Recent Progress in ETSI TC SmartBAN Standardization

1st Matti Hämäläinen
Centre for Wireless Communications
University of Oulu
Oulu, Finland
ORCID 0000-0002-6115-5255

2nd Lorenzo Mucchi
Department of Information Engineering
University of Florence
Florence, Italy
ORCID 0000-0001-6389-0221

3rd Tuomas Paso
Centre for Wireless Communications
University of Oulu
Oulu, Finland
ORCID 0000-0001-8977-750X

4th Daisuke Anzai
Graduate School of Engineering
Nagoya Institute of Technology
Nagoya, Japan
ORCID 0000-0003-4872-1539

5th Hirokazu Tanaka
Toshiba Bristol Research and Innovation Laboratory
Toshiba
Bristol, U.K.
ORCID 0000-0002-4647-9075

6th Cees J.M. Lanting
R&D
DATSA Belgium
Leuven, Belgium
ORCID 0000-0001-5858-7295

7th Marco Hernandez
CWC, University of Oulu, Finland
YRP-IAI, Japan

***Abstract*—In this paper we are updating the current status of the development of the smart body area network standardization process carried out at ETSI, the European Telecommunications Standards Institute under the Technical Committee Smart Body Area Networks, TC SmartBAN. Due to the increasing interest in monitoring personal health and wellness related vital signs, daily activity and so on, a person is nowadays, and in the future expected even more, to carry various wearable interconnected sensing devices. This forms a base for creating and using wireless body area networks (WBAN), which can simplify the architecture to link various wearable sensor nodes distributed around a human body jointly with a low-power radio and sensing technologies.**

***Index Terms*—low energy, security, smartness, vital signs, wireless body area networks**

I. INTRODUCTION

During the previous years, people's interest to monitor their personal vital signs and more generally health related information has considerably increased. For example, the COVID-19 pandemic the world has suffered under since early 2020 is one motivator which has accelerated this process, as the normal daily work related exercises vanished, as people mostly stayed at home all day. Those who were already active in physical exercises still continued their habits following the regional restrictions on how to practice outside or elsewhere. On the other hand, persons, who used not to move much started to do some exercise as well. In addition, the lack of physical contacts with medical professionals as well as others outside the 'family' also encouraged people to start monitoring themselves, and maybe compare their activities with others in virtual environments. This can be seen as a booster for utilization of personal, wearable sensing devices, such as fitness watches, rings, etc, which are easy to wear and use.

The usage of wireless body area network (WBAN), which is a centralized network architecture enabling connectivity between various wearable sensor nodes attached around a human body can be seen as an enabler for personal vital and activity data collection. In addition to on-body nodes, special cases are medical in-body and implantable devices, which can be inside a human body but still are connected to an on-body network, or even between each other. The WBAN sensor nodes can monitor, for example, activity, temperature, heart and respiratory rates, and oxygen saturation amongst others parameters, as illustrated in Fig. 1. The network architecture itself does not limit the utilization of different kinds of sensing devices as a part of the personal WBAN. Sensing nodes can be selected according to the actual need.

Collected multimodal vital information can then be used, e.g., in a diagnosis of person's sleeping, health status, healing process, or just to follow their activity or health condition development over a long period of time. The devices are also able to detect sleep efficiency and other parameters, which help to express indications about the individual's health condition. In addition to process the information in visual form to be shown, e.g., in portable device apps, all the data can be collected to a cloud service as the WBAN enables connection to other, non-body networks. Then, data delivery to digital health records is also possible using external networks, such as connecting to Wi-Fi or cellular networks and then, via Internet, to the destination anywhere.

The WBAN network topology is typically a one-hop star

This work is partially funded by Academy of Finland via 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.

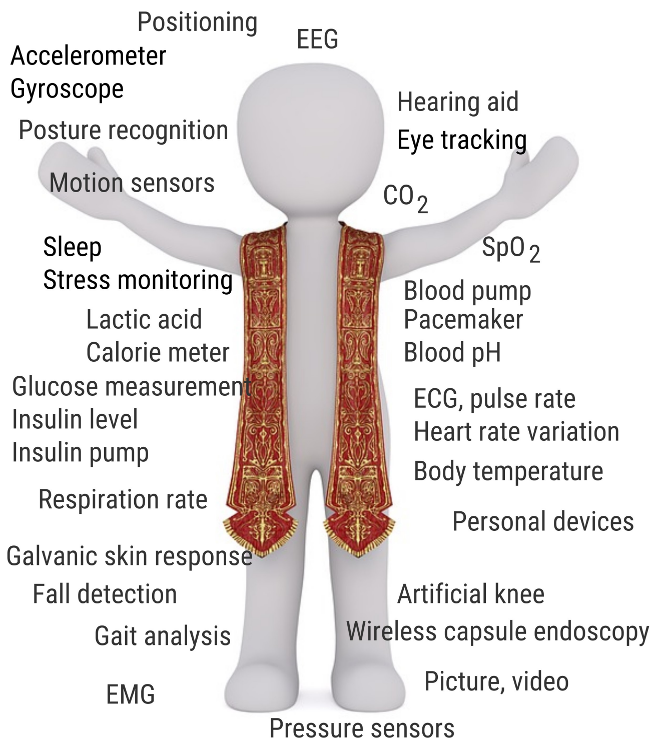

Fig. 1. Examples of available sensor nodes in WBAN context.

network and is coordinated by a central node, called as a hub. The one-hop star topology is adopted, e.g., in the IEEE 802.15.6 [1], which is the first dedicated WBAN standard. Also other wireless personal area network (WPAN) technology deployments, such as Bluetooth Low Energy (BLE) based networks (latest version of the specification is [2]), are mostly utilizing a star network topology, although also mesh topology is nowadays supported. As the expected various SmartBAN use-cases assume, it will be used in environments where also other users and radio systems are simultaneously operating, efficient co-existence management is required. This feature has already been studied in [3] using the measurement based interference model to disturb the SmartBAN communications.

