The Internet of Bodies: The Human Body as an Efficient and Secure Wireless Channel

Article *in* IEEE Internet of Things Magazine · April 2022

DOI: 10.1109/IOTM.001.2100209

3 authors, including:

Abdulkadir Çelik
King Abdullah University of Science and Technology
137 PUBLICATIONS **2,108** CITATIONS
SEE PROFILE

Ahmed Eltawil
King Abdullah University of Science and Technology
393 PUBLICATIONS **4,420** CITATIONS
SEE PROFILE

The Internet of Bodies: The Human Body as an Efficient and Secure Wireless Channel

Abdulkadir Celik, *Senior Member, IEEE,* and Ahmed M. Eltawil, *Senior Member, IEEE.*

***Abstract*—The Internet of Bodies (IoB) is a network of smart objects placed in, on, and around the human body, allowing for intra- and inter-body communications. This position paper aims to provide a glimpse into the opportunities created by implantable, injectable, ingestible, and wearable IoB devices. The paper starts with a thorough discussion of application-specific design goals, technical challenges, and enabling communication standards. We discuss why the highly radiative nature of radio frequency (RF) systems results in inefficient communication due to over-extended coverage, causing interference and becoming susceptible to eavesdropping. Alternatively, body channel communication (BCC) uses the human body as a transmission medium by coupling harmless electrical signals, yielding secure and efficient communication thanks to better channel conditions and lower signal leakage than over-the-air RF systems. Numerical results show that various BCC topologies can respectively reach 8-12 Mbps and 1.5-3 Mbps max-sum and max-min rates with 1 MHz bandwidth and -30 dBm transmission power, which is three orders of magnitude lower than safety limits. Moreover, the BCC is capable of accommodating tens of IoB nodes up to 1 Mbps rates, which is sufficient for most IoB applications. Furthermore, as the cyber and biological worlds meet, security risks and privacy concerns take center stage, leading to a discussion of multi-faceted legal, societal, ethical, and political issues related to technology governance.**

INTRODUCTION

THE Internet of things (IoT) is a revolutionary technology that interconnects uniquely identifiable smart objects to integrate the physical worlds into digital domains. IoT is generally classified in the form of '*Internet of X-Things*' where *X* may refer to underwater, space, underground, etc. Herein, we shift our focus from things to humans and narrow the scope to body-centric IoT, which is also referred to as '*Internet of Bodies*' (IoB). IoB can be defined as a network of smart objects placed in-on-and-around the human body [1]. The advent of wearable, implantable, digestible, and injectable IoB devices has recently become possible by parallel advancements in microelectronics, wireless communications, and signal processing. IoB can be regarded as an enabling technology that can overcome three major challenges faced by mankind as the world population rapidly grows: baby boomers coming of age, preventative vs. reactive healthcare, and skyrocketing healthcare expenditures, which have become exacerbated due to the humanitarian and economic crises caused by COVID-19. Fortunately, IoB can help fight future pandemic diseases through early detection of initial cases, timely identification of spread through contact tracing, remote monitoring of patients in institutional or home quarantine, and the minimization of infection risk for healthcare providers. Considering the millions of deaths caused by fatal and chronic diseases each year, IoB may pave the way for a scalable and affordable medical system that offers proactive and preventative care for all. In addition to healthcare, IoB can revolutionize many other sectors such as smart-home assisted independent living, occupational health and safety, wellness & fitness, sports, and entertainment.

The remainder of this paper starts with a taxonomy of IoB devices and applications, providing a myriad of opportunities. We discuss IoB design goals, candidate communication and networking standards, and enabling technologies. Following a point-by-point comparison of radio frequency (RF) and body channel communication (BCC) systems, we evaluate the performance of various BCC schemes. Lastly, we discuss technology governance, security risks, and privacy concerns, before concluding the article.

IOB OPPORTUNITIES: A TAXONOMY OF IOB DEVICES & APPLICATIONS

IoB devices can be categorized as invasive (i.e., implantable, injectable, and ingestible) and non-invasive (i.e., wearable) based on their node deployment location. Another classification can be made based on consumer and medical-grade devices. While the former typically covers non-invasive devices, the latter includes almost all invasive devices and other non-invasive types. Such a wide variety inherently fuels the transformation of various sectors through a myriad of innovative data-driven applications, some of which are illustrated in Fig. 1* and discussed below.

Personalized Healthcare and Remote Patient Monitoring: Fatal or chronic diseases (e.g., cancer, diabetes, cardiovascular diseases, obesity, asthma, etc.) cause millions of deaths every year. The vast majority share one critical feature: being diagnosed a long time after experiencing early symptoms, thus missing the chance of controlling or even preventing diseases via earlier screening and diagnosis. To this aim, personalized medicine evaluates individuals' biological system dynamics and exploits data-driven predictive methods to identify patient-specific health risks. This naturally necessitates long-term continuous monitoring to collect behavioral and contextual data on physiological activity. Consider the hypothetical scenarios shown in Fig. 1, wherein the IoB can be deployed as a viable solution to collect required data through IoB sensor nodes and store it in a secure personal cloud. In such a system, private and sensitive information should only be accessible by authorized physicians through biometric authentication, such as RFID chips, fingerprints, or iris/face recognition. By

The authors gratefully acknowledge financial support for this work from the KAUST, Thuwal, KSA and the Smart Health Initiative (SHI) at KAUST.

