Remote Secure eHealth Provision: ETSI SmartBAN as an Enabler

Matti Hämäläinen
Centre for Wireless Communications
University of Oulu
Oulu, Finland
ORCID 0000-0002-6115-5255

Lorenzo Mucchi
Department of Information Engineering
University of Florence
Florence, Italy
ORCID 0000-0001-6389-022

Tuomas Paso
Centre for Wireless Communications
University of Oulu
Oulu, Finland
ORCID 0000-0001-8977-750X

***Abstract*— Utilisation of Internet of Things (IoT) is spreading fast in modern home and industrial automation, but IoT solutions can also be widely utilised in healthcare domain. Monitoring of a person's vital signs and the connectivity between different medical devices are moving towards wireless implementation. Wearables and other health and wellbeing related personal gadgets carried by humans, or even implanted inside a human, are seeing to be more popular in healthcare applications. To respond to these challenges, new technologies in different domains are continuously developed. This paper is discussing the possibilities to effectively and reliably deliver eHealth services outside hospitals or other care units. In addition, we will introduce how ETSI SmartBAN can be utilised in various eHealth applications as well as how the security aspects should be taken into account when dealing with personal data.**

Keywords—WBAN, use case, protocol, medical, wireless

I. INTRODUCTION

The current practice in habitation is that the young and healthy people mostly live typically in urban areas, close to the healthcare and other services. On the other side, elderly people, who have more diseases and require assistance, populate more often remote areas, probably far away from the services. This is a fundamental contradiction: services might not locate where they should be from the population's location point-of-view. As the global demographic prognoses indicate [1], in the future there will also be much more inhabitants requiring healthcare services due to the increasing longevity. A global tendency is that there will be much more elderly people than younger one, year by year. Simultaneously the birth rate is decreasing, as predicted by example to Finnish population by the Statistics Finland in [2]. All these demographic changes will increase the expected workload for healthcare professionals in the future, and simultaneously, the societal healthcare costs will increase.

Tele-healthcare, which is a part of eHealth concept [3], is a credible way to provide efficient and remote care services outside hospitals and other care units, also in rural areas. Moreover, it is possible to better personalise services to each user's individual needs and to promote the public health functions utilising advanced remote procedures. As the environment, where remotely monitored people presumably locate, are their homes, the services can be provided there using modern communications technologies. The use of wearable health monitoring systems does not limit a person's mobility, and the user is not tied to stay only at home, but still can be under medical surveillance. Long-term measurements are possible independently on the person's location, which improves the diagnostics and healthcare services' effectiveness. Long-term data from real-life usage can also highlight medical symptoms which cannot be seen in short-term hospital-based samplings.

How to cope with this issue and how to utilise modern technology to produce enough services in an efficient, secure, and cost-effective way? In this paper, we are concentrating on this question via some exemplifying use cases, which are defined by the European Telecommunications Standards Institute (ETSI) via its Technical Committee (TC) SmartBAN, which is a European initiative towards wider wireless body area network (WBAN) utilisation.

We need to improve the efficiency and scalability of the public healthcare services by stretching the wireless healthcare provision closer to home. One important direction is to focus efforts more on prevention instead of aftercare. This would have not only a straight impact on patients' recovery but also to overall healthcare expenditure for society, which is now increasing. The fact is that sooner the patient is getting health services after falling ill, better will be her/his prognosis, minor problems need to be treated, shorter time in hospitalisation, and so on. However, in rural and developing areas getting immediate medical assistance could be a problem due to the unavailable or limited healthcare services in the neighbourhood. We envision that the wirelessly operating eHealth concept will play a key role in the future healthcare service provision, and this is a global tendency.

Wireless body area networks are one option to benefit wearable electronics in tele-health service provision. Various sensor nodes attached to different places of the human body can measure a person's multiple vital signs, also in real time if needed. Data can then be collected and analysed inside a WBAN by the central node of the network (called as a WBAN coordinator or a hub), or data can be transferred to servers located away from a human. Such domains can be edge or cloud -based data repositories or computation units, electrical health records or any combination of those. Jointly analysed, time-stamped and correlated multimodal information related to a specific event will improve the decision's reliability, independently on the use case.

As a centralised data collection can be adopted, complementary manifold information relating to a person's health, presence and activity is possible to be included in the data analytics. Thus, the concept of active assisted living can be supported by ambient, heterogeneous technology and sensing with fresh and diverse data, which are linked to the individual's health related information. All these approaches open doors for big health data analytics, which could utilise artificial intelligence (AI) and machine-learning (ML) in an efficient way, and finally provides better healthcare services for individuals, independently where they are living. Surely, such analytics part can also be adopted inside hospitals and other care residences as well as homes, thus the technology utilisation will be flexible.

