Proceedings of International Conference on Technology and Social Science 2017
Invited Paper

Unintentional Path of Intra-body Communication at Dynamic Situation in Secure Gate

Yuki Wada[1,a], Keisuke Furuya[1], Ryota Kato[1], Kenta Nezu[1], and Mitsuru Shinagawa[1]

[1]Faculty of Science and Engineering, Hosei University, 3-7-2, Kajino-cho, Koganei-shi, Tokyo, 184-8584, Japan

[a]<yuki.wada.3q@stu.hosei.ac.jp>

Keywords: intra-body communication, unintentional path signal, secure gate, transmitter, receiver

Abstract. The estimation of an unintentional path during intra-body communication with two walking persons is described. The unintentional path is defined as an electric field signal propagation between free space and the human body. A gate system cannot distinguish the unintentional path from a correct path. The unintentional path is therefore examined by changing the distance between two walking persons. Unintentional authentication was not observed in an ordinary condition.

1. Introduction

Intra-body communication [1] uses a human body (HB) as a transmission path. In this type of communication, a natural action functions as a communication trigger, and the usability of a security system is improved. There is an unintentional path in intra-body communication, caused by a return path [2] signal of the communication device. It is important to estimate this unintentional path in dynamic situations with walking people in order to develop a walk-through secure gate.

2. Unintentional path

The schematic of an unintentional path in a secure gate is shown in Fig. 1. One human body (HB1) has a card device (CD1), and the other (HB2) has a CD2. A floor electrode is connected to a floor device. The operation of the CD1 and CD2 is a transmitting mode, and that of the floor device is a receiving mode. When the HB1 steps on the floor electrode, a correct path signal with the ID data of the CD1 is authenticated by the floor device through the HB1 and the electrode. When the HB2 is walking near the HB1, an electric field signal with the ID data of the CD2 can also be authenticated through the HB1. This phenomenon is known as an unintentional path.

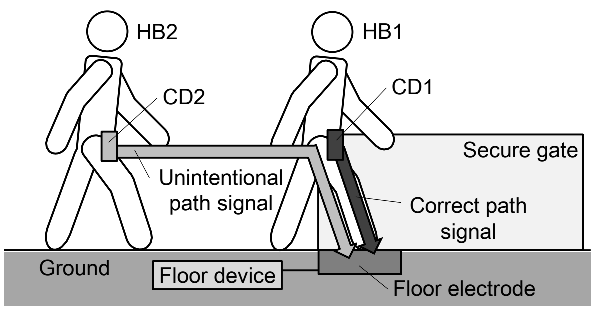

Fig. 1. Schematic of unintentional path in secure gate.

3. Experimental setup

The communication system used for experimentation is shown in Fig. 2. The CD is driven by a coin type lithium battery, sized 60 × 97 × 7.3 mm. It is located at the center of the HB at a height of 1000 mm above the floor. The distance *T* between the HB and the CD is maintained by a foamed styrol thickness. The foamed styrol and the CD are fastened to the HB by a belt. The floor device is controlled by the PC through an Ethernet interface. The size of the floor device is 178 × 56 × 116 mm, and that of the floor electrode is 430 × 415 × 8 mm. The communication device uses binary phase shift keying (BPSK) modulation. The carrier frequency is 6.75 MHz and the communication speed is 422 kbps. The PC sends polling data at a repetition rate of 250 msec. The HB steps on the floor electrode, the CD receives the polling data, and the CD outputs the response data. The PC then authenticates the ID of the response data.

