96.0%
User #2	100%	94.0%	96.0%	100%	98.0%
User #3	98.0%	96.0%	94.0%	96.0%	98.0%
User #4	96.0%	100%	100%	96.0%	92.0%
User #5	100%	100%	94.0%	94.0%	92.0%



(a) Distribution of k (b) Accuracy Rate



(c) Delay of Basic Rotations among Different Users (d) Distribution of Delay of Basic Rotations

Fig. 9. Experimental results with 20 users.

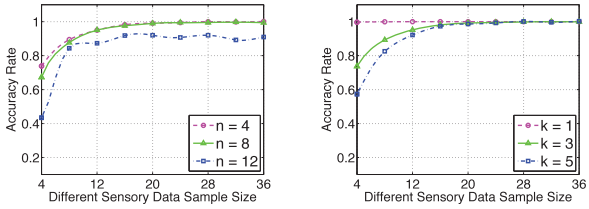
of basic rotation of different users and distribution of delay of all basic rotations among different users, respectively. From Figs. 9b and 9c, we can see that rotation delay varies. This is due to different user habits and different rotation degrees among different basic rotations. However, in spite of the variation of rotation delay, accuracy rates of the 20 users decrease little as shown in Fig. 9d. The majority of accuracy rates remain above 90 percent and the variance of accuracy rates among 20 users, which equals to 4.8, is quite small. Results shown in Fig. 9 fully demonstrate the effectiveness of our system in real life.

5 Simulations

Simulation results of system performance of our authentication methods are provided in this section. First in Sections 5.1 and 5.2, we comprehensively analysis impacts of various environment conditions on the accelerometer-based design, which has a more complex authentication algorithm. The simulation results of the gyroscope-based design can be found in Appendix D, available in the online supplemental material.

In the accelerometer-based design, while higher granularities of recognition and basic rotation numbers lead to larger key spaces and security levels, they also cause heavier workload and lower authentication accuracy rates. Therefore, we are interested to investigate the impact of these two parameters on the overall system performance. In addition, during experiments, we notice that sensor data sample rate and communication quality between sensors and access control clients are dominant factors to affect the system performance. Therefore, simulations of various sensory data sample sizes and sensory data fractures are performed to evaluate our algorithm with respect to the accuracy rate r.

In the simulation, we first randomly generate basic rotations based on a given n and k and then compute acceleration data of these rotations based on a specified sensor data sampling rate. After that, k basic rotations are performed sequentially with static intervals (pauses between basic rotations, e.g., 1.5 seconds). Except otherwise specified, we set $n = 4$ and k follows a uniform distribution



(a) Accuracy Rate vs. Granularity of Recognition (k=3) (b) Accuracy Rate vs. Basic Rotation Numbers (n=4)

Fig. 10. Impact of different sensory data sample sizes.

from 0 to 5 in simulations. To further emulate the actual rotations, we also add measurement noise to the raw simulated rotation data according to the observation in the experiments.

5.1 Impact of Sensory Data Sample Sizes

Sensors powered by harvested RF energy face a severe constraint of energy budget. Higher data sample rate leads to increasing sensor/processor activities and, therefore, higher energy consumption. As RF signals can only supply a limited amount of energy, such excessive sensor/processor activities then can lead to a lot of data loss. Here, we use the amount of sensory data sampled in one basic rotation action to describe sample size. Specifically, we assume that system users perform rotation actions with the same speed. Therefore, sample size S is denoted as the amount of samples per 90 degrees of an individual action. Due to the constraints of energy and radio physical limitations on WISP nodes, in practical settings we can receive at most 50 samples per second in our prototype system. If we perform the 90-degree rotation as slow as 1 second, the maximal possible sensory data sample size is $S_{max} = 50/1 = 50$.

In this part, we study the impact of sample size S on the accuracy rate r. Figs. 10a and 10b show accuracy rate with different granularities of recognition n and numbers of basic rotation k, respectively. From Fig. 10b, we can see that when granularity of recognition $n = 4$ and sample size $S > 20$, the accuracy rate is approximately 100 percent and remains stable. This result validates our authentication effectiveness as maximal sensory data sample size in actual systems is much higher than 20. However, in Fig. 10a, if granularity of recognition continues increasing (e.g., $n = 12$), higher sensory data sample size cannot guarantee better system performance. This is because higher granularity of recognition has smaller tolerance of measurement noise. Simulation observations shown in this section also matches our empirical experiences that accuracy rate remains stable when sample size is above 25.

