Sensory - Data - Enhanced Authentication by Accelerometer Sensor for Access Control Systems

G. Annapoorani [1], K. Prem Kumar [2]

Abstract - Access card authentication used to specify the authorized persons and maintains the static information about them. It provides access to their authorizers in various governments, commercial and banking locations. By exchanging the information among the access card and its clients, access card plays a vital role to fight against stolen, loss and duplications of the access cards. In the proposed work, it merge the access card ID information and sensory information obtained from accelerometer sensor and introduces a dynamic authentication system. This can be able to solve the issues like access card loss, stolen and duplication. This solution is backward-compatible. This helps to increase the authentication key space and thereby make the environment more secure. We theoretically demonstrate simple rotations can increase key space by more than 1, 00,000 times and with an authentication accuracy of 90%. We implemented the simulations under different scenarios and applied our design to achieve the system performance experimentally.

Index Terms - Authentication, Sensory Data, Access Control System, Accelerometer Sensor, F-Vector, Data Preprocess, Rotation Recognition.

1 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 authenticating 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. 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.

In this work, we aim at bridging the gap between insufficiency of existing electronic authentication solutions and 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 etc. 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. Our contributions in this work are as follows. We design and implement a dynamic authentication framework with sensory information for the access control systems.

Our design is backward compatible with existing, deployed RFID or access card readers. We demonstrate the proposed framework and theoretically prove and 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. Based on the running prototype, we have extensively evaluated system accuracy and usability in the real-world settings.

2 DYNAMIC 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 loss stolen and duplications. In this work, we propose to use sensory information obtained from wireless rechargeable sensors to further enhance the security of

- *G. Annapoorani is currently pursuing masters engineering degree program in Communication and Networking in Rajiv Gandhi College of Engineering, Chennai, India. E-mail:* annapoorani.g@live.com
- *K. Premkumar is currently working as an assistant Professor in Rajiv Gandhi College of Engineering, Chennai, India. E-mail:* prem.embedded@gmail.com

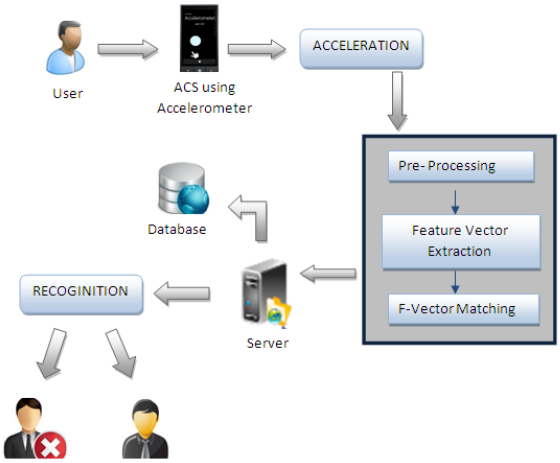

Fig. 1. System Function Diagram

existing electronic proximity authentication systems. The 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 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.

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 level of security for existing electronic authentication systems. A wide variety of sensors including accelerometer, gyroscope and etc. 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 three-axis accelerometer. Here, we utilize the sensory data generated from the rotation of accelerometer to introduce a reference design for the proposed sensory data enhanced authentication scheme.

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

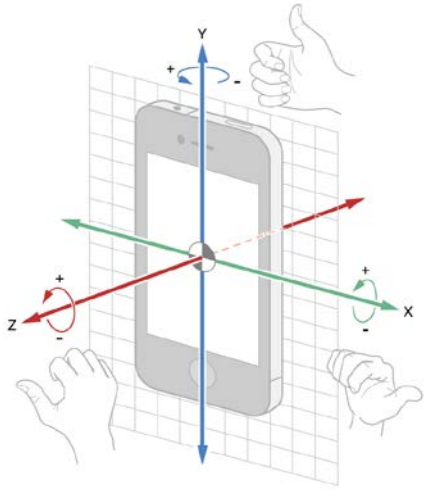

Fig. 2. Accelerometer Rotation

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, Ax and Ay are acceleration components of gravity on Axis-X and Axis-Y, respectively. The tilt angle α can then be calculated by equation Ax = Gcosα and Ay = Gsinα, where G is the static acceleration of gravity.