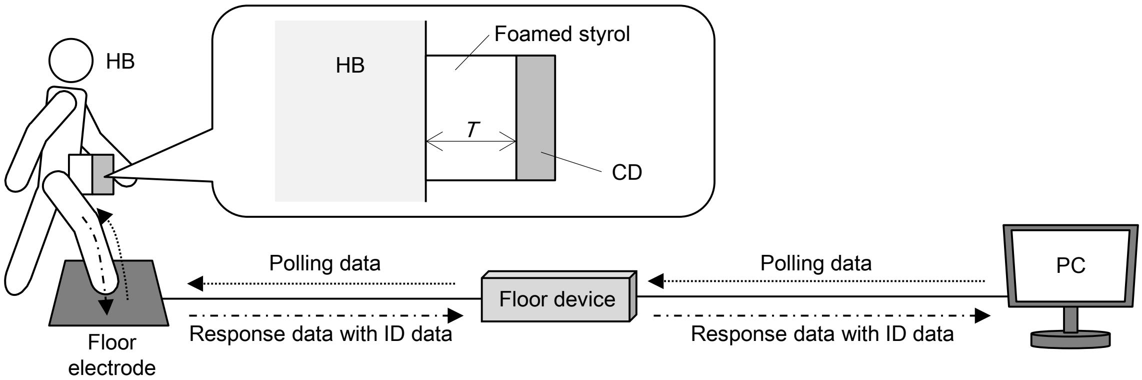

Fig. 2. Communication system.

A schematic of the experimental setup in a dynamic situation with two walking persons is shown in Fig. 3. The HB1 and HB2 walk through the secure gate. The walking speed is 1 m/s, the step size is 600 mm, and the distance *D* from the HB1's back to the HB2's chest is changed from 600 to 1000 mm. The walking speed and the distance *D* are kept constant by a metronome and the floor step marks. The foamed styrol thickness *T* is changed to 10, 50, and 100 mm.

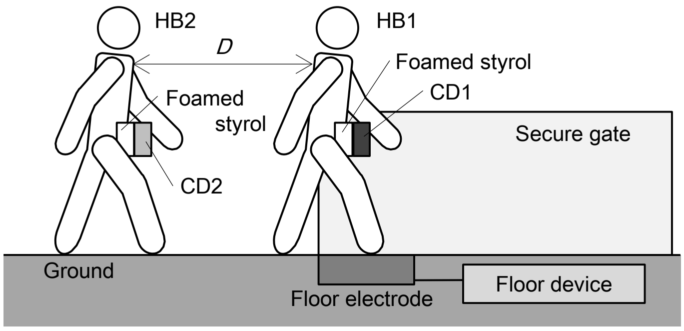

Fig. 3. Schematic of experimental setup in dynamic situation with two walking persons.

4. Experimental results

A Venn diagram of the authentication pattern at the dynamic situation is shown in Fig. 4. The authentication pattern is defined as A_{mn} (m, n = 1, 2). The m is the HB number stepping on the floor electrode, and the n is the CD number. m = n means a correct authentication pattern and m ≠ n means an unintentional authentication pattern. For example, A_{11} shows that the ID data of the CD1 is authenticated by the floor device through the HB1. When two persons walk through the gate, the authentication pattern is expressed by $A_{mn}\cdot A_{m'n'}$. The authentication pattern of m = m' is null because two persons step on the floor electrode one by one. When two persons walk through the secure gate, there are eight authentication patterns. In the experiment, $A_{11}\cdot A_{22}$, $(A_{11}\cdot \bar{A}_{21})\cdot(A_{11}\cdot \bar{A}_{22})$, $(\bar{A}_{11}\cdot A_{22})\cdot(\bar{A}_{12}\cdot A_{22})$, and $A_{12}\cdot A_{22}$ were observed. $A_{11}\cdot A_{22}$ is the best authentication pattern. $(A_{11}\cdot \bar{A}_{21})\cdot(A_{11}\cdot \bar{A}_{22})$ means that only the ID data of the CD1 is authenticated correctly. $(\bar{A}_{11}\cdot A_{22})\cdot(\bar{A}_{12}\cdot A_{22})$ means that only the ID data of the CD2 is authenticated correctly. These authentication patterns are caused by environmental noise [3][4][5] or a data collision. It is not a problem because these patterns can be distinguished by the secure gate system. These authentications will be solved by an infrared position sensor. $A_{12}\cdot A_{22}$ is the unintentional authentication pattern. The unintentional path signal with the ID data of the CD2 is authenticated when the HB1 steps on the floor electrode─in other words, the HB1 can pass the secure gate using the ID data of the CD2. The secure gate system cannot distinguish the unintentional authentication from the correct one.

