Sensory-Data-Enhanced Authentication for RFID-based Access Control Systems

Yuanchao Shu*†, Yu Gu† and Jiming Chen*,
*State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, 310027 China
Email: ycshu@zju.edu.cn, jmchen@iipc.zju.edu.cn
† Singapore University of Technology and Design, Singapore
Email: jasongu@sutd.edu.sg

***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 can not be transferred among trusted users. In this work, we introduce a sensory-data-enhanced authentication for access control systems. By combining sensory-data 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 and stolen. 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 simple sensor data and empirically demonstrate simple rotations can increase key space by more than $30,000$ times with an authentication accuracy of 95%. We performed extensive simulations under various environment settings and implemented our design on WISP to experimentally verify the system performance.**

I. Introduction

Access control is a mechanism which 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 etc. 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 loss of keys problem since 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.

In order 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 can not 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 method 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 etc.. This authentication method 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, our contributions in this work are as follows:

- We design and implement a sensory-data-enhanced authentication mechanism for access control systems. Our design is backward compatible with existing, deployed RFID or access card readers.
- We theoretically prove and demonstrate that our sensory-data-enhanced authentication significantly increases the key space for proximity authentication systems with the integration of just one low-cost sensor.
- We have fully implemented and built a running prototype of the proposed sensory-data-enhanced authentication mechanism on the Intel Wireless Identification and Sensing Platform (WISP). Based on our running prototype, we have extensively evaluated our design in terms of system accuracy and usability in the real-world settings.

978-1-4673-2433-5/12/$31.00 ©2012 IEEE

The remainder of this paper is organized as follows. After describing related work in Section II, we provide sensor data based authentication method in Section III. We then provide algorithm of our system in Section IV. System working performance and simulations of our authentication method is shown in Section V and Section VI. Finally, we conclude in Section VII.

II. Related Work

Recently, researchers have introduced several RFID-based solutions to improve the security level of access control systems [1], [2], [3]. Sample et al. present a solution for adding capacitive touch sensing onto RFID tags for capacitive user input [1]. To further improve the system security, Saxena et al. [2] introduce a method to generate random numbers to achieve motion detection based on the ambient noise of onboard accelerometer of RFID tags. In [3], by utilizing onboard sensors, authors design multiple context-aware selective unlocking mechanisms to prevent unauthorized reading and replay attacks.

The most similar paper to this work is the "RFIDs and secret handshakes" [4]. 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 which 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 data and static identification information during authentication process. Our method is also compatible with the context-aware solution proposed in [4].

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 design, we ensure that our system combines the best of mechanical and electronic authentication methods which is backward compatible with the existing deployed RFID authentication systems and has large key space increases with simple sensor readings. 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 compromise of the access control system.

III. Sensory-Data-Enhanced Authentication Design

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 data 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 Figure 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 a 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 can not 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 cards and predefined actions with each other which is unavailable in biometric authentication systems.

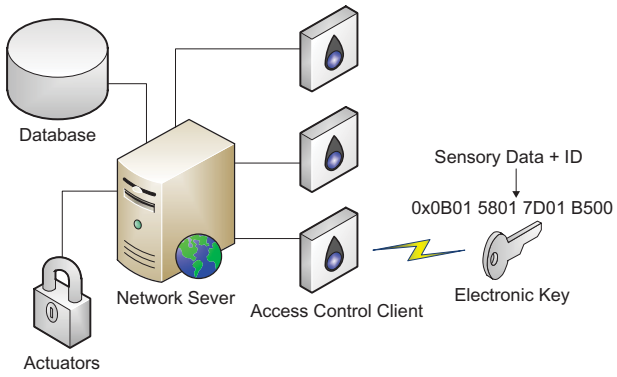


Fig. 1. System Function Diagram

Different from existing authentication methods such as combining RFID and an additional keypad near the reader, our method only revises authentication algorithm on the network server without any modification of access clients. In fact, since we piggyback sensory data to ID information before transmitting to the reader, most existing works on communication encryption for RFID system can be easily adopted into our authentication method [5], [6], [7], and therefore deal with several security vulnerabilities such as replay attack and eavesdropping.

