Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.6, Dec. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.6.1405

걸음걸이 비디오를 활용한 웨어러블 기기 사용자 걸음걸이 가속도 신호 추정*

이 두 형,† 최 원 석, 이 동 훈‡
고려대학교 정보보호대학원

A Study on Estimation of Gait Acceleration Signal Using Gait Video Signal in Wearable Device*

Duhyeong Lee,† Wonsuk Choi, Dong Hoon Lee‡
Graduate School for Information Security, Korea University

요 약

웨어러블 기기에서 측정되는 사용자의 걸음걸이로 인한 가속도 신호를 인증 기술에 적용하는 연구결과들이 최근에 발표되고 있다. 현재까지 발표된 걸음걸이 가속도 신호 기반의 인증 기술들은 공격자가 사용자의 몸에 직접 가속도 센서를 부착하는 방식으로만 사용자의 걸음걸이 가속도 신호를 얻을 수 있다고 가정해왔다. 그리고 걸음걸이 가속도 신호 기반의 인증 기술에 대한 실질적인 공격방법으로는 걸음걸이 모방공격이 존재하고, 공격대상과 신체조건이 유사한 사람을 이용하거나 공격대상의 걸음걸이를 촬영한 비디오를 통해서 걸음걸이 특징을 파악하는 방법을 사용해왔다. 그러나 모방공격은 효과적이지 않을 뿐 아니라, 공격 성공률 또한 매우 낮기 때문에 심각한 위협으로 받아들여지지 않고 있다. 본 논문에서는 걸음걸이 가속도 신호 기반의 인증 기술에 대한 새로운 공격 방법으로 Video Gait 공격을 제안한다. 사용자 걸음걸이 비디오 신호로부터 웨어러블 기기의 위치를 확인하고, 위치 값을 동역학적 방정식에 대입하여 사용자 걸음걸이 가속도 신호와 매우 유사한 신호를 생성할 수 있다. 8명의 피 실험자로부터 수집한 걸음걸이 비디오 와 가속도 신호를 이용하여 유사도를 비교한 결과를 보여준다.

ABSTRACT

Researches that apply the acceleration signal due to user's gait measured at the wearable device to the authentication technology are being introduced recently. The gait acceleration signal based authentication technologies introduced so far have assumed that an attacker can obtain a user's gait acceleration signal only by attaching accelerometer directly to user's body. And the practical attack method for gait acceleration signal based authentication technology is mimic attack and it uses a person whose physical condition is similar to the victim or identifies the gait characteristics through the video of the gait of the victim. However, mimic attack is not effective and attack success rate is also very low, so it is not considered a serious threat. In this paper, we propose Video Gait attack as a new attack method for gait acceleration signal based authentication technology. It is possible to know the position of the wearable device from the user's gait video signal and generate a signal that is very similar to the accelerometer's signal using dynamic equation. We compare the user's gait acceleration signal and the signal that is calculated from video of user's gait and dynamic equation with experiment data collected from eight subjects.

Keywords: Biometric Authentication, Gait signal, Spoofing Attack

Received(10. 16. 2017), Modified(11. 08. 2017), Accepted(11. 16. 2017)

* 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-01864,(안전성 연구 3세부) 암호 소프트웨어 안전성 연구)

† 주저자, hyewon815@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr(Corresponding author)

I. 서 론

최근 스마트워치나 스마트밴드와 같은 형태의 웨어러블 기기 사용이 증가하고 있다[4]. 웨어러블 기기는 항상 사용자의 몸에 부착되어 있기 때문에 긴 시간의 생체변화를 자세히 측정할 수 있고, 이러한 정보를 기반으로 하여 여러 서비스들이 등장하고 있다. 예를 들어, 모바일 헬스 케어 분야에서는 만성 신장질환자들의 생체리듬을 실시간으로 모니터링하여 위급 상황을 예측하고 사전에 경고하고 있다[5]. 일반인들도 건강관리를 위하여 웨어러블 기기를 사용하고 있다. 매일 새롭게 주어지는 건강관련 미션을 수행함으로써, 운동에 대한 흥미를 유지할 수 있게 도와주는 역할을 한다[25]. 웨어러블 기기는 사용자의 건강정보나 주변정보를 오랜 시간 동안 측정하여 맞춤형 서비스를 제공할 수 있는 장점을 가지고 있다.

하지만 이러한 서비스는 사용자 편의성과 만족도를 높여주는 동시에, 개인정보 유출의 위험성이 존재한다[6]. 특히, 웨어러블 기기에서 측정된 생체정보가 유출되면 사용자의 건강상태를 쉽게 유추할 수 있기 때문에, 웨어러블 기기로부터 측정되는 사용자의 민감한 데이터는 반드시 안전하게 관리되어야 한다. 웨어러블 기기 보안을 위하여, 동일한 신체에 부착되어 있는 웨어러블 기기들 간에 안전한 네트워크 형성을 위한 웨어러블 기기 간 인증 기술[2, 3, 10, 22, 26, 27, 28, 35, 36, 38]과 웨어러블 기기가 정당한 사용자 여부를 확인하는 웨어러블 기기 사용자 인증 기술이 연구되고 있다[7, 8, 9, 11, 14, 16, 20, 21, 22, 29, 30, 31, 32, 34, 37]. 웨어러블 기기 간 인증 기술과 웨어러블 기기 사용자 인증 기술 모두 일반적으로 웨어러블 기기에 내장된 센서로 사용자의 생체정보 (Biometric)를 측정하여 인증패턴으로 사용한다. ECG (Electrocardiography) 신호와 사용자 걸음걸이 (Gait) 패턴이 대표적으로 활용되고 있는 생체정보이다[2, 3, 8, 9, 10, 11, 14, 16, 20, 21, 26, 27, 28, 30, 32, 34, 35, 36, 37, 38]. 웨어러블 기기 간 인증 기술의 경우, 같은 신체 그리고 같은 시간에 생체정보를 측정하여 두 생체정보가 매우 유사한 경우 기기 간 상호 인증을 통과하게 된다. 두 생체정보가 정확히 일치하지 않고 매우 유사하기만 하더라도, 신호처리 과정을 거치면 기기 간 인증이 가능해 진다. 웨어러블 기기 사용자 인증은 측정된 생체정보로부터 사용자만이 가지고 있는 고유한 패턴을 추출, 저장, 그리고 비교하는 과정을 수행하고 비교 결과를 통해서 정당한 사용자임을 확인한다.

웨어러블 기기 간 인증 기술과 웨어러블 기기 사용자 인증 기술 모두 원격에서는 생체정보를 측정할 수 없다는 가정 아래에서 인증 기술이 설계되어 왔다[2, 3, 7, 8, 9, 10, 11, 14, 16, 20, 21, 22, 26, 28, 29, 30, 32, 34, 35, 36, 37, 38]. 하지만 최근에 일반 RGB 카메라를 이용하여 피부색 변화나 몸의 움직임과 같이 사용자의 미세한 신체변화를 관찰하여 심박 간격 (Inter-Pulse Interval, IPI)을 유추할 수 있다는 연구결과가 발표되었다[39, 40, 41]. ECG 신호를 이용하는 인증 기술 대부분의 경우, ECG 신호로부터 심박 간격에 대한 정보를 얻고 이 정보를 인증을 위한 특징 추출에 활용한다. 즉, ECG 신호를 이용하는 인증 기술은 생체정보를 원격에서 측정하는 공격자로부터 안전하지 않음을 의미한다. 게다가, 병원의 경우 ECG 신호를 측정하고 환자의 상태를 확인하면, 측정 결과 용지를 별도로 관리하지 않고 방치하는 것이 일반적이다. Eberz 등은 이와 같이 쉽게 ECG 신호를 얻을 수 있다는 가정 아래에서 상용 웨어러블 밴드인 Nymi 밴드에 적용되어 있는 사용자 인증 방법을 스푸핑 공격 (Spoofing Attack)하는데 성공하였다[33].