As the personal medical data can always be available for the healthcare professionals, early interventions in the case of emergency situations are possible. This has a great impact on the whole care and emergency processes.

This paper is organised as follows. Chapter II describes the challenges the remote healthcare is facing. In Chapter III, the ETSI SmartBAN architecture is briefly introduced. In Chapter IV, the potential use cases introduced in the technical SmartBAN documents are discussed. Chapter V focuses on related security challenges and finally, the conclusions are given in Chapter VI.

II. CHALLENGES

From a connection point-of-view, communications in eHealth situations can be set-up either by health professionals, health authorities or patients, and terminated by one of these listed actors [3]. From the case, where WBANs are actively involved, the first assumption is that the connection towards the medical operators is launched automatically by the WBAN node/hub, thus a patient from the taxonomy mentioned above. Typically, this can also be the case if personal actuators are controlled via the network. The need of manipulation is based on the contemporary measurement of the vitals carried out inside a personal WBAN. Associated potential reaction via personal actuator can then immediately be launched, if needed, if the data can be locally processed.

Some of the potential use cases where WBAN's can be efficiently used in the healthcare domain are introduced in the Technical Reports [4][5] by ETSI TC SmartBAN, and shortly presented in [6]. Also, some technical requirements for the parameters to be measured relating to the different vital signs can be found, e.g., from [7][8]. According to the person's prescription or pathology, a WBAN can consist of a different set of sensors [9][10]. As defined in [4], the maximum number of nodes one SmartBAN can support is 16 but the listed use cases have nominally 1 – 6 nodes, which is a feasible amount from the user's point-of-view. The wearable network is more complex, and its weight is higher when the number of nodes is increasing. This might have a negative impact on the willingness to take this kind of network in use. User experience is one of the highest indicators when evaluating any system's deployment.

Beneficial for wearable sensors is that they can be seamlessly connected to BAN and other existing wireless networks. However, wearables are prone to motion artefacts, as radio links' characteristics and nodes' instantaneous positions could be rapidly changed when a person moves. A high number of simultaneously connected wireless devices are also causing interference towards other radio systems, which gives pressure to more advanced mutual interference and interoperability management.

Moreover, the practicalities limit the number of simultaneously operating WBANs within a certain space, like a room. Jointly with the low transmission power, which needs to follow the radiation guidelines for maximum safe transmission power, such as provided, e.g., in [11] for non-ionizing radiation, limits the interference range caused by the individual SmartBANs. However, the SmartBAN technical specifications [4][12] do not define any transmission power level so it is left for the manufacturers' decision.

III. SMARTBAN ARCHITECTURE

The technical specifications for SmartBAN are defined in ETSI Technical Specifications for physical and medium access control layers in [12] and [13], respectively. Comprehensive SmartBAN reviews are given in [14],[15] for a quick technology overview.

The SmartBAN architecture is currently based on one-hop star network topology where each node is directly connected only with the network coordinator, which is providing connectivity outside a SmartBAN [4]. The network coordinator in SmartBAN is called a hub, and it is the most powerful device associated with the network. From the operational point-of-view, the hub includes all the functionalities the network and the associated nodes have, while the other peripheral nodes could be based on a reduced set of functionalities. As an example, a hub is in response to heterogeneous network management, it will take care of routing and interactions with other functional domains targeted to various application areas, such as automotive or smart environment [4]. Peripheral node in its simplest realisation can include only the radio and a dedicated sensing functionality. This makes it possible to build cheaper nodes as the main functionalities and computational power are concentrated to the hub. It is envisioned that smartness of the SmartBAN can also be based on multi-level interoperability handling, including semantic approaches. The current state of the ETSI TC SmartBAN work on increased smartness is going to start as a definition work of required functionalities for a smart coordinator.

In one SmartBAN network, the maximum number of nodes is limited to 16, but in a realistic case, typically less than eight nodes are assumed. As the WBAN enables a person's free mobility, it should be noted that the sensor nodes can move as a group, when WBANs are moving. In addition, within one WBAN, individual nodes associated with a WBAN can also move independently of each other. This mobility requires efforts to be put to a co-existence and interference management as several systems can share simultaneously the same space and frequency bands.

To improve the usage and functionalities of the SmartBAN even further, the current work is going to extend the network topology towards a relay functionality (i.e., two-hop star network) [16] and a hub-to-hub communications [17], as shown in Fig. 1. In addition, as the smartness of the SmartBAN is designed to be in a hub, it enables the development of the network, as well as increasing new functionalities to the system simply via updating just a hub.