A. Accelerometer-based Reference Design

The underlying 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 and hence the level of security for existing electronic authentication systems. A wide variety of sensors including accelerometer, gyroscope and etc. can be used in

TABLE I
KEY SPACE BETWEEN DIFFERENT BASIC ROTATION NUMBERS k AND GRANULARITY OF ROTATION RECOGNITION n

	$n=4, k=3$	$n=4, k=5$	$n=4, k=8$	$n=8, k=3$	$n=8, k=5$	$n=8, k=8$
Key Space	864	31104	6718464	21952	4302592	1.18×10^{10}

our system. To illustrate the basic concept and the resulting security enhancement of our sensory data enhanced access control system design, we use three-axis accelerometer as an example in the following sections. In particular, we utilize the sensory data generated from the rotation of accelerometer to introduce a reference design for the proposed sensory data enhanced authentication scheme. Through our prototyping system and real world experiments, we notice such a rotation-based design is a feasible and practical option for the proposed generic sensory-data-enhanced authentication scheme.

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-Axis and Y-Axis to determine the position of the accelerometer in a two-dimensional plane.

In Figure 2 we illustrate a simple example on how to determine the position of an accelerometer. In Figure 2, A_x and A_y are acceleration components of gravity on Axis-X and Axis-Y, 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

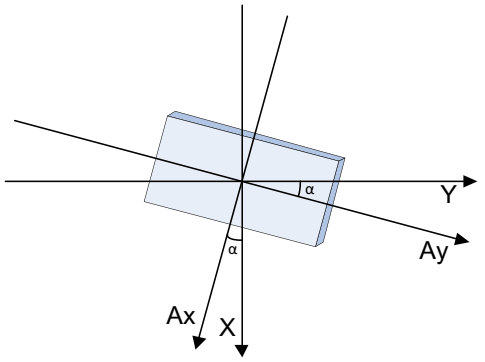


Fig. 2. Accelerometer Rotation Example

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 rotation is omnidirectional, either clockwise or counterclockwise;
  - 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.

Figure 3 shows an example of rotation sequence with three basic rotations ($k = 3$) and granularity of the recognition $n = 8$. CW and CCW in Figure 3 denotes clockwise and counterclockwise, respectively. In Figure 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.

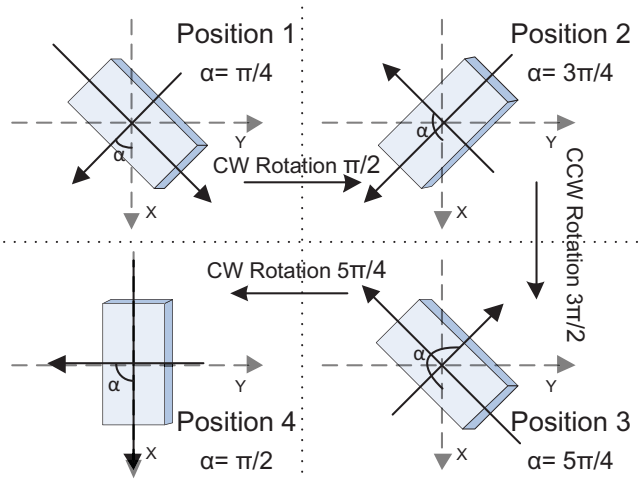


Fig. 3. Rotation Sequence Diagram (2D)

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

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

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

In Table I, we summarize possible key spaces for two-dimensional rotations with different number 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, with the number of basic rotations increases from k to $k+1$, the key space will be multiplied by $P_{2D}(n,k+1)/P_{2D}(n,k) = 2n-2$. If $n=4$, which is a relatively small value, by just adding one simple basic rotation, the key space will increase six-fold! In addition, since 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 sensory-data-enhanced authentication mechanism.

IV. Rotation Detection and Recognition

In the previous section, we discuss the potential of large key space increase for our sensory-data-enhanced authentication design. In this section, we further elaborate on the detailed sensor rotation detection and recognition algorithms.