사용자 걸음걸이를 기반으로 한 인증 기술의 경우 영상 신호를 이용한 방법과 가속도 신호를 이용한 방법으로 구분된다. 대부분의 웨어러블 기기에는 가속도 센서가 탑재되어 있기 때문에, 두 가지 방법 중 가속도 신호를 이용한 인증 기술이 적용되고 있다. 사용자 걸음걸이 가속도 신호를 이용하는 인증 기술의 스푸핑 공격 방법으로는 공격자가 웨어러블 기기를 착용한 상태에서 단순히 걸음걸이를 모방하는 방법만이 현재까지 제안되었다[1, 12, 13, 15, 16]. 걸음걸이를 모방하기 위해, 비슷한 체형의 사람을 이용하거나 걸음걸이의 특징을 자세히 파악하기 위해 영상을 이용하는 방법이 있지만, 이러한 방법은 모두 매우 낮은 공격 성공률을 보여주었다. 다시 말해, 사용자 걸음걸이 가속도 신호를 이용하는 기존의 인증 기술들은 걸음걸이 모방 공격을 심각한 위협으로 간주하지 않고 있다. 본 논문에서 우리는 사용자 걸음걸이 가속도 신호를 이용하는 인증 기술에 대하여 새로운 형태의 효과적인 공격 방법을 제안한다.

사용자 걸음걸이 가속도 신호를 이용하는 기존 인증 기술의 경우에는, 공격자가 사용자 걸음걸이 가속도 신호를 얻기 위해서는 반드시 사용자 몸에 가속도

센서를 직접 부착해야 한다는 가정을 하고 있다. 하지만 우리는 사용자의 걸음걸이 비디오를 촬영하여, 이로부터 사용자 몸에 부착되어 있는 가속도 센서의 가속도 신호를 유추할 수 있는 방법을 제안한다. 그리고 피 실험자로부터 측정한 실제 데이터를 이용하여 제안하는 방법에 대한 실험 결과를 제시한다. 본 논문의 자세한 기여도는 다음과 같다.

- 사용자 걸음걸이 가속도 신호를 이용하는 웨어러블 기기 인증 기술에 대한 새로운 형태의 공격 방법 (Video Gait Attack)을 제안한다.
- 사용자의 걸음걸이를 촬영한 비디오 신호를 동역학 (Dynamics)의 강체 (Rigid body) 운동 방정식에 적용하여, 사용자 몸에 부착되어 있는 스마트워치의 가속도 신호를 계산하는 방법을 제안한다.
- 실제 8명의 피 실험자에게 스마트워치를 착용시켜 걷게 함으로써, 스마트워치의 가속도 센서로부터 얻어진 가속도 신호와 스마트폰의 카메라로 촬영한 비디오 신호로부터 계산한 Video Gait 신호가 매우 유사함을 보여준다.

II. 배경지식

이번 장에서는 우리가 제안하는 공격 방법을 이해하기 위해 1) MEMS (Micro Electro Mechanical Systems) 가속도 센서 측정 원리와 2) 동역학의 강체 운동 방정식에 대하여 설명한다.

2.1 MEMS 가속도 센서 측정 원리

MEMS 가속도 센서 내부는 도체 사이에 위치한 질량체 (Proof of Mass)가 외부의 힘에 의해 움직이도록 설계되었다. 질량체의 위치 변화로 인해 전압차이가 발생하고 MEMS 가속도 센서의 전자 시스템은 전압차를 감지하여 질량체의 위치 변화를 파악한다. 다시 말해, 외부의 힘에 의해 도체 사이의 전압차가 발생하고 이로부터 질량체의 위치 변화를 확인하여 가속도를 계산할 수 있다[18]. Fig.1.은 MEMS 가속도 센서에 외부의 힘이 작용되었을 때 동작 원리를 보여주고 있다.

질량체의 위치 변화를 이용하여 가속도를 계산하는 방법은 물체의 운동을 공학적으로 설명하는 동역학적 방법을 이용하고 있다[19]. 질량체의 위치 변화를 이용하여 MEMS 가속도 센서의 가속도를 계산하는 식을 미분방정식 형태로 유도할 수 있다. MEMS 가속도 센서는 질량체의 위치 변화를 가속도 계산식에 적용하여 가속도를 계산한다.

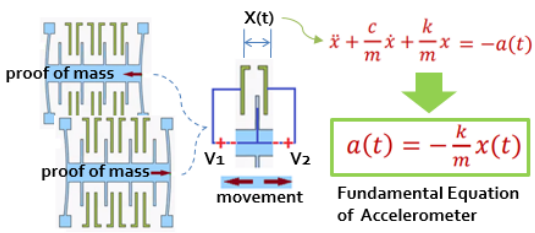

Fig. 1. Accelerometer Working Principle

2.2 동역학(Dynamics)의 강체 운동 방정식

동역학에서 설명하는 물체의 운동은 입자 (Particle)의 운동과 강체 (Rigid Body)의 운동으로 구분된다. 강체의 운동은 강체 동역학 (Rigid Body Dynamics)이라고도 하며, 이를 이용하여 움직이고 있는 강체의 운동을 설명할 수 있다. 우리는 비디오 신호를 이용하여 가속도 센서의 가속도를 계산하기 때문에, 우리가 제안하는 공격 방법은 강체 동역학을 적용하여 설명할 수 있다. 강체 동역학을 쉽게 이해하기 위한 가장 대표적인 문제로 "원반 위 거미 문제 (Spider-on-the-frisbee Problem)"를 예로 들 수 있다[19]. 고정된 위치에서 원반 위 거미를 관찰하여 거미의 속도 또는 가속도를 계산하는 문제이다. 회전하며 날아가는 원반 위 거미의 속도 또는 가속도를 계산하기 위해서 관찰자의 시점을 고정 프레임으로 두고, 원반을 이동 프레임이라고 했을 때, 고정 프레임 상에서 거미의 위치 변화와 이동 프레임 상에서 거미의 위치 변화를 관계식으로 설명할 수 있다. Fig.2.는 원반 위 거미 문제에 고정 프레임 O와 이동 프레임 P를 적용한 모습을 보여주고 있다.

우리는 고정된 위치에서 스마트워치의 위치 변화를 촬영하기 때문에, 비디오 신호의 이미지 축이 고정 프레임이 되고, 스마트워치의 가속도 센서의 축이 이동 프레임이 되며, 가속도 센서는 거미에 해당한다. 우리는 이미지 축 상에서 움직이는 스마트 워치의 위치 변화를 이용하여 스마트워치에 내장된 가속도 센서의 위치 변화에 대한 관계식을 유도하고, 이를 이용하여 가속도를 계산한다. 또한 앞서 설명한

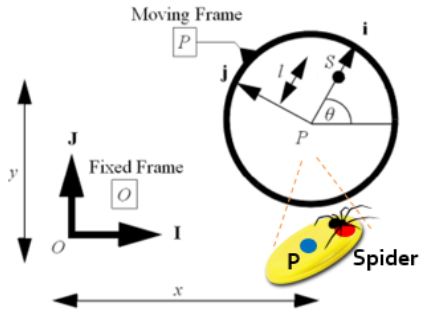

Fig. 2. Spider-on-the-frisbee Problem in Rigid Body Dynamics

MEMS 가속도 센서는 질량체의 축을 고정 프레임으로, MEMS 가속도 센서 축은 이동 프레임으로 하여 MEMS 가속도 센서의 가속도를 계산한다.