5.2 Impact of Sensory Data Fractures

Data loss is a common issue in wireless communication. For instance, sensory data between 10 s and 11:8 s in Fig. 12 is lost during one of our experiments. We empirically measured the probability of losing a continuous data block (data fracture) in our prototype with single WISP and results are shown below in Table 7.

In Table 7, we count these fractures lasted more than 10 percent of the duration of the whole action. From this table, we find the probability of data fracture is higher

TABLE 7
Data Fracture Analysis

Num. of Fracture	0	1	2	3
Existence Ratio	30.0%	50.0%	10.0%	10.0%

than nonfractures (70 percent versus 30 percent). It could be inferred that the occurrence of fracture will increase during complex actions as more rotations are continuously performed. In this section, we evaluate accuracy rate r under different data fractures. Denote N_s as the maximal number of fractures and T_s as maximal percentage of data fractures in an independent action. N_s ranges between 0 and 3 whereas T_s ranges between 0 and 30. Both of these two parameters follow the uniform distribution. For example, if $N_s = 2$ and $T_s = 20$, it means that two data fractures with each one occupies at most 20 percent data would exist in one rotation. Fig. 11 shows accuracy rates under various data fractures percentage T_s. In all two figures, maximal numbers of fracture $N_s = 2$.

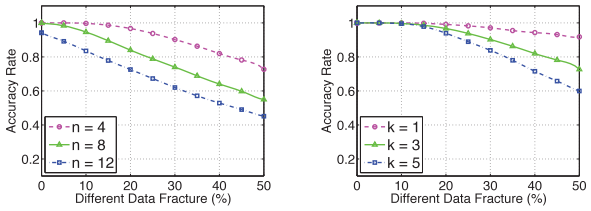
Fig. 11a is a comparison of accuracy rate with different granularities of recognition n and Fig. 11b shows accuracy rate of different basic rotation numbers k. By comparing Fig. 11a and Fig. 11b, we can see that although authentication performance in all figures decreases when data loss gets severe, accuracy rate with different basic rotation numbers k observes relatively much less impact than the change of granularity of recognition. This is because authentications with higher granularity of recognition are more sensitive to data loss. From Fig. 11, we find that our recognition algorithm is fracture-tolerant. In most cases, up to 20 percent sensory data fracture could be tolerated in systems with little performance degradation.

6 Comparison between the Two Reference Designs

Different from accelerometer-based design that relies on precise rotations, gyroscope-based design adopts the impulse of the amplitude of the angular velocity (see Section 2.2). Compared with accelerometer-based design, gyroscope-based design owns a higher authentication accuracy and smaller authentication delay (see Section 4). However, the accelerometer-based design is more robust under changing environmental conditions as the gyroscope-based design is more sensitive to data loss (see Section 5). Both of these two designs have large key space.

7 Related Work

Recently, researchers have introduced several RFID-based solutions to improve the security level of access control systems [11], [12], [13]. Sample et al. [11] present a solution for adding capacitive touch sensing onto RFID tags for capacitive user input. To further improve the system security, Saxena and Voris [12] introduce a method to generate random numbers to achieve motion detection based on the ambient noise of onboard accelerometer of RFID tags. In [13], by utilizing on-board sensors, authors design multiple context-aware selective unlocking mechanisms to prevent unauthorized reading and replay attacks.



(a) Accuracy Rate vs. Granularity of Recognition (k=3) (b) Accuracy Rate vs. Basic Rotation Numbers (n=4)

Fig. 11. Impact of different sensory data fractures.

The most similar paper to this work is the "RFIDs and secret handshakes" [14]. In this work, based on WISP, authors introduce an approach to tackle the ghost-and-leech attack between contactless cards and readers. Specifically, authors propose a context-aware authentication method by allowing contactless cards to communicate with readers only if the card owner performs a secret handshake. However, different from this quasi-biometrical authentication method that relies on the unique user patterns exhibited during the authentication process, we proposed an orthogonal solution which has a large key space increase by combining dynamic sensory information and static identifier during authentication process. By doing so, our method is also compatible with the context-aware solution in [14].

Although currently there exist several sensor-aided solutions to improve the security of access control systems, they have relatively small improved key space and operate in limited environment settings. Different from previous approaches, in our proposed design, we ensure that the dynamic authentication framework with sensory information combines the best of mechanical and electronic authentication methods which is backward compatible with the existing deployed RFID authentication systems. Apart from the accelerometer and gyroscope, various low-power sensors including temperature, microphone, electronic compass and barometer [15], [16], [17] are also desirable candidates of the proposed framework that would bring large key space increases with simple sensor readings. In addition, trusted users can share and reset access privilege among themselves. With such embedded sensor information and significantly increased key space, we can effectively counterattack the compromises of the access control system.