One complete sensory-data-enhanced authentication process consists of a sequence of basic rotations. In order to accurately identify each individual basic rotations from raw accelerometer data, we perform following three operations in the network server.

A. Data Pre-Processing

The first step of rotation recognition is data pre-processing. In this step, the main goals are to separate and filter each individual basic rotations from a series of raw accelerometer data.

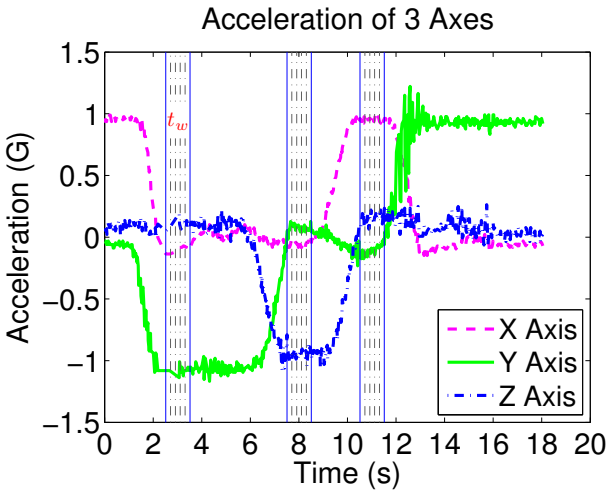


Fig. 4. Example Sensory Data for a 3D Rotation

In order 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. In order 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 (1 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 $t_w = 1s$ and $t_s = 0.3s$ in our system implementation. In this way, we have achieved accurate separation of basic rotations in one complete authentication. To visualize above data pre-processing step, Figure 4 shows one authentication with 4 basic rotations that performed slowly on our prototype implementation. The shaded regions represent sliding windows at three pauses. Clearly from Figure 4, we can see 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:

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

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

$$y = f(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_{m-1}x + b \quad (2)$$

such that

$$\begin{aligned} min(F(\boldsymbol{a}_k, b)) &= min(\sum_m (f(x_i) - p_i)^2) \\ &= min(\sum_{i=0} (f(x_i) - p_i)^2) \\ k &= 0, \ldots, m-1 \end{aligned} \quad (3)$$

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

B. 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. Figure 5 shows the F-vectors of fitted basic rotation in Figure 7 on the X-Axis.

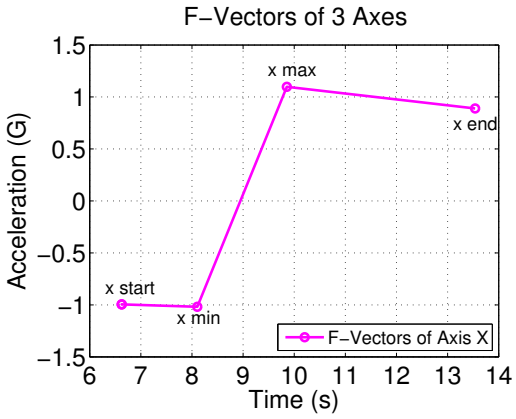


Fig. 5. F-Vectors of An Example Basic Rotation

C. F-Vectors Matching

After extracting feature vectors, we then try to match the extracted feature vector 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 Figure 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.

In order to match extracted F-vectors of a basic rotation to standard ones in database, we use Euclidean distance between them 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 vectors 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.

V. Testbed Evaluation

To evaluate our proposed sensory-data-enhanced authentication method, a prototype system is built based on the Intel Wireless Identification and Sensing Platform (WISPs) [8]. WISP is a fully-passive ultra high frequency (UHF) RFID tag which integrates an ultra-low-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.

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 backend authentication computer servers. Figure 6 is a picture of our prototype system.

Fig. 6. Antenna-reshaped WISP Tag and Reader

A. Performance Evaluation

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 this paper. However, our design also supports three-dimensional rotations and has been implemented on our prototype as well.