III. 가속도 센서 기반 걸음걸이 인증 시스템

우리가 제안하는 사용자 걸음걸이 가속도 신호를 이용한 인증 기술에 대한 공격방법을 설명하기에 앞서, 사용자 걸음걸이 패턴을 이용한 인증 기술에 대하여 설명하겠다. 걸음걸이는 다리 길이, 체중, 관절의 작동 범위, 걷는 습관 등으로 인해 사람마다 고유한 특징을 가진다. 그리고 서로 다른 두 사람의 발이 동일한 경로를 정해진 시간동안 움직인다고 하더라도, 경로를 지나가는 순간적인 속도가 서로 다르기 때문에 걸음걸이 특징이 서로 같기 어렵다. 이러한 사실을 이용하여 인증 기술 설계를 위해 사용자 걸음걸이 가속도 신호를 적용하고 있다.

사용자 걸음걸이 패턴은 비디오 신호나 가속도 신호로부터 추출할 수 있다. 웨어러블 기기에는 일반적으로 가속도 센서가 내장되어 있기 때문에, 가속도 신호부터 사용자의 걸음걸이 패턴을 추출하고 이를 이용하여 인증 기술을 설계하고 있다[10, 11, 14, 16, 20, 21, 26, 27, 28]. 웨어러블 기기 보안을 위한 인증 기술은 웨어러블 기기 간 인증 기술과 웨어러블 기기 사용자 인증 기술로 구분할 수 있고, 사용자 걸음걸이 신호는 두 가지 인증 기술 모두에서 활용 될 수 있다.

사용자 걸음걸이를 이용한 웨어러블 기기 간 인증 기술은 사용자 몸에 부착되어 있는 두 개의 웨어러블 기기가 동시에 걸음걸이 가속도 신호를 측정하고 두 신호의 유사도를 이용하여 상호 인증을 수행하는 과정을 말한다[10, 26, 27, 28]. 사용자 걸음걸이 가속도 신호를 이용한 웨어러블 기기 사용자 인증 기술은 걸음걸이 가속도 신호로부터 사용자 걸음걸이 패턴의 고유한 특징 정보를 추출하여 템플릿으로 저장하고, 인증 시 새롭게 측정된 가속도 신호로부터 추출한 특징 정보와 템플릿간의 유사도 비교를 통해 인증을 수행한다[11, 14, 16, 20, 21]. 본 논문의 공격 대상인 걸음걸이 가속도 신호를 이용한 웨어러블 기기 사용자 인증 기술은 일반적으로 1) 걸음걸이 측정 및 신호 처리 단계, 2) 특징 추출 단계, 그리고 3)유사도 검증 단계 3가지 단계로 구성되어 있으며 각 단계에 대한 자세한 설명은 다음과 같다.

3.1 걸음걸이 측정 및 신호 처리 단계

발을 내딛을 때 발생하는 충격과 그 충격을 흡수하기 위한 몸의 움직임 등이 사용자 몸에 부착된 웨어러블 기기에 외부의 힘으로 작용한다. 이로 인해 사용자가 걷는 동안, 웨어러블 기기의 가속도 센서로 걸음걸이 가속도 신호를 측정할 수 있다. 이렇게 측정된 걸음걸이 가속도 신호는 다음과 같은 신호처리 과정을 거친다.

전처리 과정. 측정된 걸음걸이 가속도 신호에서 노이즈를 제거하는 단계이고, 일반적으로 로우패스 필터 (Low Pass Filter)가 사용된다.

걸음걸이 탐지 과정. 전체 가속도 센서 신호 중 실제 걸음걸이로 인한 가속도 신호만을 추출하고, 피크 검출 (Peak Detection) 알고리즘이 사용된다.

걸음단위 구분 과정. 걸음걸이로 인한 가속도 신호가 탐지되면 연속된 걸음걸이 가속도 신호를 걸음 단위로 구분 (Segmentation) 한다.

3.2 특징 추출 단계

걸음단위로 구분된 가속도 신호로부터 사용자 걸음걸이 패턴의 고유한 특징 정보를 추출하기 위하여 여러 특징 (Feature) 값들을 활용한다. 일반적으로 통계적 특징 (Statistical Feature) 값들이 사용된다[23]. 우리는 기존의 걸음걸이 가속도 신호를 이용한 인증 기술 연구에서 많이 사용된 통계적 특징은 다음과 같이 20개로 정리하였다.

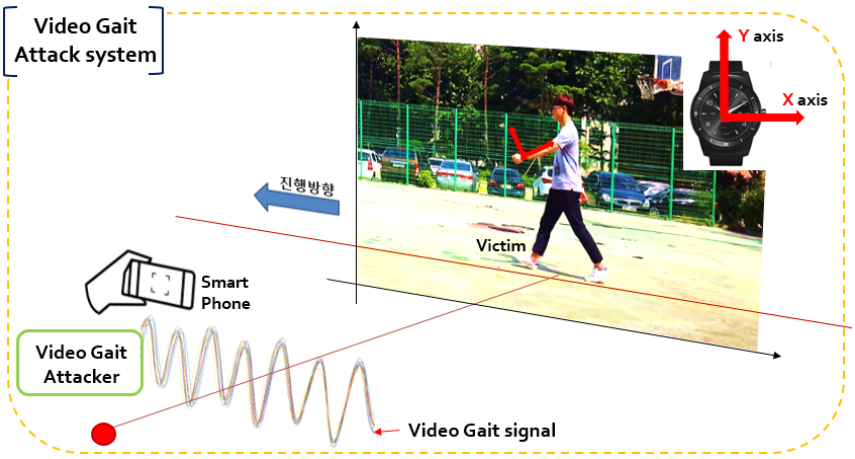

Fig. 3. Video Gait Attack Model

- 평균 (Average), 중앙값 (Median), 분산 (Variance), 표준편차 (Standard Deviation), 왜도 (Skewness), 첨도 (Kurtosis), 백분위수 25 (Percentile 25), 백분위수 50 (Percentile 50), 차분 (Difference), 평균절대차이 (Average Absolute Difference), 피크 출현수 (Peaks Occurrence), 최소 피크 (Minimum Peaks), 최대 피크 (Maximum Peaks), 피크 시간 간격 (Time Between Peaks), 최솟값 (Minimum), 최댓값 (Maximum), 영점교차율 (Zero Crossing Rate), 제곱평균제곱근 (Root Mean Square), 사분위 범위 (Inter-Quartile Range), 교차 상관(Cross Correlation)

3.3 유사도 검증 단계

유사도 검증 단계는 사전에 등록해둔 사용자 걸음걸이 템플릿과 인증 시점의 새로운 걸음걸이 특징과의 유사도를 확인한다. 유사도 비교 방법으로는 기계학습 (Machine Learning) 알고리즘을 이용하는 방법과 유클리디안 거리 (Euclidean Distance), 교차 상관 (Cross Correlation) 등과 같은 거리 함수 (Metric Function)를 이용하는 방법으로 구분된다.