8 Conclusions

In this paper, we propose a dynamic authentication with sensory information for the access control systems. Different from existing schemes of authentication in access control systems, which mainly based on static information on cards, our dynamic authentication method combines sensory information from onboard sensors and conventional static ID information. Two case studies of the dynamic authentication are proposed. We theoretically analyze their highly increased key space, which exponentially multiplied static key space in existing authentication methods. To evaluate performance of our design, we built a prototype system and validate authentication mechanism experimentally. In experiments, the proposed authentication algorithm showed a 95 percent high accuracy rate among different users. In the simulation part, we comprehensively study the impact of

sensory data sample size and sensory data loss, which found to be critical factors from experiments on authentication algorithm. Most simulation results validate our algorithm effectively. Growing popularity of electronically based authentication in proximity access control systems calls for a higher security level and greater ubiquity. We believe that authentication bound with dynamic sensory information can effectively enhanced security level of access control systems and will take an important step toward electronically access authentication in the future.

ACKNOWLEDGMENTS

This work was supported in part by the NSFC under Grants 61004060, 61222305, the 863 High-Tech Project under Grant 2011AA040101-1, the SRFDP under Grants 20100101110066, 20120101110139, NCET-11-0445, the Fundamental Research Funds for the Central Universities under Grants 2013QNA5013 and 2013FZA5007, the SUTD-ZJU/RES/03/2011 and iTrust. Jiming Chen is the correspoding author.

REFERENCES

[1] Y. Shu, Y. Gu, and J. Chen, "Sensory-Data-Enhanced Authentication for RFID-Based Access Control Systems," *Proc. IEEE Ninth Int'l Conf. Mobile Ad Hoc Sensor Systems (MASS),* 2012.

[2] A. Juels, "RFID Security and Privacy: A Research Survey," *IEEE J. Selected Areas Comm.,* vol. 24, no. 2, pp. 381-394, Feb. 2006.

[3] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Authentication Based on Accelerometer Data," *Proc. Fifth Int'l Conf. Pervasive Computing,* pp. 144-161, 2007.

[4] M. Burmester, T.V. Le, B.D. Medeiros, and G. Tsudik, "Universally Composable RFID Identification and Authentication Protocols," *ACM Trans. Information and System Security,* vol. 12, no. 4, article 21, 2009.

[5] J. Kong, H. Wang, and G. Zhang, "Gesture Recognition Model Based on 3D Accelerations," *Proc. IEEE Fourth Int'l Conf. Computer Science & Education (ICCSE),* 2009.

[6] S. Mitra and T. Acharya, "Gesture Recognition: A Survey," *IEEE Trans. Systems, Man and Cybernetics,* vol. 37, no. 3, pp. 311-324, May 2007.

[7] S. Zhou, Q. Shan, F. Fei, W.J. Li, C.P. Kwong, P.C.K. Wu, B. Meng, C.K.H. Chan, and J.Y.J. Liou, "Gesture Recognition for Interactive Controllers Using MEMS Motion Sensors," *Proc. IEEE Fourth Int'l Conf. Nano/Micro Engineered Molecular Systems (NEMS),* 2009.

[8] T. Park, J. Lee, I. Hwang, C. Yoo, L. Nachman, and J. Song, "E-Gesture: A Collaborative Architecture for Energy-Efficient Gesture Recognition with Hand-Worn Sensor and Mobile Devices," *Proc. Ninth ACM Conf. Embedded Networked Sensor Systems (SenSys),* 2011.

[9] A.P. Sample, D.J. Yeager, P.S. Powledge, A.V. Mamishev, and J.R. Smith, "Design of an RFID-Based Battery-Free Programmable Sensing Platform," *IEEE Trans. Instrumentation and Measurement,* vol. 57, no. 11, pp. 2608-2615, Nov. 2008.

[10] M. Buettner and D. Wetherall, "An Empirical Study of UHF RFID Performance," *Proc. ACM MobiCom,* 2008.

[11] A.P. Sample, D.J. Yeager, and J.R. Smith, "A Capacitive Touch Interface for Passive RFID Tags," *Proc. IEEE Int'l Conf. RFID,* 2009.