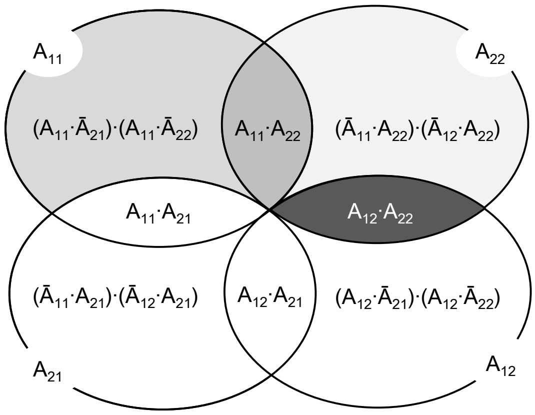

Fig. 4. Venn diagram of authentication pattern in dynamic situation.

Counts of authentication in the experiment at the *D* of 600 and 700 mm are shown in Table 1. (All of the experimental results at the *D* of 800, 900, and 1000 mm are the best authentication pattern $A_{11}\cdot A_{22}$, so they are not listed.) There were 30 counts in total. The unintentional authentication pattern $A_{12}\cdot A_{22}$ was authenticated four times at the *D* of 600 mm and the *T* of 100 mm. The distance between the HB1 and the CD2 became short, and we think that the coupling capacitance between the HB1 and the CD2 was strong. Then, we infer that the unintentional path signal became large. We think that $A_{12}\cdot A_{22}$ was sometimes observed when the unintentional path signal strength was nearly equal to the correct signal one. The situation of the *D* of 600 mm and the *T* of 100 mm was extremely rare case in the secure gate, which indicates that the unintentional path did not occur in normal situations.

Table 1. Counts of authentication in experiment at dynamic situation

Counts of experiment 30	D [mm]					
	600			700		
Authentication pattern	T [mm]			T [mm]		
	10	50	100	10	50	100
$(A_{11}\cdot\bar{A}_{21})\cdot(A_{11}\cdot\bar{A}_{22})$	1	0	0	0	0	0
$(\bar{A}_{11}\cdot A_{22})\cdot(\bar{A}_{12}\cdot A_{22})$	20	21	17	0	10	16
$A_{11}\cdot A_{22}$	9	9	9	30	20	14
$A_{12}\cdot A_{22}$	0	0	4	0	0	0

5. Conclusion

The unintentional path in the dynamic situation in a secure gate was investigated. We developed an experimental setup using two persons, a card device, floor device, metronome, and floor step marks. The unintentional authentication pattern of two walking persons was not observed except in an extremely rare case.

References

[1] T. G. Zimmerman, "Personal area networks: Near-field intrabody communication," ***IBM System Journal***, vol. 35, no. 3–4, pp. 609–617, 1996.

[2] I. Yokota, H. Shimasaki, T. Nakamura, Y. Kada, and M. Ishida, "Analysis of signal propagation loss on the human body in intrabody communication," ***2015 9th International Symposium on Medical Information and Communication Technology*** (ISMICT), pp. 35–39, 2015

[3] N. Haga, K. Motojima, M. Shinagawa, and Y. Kado, "Equivalent-Circuit Expression of Environmental Noise Electric Fields in Intrabody Communication Channels," ***IEEE Transactions on Electromagnetic Compatibility***, vol. 58, no. 1, pp. 294–306, 2016.

[4] M. Shinagawa, J. Katsuyama, K. Matsumoto, S. Hasegawa, R. Sugiyama, and Y. Kado, "Noise analysis for intra-body communication based on parasitic capacitance measurement," ***Measurement Elsevier***, vol. 51, pp. 206–213, 2014.

[5] Y. Hayashida, M. Hasegawa, A. Suzuki, M. Shinagawa, Y. Kado, and N. Haga, "Radiated noise analysis via human body for intra-body communication," ***Measurement Elsevier***, vol. 89, pp. 159–165, 2016.