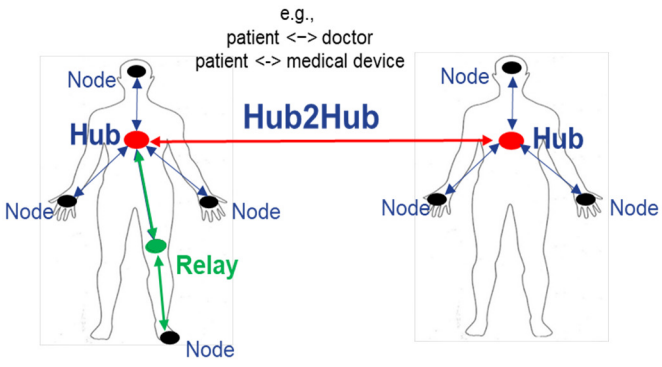

FIGURE 1. SmartBAN Network Topology.

From a data flow perspective, we could divide the overall system into three tiers, as many times used with Internet of Things (IoT) discussion: the body, the edge, and the cloud tiers. The body tier includes the sensors in/on the body and the hub. The edge tier includes, if present, environmental sensors (e.g., radar for presence, or any other sensor not directly placed in/on the body) and the gateway, which could be a smartphone or a dedicated device. The gateway functionalities could also be directly inserted into the hub. The cloud tier includes the storage server where data is stored, (long-termly) analysed, and can be accessed by the authorised persons, such as medical professionals, relatives, etc.

IV. Use cases for SmartBAN Utilisation

As the main application area of the ETSI SmartBAN is relating to healthcare, the technical committee has documented several use cases, with associated performance measures. As an example of technology usage, a person's vital signs can be automatically collected, analysed, and transmitted to electrical health records from where the data can be accessed by the authorised health professionals.

The initial use case descriptions are given in [4][5]. It should be noted that the use cases discussed in these documents are not comprehensive. The indicative applications can be divided into three main categories: medical, safety and wellness, as described in Table I.

TABLE I. Indicative SmartBAN use cases

Medical	Safety	Wellness
Blood pressure	General safety	Stress
Abnormal cardiac rhythm	Fall monitoring	Sleep
Sleep apnea	Rescue	Sports
Musculoskeletal disorder	Emotion	Entertainment
Neuromuscular disorder	Emergency	

The medical applications listed in Table I are based on measuring different vital signs from a human body. The safety category includes use cases relating to general safety features, not necessary psycho-physiological signs, detected for different kinds of application areas. As SmartBAN supports mobility and is dedicated to wearable use, it will also be a suitable solution for various sports and welfare related applications to collect human's psycho-physical information during a person's daily activities. SmartBAN is also a potential technology for smart living and smart home solutions to provide additional information of the person's lifestyle.

Due to the various needs for quality-of-service (QoS) different applications have, the SmartBAN system is scalable in the means of data rates, latency, allowed errors, and so on. Novel multi-use channel access mechanism included in SmartBAN enables efficient channel usage as well as fast channel access for emergency traffic [5]. As the connectivity in SmartBAN can be based on heterogeneous solutions, it can operate with current wireless technologies via multi-radio hub. The goal of the SmartBAN technical committee is to develop a future proof WBAN concept, whose features can be updated easily via the smart coordinator, which is the master element of the network functionalities and management.

Smart coordinator is an edge device between the personal network and the backbone network, and it is capable of controlling and coordinating all the WBAN operations effectively and in a transparent manner. Thus, inside a SmartBAN network, the wireless connectivity solution is based on the specifications from [12],[13] but the connection outside the network can differ, depending on the implementation of the hub, thus, a smart coordinator.

V. SmartBAN Security

From a security perspective, the weak point at the data flow is the body tier since the sensors are low-resourced (low computation capability and low memory space), they should consume a small amount of power, but they still carry very sensitive information, as we are dealing with health-related data. Another weak point is the (portable) hub, in particular if the hub is used also for other services (e.g., if the hub is integrated into a smartphone), instead of being a dedicated device. In fact, a smartphone can be hacked while used for other businesses. When once hacked, it can forward malicious consequences to or from the BAN. On the contrary, the cloud server can be protected by well-known and matured security strategies, and this tier is somehow less in emergency from the security point of view.