*Fig. 1 was produced by Heno Hwang, a scientific illustrator at KAUST

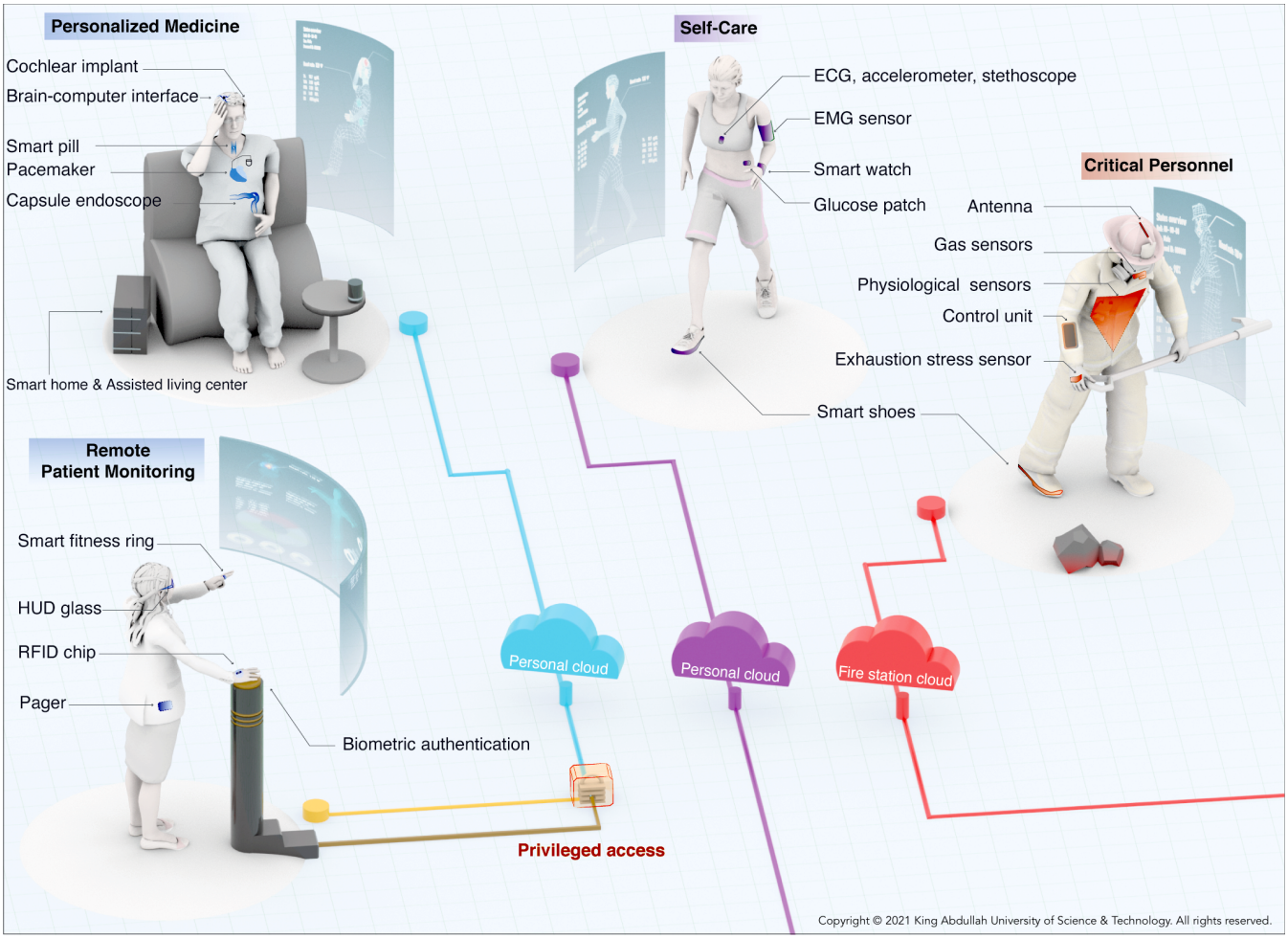

Fig. 1: Potential use cases of IoB devices.

translating such pervasive technologies into clinical use, IoB can enable personalized medicine concepts towards innovative and transformative healthcare approaches by mitigating risks and preventing diseases via proactive strategies. In case of disease occurrence, IoB can assist physicians to remotely monitor and treat patients with high precision devices, such as smart pills, pacemakers, capsule endoscopes, cochlear implants, intraocular lenses, and brain-computer interfaces.

Smart Home Assisted Independent Living: The context-rich, accurate, and timely information gathered by IoB devices could also facilitate smart-home assisted independent living applications for seniors, people with disabilities, and rehabilitating patients. Smart-home applications can operate more efficiently through interaction with IoB nodes. For instance, by profiling the activity patterns of users with inertial and ambient sensors of wearable IoB devices, heating systems can preserve a comfortable temperature, prevent hypothermia, and minimize energy costs in the meantime [2]. Likewise, IoB sensors can talk to household robots to deliver drugs and nutrients, prevent accidental wandering by geofencing, and reduce the risk of accidents. More importantly, IoB devices can detect falls and accidents more accurately and alert caregivers and hospital to detected events and vitals. Integrating smart homes with IoB-based close monitoring can also be an effective tool for the in-home rehabilitation of patients recovering after surgery or medication. In this way, in-home nursing costs can be reduced by giving more information to caregivers and receiving on-demand support. Therefore, IoB-assisted smart homes can enable this group of people to live effectively and independently, while providing a feeling of independence to accomplish personal and professional goals, which plays a vital role in mental well-being.

Self-Care and Welfare: Dietary habits, sedentary behaviors, and physical activity are three main factors in achieving a healthy lifestyle. Thanks to the ever-increasing awareness of the long-term impacts of a healthy diet and active lifestyle on developing chronic and fatal diseases, people are now more interested in wellness and fitness to increase their quality of life. Since human physiology opens a window to our physical, mental, and emotional well-being, wearable devices have become an integral part of modern daily lives, continuously and unobtrusively measuring physiological signs. Although smartwatches have recently gained popularity, they can only provide macro-information such as heart rate, body temperature, etc. Therefore, as shown in Fig. 1, smartwatches should communicate with custom-built IoB sensors (e.g., elec-

trocardiography (ECG) and electromyography (EMG) sensors, accelerometers, stethoscopes, and glucose patches) to acquire accurate readings and present users with a more holistic view of their health. Once dietary, sedentary, and physical activity patterns are profiled based on accurate physiological signs, mobile apps can draw inferences and provide users with a set of timely recommendations to improve their wellness, fitness, and health conditions. Especially considering that the happiness, alertness, and relaxation of humans are linked with physiological signs [3], mobile apps can even make suggestions for mental and emotional well-being.

