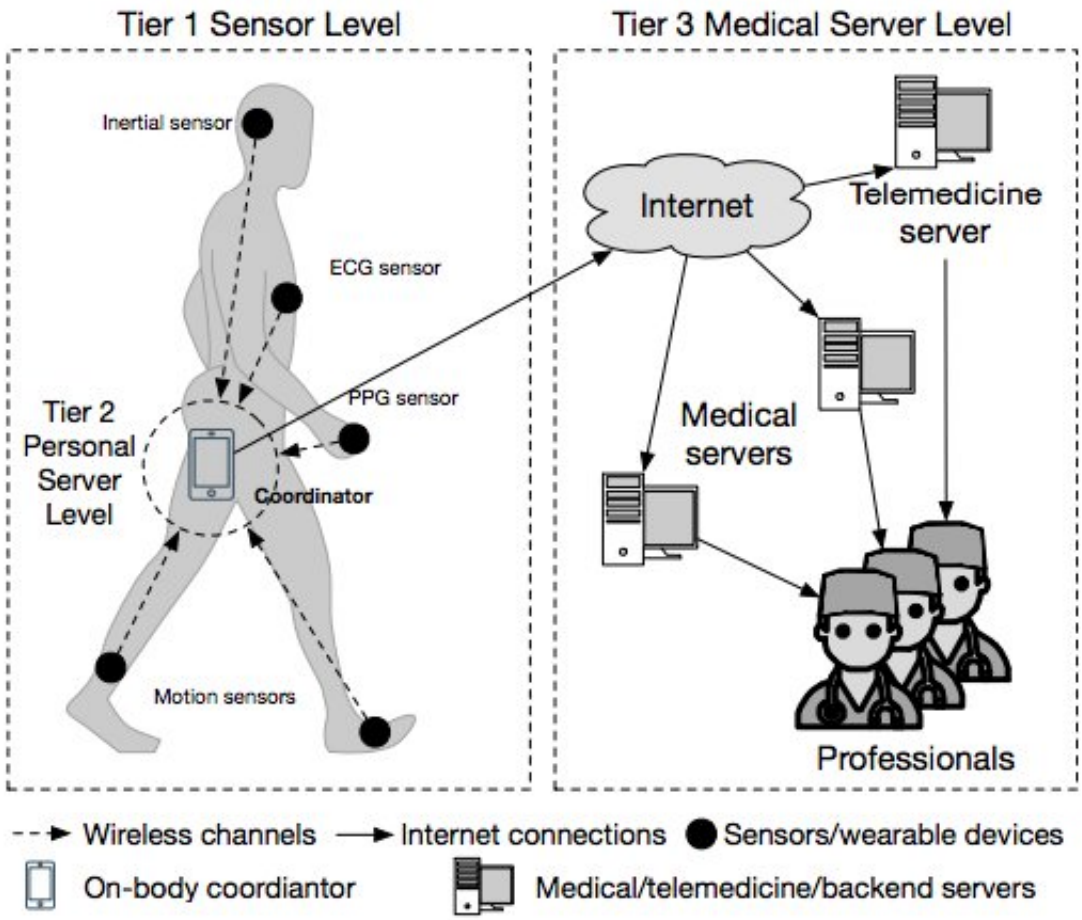
A new artificial neural network framework for gait based biometrics