1) Accuracy Rate of the System Authentication: Firstly, a total of 600 basic rotations are performed by one user. The experiment results are summarized in Table II. From Table II,

TABLE II
ACCURACY RATE VS. 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

we can see 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 II, we can observe 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 $15s$. By improving hardware design and optimizing authentication algorithm, delay could be further reduced.

In order to further evaluate the practicability of our design for daily usage, 50 complex rotations under each number of basic rotations k are designated to 5 users. Accuracy rates of authentication for each users are reported in Table III.

TABLE III
ACCURACY RATE VS. 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%

From Table III, we can see individual accuracy rate varies. When $k = 1$ and $k = 2$, average accuracy rate are higher than 90% (98% and 94% respectively), while most of accuracy rates when $k > 4$ are below 80%, 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 III, system achieves high security level on both average accuracy rate and variance when $k \leq 2$ if $n = 4$.

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 2 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 IV and Table V(line of delay is omitted as there is no difference with single accelerometer's). From Table IV and Table V, compared with

TABLE IV
ACCURACY RATE VS. 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%

single sensor experiments, it can be found that authentication accuracy rate increased effectively in dual-sensor situation where two accelerometers works at the same time. Specifically, compare Table IV with Table II, when the granularity of recognition $n = 4$, accuracy rates are all higher than 95% with dual accelerometers while 80% under single accelerometer situation are below 95%. In Table V, average accuracy rates of all five columns are higher than 95% while in single accelerometer experiment, accuracy rates in 14 of 25 cases are below 90% and the worst case of accuracy rate is as low as 70% which is occurred when user 3 performs a 5 basic-rotation authentication. Based on Table I, these experiment results demonstrate our proposed method could increase the key space by more than 30000 times with a high enough accuracy rate of authentication. Besides, accuracy rates with dual accelerometers are much more stable. Among different users, all accuracy rate variances among five distinct k are below 7.5 and average variance of different k is 71.8% less than that of single sensor (5.312 vs. 18.816).

TABLE V
ACCURACY RATE VS. 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%

B. System Insight

In our testbed implementation, we empirically choose the order of least square estimation function $m = 10$ through a series of experiments. From our experiments, we observe lower order fitting can not guarantee a smooth curve (shown in Figure 8(a)) while higher order fitting is not only increasing computational complexity, but also introduce undesirable fluctuation at the beginning and the end part of a basic rotation (shown in Figure 8(b)). In Figure 7, we show an example

of a fitted curve for one single basic rotation on the X-Axis ($m = 10$). From this figure we can see although sample readings of the accelerometer are unevenly distributed, the resulting fitting curve is still very satisfactory. Therefore, 10th degree polynomial is accepted in our system.

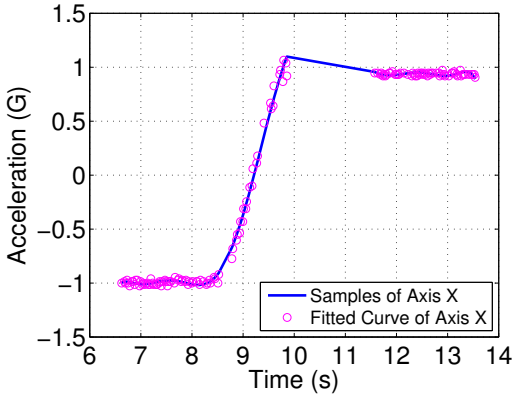
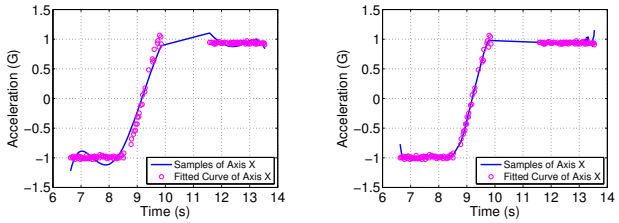


Fig. 7. Fitted Curve of An Example Action ($m = 10$)



(a) Fitted Curve of An Example Action ($m = 6$)

(b) Fitted Curve of An Example Action ($m = 40$)

Fig. 8. Fitted Curve of An Example Action($m \neq 10$)

Another practical issues of our proposed sensory-data-enhanced authentication method is determining start and stop of rotations. To solve this problem, various accelerometer-based event detection algorithms can be adopted and we implemented a function which triggers/ceases the main sensory-data-enhanced authentication process when detecting a vibration of the accelerometer. This simple method exhibits a high reliability during our testbed experiments and demonstrations at Sensys 2011 [9]. In some cases, access card can be observed by others when card holder performing rotation actions. In case of movement forging, rotation can be performed in a covert manner such as performing rotations within a black box.