Occupational Health & Safety (OHS): According to the International Labor Organization, occupational accidents and work-related diseases annually cause 374 million non-fatal injuries and 2.78 million deaths, which accounts for around 4% of global gross domestic product[†]. Even though strict rules and regulations exist regarding OHS and personal safety equipment, these practices are not sufficient to inform supervisors about acute dangers that may occur in workplaces or about workers reaching their physical limits. When integrated with the industrial IoT (a.k.a, Industry 4.0) ecosystem, IoB can provide an unprecedented level of visibility into the workplace and workers' health. This is possible by placing intelligent gadgets (vests, helmets, shoes, watches, etc.) equipped with a necessary sensor (e.g., physiological, temperature, exhaustion, stress, location, activity, toxic gas, etc.) to monitor workers and the workplace (e.g., toxic-gas sensors), as shown in Fig. 1. IoB can also play a vital role in protecting critical personnel (e.g., firefighters, miners, security forces, etc.) working in extreme conditions off premises. Moreover, IoB devices can improve travel safety by measuring levels of driver fatigue/drowsiness and sending alerts to pull off the road. By leveraging data analytics on sensor readings transferred to a corporate cloud, situational data can then be distilled into actionable insights and visualized at a remote management console to take on-site corrective actions. Such a data-driven decision-making approach may allow faster emergency responses, as automated workflows can be executed to accelerate evacuation and rescue activities once critical events (e.g., falls from heights, pass-outs, exposure to toxic gasses, explosions, etc.) are detected. Furthermore, monitoring work environments can also help avoid prolonged exposure to harsh conditions, such as radiation, CO_2, noise, heat, and humidity. Likewise, IoB can enable supervisors to encourage workers to take recovery breaks when any signs of dehydration, exhaustion, and fatigue are identified. In this way, IoB can minimize overexertion, increase overall productivity, and diminish the risk of accidents, injuries, and work-related chronic diseases.

Sports and Entertainment: IoB can reshape the sports world by tracking and recording athletes' training and fitness data, which is then processed to help coaches evaluate athletic performances, form ideal teams based on opponents' strengths and weaknesses, and develop correct game strategies. Likewise, virtual reality (VR) and augmented reality (AR) applications can be integrated with IoB sensors/actuators to provide users with a more realistic experience. This unification may substantially improve current VR/AR applications designed for gaming, entertainment, training, and education.

[†]https://www.ilo.org/global/topics/safety-and-health-at-work

IoB Design Goals and Technical Challenges

In order to meet the quality of service (QoS) and quality of experience (QoE) requirements of the applications mentioned above, IoB devices and networks must reach some, if not all, of the following design goals: ultra-low-power, low-cost, low-complexity, ultra-reliable, low-latency, secure, miniature, and comfortable.

Size, Weight, and Power-Cost (SWaP-C) Constraints: Achieving the above IoB design goals is a challenging task under the stringent and conflicting constraints of SWaP-C. Since state-of-the-art microelectronics already provide commercial off-the-shelf (COTS) system-on-chip (SoC) integrated circuits (ICs) in sizes below the millimeter scale, the SWAP-C constraint is often determined by the size, shape, and weight of the power source. IoB applications typically require the battery to last for several days, weeks, and even years for ingestible, wearable, and injectable/implantable devices, respectively. At this point, we must note that the power consumption of SoC-ICs is heavily dominated by communications and networking interfaces (CNIs). For instance, the CNI of the Texas Instruments' CC2640 Bluetooth low-energy (BLE) SoC-IC constitutes 80% of 1138 μ W power consumed for 8 kHz Nyquist rate streaming, while the rest is used by sensors, an analog-to-digital converter, a digital signal processor, etc. Therefore, CNIs must adhere to energy-efficient and self-sufficient design criteria to minimize battery size, while also increasing IoB network lifetime. Achieving such conflicting objectives is possible only by keeping the complexity of the underlying communications hardware and networking protocols low, which reduces monetary costs. While implantable, ingestible, and injectable IoB devices follow reliable, durable, and biocompatible hardware design, wearables should target QoE by enhancing comfort through stretchable, textile ink-jet printable electronics.

Ultra-Reliable and Low-Latency Communications (URLLC): For mission-critical and real-time IoB applications, reliability first requires precise and accurate sensor/actuator data, which is commonly limited by drift and ambiguity. Therefore, observation necessitates redundant and multimodal sensing of bioelectrical, biochemical, and biomechanical phenomena. By employing on-node statistical signal processing techniques, the integrity of such multimodal readout signals can be further improved through frequency-selective filtering, baseline readjustments, artifact corrections, etc. Then, URLLC is required to transfer pre-processed data within a tolerable latency limit reliably. Therefore, URLLC requires cross-layer approaches to provide solutions for delay-sensitive real-time applications, as well as mission-critical operations that require ultra-reliability.