Security issues at body tier are such as: *i*) Usual cryptography protocols are hard to be applied by the tiny sensors on the body; *ii*) Authentication of each tiny sensor should be verified periodically, and not only during the set-up phase; *iii*) Efficiency, scalability and usability could make the security design more challenging than in traditional networks; *iv*) Secret keys' generation and distribution should be lightweight; *v*) Intrusion detection methods should be re-designed taking into account the presence of low complex devices.

While general security requirements are valid for all the tiers, the variety of communications protocols and devices' capabilities (e.g., computational, storage, memory size, etc.) ask for a specific characterization of the security threats and solutions defined separately for each tier. This allows the implementation of a complete and secure system. Data confidentiality, integrity, authentication, freshness, availability, secure management, access control and scalability are some of the key requirements that need to be considered in a WBAN implementation [18]. In [19], an extensive list of requirements including resources' consumption, memory limitations, and dynamic network features is provided. In [20], the best practice guidelines for the design of a secure IoT-based system are described. Different aspects are considered, including classification of data based on the sensitivity level (storage and transmission), physical, network and application layer securities, securing software updates and credential management.

Due to the increasing number of IoT health devices and services, different types of security threats may compromise a WBAN. In [21], an attack taxonomy, classifying the main security threats is provided, based on: *i*) information disruption; *ii*) host properties and *iii*) network properties. The first category includes service interruption (denial of service,

DoS), data interception and tampering; while the second one takes into account user, hardware and software attacks (e.g., password stealing, device reprogramming and exploiting software vulnerabilities). Finally, the third category includes protocol and network layer specific threats.

Let us focus on the two main security attacks that can compromise a WBAN [22]: DoS and data tampering. Both attacks are described focusing on the less investigated links in the literature - the body and the edge tiers. A DoS attack consists of a communications blockage, and it may occur both on sensors or on the hub, preventing communications among in-body sensors or between in/on body devices and the hub. Communications disruption can be due to flooding interference, jamming communications, or useless power depletion. On the other hand, data tampering refers to the act of manipulating, modifying, or editing data through unauthorised means. Although tampering at the body tier is challenging, illegitimate nano-devices may be introduced inside a body for intercepting communications among the legitimate ones as well as modifying data. Due to their open environment placement, it is compromising the integrity of the WBAN at both the body and the edge tiers.

Both the adoption of modified traditional security mechanisms and new security algorithms should be considered for the definition of advanced security solutions for SmartBAN. To achieve scalability and to handle and maintain end-to-end security, based on the specific applications, a trade-off analysis should be carried out, taking into account the target security level versus *i*) complexity, *ii*) resource usage, *iii*) power consumption, and *iv*) cost. A layered approach may be adopted to identify potential solutions, addressing specifically the requirements of the nodes, represented by their very low power capabilities, and the ones of the hub. Focusing on the former, physical-layer techniques, light cryptography, fast cypher-keys' generation and exchange can be considered against eavesdropping, while active learning (e.g., using ML/AI techniques) and intelligent monitoring (e.g., using energy detection) may be used to cope with DoS [22]. As an example of an implementable physical-layer technique, it is worth mentioning the noise–loop (NL) modulation [23][24]. The NL is a technique that intrinsically protects confidential data from eavesdroppers by exploiting the unique characteristics of the thermal noise, inside any electronic device [25]. The NL has also low hardware resource occupancy and low computational cost [25], which make it suitable for secure cypher-key distribution or to directly protect short-range wireless communications, as is the case in SmartBAN applications and deployment.

The security issues relating to SmartBAN will be described in yet unpublished document [26], which content is currently under preparation.

VI. SUMMARY

In this paper, we have discussed how ETSI SmartBAN can be used to enable humans' individual automated monitoring. SmartBAN is a European version of wireless body area network standard targeted for healthcare related applications. The SmartBAN architecture has shortly been described, with practical use cases for health monitoring as an example of intelligent body networks utilisation.

Finally, the security issues and challenges relating to SmartBAN, and WBANs in general, have been discussed. As such body area networks are in charge of carrying very sensitive information, their security features need to be carefully designed and implemented. This work is currently ongoing.

ACKNOWLEDGMENT

This research has been financially supported in part by Academy of Finland 6G Flagship (grant 318927), by the European Union's Horizon 2020 programme under the Marie Skłodowska-Curie grant agreement No. 346208 and by Infotech Oulu. The authors would like to give big thanks to the ETSI TC SmartBAN colleagues involved in the standard development process

REFERENCES

[1] 2019 Revision of World Population Prospects, https://population.un.org/wpp/Graphs/DemographicProfiles/Pyramid/900. Online: Accessed Oct 28, 2021.