VI. Simulations

To evaluate the system performance of our authentication method under various environment conditions, we provide simulation results in this section. In our design, while higher granularity 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 interference, 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 noises, 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 from 0 to 5 in simulations. To further emulate the actual rotations, we also add noises, data fractures to the raw simulated rotation data.

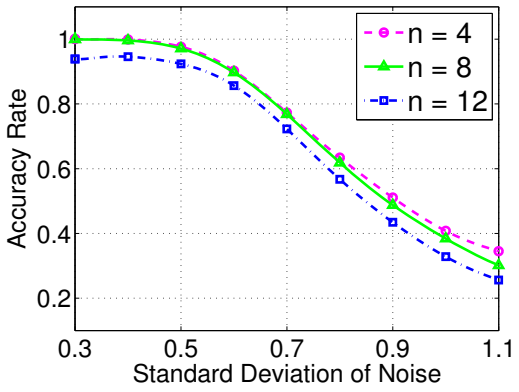
A. Impact of Noises on Authentication Accuracy

Firstly, we study the impact of noises on the system performance. The measurement noise is denoted by the standard deviation of measurements σ_p. In this part, we compare accuracy rate r on sequential actions with different standard deviations σ_s of noises. Impact of noises are shown in Figure 9. From Figure 9, we can see as noise increases, authentication accuracy rate decreases. Specially, figure 9(a) shows the accuracy rate of different granularities of recognition n under different noises and Figure 9(b) shows the accuracy rate under different basic rotation numbers k. In Figure 9(a) and Figure 9(b), when standard deviations $\sigma < 0.4$, accuracy rate for most k and n (5/6) are approximately 100%. It demonstrates that in random action process with serious impact of noise, proposed authentication method still has a good performance. During our experiments, we observe the standard deviation of sensory readings is around $\sigma_p = 0.3$, and this further demonstrates the robustness of our system design.

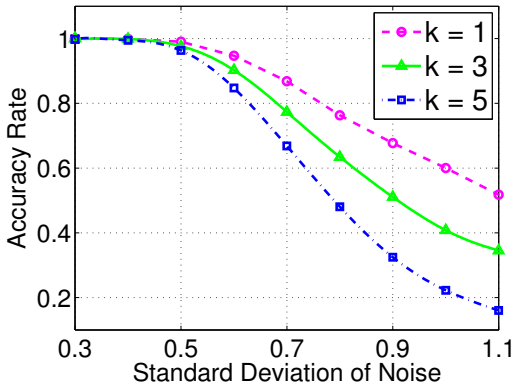
B. Impact of Sensory Data Sample Sizes

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. In Figure 10, we set the standard deviations of white noise to 0.5 and plot authentication accuracy rate

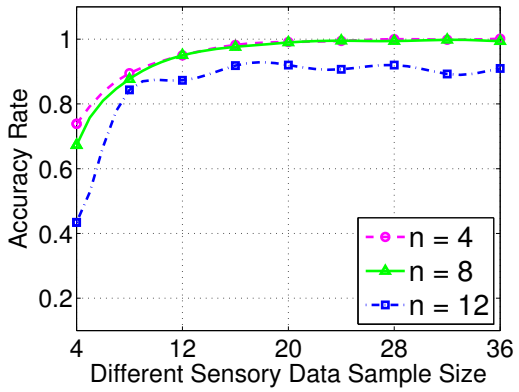


(a) Accuracy Rate vs. Granularity of Recognition (k=3)