Safety Regulations: The safety and security requirements pose extra challenges on top of SWaP-C constraints. IoB design must account for heating effects caused by the overexposure of electromagnetic fields, whose degree depends on signal intensity, duration of exposure, carrier frequency,

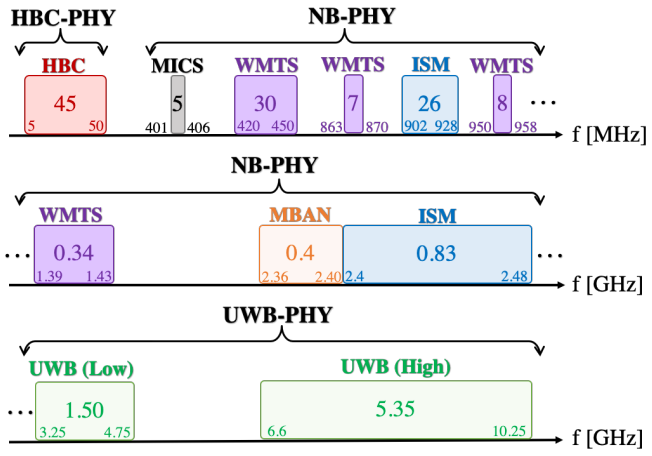

Fig. 2: PHY specifications of IEEE 802.15.6 Standard.

node location, and distance between transmitter and tissues. RF-based IoB devices must limit time-varying electromagnetic field exposure on the human body under a Specific Absorption Rate (SAR), expressed in units of watts-per-kilogram. Since IoB nodes are inherently low-power devices, standardization efforts should focus more on the local SAR requirements rather than on the whole body. Minimum SAR levels are determined by global or regional regulatory bodies such as the International Commission on Non-Ionizing Radiation Protection (ICNIRP) guidelines [4], which also specifies maximum contact current conducted through children and adult body channel to be 10 mA and 20 mA, respectively. Although many of the devices can potentially be used clinically, most wearable devices are designed as consumer products to avoid the long and expensive regulatory approval process for clinical deployment [2]. This could be the reason that such technologies still cannot penetrate the health care market and find use in clinical practice.

Security & Privacy: IoB system security and user privacy is of paramount importance as processing biometric data reveals sensitive personal information that is open to abuse by targeted marketing, surveillance, malicious attacks, etc. Indeed, wirelessly connected medical devices may come under attack by biohackers, who can use high-gain antennas to remotely eavesdrop, overheard, intercept, or even alter original unencrypted data. Matters can get even worse when biohackers cause fatal harm by hacking a pacemaker to lethally shock the heart or hacking an insulin pump to lead to diabetic coma by manipulating insulin levels. Hence, IoB devices and data must always be contained, uncompromised, and available, which is viable through authentication and encryption protocols. Nevertheless, physical layer security must be considered as a proactive measure to prevent data transmission beyond the range of the human body, unless it is intended for a trusted off-body wireless hub.

IoB Standards and Enabling Technologies

The communications and networking aspects of IoB were originally conceptualized in the realm of wireless body area networks (BANs). Considering the broad range of IoB devices and divergent QoS and QoE demands of IoB applications, standardization is a daunting challenge, and yet is necessary for compatibility/interoperability among products manufactured by different vendors and the rapid/broad spread of the technology. Therefore, IoB standards must be capable of supporting a wide range of QoS requirements and prioritizing urgent and critical applications over others. In the early stages of standardization efforts, Zigbee, 6LoWPAN, and Bluetooth have been recognized to be potential technologies to be adopted for WBANs. While Zigbee and 6LoWPAN are wireless personal area network (WPAN) protocols built upon physical layer (PHY) and medium-access layer specifications of *IEEE 802.15.4* standard, Bluetooth is a whole protocol stack PAN network standard designed and maintained by a Bluetooth special interest group. Since none of these WPAN standards meet ultra-low-power device requirements, two alternative standards are developed and embraced later on:

■ ***Bluetooth Low Energy*** (BLE) is a low-power low-rate protocol stack designed for low-cost devices and maintains a communication range similar to Bluetooth classic. BLE operates on the 2.45 GHz industrial-scientific-and-medical (ISM) band, which is split into 2 MHz wide 40 sub-bands and can provide up to 1 Mbps data rate. BLE has a security mode for data integrity and encryption with or without authentication. It implements encryption and authentication by chaining message authentication codes and using the 128-bit key length Advanced Encryption Standard (AES), respectively.

■ ***IEEE 802.15.6*** standard is particularly developed for WBANs as limiting the PHY to ISM bands is not a satisfactory solution to support the wide range of IoB applications. This is mainly due to the fact that signal propagation in, on, and around the human body is quite distinct from its off-body counterparts because of the peculiar and dynamic factors imposed by the lossy, frequency-dependent, and heterogeneous dielectric nature of the human body. That is, first-order channel statistics (e.g., path loss and shadowing) are primarily determined by node locations (e.g., in-body, on-body, off-body), communication distance, carrier frequency, and link types (e.g., line-of-sight or non-line-of-sight), as well as body postures and gaits. Likewise, second-order channel statistics are mainly influenced by body movements and govern time-varying performance metrics such as delay spread, power delay profile, level-crossing rate, average fade duration, and channel coherence time. For instance, let us consider a link between left-wrist to right-hip on a moving human subject. In addition to multipath components varying in number and magnitude due to the dynamically changing surrounding environment, this link also alternates between LoS and non-LoS states as the subject walks and swings his arms. Therefore, varying multipath components, propagation distances, and link types directly impact delay and attenuation levels, which change with mobility speed (e.g., running, walking, sports activities). On the contrary, the link budget between in-body devices is not affected by the surrounding environment, but rather determined by the dielectric properties of tissues, organs, and bones. For an in-depth discussion of IoB channel characterization, we refer interested readers to this detailed survey on this topic [1]. As shown in Fig. 2, the IEEE 802.15.6 supports three