IV. 제안하는 Video Gait 공격 모델

사용자 걸음걸이 가속도 신호를 이용한 인증 기술들은 사용자 몸에 부착되어 있는 가속도 센서의 신호를 활용하여 기기 또는 사용자를 인증 한다. 사람들의 고유한 걸음걸이 특성이 가속도 신호에 반영되기 때문이다. 따라서 사용자 몸에 부착되어 있는 정당한 웨어러블 기기 (가속도 센서) 만이 걸음걸이로 인한 가속도 신호를 측정할 수 있도록 설계되어야 한다. 하지만 걸음걸이 가속도 신호를 이용한 기존 인증 기술들은 단순히 사용자와의 신체접촉 없이 원격에서 걸음걸이로 인한 가속도 신호를 추정 할 수 없다고 가정하고 있다.

하지만 Video Gait 공격 모델에서 공격자의 목표는 사용자와의 신체접촉 없이 원격에서 사용자 걸음걸이 가속도 신호를 올바르게 추정하는 것이다. Video Gait 공격자는 사용자가 걸을 때, 웨어러블 기기의 움직임을 비디오로 촬영하고 이로부터 실제 걸음걸이 가속도 신호를 유추한다. 이렇게 얻어진 신호를 우리는 Video Gait 신호라 부른다. Fig.3.은 Video Gait 공격 모델의 개념을 보여주고 있다. Video Gait 신호는 이후 사용자 걸음걸이 가속도 신호를 이용한 인증 기술의 스푸핑 공격에 활용될 수 있다. 따라서 우리가 제안하는 Video Gait 공격 모델은 사용자 걸음걸이 가속도 신호를 이용한 웨어러블 인증 기술의 새로운 공격 모델이 된다.

V. Video Gait 신호

이번 장에서는 고정된 위치에서 웨어러블 기기 (가속도 센서)의 움직임을 촬영한 비디오 신호로부터 가속도 센서의 픽셀단위 위치변화를 확인하고 가속도

신호를 계산하는 방법에 대하여 설명한다. 이 때, 단순히 가속도 센서를 면적이 없는 입자로 간주하면 제자리 회전으로 인한 위치변화를 설명할 수 없다. 즉, 가속도가 0이 된다. 실제로 웨어러블 기기는 사용자 손목 등에 착용된 상태에서 회전으로 인한 위치변화가 관찰된다. 따라서 우리는 가속도 센서를 입자가 아닌 강체로 간주하여 운동을 설명한다.

5.1 웨어러블 기기 위치변화 확인

공격자는 고정된 위치에서 걸어가고 있는 사용자를 카메라로 촬영하여 비디오 영상을 얻는다. 비디오 신호를 전체 n개의 프레임이라고 할 때, 공격자는 각 프레임에서 웨어러블 기기의 위치 (u,v)와 각도 Θ를 다음과 같은 절차로 확인한다. 웨어러블 기기의 위치를 표현하기 위해 웨어러블 기기 상에 임의의 점 P를 설정하여, 각 프레임마다 P의 위치를 표시한다. 웨어러블 기기에서 가속도 센서의 위치를 점 S라고 하였을 때, 임의로 설정된 점 P는 점 S와 같지 않도록 선택되어야 한다. 만약, 점 P와 점 S가 일치하면 강체의 운동이 아닌 입자의 운동에 해당하기 때문이다. 일반적으로 점 P는 웨어러블 기기의 중심 지점으로 선택하고, 가속도 센서의 위치에 대한 정보는 인터넷에 공개되어 있다.

웨어러블 기기의 가속도 센서의 위치뿐만 아니라 가속도 센서의 센싱 축 정보도 공개되어 있기 때문에, 해당 센싱 축과 점 P를 원점으로 하는 프레임을 정의한다. 이 프레임은 강체 동역학에서 이동 프레임에 해당하며, 영상은 고정 프레임에 해당한다. 웨어러블 기기의 각도 변화는 고정 프레임과 이동 프레임 사이의 각도 Θ로 표현한다.

5.2 Video Gait 신호

Video Gait 신호는 웨어러블 기기에서 측정되는 걸음걸이 가속도 신호를 유추하기 위해 걸음걸이 비디오 신호로부터 계산된 값을 의미한다. 이는 앞서 2.2 절에서 설명한 '원반 위 거미' 문제로 대응된다. 여기서 원반은 웨어러블 기기에 해당하고 가속도 센서는 거미에 해당한다. 이동 프레임 상의 원점 P를 기준으로 하면 가속도 센서의 위치인 점 S의 위치변화는 관찰되지 않지만, 이동 프레임이 움직이거나 회전하기 때문에 고정 프레임 상의 원점 O를 기준으로 하면 점 S의 위치는 변화한다. 다시 말해, 이동 프

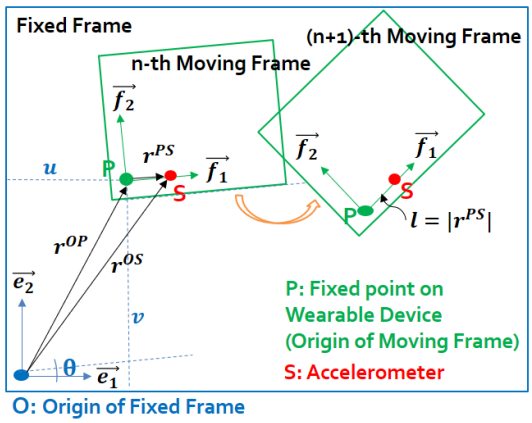

Fig. 4. Dynamics of Wearable Device

레임 상에서 벡터 r^{PS}를 표현하며 벡터의 성분은 항상 일정하지만, 고정 프레임 상에서 벡터 r^{PS}를 표현하면 벡터의 성분은 변화한다. Fig.4.는 고정 프레임과 이동 프레임 상의 관계와 보여주고 있다.

고정 프레임 상에서 가속도 센서의 위치를 벡터 r^{OS}로 표현하면 식(1)과 같이 벡터 r^{OP}와 벡터 r^{PS}로 표현된다.

$$r^{OS} = r^{OP} + r^{PS} \tag{1}$$

벡터 r^{OP}는 고정 프레임 상에서 웨어러블 기기의 위치 P를 표현한 벡터이고, 우리는 앞서 P의 위치를 (u,v)라 표현하였기 때문에 벡터 r^{OP}는 식 (2)와 같이 된다. 벡터 e_1, e_2는 고정프레임의 직교 좌표계의 각 축을 표현하는 단위 벡터이다.

$$r^{OP} = (e_1 u + e_2 v) \tag{2}$$

벡터 r^{PS}는 동일한 방법으로 이동 프레임의 직교 좌표계의 각 축을 표현하는 단위 벡터 f_1, f_2와 이동 프레임 상에서 점 S의 위치 (u',v')로 표현할 수 있다. 하지만 이동 프레임의 직교 단위 벡터 f_1, f_2는 가속도 센서의 센싱 축과 일치하므로 웨어러블 기기의 임의의 지점으로 선택되는 점 P에 위치에 따라 벡터 r^{PS}는 간단하게 표현될 수 있다. 즉, 벡터 r^{PS}의 방향이 이동 프레임의 직교 단위 벡터 f_1과 방향이 일치하면 벡터 r^{PS}는 식 (3)과 같이 표현할 수 있다. l은 점 P와 점 S 사이의 거리이다.