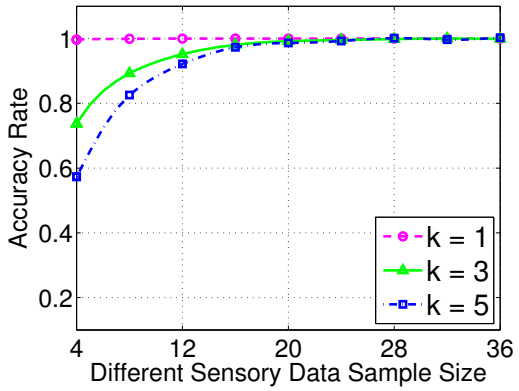


(b) Accuracy Rate vs. Basic Rotation Numbers (n=4)

Fig. 9. Impact of Different σ for a Fixed Number of Iterations (5000).



(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 Size for a Fixed Number of Iterations (5000).

versus varied sensory data sample sizes. Figure 10(a) and Figure 10(b) show accuracy rate with different granularities of recognition n and numbers of basic rotation k, respectively. From Figure 10(b), we can see that when granularity of recognition $n = 4$ and sample size $S > 20$, the accuracy rate is approximately 100% 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 Figure 10(a), if granularity of recognition continues increasing (e.g. $n = 12$), higher sensory data sample size can not guarantee better system performance. This is because we set the standard deviations of noise to 0.5 whereas higher granularity of recognition has smaller tolerance of noise. Simulation observations shown in this section also matches our empirical experiences that accuracy rate remains stable when sample size is above 25.

C. Impact of Sensory Data Fractures

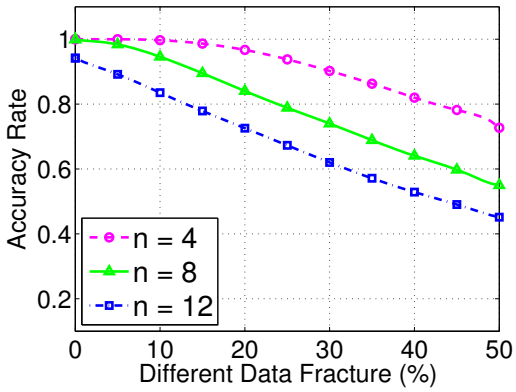
Data loss is a common issue in wireless communication. For instance, sensory data between $10s$ and $11.8s$ in Figure 7 is lost during one of our experiments. We empirically measured the probability of losing a continuous data block (data fracture) in our prototype system and results are shown below in TABLE VI.

In TABLE VI we count these fractures lasted more than 10% of the duration of the whole action. From this table, we find the probability of data fracture is higher than non-fracture's (70% vs. 30%). It could be inferred that the occurrence of fracture will increase during long 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 to 3 whereas T_s ranges between 0 to 30. Both of these two parameters follow the uniform distribution. For example, if $N_s = 2$ and $T_s = 20$, it means that 2 data fractures with each one occupies at most 20% data would exist in one rotation. Figure 11 shows accuracy rates under various data fractures percentage T_s. In all two figures, maximal numbers of fracture $N_s = 2$.

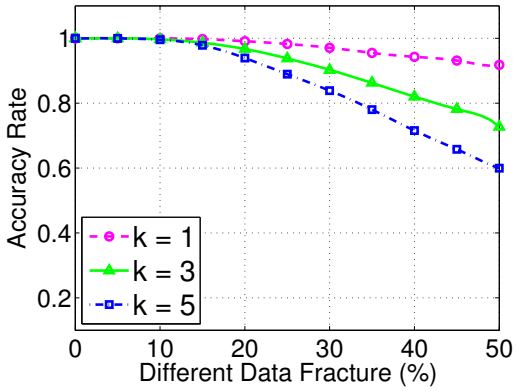
TABLE VI
DATA FRACTURE ANALYSIS (20 ITERATIONS)

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

Figure 11(a) is a comparison of accuracy rate with different granularities of recognition n and Figure 11(b) shows accuracy rate of different basic rotation numbers k. By comparing Figure 11(a) and Figure 11(b), we can see that although authen-



(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 for a Fixed Number of Iterations (5000).

tication 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 Figure 11, we find that our recognition algorithm is fracture-tolerant. In most cases, up to 20% sensory data fracture could be tolerated in systems with little performance degradation.