different PHY specifications to adequately address distinctive channel characteristics. Narrowband (NB) PHY supports rates between 50 Kbps and 1 Mbps on ISM bands, medical implant communication service (MICS) bands, wireless medical telemetry system (WMTS) bands, and medical body area network (MBAN) bands. Since the ISM bands are license-free, they are overcrowded with the ever-increasing number of IoT devices and suffer from co-existence issues (e.g., interference, collisions, outage). Thus, licensed WMTS and MBAN bands have been introduced for more reliable communication. The MICS band is specially defined for in-body links thanks to its suitability for small-size antennas and favorable channel characteristics inside the human body. On the other hand, the ultra-wide-band (UWB) PHY can be employed for both in and on/off body links and can deliver rates above 10 Mbps. Any severe attenuation of in-body UWB channels can be compensated for by wider bands (500 MHz). Since unintended receivers cannot easily detect the noise-like UWB signals, they have inherent robustness against jamming, thereby alleviating the need for advanced encryption methods. Furthermore, the simple structure of impulse radio UWB transceivers can pave the way for low-power and miniature IoB devices. As an alternative to NB and UWB radio frequency (RF) communications, IEEE 802.15.6 also supports BCC (a.k.a. human body communication), which will be discussed in detail in the next section. All PHY options share a common medium-access layer protocol based on three-phased superframes: 1) exclusive access phase for critical/emergency data, 2) random-access phase for CSMA/CA, and 3) contention access phase for slotted ALOHA. Medium-access protocol can operate in one of three transmission modes: 1) beacon mode with superframes, 2) non-beacon mode with superframes, and 3) non-beacon mode without superframes. Moreover, it has three levels of security: Level-0) non-secure, Level-1) authenticated but not encrypted, and Level-2) both authenticated and encrypted.

■ ***Wi-Fi and B5G*** are two powerful off-body communication candidates for connecting WBANs with the outside world. Wi-Fi operates on 2.4 GHz and 5 GHz ISM bands based on the IEEE 802.11 family of standards, which has worldwide acceptance for local/metropolitan area networking and Internet access. On the other hand, beyond fifth-generation (B5G) cellular networks differ from past generations in embracing software-defined networking and network function virtualization. This enables network slicing, i.e., the multiplexing of independent, isolated, and virtual end-to-end networks on the same physical infrastructure. In this way, B5G networks can provide dedicated slices to support different classes of IoB applications.

BODY CHANNEL COMMUNICATION FOR EFFICIENT & SECURE INTRA-BODY NETWORKING

RF systems are the first to come into mind for the facilitation of IoB networks due to their maturity, availability, and widespread exploitation. However, the bias in favor of RF systems does not necessarily make RF the best fit in all circumstances, especially when intra-body (i.e., in-body and on-body) IoB networks are considered, due to the highly radiative and omnidirectional propagation nature of RF communications that can extend beyond the human body. The negative consequences of this propagation behavior are manifold and can be summarized as follows:

- ⊗ Omni-directional radiation associated with RF makes the privacy and confidentiality of sensitive data susceptible to overhearing, eavesdropping, bio-hacking, and interception. Since system complexity and monetary cost increase with additional security measures, which negatively impact SWaP-C constraints, it is better to use communication methods with inherent physical layer security features.
- ⊗ The radio front-end is one of the most complex and power-hungry sub-systems of RF devices, which increases the battery size and causes violation of the SWaP-C constraints. The resulting form-factors and frequent charging requirements naturally decrease QoE and commercialization success.
- ⊗ Nearby RF devices operating at the same band cause interference and co-existence issues. This is an incredibly challenging issue, especially for the ISM band that rapidly becomes saturated and interference-limited by the ever-increasing number of IoT devices.

BCC is an alternative wireless technology that operates on 100 kHz-100 MHz band and mostly confines signal propagation to the human body by using body tissues as a transmission medium. Galvanic coupling (GC) and capacitive coupling (CC) are the two most common signal transmission schemes adopted in the literature [c.f. Fig. 3]. In the former, body tissues are in contact with both signal electrodes (SEs) and ground electrodes (GEs) of transceivers. That is, both the signal (forward) path and the return (backward) path are formed through the body, which is used as a transmission line. For this reason, the GC–BCC is mainly characterized by the dielectric properties of tissues between the transceivers. In the latter, the signal path is formed through signal electrodes attached to the skin, whereas the floating ground electrodes form the return path over-the-air, and thus remains susceptible to environmental changes. Based on these fundamental distinctions, the GC–BCC and CC-BCC are more suitable for in-body and on-body communications, respectively. Their common advantages over RF systems can be summarized as follows:

- ✓ Since the human body is a better conductor than air, the BCC experiences a lower path loss than RF counterparts and thus requires lower transmission power. For instance, the RF path loss between nodes located on the chest and wrist is around 70 dB, whereas it is rated at 50 dB for the CC–BCC. Furthermore, the actual benefits of CC–BCC become obvious when the heavy body shadowing effects on RF channels are taken into account. The experimental studies show that standard deviation of the CC–BCC path loss during walking, running, and arm movement is at most 2.5 dB, in contrast to 30-40 dB RF attenuation variability [5].
- ✓ As the human body does not act as an antenna below 100 MHz, transceiver size can be decoupled from car-