Rules of Rotation: All rotations are two-dimensional and the rotation always starts from the end position of the past rotation. The rotations can be either clockwise or anticlockwise direction. One rotation should not exceed 360 degrees.

Parameters of Rotation: n and k are the two basic rotational parameters represent Granularity of the rotation recognition and Number of Basic rotations.

n = maximal number of recognizable rotations within one round.

k = number of rotations in one sequence.

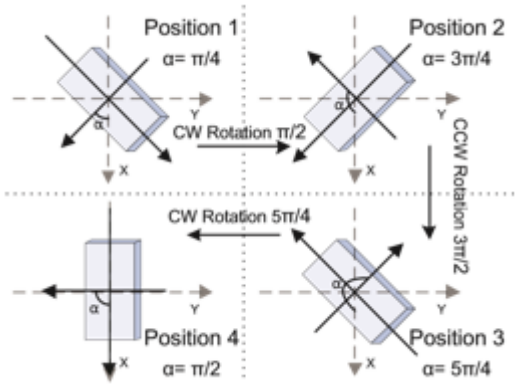

Fig. 3. Rotation Sequence Diagram (2D)

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.

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 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.

2.1.2 THREE – DIMENSIONAL ROTATION

In this part, we extend our design to rotations in three dimensional spaces. 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:

i) During the whole rotation process, either plane XY, YZ, or XZ under the coordinate of accelerometer is perpendicular to the ground

ii) Accelerometer only rotates in one plane under its own coordinate (XY, XZ or YZ) during one basic rotation.

iii) Rotation in a different plane is allowed if one axis among ±X, ±Y or ±Z of the accelerometer is perpendicular to the ground at the end of the previous basic rotation.

Figure 4(a) demonstrates an example of a 3D rotation sequence. We co-plot the coordinate of the accelerometer to illustrate 3D rotations. In Figure 4(a), 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. Corresponding sample data of this three-dimensional rotation are shown in Figure 5 and it could be found that

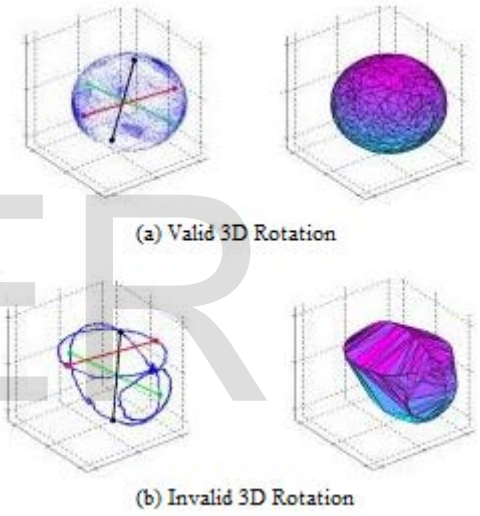

Fig. 4. Rotation Sequence Diagram

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. 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 ±X, ±Y and ±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.

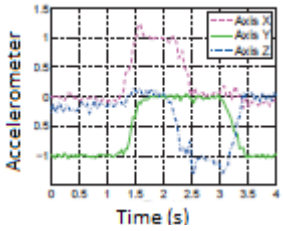

Fig. 5. 3D Rotations of an Accelerometer

The total key space of rotation in three-dimensional space and the recursive formula of a_k and b_k can be written as

$$Pacc3D(n,k) = a_{k+1} + b_{k+1} \quad (2)$$

Where,

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

With the initial value a0 = 6 and b0 = 3(n − 4), n = 4m, m ≥ 1 ∈ N. 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 Pacc2D(n,k + 1) / Pacc2D(n,k) = 2n − 2.