$$r^{PS} = f_1 l \tag{3}$$

식 (2)와 식 (3)을 이용하여 벡터 r^{OS}는 식 (4)와 같이 표현 할 수 있다.

$$r^{OS} = (e_1 u + e_2 v) + f_1 l \tag{4}$$

우리는 비디오 신호의 각 프레임으로부터 벡터 r^{OS}를 계산할 수 있고, 이 값은 고정 프레임 상에서 점 S의 위치변화라 할 수 있다. 가속도 센서의 위치 변화를 시간에 대해서 미분하여 우리는 가속도 센서의 가속도를 계산할 수 있다. 직교 단위 벡터 e_1, e_2는 시간에 따라 변하지 않는 고정된 값이지만, 직교 단위 벡터 f_1은 시간에 따라 변화한다. 우리는 앞서 고정 프레임과 이동 프레임 사이의 각도 Θ를 계산하였고, 각도 Θ의 변화율을 이용하여 직교 단위 벡터 f_1의 변화율을 식 (5)와 같이 표현할 수 있다.

$$f_1 = e_1 \cos\theta + e_2 \sin\theta \tag{5}$$

결과적으로 가속도 센서의 위치 변화인 벡터 r^{OS}를 두 번 미분하여 얻어지는 가속도 센서의 가속도 값인 벡터 a^{OS}는 식 (6)과 같이 된다. 여기서, $\dot{x} = \frac{dx}{dt}$, $\ddot{x} = \frac{d^2x}{dt^2}$ 를 의미 한다.

$$\begin{aligned} a^{OS} = e_1(&\ddot{u} + \ddot{l}\cos\theta - 2\dot{\theta}\dot{l}\sin\theta - \ddot{\theta}l\sin\theta - \dot{\theta}^2 l\cos\theta) \\ &+ e_2(\ddot{v} + \ddot{l}\sin\theta + 2\dot{\theta}\dot{l}\cos\theta + \ddot{\theta}l\cos\theta - \dot{\theta}^2 l\sin\theta) \end{aligned} \tag{6}$$

VI. 평가 결과

이번 장에서는 제안하는 공격 모델을 평가하기 위해 사용된 실험 환경을 설명하고, Video Gait 신호와 가속도 센서에서 측정된 실제 가속도 신호와의 유사도 측정 방법 및 그 결과를 보여준다.

6.1 실험 환경

걸음걸이 가속도 신호를 측정하기 위하여, 우리는 안드로이드 웨어 (Android Wear) 기반의 스마트 워치 (LG G WATCH R)를 이용하였다. 스마트워치를 손목에 착용하여 걸음걸이로 인한 가속도 신호를 측정하였고, 약 7m 떨어진 고정된 위치에서 삼각대와 스마트 폰 (SAMSUNG GALAXY 6)를 이용하여 비디오 영상을 촬영하였다. 기본적으로 가속도 센서로 측정되는 가속도 신호에는 중력 가속도가 함께 포함되기 때문에, 안드로이드에서 소개하고 있는 중력제거를 위한 신호 전처리 방법을 적용하였다. 8명 (남자 5, 여자 3)의 피 실험자를 선정하여 가속도 신호와 비디오 신호 쌍의 실험 데이터를 수집하였다. 이 때, 1명의 피 실험자의 걸음걸이를 보고, 나머지 7명의 피 실험자는 걸음걸이를 흉내 내는 공격자 (Mimic Attacker) 역할을 수행 하도록 요청하여 걸음걸이를 흉내 내는 공격자 가속도 신호 데이터를 추가적으로 측정하였다. 이러한 실험은 각 피 실험자에 대하여 30번씩 반복하였다.

고정 프레임 상의 원점 O는 비디오 신호의 각 영상 프레임 좌측 하단 부분으로 설정하였고, 스마트워치의 가속도 센서 위치와 센싱 축 정보를 바탕으로 하여 이동 프레임의 점 P와 S를 설정하였다. Fig.5.(1)은 우리가 사용한 스마트워치의 가속도 센서의 위치와 센싱 축을 보여주고 있으며, Fig.5.(2)는 비디오 신호의 각 영상 프레임에서 고정 프레임과 이동 프레임의 관계를 보여주고 있다.

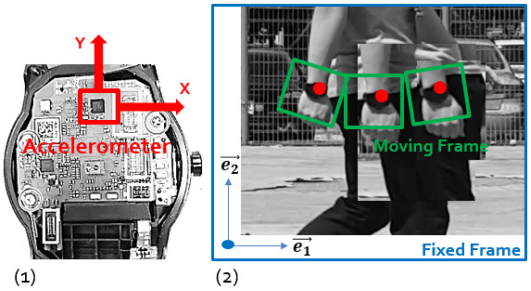

Fig. 5. Sensing axis of Accelerometer (left) and relation between fixed frame and moving frame in video images (right)

6.2 가속도 신호와 Video Gait 신호 간의 유사도

시간에 따라 변화하는 두 신호 X(t)와 Y(t) 간의 유사도 $Score_{XCorr}$를 확인하기 위해, 우리는 식 (7)과 같이 신호처리 분야에서 널리 사용되는 교차상관 (Cross-correlation)을 이용하였다.

$$Xcorr_{X,Y}(d) = \sum_{t=0}^{n-1} X(t)\, Y(t-d) \quad (7)$$

$XCorr_{X,Y}(d)$는 두 신호 X(t)와 d시점 이전의 신호 Y(t-d)의 교차상관을 계산하는 함수이다. 여기서 d는 시간 지연 (lag)라 하고, 교차상관 함수 $XCorr_{X,Y}(d)$의 최댓값을 최대교차상관 (Maximum Cross-correlation)이라 한다. 우리는 식(8)과 같이 유사도를 정의하였다.

$$Score_{XCorr} = XCorr_{X,Y}(d^*) \quad (8)$$
$$where \;\; d^* = \arg max_d(|XCorr_{X,Y}(d)|)$$

교차상관 함수 $XCorr_{X,Y}(d)$이 최대가 되는 시간 지연 값 d*를 찾고, 최대교차상관 $XCorr_{X,Y}(d^*)$을 유사도 $Score_{XCorr}$로 이용한다. 우리는 최대교차상관 값을 0과 1사이 값으로 정규화 하였기 때문에 유사도 $Score_{XCorr}$가 1에 가까울수록 두 신호간의 유사도가 높다고 판단한다.

Fig.6.는 최대교차상관을 이용한 두 신호간의 유사도결과를 보여주고 있다. Subject는 동일한 사용자의 30개의 걸음걸이 가속도 신호들 간의 최대교차상관 값을 의미한다. V-Gait은 피 실험자의 걸음걸이 가속도 신호와 같은 시간에 촬영된 비디오 신호로부터 계산된 Video Gait 신호 간의 최대교차상관 값을 의미한다. 그리고 Mimic1~Mimic7은 피 실험자의 걸음걸이를 보고 나머지 피 실험자들이 걸음걸이를 흉내 내면서 걸었을 때 가속도 신호를 이용한 최대교차상관 값을 의미한다. 걸음걸이를 흉내 내는 사람의 신장이나 체중에 따라 유사도 결과가 달라지는 것을 확인할 수 있다.