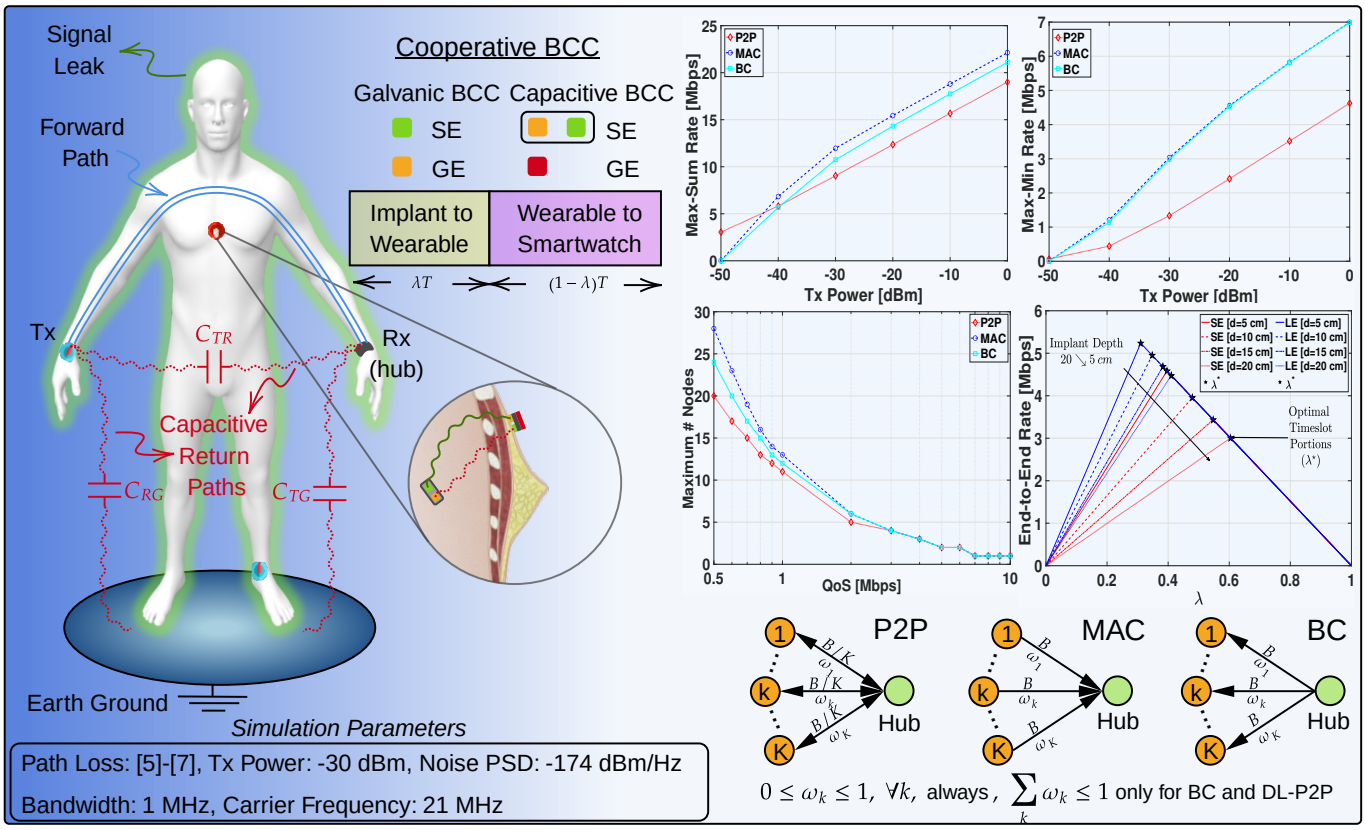

Fig. 3: Illustration and performance evaluation of the BCC schemes.

rier wavelength. This naturally enables carrierless communication and eliminates the need for complex and power-hungry radio front-ends. Moreover, considering the substantially lower path loss mentioned above, BCC can principally deliver throughput and energy-efficient communications with small-form factor transceivers.

✓ By confining the transmission to the human body, the BCC leaks negligible signal levels, especially at lower frequencies [6]. That is, BCC offers wireless connectivity while keeping the physical layer security attributes of wired communications. This intuitively eliminates the need for complex and power-consuming signal processing components and security algorithms. Noting that the BCC channel already operates out of RF bands, its low signal leakage level prevents interference and co-existence issues among IoB devices operating on nearby bodies.

For more efficient and physically secure IoB networks, the above point-by-point comparison strongly advocates the use of BCC and RF systems for intra-body and off-body communications, respectively. To this aim, consider an IoB network whose nodes avoid collisions through three BCC topologies: peer-to-peer (P2P) channel, multiple-access channel (MAC), and broadcast channel (BC). In the P2P topology, multi-user interference (MUI) is avoided by allocating radio resources orthogonally. For instance, Fig. 3 shows that the P2P equally shares total bandwidth B by K nodes. Alternatively, the MAC and BC employ a non-orthogonal multiple access scheme where all nodes exploit the entire bandwidth by controlling transmit power weights $(\omega_k, 1 \leqslant k \leqslant K)$ to ensure distinct power reception at the receiver side. The power reception disparity is then leveraged by a successive decoder that iteratively decodes and extracts received messages in the descending order of the reception power. In this way, the node with the highest (lowest) reception power experiences no (all) MUI at the end of successive interference cancellations (SIC). If power weights are chosen appropriately, the MAC and BC utilize the available bandwidth more efficiently to accommodate more nodes without requiring medium access control. Based on these topologies, the IoB network's optimal max-min and max-sum rate is compared in Fig. 3, wherein BCC-enabled IoB nodes (blue) located on the right wrist and left ankle exchange packets with a smartwatch on the left wrist, that is also responsible for communication with off-body parties. The nodes perform uplink and downlink communications over a $[1]MHz$ bandwidth centered at $[21]MHz$. The channel gains between the IoB nodes and the smartwatch follow the channel model presented in [7]. The transceiver can reach up to 0 dBm transmission power which corresponds to 1-5 mA contact current for 1-5 V supply voltage and remains within the safety limits. Compared to the BLE that typically achieve 1 Mbps by consuming $[10]dBm$ transmission power over $[2]MHz$ bandwidth, the BCC can deliver a max-min rate above $[1]Mbps$ by consuming $[-30]dBm$ and $[-40]dBm$ over $[1]MHz$ bandwidth in P2P and MAC/BC topology,