VII. Conclusions

In this paper, we proposes a sensory-data-enhanced authentication for access control systems. Different from existing schemes of authentication in access control systems, which mainly based on static information on cards, our sensory-data-enhanced authentication method combines sensory-data from onboard sensors and conventional static ID information. For sensory-data-enhanced authentication, we first theoretically analyzes its 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% high accuracy rate within different users. In the simulation part, we comprehensively study the impact of noise of measurement, 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 data can effectively enhanced security level of access control systems and will take an important step towards electronically access authentication in the future.

Acknowledgement

This research was supported in part by NSFC under grant 61190110 and 60974122, Natural Science Foundation of Zhejiang (NSFZJ) under grant R1100324, 863 High-Tech Project under grant 2011AA040101-1 and the SUTD-ZJU Collaboration Grant SUTD-ZJU/RES/03/2011.

References

[1] A. P. Sample, D. J. Yeager, and J. R. Smith, "A capacitive touch interface for passive RFID tags," in *IEEE RFID*, 2009.
[2] N. Saxena and J. Voris, "Still and silent: motion detection for enhanced RFID security and privacy without changing the usage model," *Radio Frequency Identification: Security and Privacy Issues*, pp. 2–21, 2010.
[3] D. Ma and N. Saxena, "A context-aware approach to defend against unauthorized reading and relay attacks in RFID systems," *Security and Communication Networks*, December 2011.
[4] 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," in *ACM CCS*, 2008.
[5] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, 2006.
[6] R. Mayrhofer and H. Gellersen, "Shake well before use: Authentication based on accelerometer data," *Pervasive Computing*, pp. 144–161, 2007.
[7] M. Burmester, T. Van Le, B. De Medeiros, and G. Tsudik, "Universally composable RFID identification and authentication protocols," *ACM Transactions on Info. and System Security*, vol. 12, no. 4, p. 21, 2009.
[8] 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. Instrum. Meas.*, 2008.
[9] Y. Shu, J. Chen, F. Jiang, Y. Gu, Z. Dai, and T. He, "Demo: WISP-based access control combining electronic and mechanical authentication," in *ACM SenSys*, 2011.
[10] M. Buettner and D. Wetherall, "An empirical study of UHF RFID performance," in *ACM MobiCom*, 2008.
[11] R. Chaudhri, J. Lester, G. Borriello, and Acm, "An RFID based system for monitoring free weight exercises," in *ACM Sensys*, 2008.
[12] J. Gummeson, S. S. Clark, K. Fu, and D. Ganesan, "On the limits of effective hybrid micro-energy harvesting on mobile CRFID sensors," in *ACM MobiSys*, 2010.
[13] B. Jiang, J. R. Smith, M. Philipose, S. Roy, K. Sundara-Rajan, and A. V. Mamishev, "Energy scavenging for inductively coupled passive RFID systems," *IEEE Trans. Instrum. Meas.*, 2007.
[14] Y. Ko, S. Roy, J. R. Smith, H. Lee, and C. Cho, "RFID MAC performance evaluation based on ISO/IEC 18000-6 type C," *IEEE Communications Letters*, 2008.
[15] J. Kong, H. Wang, and G. Zhang, "Gesture recognition model based on 3D accelerations," in *IEEE ICCSE*, 2009.
[16] S. Mitra and T. Acharya, "Gesture Recognition: A survey," *IEEE Transactions on Systems, Man and Cybernetics*, 2007.
[17] D. J. Yeager, P. S. Powledge, R. Prasad, D. Wetherall, and J. R. Smith, "Wirelessly-charged UHF tags for sensor data collection," in *IEEE RFID*, 2008.
[18] 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," in *IEEE NEMS*, 2009.