[2] Statistics Finland, https://www.stat.fi/til/vaenn/2018/ vaenn_2018_2018-11-16_tie_001_en.html. Online: Accessed Oct 28, 2021.

[3] eHEALTH: Standardization use cases for eHealth. ETSI TR 103 477.

[4] Smart Body Area Networks (SmartBAN); System Description. ETSI TR 103 394.

[5] Smart Body Area Network (SmartBAN); Applying SmartBAN MAC (ETSI TS 103 325) for various use cases. ETSI TR 103 711.

[6] M. Hämäläinen, T. Paso, "Adapting ETSI SmartBAN to eHealth", Proceedings of eHealth2021: The 26th Finnish National Conference on Telemedicine and eHealth. "eHealth in a Lifecycle", Oulu, Finland, Oct 7-8, 2021.

[7] R.A. Khan, A.-S. Khan Pathan, "The state-of-the-art wireless body area sensor networks: A survey", International Journal of distributed Sensor networks, Vol 14(4), 2018.

[8] J. Khan, M. Yuce, "Wireless body area networks (WBAN) for medical applications", New developments in biomedical engineering, Intechopen, 2010. DOI: 10.5772/7598.

[9] G. Acampora, D. Cook, P. Rashidi, A. Vasilakos, "A survey on ambient intelligence in healthcare", Proceedings of the IEEE, Vol. 101, No. 12, Dec. 2013.

[10] M. Chana, D. Estèvea, J.-Y. Fourniolsa, C. Escribaa, E. Campo: Smart wearable systems: Current status and future challenges. Artificial Intelligence in Medicine 56 (2012) 137–156.

[11] www.icnirp.org. Online: Accessed March 25, 2022.

[12] Smart Body Area Network (SmartBAN); Enhanced Ultra-Low Power Physical Layer. ETSI TS 103 326.

[13] Smart Body Area Network (SmartBAN); Low Complexity Medium Access Control (MAC) for SmartBAN. ETSI TS 103 325.

[14] M. Hämäläinen, L. Mucchi, M. Girod-Genet, T. Paso, J. Farserotu, H. Tanaka, D. Anzai, L. Pierucci, R. Khan, Md M. Alam, P. Dallemagne, "ETSI SmartBAN Architecture: the Global Vision for Smart Body Area Networks", IEEE Access, Vol. 8, pp. 150611 – 150625, 2020, Print ISSN: 2169-3536, Online ISSN: 2169-3536, DOI: 10.1109/ACCESS.2020.3016705.

[15] M. Hämäläinen, T. Paso, L. Mucchi, ETSI SmartBAN in Medical IoT, URSI GASS 2020, Rome, Italy, 28 Aug. - 4 Sep. 2021.

[16] Smart Body Area Network (SmartBAN) Relay Functionality for SmartBAN Medium Access Control (MAC). ETSI TS 103 805.

[17] Smart Body Area Network (SmartBAN) Hub to Hub Communication for SmartBAN Medium Access Control (MAC). ETSI TS 103 806.

[18] A. Tewari and P. Verma,"Security and Privacy in E-Healthcare Monitoring with WBAN: A Critical Review", International Journal of Computer Applications, Volume 136 – No.11, February 2016.

[19] IoT Security Foundation Connected Consumer Products Release 1.1, Secure Design Best Practice Guidelines, December 2017.

[20] S. M. R. Islam, and others, "The Internet of Things for Health Care: A Comprehensive Survey," in IEEE Access, vol. 3, pp. 678-708, 2015.

[21] Shikha Pathania et al, "Security Issues In Wireless Body Area Network", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 1171-1178.

[22] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in IoT: A novel perspective," MDPI Information, vol. 7, no. 3, pp. 49-66, Sept 2016.

[23] L. Mucchi, L. Ronga, and E. Del Re, "Physical layer cryptography and cognitive networks," Wireless Personal Communications, vol. 58, no. 1, pp. 95–109, May 2011.

[24] L. Mucchi, et al, "Noise-loop multiple access," IEEE Transactions on Vehicular Technology, vol. 65, no. 10, pp. 8255–8266, Oct 2016.

[25] L. Mucchi, S. Caputo, P. Marcocci, G. Chisci, L. Ronga, and E. Panayrci, "Security and reliability performance of noise-loop modulation: theoretical analysis and experimentation", in IEEE *Trans. on Veh. Tech.*, early access, Mar 2022. [doi: 10.1109/TVT.2022.3160094]

[26] Smart Body Area Networks (SmartBAN); Security, privacy and trust; state of the art, use cases, treats and requirements analysis. ETSI TR 103 638.