respectively. Moreover, Fig. 3 illustrates the fact that the MAC and BC can yield a much better max-min and max-sum rate performance thanks to the SIC receivers. The extra energy and throughput efficiency offered by MAC/BC topology also accommodate more IoB nodes on the body. For example, the P2P, BC, and MAC can accommodate 20, 24, and 28 nodes each with a $[0.5]Mbps$ rate over $[1]MHz$ bandwidth, respectively. It is worth noting that MAC can sustain a larger network than BC, when all nodes share the transmission power of the transmitting node. To transmit a packet containing 21 bytes of payload and 8 bytes of PHY headers and footers, the BLE and ZigBee consumes $[12]\mu J$ and $[30]\mu J$ [8], which corresponds to $[50]\mu J/b$ and $[130]\mu J/b$ energy efficiency, respectively. On the other hand, the state-of-the-art BCC transceivers can reach energy efficiency up to $[1]pJ/b$ [9], based on the underlying hardware architecture and application. Considering interwoven relations between energy efficiency and cost-size-complexity of the hardware, the BCC can provide QoS demanded by most on-body IoB applications while satisfying aforementioned SWaP-C constraints.

Fig. 3 illustrates how galvanic and capacitive BCC can facilitate a cooperative communication system among in-body and on-body IoB nodes. For the implant node, we consider different sizes of electrodes located $[\{5, 10, 15, 20\}]cm$ away from the relay node: disc-shaped small electrodes with a radius of $[0.2]cm$ and cylindrical large electrodes with a radius of $[0.2]cm$ radius and $[1]cm$ height [10]. Denoting the data rates in the first and second hop by R_1 and R_2, respectively, Fig. 3 shows the end-to-end data rate, $\mathrm{R}_{\mathrm{e2e}} = \min\{\mathrm{R}_1, \mathrm{R}_2\}$, against λ. By optimizing the timeslot portions, which is exactly attained when $\lambda^\star = \frac{\mathrm{R}_2}{\mathrm{R}_1+\mathrm{R}_2}$, the cooperation of galvanic and capacitive BCC can provide several $[]Mbps$ of rates depending on distance and electrode size, which is also sufficient for most implant IoB devices.

Technology Governance, Security Risks, and Privacy Concerns

Although constantly advancing microelectronics and communication technologies are expected to make the above IoB concept a reality sooner or later, there is still a dire need to face the tremendous challenges of technology governance. The foremost technical challenge is to overcome cybersecurity and privacy concerns, which may lead to social inertia due to increasing awareness of the vulnerability of wearables and IoT devices in general. Besides the leakage of fine-grained private data about personal life and mental/physiological conditions, a cybersecurity flaw can even allow biohackers to physically harm someone by attacking vital devices such as pacemakers and insulin pumps. Another challenge is storing, archiving, and processing the vast, versatile, multi-dimensional, and highly unstructured data generated by millions of IoB devices, which must be interoperable for data analytics and cross-reference purposes. Although adopting big data analytics in decision-making can lead to breakthroughs, protecting such vast sensitive data is susceptible to security risks and privacy concerns, especially when personal data goes beyond the health sector. For example, when biological data collected by IoB devices is combined with data derived from other myriads of sources (e.g., retail stores, web services, financial and government institutions, etc.), profiling and grouping people based on inaccurate/incomplete data may result in biased decisions and policies in various sectors such as insurance, employment, finance, education, criminal justice, and social services, to name a few [11]. Even if policy- and decision-makers have no such intention, there are still implicit risks of discrimination and bias that may unnoticeably affect not only individuals but also groups, minorities, and vulnerable populations. From the standpoint of governments, the data of top officials generated by IoB devices is essential to avoid the irreversible impacts of spying and espionage on national security. Because big data analytics can infer critical insights from the personal and health data of a large population, governments may even be confronted with global geopolitical risks if their respective nation's data is exposed to nefarious entities [12]. Therefore, governments, business sectors, and non-profit organizations should cooperate on necessary laws, standards, and regulations in order to avoid undesirable legal, societal, ethical, and political outcomes.

Conclusions and Future Research Directions

IoB can significantly impact social life by revolutionizing scientific studies and transforming various business sectors. This position paper aims to provide a glimpse into IoB's multi-faceted and complex nature formed by bringing the cyber and biological worlds together. Adopting data-driven algorithms on big data generated by IoB devices may have a massive impact on personal and social life, whether positive or detrimental. It all depends on the ways in which laws, standards, and regulations effectively secure IoB devices and data in order to avoid abominable legal, societal, ethical, and political outcomes. Various communication standards and technologies can enable IoB devices and applications to open up all these fantastic opportunities. Although RF systems have a wide-spread usage, the BCC systems are a better fit for intra-body communications because they are more efficient, more physically secure, and free of the interference coming from nearby RF-based IoT devices. The following points present open research challenges from a communication and networking point of view:

♦ ***Channel Modeling:*** While characterizing the body channel has been addressed by existing work such as [1] , a parametric and statistical intra-body channel model is still missing. In particular, fluctuations in return path capacitance (C_{TR}, C_{TG}, C_{RG} in Fig. 3) caused by surrounding environment, body postures, and node locations yield random path loss variations. A distance and frequency dependent modeling of dynamic body channel behavior is vital for both transceiver design as well as provisioning and analyzing the performance of BCC-based IoB networks.

♦ ***Inter-Body Coupling and Interference (IBCI):*** Even though BC/MAC topologies can mitigate intra-body MUI, the IBCI can still degrade security and intra-body communication performance, whose in-depth analysis also requires a full-scale characterization. In [13], Yang et al. showed negligible

IBCI makes covert communication possible in the electro-quasi-static region (EQS) below 10 MHz, beyond which information becomes susceptible to eavesdropping. Considering limited bandwidth and relatively higher intra-body path loss in the EQS region, dynamic interference management schemes should be developed to accommodate bandwidth-hungry and insensitive IoB applications over 10-100 MHz.