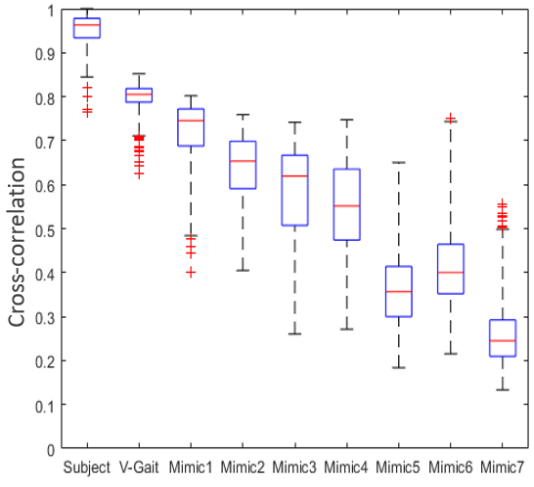

Fig. 6. Box plot: maximum cross correlation between acceleration of subject05 and attacker(V-Gait,Mimic1~7) signal

Table 1.은 모든 피 실험자에 대한 최대교차상관 값들의 평균값을 보여주고 있다. 이 결과는 걸음걸이를 흉내 내는 공격자보다 Video Gait 공격자가 더 유사한 신호를 추정 할 수 있음을 의미한다. Fig.7.은 피 실험자의 걸음걸이로 인한 가속도 신호, 비디오 신호로부터 계산한 Video Gait 신호, 그리고 피 실험자의 걸음걸이를 흉내 내었을 때의 가속도 신호를 동시에 보여주고 있다. 시각적으로 확인한 결과로도 Video Gait 신호가 걸음걸이를 흉내 내었을 때의 가속도 신호보다 매우 효과적임을 알 수 있다.

Table 1. Averaged maximum cross correlation of all subject's signal between Video Gait signal and Mimic signal

Subject ID	averaged maximum cross correlation		
	Subject	Video Gait	Mimic
01	.86	.73	.51
02	.93	.76	.50
03	.74	.70	.46
04	.87	.79	.46
05	.95	.89	.51
06	.68	.57	.37
07	.75	.62	.34
08	.78	.56	.28

6.3 특징 추출을 이용한 유사도

III장에서 설명한 것과 같이, 일반적으로 걸음걸이 가속도 신호를 이용한 인증 시스템은 원본의 걸음걸이 가속도 신호로부터 특징 정보를 추출한다. 따라서 이번 절에서는 원본 신호에서 특징 정보를 추출하고 특징 값들 간의 유사도를 비교한다. 두 개의 특징 값의 유사도 $Score_{ED}$를 계산하기 위하여 식 (9)와 같이 유클리디안 (Euclidean) 거리 함수를 사용하였다. 앞에서 사용한 최대상관계수와 달리, 두 특징 값 사이의 유클리디안 거리가 0에 가까울수록 유사도가 높다고 판단한다.

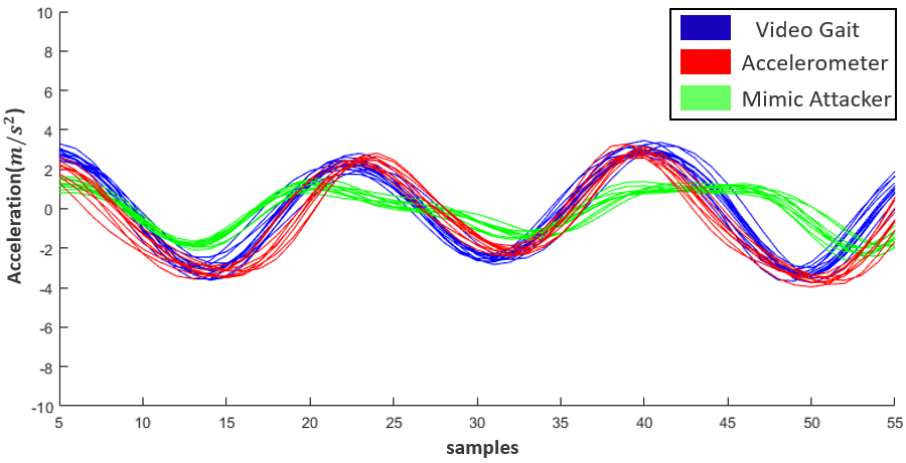

Fig. 7. Video Gait signal, Accelerometer signal and Mimic Attacker signal of x axis form subject's two steps

$$Score_{ED} = Euclidean(F_{ACC_A}, F_{ACC_B}) \quad (9)$$

여기서, F_{ACC_A}와 F_{ACC_B}는 각각 가속도 신호 ACC_A와 ACC_B로부터 계산된 특징 값이고, 두 특징 간의 유클리디안 거리 $Euclidean(F_{ACC_A}, F_{ACC_B})$는 유사도 $Score_{ED}$로 이용된다.

3.2절에서 설명한 것과 같이, 사용자 걸음걸이 가속도 신호를 이용한 인증 시스템에서 널리 사용하는 특징 정보 20개를 원본 신호로부터 추출하였다. Fig.8.은 두 신호로부터 20개의 특징 정보를 추출하고 각 특징 정보를 0과 1사이의 값으로 정규화(normalization)한 상태에서 계산한 유클리디안 거리들의 평균을 보여주고 있다. 원본 신호로부터 특징 정보를 추출하여 유사도를 비교한 경우에도, 걸음걸이를 흉내 내었을 때 가속도 신호보다 Video