3 ROTATION RECOGNITION

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

3.1 ACCELEROMETER DATA PRE - PROCESSING

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

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 ts seconds, with ts duration of new data appended to the end of the sliding window while the first ts duration of sensory data are discarded.

Key Space	N=8, K=8	N=8, K=5	N= 8, K=
2D	1.17 × 10 10	4302691	22862
3D	5.24 × 10 11	6.28 × 107	148963

TABLE 1. Key space of the Accelerom

After ident
use least sq
individual basic rotation from the accelerometer. Then the least square estimation tries to build a polynomial function below:

$$y = f(x) = a0x^m + a1x^{m-1} + \cdots + a_{m-1}x + b \quad (3)$$

Such that

$$\min(F(a_{k,b})) = \min(\sum (f(xi) - pi)^2)$$
$$= \min(\sum (f(xi) - pi)\,2) \quad (4)$$

Where, k = 0,…, m, 1

3.2 FEATURE VECTOR EXTRACTION

After separating basic rotations for one single authentication, we match them with standard feature vectors. First, feature vectors (F-Vectors) for each 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:

$$T_x = \{v_x\} = \{v_{x\_start}, v_{x\_end}, v_{x\_max}, v_{x\_min}\}$$
$$T_y = \{v_y\} = \{v_{y\_start}, v_{y\_end}, v_{y\_max}, v_{y\_min}\}$$
$$T_z = \{v_z\} = \{v_{z\_start}, v_{z\_end}, v_{z\_max}, v_{z\_min}\}$$

$$V \in R_2$$

Where v = (value, time) is a vector consisting of fitted acceleration value and its relative time within one basic rotation.

3.3 F-VECTOR 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.

In order 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:

$$d_x = |T_x - S_x|$$

$$d_y = |T_y - S_y|$$

$$d_z = |T_z - S_z|$$

Where,

$$S_x = \{\bar{v}_x\} = \{\bar{v}_{x\_start}, \bar{v}_{x\_end}, \bar{v}_{x\_max}, \bar{v}_{x\_min}\}$$
$$S_y = \{\bar{v}_y\} = \{\bar{v}_{y\_start}, \bar{v}_{y\_end}, \bar{v}_{y\_max}, \bar{v}_{y\_min}\}$$
$$S_z = \{\bar{v}_z\} = \{\bar{v}_{z\_start}, \bar{v}_{z\_end}, \bar{v}_{z\_max}, \bar{v}_{z\_min}\}$$

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.

4 EVALUATION OF THE ACCELEROMETER BASED DESIGN

Both authentication accuracy and delay are two most essential factors for practical access control systems. 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.

a. Accuracy rate of the System Authentication

A total of 600 basic rotations are performed by one user. 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.

	K = 1	K = 2	K = 3	K = 4	K = 5
N = 4	99%	94%	91%	90%	88%
N = 8	99%	92%	91%	91%	82%
Delay	2s	5s	7s	9s	12s

TABLE 2. Accuracy rate with different k and n

In addition, as the number of basic rotations increases, the false negative rate will sum up and lead to a lower accuracy rate. By improving hardware design and optimizing authentication algorithm, delay could be reduced.

b. System Performance among different users

In the first experiment, 50 complex rotations under each number of basic rotations k are designated to 4 users. Experiments with both single and dual accelerometers are conducted. Accuracy rates of authentication with single accelerometer for each users are reported in Table 3.

	K = 1	K = 2	K = 3	K = 4	K = 5
User 1	99%	99%	92%	87%	80%
User 2	95%	93%	83%	75%	72%
User 3	100%	95%	92%	91%	81%
User 4	100%	94%	91%	90%	89%

TABLE 3. Accuracy Rate vs. Different Users (n = 4)

In Table 4, 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 1, 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

among different users are much more stable in Table 4. With dual accelerometers, 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.