♦ ***Energy Self-Sustainability:*** Given that pJ/b BCC transceivers have already been realized, the next step would be to prove an energy self-sustainable IoB network, whose node charges itself through various energy harvesting technologies such as tribo/piezo/thermo/pyro-electric, photovoltaic, RF, etc. Similar to attempts for minimizing BCC power consumption [14], novel communication and networking approaches should be developed and optimized to maximize IoB network lifetime based on energy arrival and departure rates.

♦ ***Flexible, Printable, and Textile Electronics:*** The quality of user experience is a crucial design factor for IoB devices. Therefore, the BCC transceiver architectures must be translated into cutting-edge manufacturing techniques such as flexible, textile, and ink-jet printable electronics. At this point, novel electrode design approaches are necessary as the skin-electrode interface plays a decisive role in the end-to-end propagation losses.

REFERENCES

[1] A. Celik, K. N. Salama, and A. M. Eltawil, "The internet of bodies: A systematic survey on propagation characterization and channel modeling," *IEEE Internet Things J.*, 2021.

[2] B. P. Lo, H. Ip, and G.-Z. Yang, "Transforming health care: Body sensor networks, wearables, and the internet of things," *IEEE Pulse*, vol. 7, no. 1, pp. 4–8, 2016.

[3] S. Park, M. Constantinides, L. M. Aiello, D. Quercia, and P. Van Gent, "Wellbeat: A framework for tracking daily well-being using smartwatches," *IEEE Internet Computing*, vol. 24, no. 5, pp. 10–17, 2020.

[4] ICNIRP, "ICNIRP guidelines for limiting exposure to electromagnetic fields (100 khz to 300 ghz)," *Health Phys.*, vol. 74, no. 4, pp. 483–524, 2020.

[5] H. Baldus, S. Corroy, A. Fazzi, K. Klabunde, and T. Schenk, "Human-centric connectivity enabled by body-coupled communications," *IEEE Commun. Mag.*, vol. 47, no. 6, pp. 172–178, 2009.

[6] D. Das, S. Maity, B. Chatterjee, and S. Sen, "Enabling covert body area network using electro-quasistatic human body communication," *Scientific Reports*, vol. 9, no. 1, p. 4160, 2019.

[7] A. Celik and A. M. Eltawil, "Enabling the internet of bodies through capacitive body channel access schemes," *IEEE Internet Things J.*, pp. 1–1, 2022.

[8] X. Fafoutis, E. Tsimbalo, W. Zhao, H. Chen, E. Mellios, W. Harwin, R. Piechocki, and I. Craddock, "BLE or IEEE 802.15.4: Which home IoT communication solution is more energy-efficient?" *EAI Endorsed Trans. Internet Things*, vol. 2, no. 5, 2016.

[9] S. Maity, B. Chatterjee, G. Chang, and S. Sen, "Bodywire: A 6.3-pj/b 30-mb/s 30-db sir-tolerant broadband interference-robust human body communication transceiver using time domain interference rejection," *IEEE J. Solid-State Circuits*, vol. 54, no. 10, pp. 2892–2906, 2019.

[10] M. S. Wegmueller, S. Huclova, J. Froehlich, M. Oberle, N. Felber, N. Kuster, and W. Fichtner, "Galvanic coupling enabling wireless implant communications," *IEEE Trans. Instrum. Meas.*, vol. 58, no. 8, pp. 2618–2625, 2009.

[11] X. Liu and J. Merritt, *Shaping the Future of the Internet of Bodies: New challenges of technology governance*. Geneva, Switzerland: World Economic Forum, 2020.

[12] M. Lee, B. Boudreaux, R. Chaturvedi, S. Romanosky, and B. Downing, *The Internet of Bodies: Opportunities, Risks, and Governance*. Santa Monica, CA: RAND Corporation, 2020.

[13] D. Yang, P. Mehrotra, S. Weigand, and S. Sen, "In-the-wild interference characterization and modelling for electro-quasistatic-hbc with miniaturized wearables," *IEEE Trans. Biomed. Eng.*, vol. 68, no. 9, pp. 2858–2869, 2021.

[14] A. Alamoudi, A. Celik, and A. M. Eltawil, "Energy efficient capacitive body channel access schemes for internet of bodies," in *IEEE Global Commun. Conf. (GLOBECOM)*, 2021, pp. 1–7.

Abdulkadir Celik (Senior Member, IEEE) received the M.S. degree in electrical engineering in 2013, the M.S. degree in computer engineering in 2015, and the Ph.D. degree in co-majors of electrical engineering and computer engineering in 2016 from Iowa State University, Ames, IA, USA. He was a post-doctoral fellow at King Abdullah University of Science and Technology (KAUST) from 2016 to 2020. Since 2020, he has been a research scientist at the communications and computing systems lab at KAUST. His research interests are in the areas of wireless communication systems and networks.

Ahmed M. Eltawil (Senior Member, IEEE) received the M.Sc. and B.Sc. degrees (Hons.) from Cairo University, Giza, Egypt, in 1999 and 1997, respectively, and the Ph.D. degree from the University of California, Los Angeles, CA, USA, in 2003. Since 2019, he has been a Professor with the Computer, Electrical and Mathematical Science and Engineering Division (CEMSE), King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia. Since 2005, he has been with the Department of Electrical Engineering and Computer Science, University of California at Irvine, where he founded the Wireless Systems and Circuits Laboratory. His research interests are in the general area of low power digital circuit and signal processing architectures with an emphasis on mobile systems. He has been on the technical program committees and steering committees for numerous workshops, symposia, and conferences in the areas of low power computing and wireless communication system design. He received several awards, as well as distinguished grants, including the NSF CAREER Grant supporting his research in low power systems.