Table 2. Average of Euclidean distances using Features

Feat-ure	Subject01			Subject02			Subject03			Subject04			Subject05			Subject06			Subject07			Subject08		
	S2S	VG	M	SS	VG	M	S2S	VG	M	S2S	VG	M	S2S	VG	M	S2S	VG	M	S2S	VG	M	S2S	VG	M
01	.17	.11	.37	.20	.06	.29	.13	.05	.23	.07	.04	.22	.06	.05	.30	.14	.08	.29	.11	.07	.26	.05	.04	.37
02	.15	.25	.25	.09	.39	.20	.18	.37	.30	.09	.19	.18	.12	.17	.26	.10	.23	.19	.12	.25	.27	.06	.18	.18
03	.05	.08	.13	.04	.14	.13	.06	.15	.14	.03	.10	.16	.03	.09	.12	.16	.14	.17	.11	.16	.17	.16	.15	.37
04	.21	.12	.43	.24	.04	.36	.15	.05	.28	.07	.03	.27	.07	.09	.39	.07	.04	.34	.13	.08	.30	.02	.02	.43
05	.23	.12	.43	.21	.06	.34	.17	.04	.29	.08	.03	.28	.08	.12	.42	.07	.03	.33	.13	.10	.29	.02	.02	.42
06	.04	.21	.17	.04	.13	.17	.08	.09	.18	.08	.14	.16	.03	.27	.17	.24	.27	.23	.08	.38	.25	.10	.35	.38
07	.04	.07	.13	.03	.09	.13	.06	.03	.14	.08	.05	.15	.01	.06	.16	.25	.21	.24	.11	.25	.15	.12	.17	.29
08	.24	.17	.43	.22	.07	.35	.15	.05	.28	.08	.05	.28	.09	.20	.42	.07	.04	.33	.12	.09	.28	.02	.03	.40
09	.15	.25	.25	.09	.39	.20	.18	.37	.30	.09	.19	.18	.12	.17	.26	.10	.23	.19	.12	.25	.27	.06	.18	.18
10	.17	.12	.38	.25	.12	.37	.14	.10	.26	.06	.07	.24	.06	.05	.31	.10	.11	.30	.11	.05	.30	.05	.04	.36
11	.17	.12	.38	.17	.15	.26	.12	.05	.23	.08	.05	.22	.06	.08	.31	.13	.07	.29	.12	.14	.24	.03	.04	.40
12	.27	.18	.24	.17	.30	.20	.25	.18	.28	.10	.18	.27	.16	.40	.20	.10	.11	.17	.14	.14	.18	.08	.10	.18
13	.21	.12	.43	.24	.04	.36	.15	.05	.28	.07	.03	.27	.07	.09	.39	.07	.04	.34	.13	.08	.30	.02	.02	.43
14	.21	.12	.43	.23	.04	.35	.16	.04	.28	.07	.03	.27	.07	.09	.39	.18	.03	.34	.13	.08	.30	.02	.02	.43
15	.06	.09	.26	.03	.12	.23	.16	.32	.28	.15	.10	.23	.02	.04	.27	.08	.17	.27	.19	.15	.30	.10	.12	.44
16	.20	.12	.44	.20	.09	.31	.21	.16	.27	.09	.05	.26	.07	.06	.41	.08	.04	.34	.17	.07	.29	.01	.03	.40
17	.21	.12	.42	.25	.11	.37	.19	.09	.29	.08	.04	.28	.07	.06	.40	.07	.04	.35	.13	.07	.29	.02	.02	.40
18	.05	.06	.23	.06	.12	.21	.20	.26	.25	.12	.10	.21	.04	.06	.23	.20	.16	.26	.18	.12	.28	.15	.16	.45
19	.27	.15	.45	.27	.05	.35	.14	.04	.25	.05	.02	.24	.09	.11	.37	.03	.01	.28	.08	.05	.25	.01	.01	.32
20	.19	.12	.26	.30	.08	.42	.08	.05	.16	.02	.10	.15	.05	.17	.16	.03	.06	.16	.02	.03	.16	.01	.03	.20

* S2S: Subject to Subject
* VG: Video Gait attacker
* M: mimic attacker

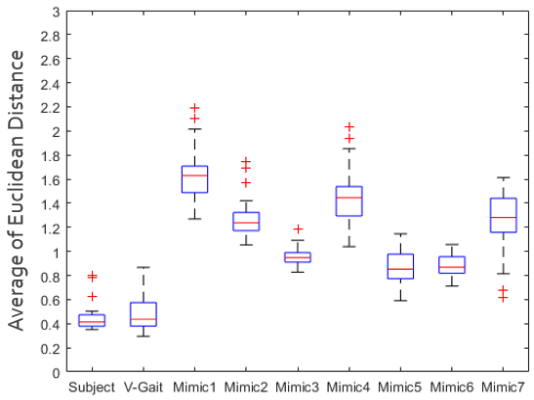

Fig. 8. Box plot: averaged euclidean distance between subject's feature and attacker(V-Gait,Mimic1~7)'s feature

Gait 신호가 더욱 효과적임을 확인 할 수 있다.

Table 2.는 8명의 피 실험자들의 실험 데이터를 이용한 유클리디안 거리들의 평균값을 모두 보여주고 있다. 이 때, 20개의 특징 값들은 모두 0과 1사이로 정규화된 결과를 사용하였다.

VII. 한계점 및 향후 연구

우리는 강체 동역학의 운동 방정식을 적용하여 걸음걸이 비디오 신호로부터 웨어러블 기기의 위치변화를 판단하고 이로부터 걸음걸이 가속도 신호를 계산하였다. 강체 동역학의 운동 방정식은 3차원으로 손쉽게 확장할 수 있지만, 1대의 카메라를 이용해서 3차원 위치변화를 판단이 어렵기 때문에 우리가 제안한 방법은 2차원 가속도 신호만을 계산할 수 있었다. 그리고 우리가 제안한 Video Gait 신호가 원본 걸음걸이 가속도 신호와 매우 유사하다 하더라도, 웨어러블 기기의 인증 시스템을 공격하기 위해서는 이 신호를 웨어러블 기기에 주입해야 한다는 문제점이 남아있다. 따라서 우리는 비디오 신호로부터 3차원 위치변화 판단하는 문제와 웨어러블 기기에 걸음걸이 가속도 신호 주입 방법에 대하여 향후 연구를 계속 진행할 예정이다.

VIII. 결 론

본 논문에서 우리는 기존의 사용자 걸음걸이 가속도 신호를 이용한 인증 기술에 적용할 수 있는 새로운 공격 모델로 Video Gait 공격을 제안하였다. 실험 결과를 통하여, 기존의 사용자 걸음걸이 가속도 신호를 이용한 인증 기술에 대한 공격 모델인 걸음걸이 모방 공격보다 매우 효과적인 공격 방법임을 보여주었다. 웨어러블 기기를 위한 인증 기술들이 많이 연구되고 있고, 걸음걸이 신호가 인증 패턴으로 주목받고 있는 가운데 우리가 제안한 공격 방법은 기존 인증기술들의 추가적인 안전성 분석을 요구하며, 향후 웨어러블 기기 인증 기술 발전에 도움이 될 것이라 기대된다.

References

[1] Gafurov Davrondzhon, Einar Snekkenes, and Patrick Bours, "Spoof attacks on gait authentication system," IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 491-502, Sept. 2007.

[2] Gafurov Davrondzhon, Kirsi Helkala, and Torkjel Søndrol, "Biometric Gait Authentication Using Accelerometer Sensor," JORNAL OF COMPUTERS, vol. 1, no. 7, pp. 51-59, Oct. 2006.

[3] Gafurov Davrondzhon, Einar Snekkenes, and Tor Erik Buvarp, "Robustness of biometric gait authentication against impersonation attack," OTM Workshops 2006, LNCS 4277, pp. 479-488, 2006.

[4] Gartner, Forecast: Wearable Electronic Devices, Worldwide, 2017, Aug. 2017.

[5] F.P. Wieringa, N. Broers, J.P. Kooman, F.M. Van Der Sande, and C. Van Hoof, "Wearable sensors: Can they benefit patients with chronic kidney disease?," Expert Review of Medical Devices, vol. 14, no. 7, pp. 505-519, Jun. 2017.

[6] Quang Do, Ben Martini, and K.K.R. Choo, "Is the data on your wearable device secure? An Android Wear smartwatch case study," Software: Practice and Experience, vol. 47, no. 3, pp. 391-403, Mar. 2017.

[7] A. Bianchi and I. Oakley, "Wearable au-

thentication: Trends and opportunities," it-Information Technology, vol. 58, no. 5, pp. 255-262, Oct. 2016.

[8] S.J. Kang, S.Y. Lee, H.I. Cho, and H. Park, "ECG Authentication System Design Based on Signal Analysis in Mobile and Wearable Devices," IEEE Signal Processing Letters, vol. 23, no. 6, pp. 805-808, Jun. 2016.

[9] W. Xu, G. Lan, Q. Lin, S. Khalifa, N. Bergmann, M. Hassan, and W. Hu, "KEH-Gait: Towards a Mobile Healthcare User Authentication System by Kinetic Energy Harvesting," NDSS Symposium 2017, Feb. 2017.

[10] W. Xu, C. Javali, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Gait-Key: A Gait-Based Shared Secret Key Generation Protocol for Wearable Devices," ACM Transactions on Sensor Networks, vol. 13, no. 1, Jan. 2017.