[12] N. Saxena and J. Voris, "Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model," *Proc. Sixth Int'l Conf. Radio Frequency Identification: Security and Privacy Issues,* vol. 6370, pp. 2-21, 2010.

[13] D. Ma and N. Saxena, "A Context-Aware Approach to Defend against Unauthorized Reading and Relay Attacks in RFID Systems," *Security and Comm. Networks,* doi: 10.1002/sec.404, Dec. 2011.

[14] A. Czeskis, K. Koscher, J.R. Smith, and T. Kohno, "RFIDs and Secret Handshakes: Defending against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications," *Proc. 15th ACM Conf. Computer and Comm. Security (CCS),* 2008.

[15] N. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. Campbell, "A Survey of Mobile Phone Sensing," *IEEE Comm. Magazine,* vol. 48, no. 9, pp. 140-150, Sept. 2010.

[16] P. Kannan, P. Seshadri, M.-C. Chan, A.L. Ananda, and L.-S. Peh, "Low Cost Crowd Counting Using Audio Tones," *Proc. 10th ACM Conf. Embedded Network Sensor Systems (SenSys),* 2012.

[17] J. Chung, M. Donahoe, C. Schmandt, I.-J. Kim, P. Razavai, and M. Wiseman, "Indoor Location Sensing Using Geo-Magnetism," *Proc. ACM Ninth Int'l Conf. Mobile Systems, Applications, Services (MobiSys),* 2011.

[18] Y. Shu, J. Chen, F. Jiang, Y. Gu, Z. Dai, and T. He, "Demo: WISP-Based Access Control Combining Electronic and Mechanical Authentication," *Proc. ACM Conf. Embedded Network Sensor Systems (SenSys),* 2011.

Yuanchao Shu is currently working toward the PhD degree in control science and engineering at Zhejiang University, Hangzhou, China. He is a member of the Group of Networked Sensing and Control (IIPC-NeSC) in the State Key Laboratory of Industrial Control Technology. His research interests include mobile computing and networked control, optimization and systems design in cyber-physical systems and wireless sensor networks. He is a student member of the IEEE.

Yu (Jason) Gu received the PhD degree from the University of Minnesota, Twin Cities in 2010. He is currently an assistant professor in the Pillar of Information System Technology and Design at the Singapore University of Technology and Design. He is the author and coauthor of more than 60 papers in premier journals and conferences. His publications have been selected as graduate-level course materials by over 20 universities in the United States and other countries. His research includes networked embedded systems, wireless sensor networks, cyber-physical systems, wireless networking, real-time and embedded systems, distributed systems, vehicular ad-hoc networks and stream computing systems. He is a member of the ACM and the IEEE.

Jiming Chen (M'08-SM'11) received the BSc and PhD degrees both in control science and engineering from Zhejiang University in 2000 and 2005, respectively. He was a visiting researcher at INRIA in 2006, National University of Singapore in 2007, and University of Waterloo from 2008 to 2010. Currently, he is a full professor with the Department of control science and engineering, and the coordinator of group of Networked Sensing and Control in the State Key laboratory of Industrial Control Technology, vice director of Institute of Industrial Process Control at Zhejiang University, China. He currently serves associate editors for several international Journals including *IEEE Transactions on Parallel and Distributed System*, *IEEE Transactions on Industrial Electronics*, *IEEE Network*, *IET Communications*, and so on. He was a guest editor of *IEEE Transactions on Automatic Control*, *Computer Communication (Elsevier)*, *Wireless Communication and Mobile Computer (Wiley)*, and *Journal of Network and Computer Applications (Elsevier)*. He also served/serves as Ad hoc and Sensor Network Symposium co-chair, IEEE Globecom 2011; general symposia co-chair of ACM IWCMC 2009 and ACM IWCMC 2010, WiCON 2010 MAC track co-chair, IEEE MASS 2011 Publicity co-chair, IEEE DCOSS 2011 Publicity co-chair, IEEE ICDCS 2012 Publicity co-chair, IEEE ICCC 2012 Communications QoS and Reliability Symposium co-chair, IEEE SmartGridComm The Whole Picture Symposium co-chair, IEEE MASS 2013 Local chair, Wireless Networking and Applications Symposium co-chair, IEEE ICCC 2013 and TPC member for IEEE ICDCS'10,'12,'13, IEEE MASS'10,'11,'13, IEEE SECON'11,'12 IEEE INFOCOM'11,'12,'13, and so on. He is a senior member of the IEEE.