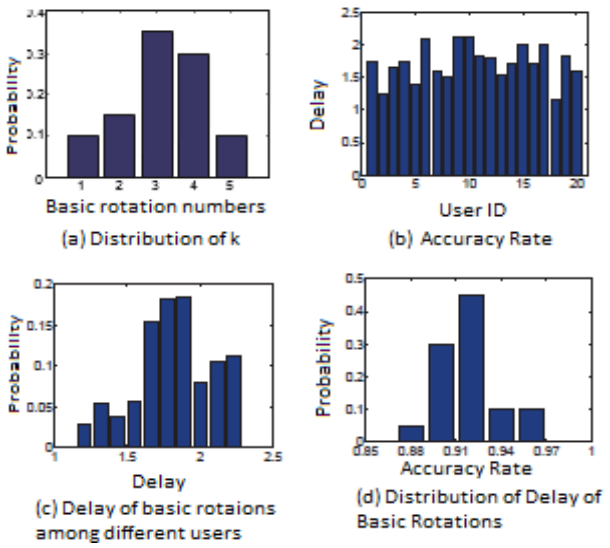

Fig 6. Experimental results with 10 users

5 RELATED WORK

Recently, researchers have introduced several RFID-based solutions to improve the security level of access control systems [6], [10]. Sample et al. present a solution for adding capacitive touch sensing onto RFID tags for capacitive user input [6]. To further improve the system security, Saxena et al. [10] introduce a method to generate random numbers to achieve motion detection based on the ambient noise of onboard accelerometer of RFID tags.

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 are backward compatible with the existing deployed RFID authentication systems. Apart from the accelerometer various low-power sensors including temperature, microphone, electronic compass and barometer [11], [12], [13] are also desirable candidates of the proposed framework that would bring large key space increases with simple sensor readings. With such embedded sensor information and significantly increased key space, we can effectively counterattack the compromise of the access control system.

6 CONCLUSIONS

In this article, we gears a dynamic authentication system for the access control systems. Authentication of present system focuses on the static information exchange and this may produce various issues such as access card stolen, loss and duplications. Our dynamic authentication system merges the sensory information from the accelerometer sensor and Static access card ID information. We academically explore that the dynamic authentication system increases the key space match than to static key space in standing authentication. To attest the dynamic authentication performance we implement the model system and prove the results manually. In prototypical tests, we achieve more key space and 95% accuracy rate among the different users. We admit that the dynamic authentication based on the sensory information can produce superior security level of access control systems and this will be a vital footstep towards forthcoming electronic growths in access authentication.

REFERENCES

[1] Y. Shu, Y. Gu, and J. Chen, "Dynamic authentication with sensory information for the access control systems," in *IEEE Transactions, vol.25, pp. 427-436, 2014.*

[2] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, 2006.

[3] R. Mayrhofer and H. Gellersen, "Shake well before use: Authentication based on accelerometer data," *Pervasive Computing*, pp. 144 – 161, 2007.

[4] 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.

[5] 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.

[6] A. P. Sample, D. J. Yeager, and J. R. Smith, "A capacitive touch interface for passive RFID tags," in *IEEE RFID*, 2009.

[7] 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.

[8] Jianfeng Liu, Zhigeng Pan, and Xiangcheng, "An Accelerometer- Based Gesture Recognition Algorithm and its Application for 3D Interaction", in ComSIS Vol. 7, No. 1, Special Issue, February 2010

[9] Jaihui Wu, Gang Pan, Daqing Zhang, Guande Qi, and Shijian Li, "Gesture Recognition with a 3-D Accelerometer" in UIC 2009, LNCS 5585, pp. 25–38, 2009.

[10] 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.

[11] N. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. Campbell, "A survey of mobile phone sensing," *IEEE Communications Magazine*, vol. 48, no. 9, pp. 140–150, Sept. 2010.

[12] P. Kannan, P. Seshadri, M.-C. Chan, A. L. Ananda, and L.-S. Peh, "Low cost crowd counting using audio tones," in *ACM SenSys*, 2012.

[13] J. Chung, M. Donahoe, C. Schmandt, I.-J. Kim, P. Razavai, and M. Wiseman, "Indoor location sensing using geo-magnetism," in *ACM MobiSys*, 2011.