[11] W. Xu, Y. Shen, Y. Zhang, N. Bergmann, and W. Hu, "Gait-watch: A context-aware authentication system for smart watch based on gait recognition," 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation, pp. 59-70, Apr. 2017.

[12] B.B. Mjaaland, P. Bours, and D. Gligoroski, "Walk the Walk: attacking gait biometrics by imitation," 13th international conference on Information security, pp. 361-380, Oct. 2010.

[13] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikäinen, J. Bustard, and M. Nixon, "Can gait biometrics be spoofed?," 2012 21st International Conference on Pattern Recognition, pp. 3280-3283, Nov. 2012.

[14] T.T. Ngo, Y. Makihara, H. Nagahara, Y. Mukaigawa, and Y. Yagi, "The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication," Pattern Recognition, vol. 47, no. 1, pp. 228-237, Jan. 2014.

[15] R. Kumar, V.V. Phoha, and A. Jain, "Treadmill attack on gait-based authentication systems," 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems, pp. 1-7, Sep. 2015.

[16] M. Muaaz and R. Mayrhofer, "Smartphone-based Gait Recognition: From Authentication to Imitation," IEEE Transactions on Mobile Computing, vol. 16, no. 11, Nov. 2017.

[17] C.L. Vaughan, B.L. Davis, and C.O. Jeremy, Dynamics of Human Gait, Volume 2, Human Kinetics Publishers, 1992.

[18] Minhang Bao, Analysis and design principles of MEMS devices, 1st Ed., Elsevier, Apr. 2005.

[19] R.C. Hibbeler, Engineering Mechanics: Statics & Dynamics, 13th Ed., Pearson Education, Apr. 2001.

[20] T. Hoang, T.D. Nguyen, C. Luong, S. Do, and D. Choi, "Adaptive Cross-Device Gait Recognition Using a Mobile Accelerometer," Journal of Information Processing Systems, vol. 9, no. 2, pp. 333-348, Jun. 2013.

[21] A.H. Johnston and G.M. Weiss, "Smartwatch-based biometric gait recognition," 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems, pp. 1-6, Sep. 2015.

[22] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K.S. Balagani, "HMOG: New behavioral biometric features for continuous authentication of smartphone users," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 877-892, May. 2016.

[23] N. Al-Naffakh, N. Clarke, P. Haskell-Dowland, and F. Li, "A

Comprehensive Evaluation of Feature Selection for Gait Recognition Using Smartwatches," International Journal for Information Security Research, vol. 6, no. 3. pp. 691-700, Sep. 2016.
[24] G.M. Weiss, J.L. Timko, C.M. Gallagher, K. Yoneda, and A.J. Schreiber, "Smartwatch-based activity recognition: A machine learning approach," 2016 IEEE-EMBS International Conference on Biomedical and Health Informatics, pp. 426-429, Feb. 2016.
[25] https://www.fitbit.com/kr/home
[26] D. Schürmann, A. Brüsch, S. Sigg, and L. Wolf, "BANDANA-Body area network device-to-device authentication using natural gAit," 2017 IEEE International Conference on Pervasive Computing and Communications, pp. 190-196, Mar. 2017.
[27] G. Revadigar, C. Javali, H.J. Asghar, K.B. Rasmussen, and S. Jha, "Mobility independent secret key generation for wearable health-care devices," Proceedings of the 10th EAI International Conference on Body Area Networks, pp. 294-300, Sep. 2015.
[28] C.L. Hsu, T.H. Chuang, and T.W. Lin, "End-to-end authenticated key exchange agreement for wearable devices in IoT environments." 2017 IEEE Great Lakes Biomedical Conference, pp. 1-1, Apr. 2017.
[29] Y. Zeng, A. Pande, J. Zhu, and P. Mohapatra, "WearIA: Wearable device implicit authentication based on activity information", 2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks, pp. 1-9, Jun. 2017.
[30] S.Y. Chun, J.H. Kang, H. Kim, C. Lee, I. Oakley, and S.P. Kim, "ECG based user authentication for wearable devices using short time Fourier transform," 2016 39th International Conference on Telecommunications and Signal Processing, pp. 656-659, Jun. 2016.
[31] R. Liu, C. Cornelius, R. Rawassizadeh, R. Peterson, and D. Kotz, "Poster: Vocal Resonance as a Passive Biometric," Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services, pp. 160-160, Jun. 2017.
[32] P. Meharia and D.P. Agrawal, "The human key: Identification and authentication in wearable devices using gait," Journal of Information Privacy and Security, vol. 11, no. 2, pp. 80-96, Apr. 2015.
[33] S. Eberz, N. Paoletti, M. Roeschlin, M. Kwiatkowska, I. Martinovic, and A. Patané, "Broken hearted: How to attack ECG biometrics," Network and Distributed System Security Symposium 2017, Feb. 2017
[34] S. Šprager, R. Trobec, and M.B. Jurič, "Feasibility of biometric authentication using wearable ECG body sensor based on higher-order statistics," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, pp. 264-269, May. 2017.
[35] F. Xu, Z. Qin, C.C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," IEEE INFOCOM 2011, pp. 1862-1870, Apr. 2011.
[36] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): authentication for implanted medical devices," Proceedings of the 2013 ACM SIGSAC conference on Computer & communications securitym, pp. 1099-1112, Nov. 2013.
[37] M. Rushanan, A.D. Rubin, D.F. Kune, and C.M. Swanson, "SoK: Security and

privacy in implantable medical devices and body area networks," 2014 IEEE Symposium on Security and Privacy, pp. 524-539, May. 2014.
〔38〕 L. Zhang, K. Xing, Z. Xu, J. Wang, S. Zhang, and J. Xu, "Human recognizer: an ECG based live biometric fingerprint," Proceedings of the 1st ACM Workshop on Privacy-Aware Mobile Computing 2016, pp. 21-27, Jul. 2016.
〔39〕 M. Poh, D.J. McDuff, and R.W. Picard, "Advancements in noncontact, multiparameter physiological measurements using a webcam," IEEE Transactions on Biomedical Engineering, vol. 58, no. 1, pp. 7 - 11, Jan. 2011.
〔40〕 S. Kwon, H. Kim, and K.S. Park, "Validation of heart rate extraction using video imaging on a built-in camera system of a smartphone," 34th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 2174 - 2177, Aug. 2012,
〔41〕 H. Wu, M. Rubinstein, E. Shih, J. Guttag, F. Durand, and W. Freeman, "Eulerian video magnification for revealing subtle changes in the world," ACM Transaction on Graphics, vol. 31, no. 4, Jul. 2012.

〈저 자 소 개〉

이 두 형 (Duhyeong Lee) 학생회원
2016년 2월: 서울시립대학교 수학과 졸업
2016년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호, 생체인증, Wearable Sensor Network

최 원 석 (Wonsuk Choi) 학생회원
2008년 2월: 서울시립대 수학과 졸업
2013년 2월: 고려대학교 정보보호대학원 석사 졸업
2013년~현재: 고려대학교 정보보호대학원 정보보호학과 박사과정
〈관심분야〉 Information Security & Medical Device Security

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학사 졸업
1987년 12월: Oklahoma University 전산학과 석사 졸업
1992년 5월: Oklahoma University 전산학과 박사 졸업
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, USN이론, 키 교환, 익명성 연구, PET 기술