August 20 2018, by Ingrid Fadelli



A typical 3-tier BSN-based healthcare system. Credit: Sun & Lo

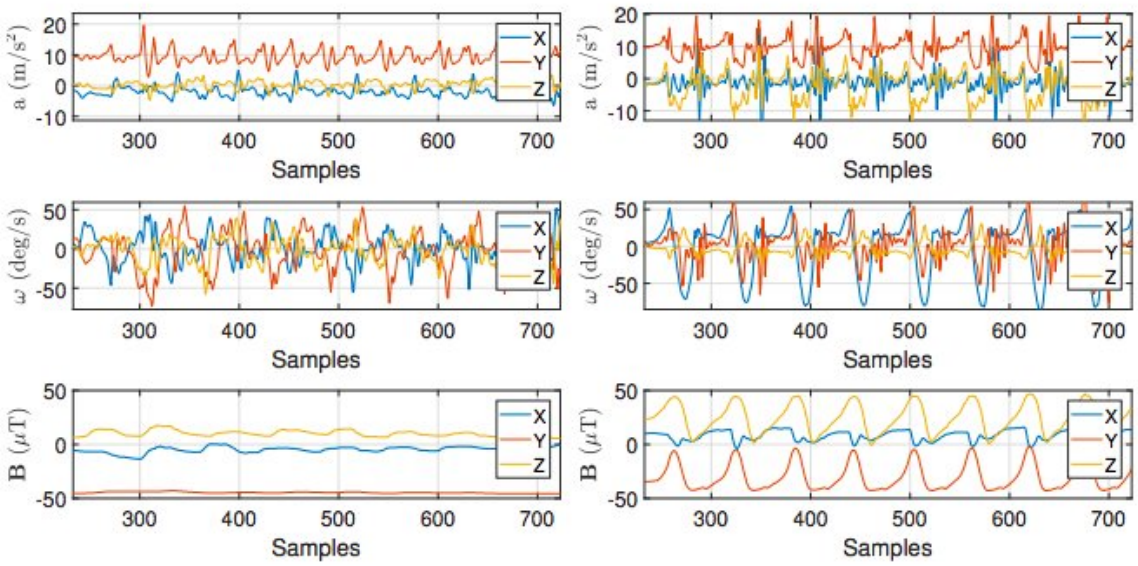
Researchers at Imperial College London have recently devised a new

biometric cryptosystem approach for securing wireless communications of wearable and implantable medical devices. Their framework, outlined in a study published on *IEEE Explore*, uses an artificial neural network (ANN) framework and gait signal energy variations.

Over the past decade, advances in wireless communication technology have fueled the development of a growing number of body sensor network (BSN) devices. These are lightweight, low-power sensor nodes that can be worn or implanted in the human body to monitor the health of elderly patients or those affected by chronic diseases.

Despite their valuable applications, BSN devices raise important security concerns, as attackers could hack these wirelessly connected sensors and breach patients' personal and health information. Given the very limited computational power of these miniaturized sensors, however, conventional computer security schemes cannot be applied for these devices. Researchers thus seek to develop new advanced security mechanisms that could effectively protect this sensitive data.

An effective solution for securing BSN devices is the biometric cryptosystem (BCS) approach, which identifies the patients' biometric traits, such as his/her face, iris, fingerprints, electrocardiogram (ECG), or photoplethysmography (PPG). The team of researchers at Imperial College has developed a new BCS approach that particularly focuses on gait signal energy variations; in other words, analyzing the way in which different people walk.



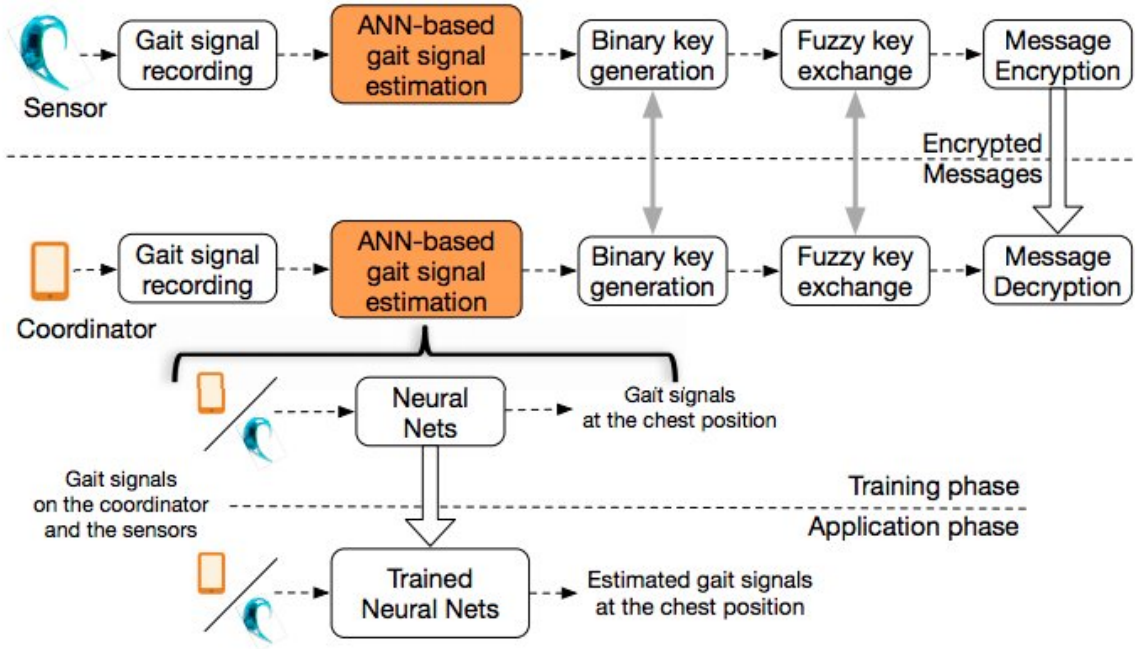
IMU outputs at the chest and shin positions, a=acceleration, ω=angular velocity, and B=magnetic field. Credit: Sun & Lo

"State-of-the-art biometrics/wearable security often uses electrocardiogram (ECG), the electrical activity of the heart, but its skin-attached electrodes greatly limit its applications," Yingnan Sun, the lead author of the paper told TechXplore. "We felt it was necessary to explore a new kind of biometrics that is both easy to collect and noninvasive, and gait, the way people walk, came to mind."

The term 'gait' refers to a pattern of movement of the limbs in animals and humans, specifically when they are walking/running. Different species of animals have their own characteristic gaits, but slight differences can also be observed between individual human beings.

Gait signals can be captured by wearing a low-cost inertial sensor, such

as an accelerometer, on the body. Currently, almost all wearable devices and many implantable devices are already equipped with inertial sensors. Using gait signals to form the BCS can establish secured communication channels among wearable and implantable devices.

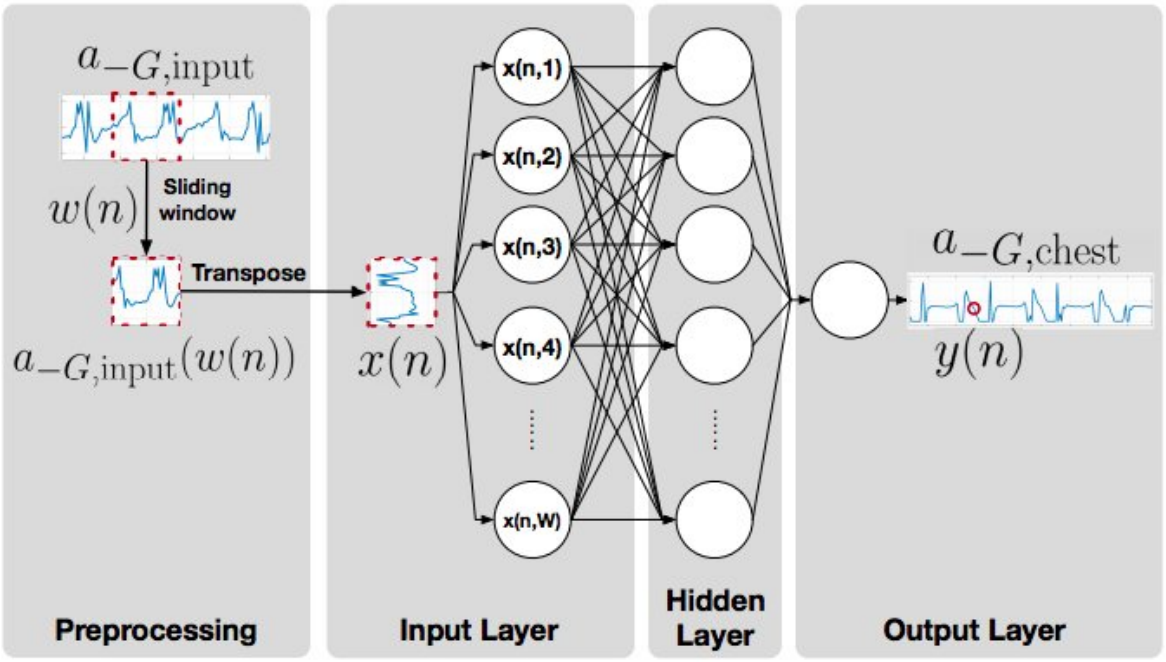


Overview of the proposed security scheme. Credit: Sun & Lo

"The challenge of using gait signals for security is that the gait signals captured by different sensors at different locations on the body have different patterns," Sun explained. "To solve this issue, we introduced an artificial neural network (ANN) framework, which projects the sensor signals to a unified frame and increases the signal correlation."

The researchers used their newly developed neural network framework

to extract similar features from BSN sensors, generating binary keys on demand, without requiring the user's intervention. When they tested their approach on a gait dataset, they found that the binary keys generated had a high entropy for all subjects.



ANN-based gait signal estimation. Credit: Sun & Lo

"We found that the use of the proposed ANN framework can significantly increase correlations between gait signals captured by different wearable sensors, resulting in a huge improvement in the performance of the security scheme," Sun said. "This newly proposed security framework is 68.75 percent more efficient than our previous work, generating a 128-bit key within only 12 seconds of walking."

The keys generated using their framework passed both National Institute of Standards and Technology (NIST) and Dieharder statistical tests, robustly discriminating between different people's gaits. The new approach shows great promise as a biometric security tool, and could eventually help to better protect the data collected by wearable and implantable devices.

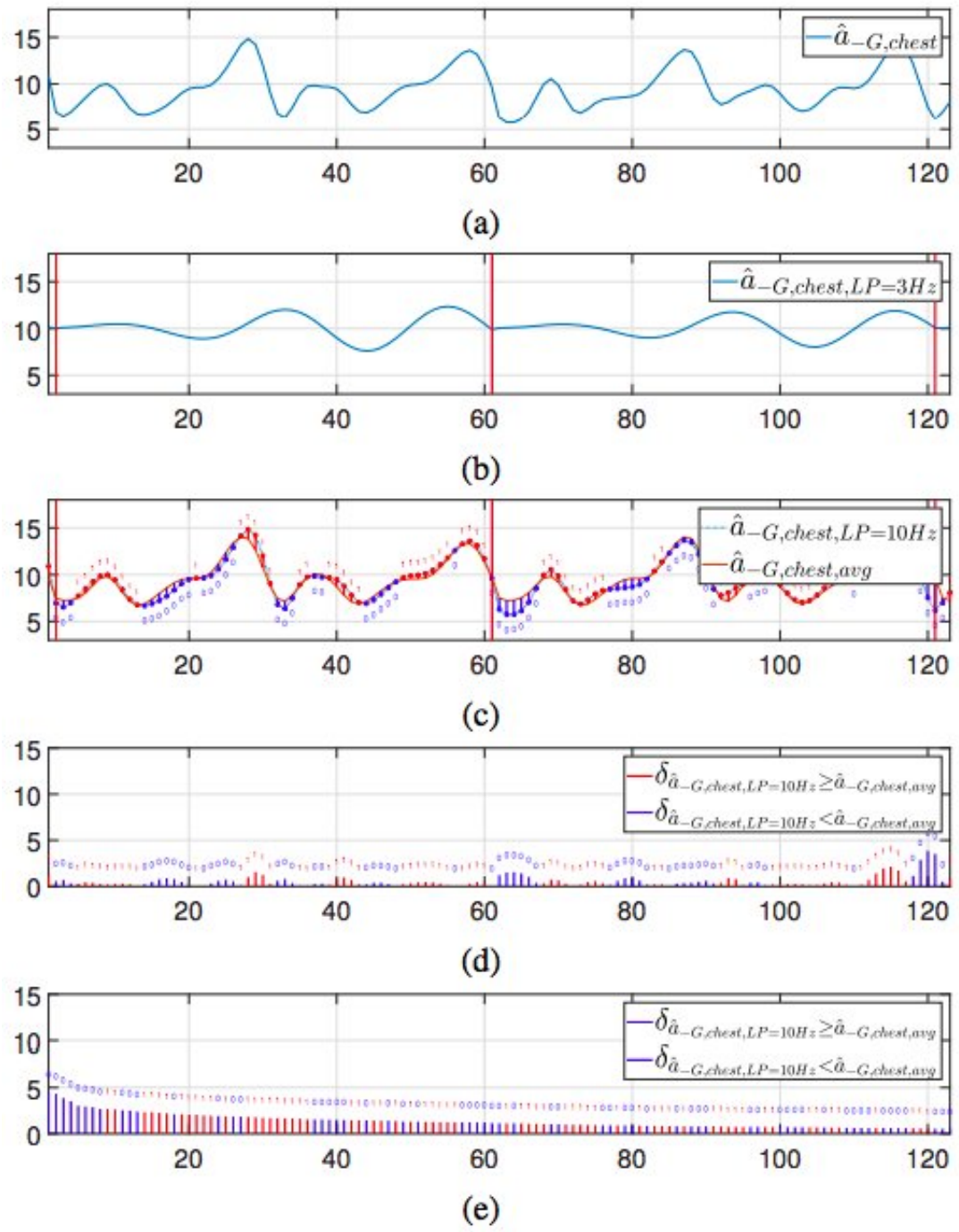
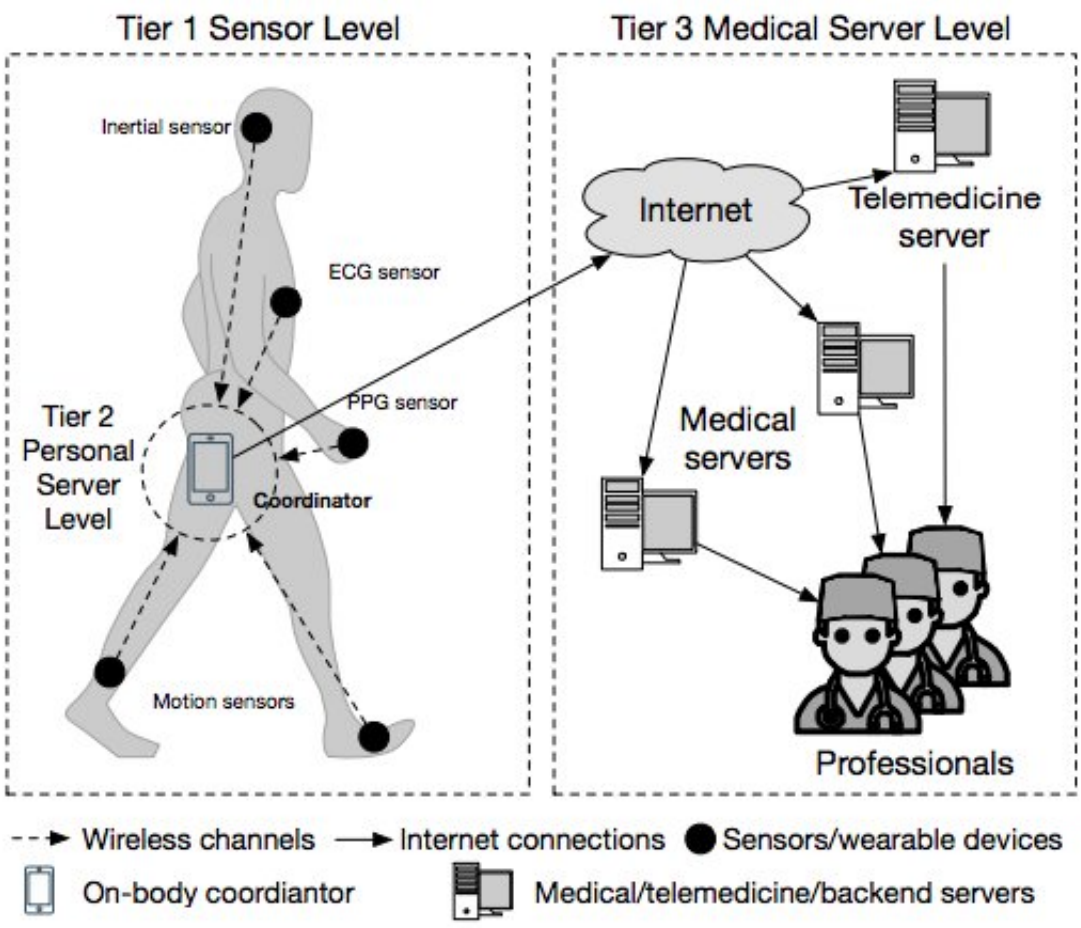


Illustration of the binary key generation block. (a) Gait signal ˆa−G,chest (m/s2). (b) ˆa−G,chest (m/s2) filtered by the 3 Hz low-pass filter. (c) Bit extraction by comparing aˆ−G,chest filtered by the 10 Hz low pass filter and the averaged aˆ−G,chest. (d) Energy difference, δ, between ˆa−G,chest,LP=10Hz and ˆa−G,chest,avg (e) Re-indexed binary keys using the associated reliability vectors. Credit: Sun & Lo

"Currently, we have only explored the use of acceleration signals for the security scheme, but gait signals also consist of other types of signals, such as gyroscope signals," Sun said. "In the near future, we would like to further improve the performance of our proposed security scheme incorporating other signals."



A typical 3-tier BSN-based healthcare system. Credit: Sun & Lo

More information: An Artificial Neural Network Framework for Gait Based Biometrics, DOI: 10.1109/JBHI.2018.2860780. ieeexplore.ieee.org/document/8424403/