SmartBAN is a European initiative to provide reliable wireless connectivity for low-power short-range services enabling personal data delivery. The technology standardization work is ongoing in European Telecommunications Standards Institute (ETSI). The compact overview of the SmartBAN standardization status at 2020 was given in [4]. The aim here is to briefly update on the current progress of the standardization process, not going into the details of the technology as there are already more detailed information available from open sources. However, some basic information is given here to make it easier for a reader to become familiar with the basics of the SmartBAN technology.

In this paper we concentrate on what is ongoing at the moment and what are the future views relating to SmartBAN. The rest of the paper is organized as follows. In Chapter II, we shortly envision the SmartBAN usage. Chapter III gives the main technical parameters to understand the SmartBAN functionalities. Chapter IV discusses shortly on the published technical specification (TS) and technical report (TR) documents technical committee (TC) SmartBAN of ETSI has produced. In Chapter V, we highlight the current activities. Chapter VI concludes the paper and shows the TC's future visions.

II. SMARTBAN VISION

From the beginning of the SmartBAN development work, the most important performance indicators have been high reliability and interoperability, ultra low power consumption, maximized security, privacy and trust. For medical and other high-priority (emergency) traffic, SmartBAN introduces very-low latency channel access mechanism called priority channel access as part of the multi-use channel access scheme that is providing also utilization of scheduled but unused time slots by secondary users [5]. The goal has also been to define a future-proof concept with an extended smartness, which distinguishes SmartBAN from other existing solutions. Smartness can be seen in advanced control and network management operations. From the use-case point-of-view, SmartBAN has always been a scalable and adaptable solution which can be used for various purposes. Enhanced interoperability in all the functional layers is also specifically taken into account. TC SmartBAN has defined and harmonized data representation formats and semantic ontologies with, in particular Alliance for the Internet of Things Innovation (AIOTI) and oneM2M [6]. Smart heterogeneity management enables also the effective interaction with neighbouring systems using other radio technologies, and existing and coming Internet of Things (IoT) and Internet of Medical Things (IoMT) systems.

III. SMARTBAN TECHNICAL FEATURES

The idea of SmartBAN is based on low power consumption, simplified sensor nodes, centralized control and a high level of intelligence. A SmartBAN is consisting of a master node, called a hub, and typically 1-15 sensor nodes, as defined in [7]. Thus, the maximum size of the network is 16 nodes. This number should be enough for most cases where WBANs can be used in personal vital sign and activity monitoring.

The network carried by a person forms an entire SmartBAN network (hub + 1 to 15 nodes). A similar network carried by another person forms then another SmartBAN network, respectively. As the network is coordinated by the hub, an asymmetrical relationship between the hub and various nodes is evident. It is hub's responsibility to perform scheduling operations and do most of the computing actions. For energy saving purposes, nodes are maximizing their sleeping time within a beacon period, which is a duration between the regular beacon signals transmitted by the hub.

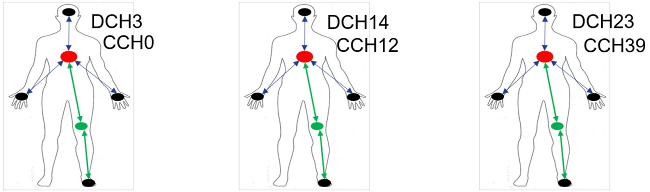

Fig. 2. Separation of three SmartBAN networks. Each SmartBAN uses its own control and data channel.

The main focus in SmartBAN standardization work has been set to interoperability and flexibility objectives. The SmartBAN is operating at the unlicensed industrial, scientific and medical (ISM) frequency band, allocating frequencies between 2.401 GHz - 2.481 GHz [8]. The 80 MHz frequency band is divided into 40 physical channels including three control and 37 data channels, each having a bandwidth of 2 MHz. In the individual SmartBAN network, data and control channels are sharing the same physical channel, thus the same carrier frequency, which makes it possible to operate using only one radio frequency (RF) chain. The control channel, as the name indicates, is used to distribute control information relating to network parameters and in it, only the hub broadcasts the control channel beacons. Bidirectional data channels are used for data transmission between the nodes and the hub.

From the topology point of view as already mentioned, SmartBAN is coordinated by a hub, which contains most of the smartness of the network. The peripheral nodes can then be simpler from the operational and implementation point-of-views. This decreases the installation cost of the whole personal network. Network separation is done using different control channels and data channels between adjacent SmartBANs. Though there are only three control channels available, physical distance between the different SmartBANs is high enough, as well as the transmission power is small, which enables efficient control channel reuse and thus, more networks can operate in a certain space. Three different SmartBANs are shown in Fig. 2. A structured description of the SmartBAN is available at [4].

IV. COVERED TOPICS AND PUBLISHED STANDARDS

The TC SmartBAN work at ETSI started 2013, and the TC has met three times a year, on the average. The TC has covered topics from data formats, ontology and application protocol interface (API) to physical layer (PHY) and medium access control layer (MAC) definitions. Interoperability management has been one of the key features SmartBAN has focused on. The work also benefitted the experimental work carried out to model the RF environment at the 2.4 GHz frequency band SmartBAN is using. Real live measurements were made at hospitals in Oulu, Finland and Florence, Italy [9], [10].

The published standards are listed in Table I. The technical documents are available for free download at [11]. According to ETSI definitions, a TS contains technical requirements defined for implementing the corresponding standard, whereas a TR provides supplementary information. Both document types are approved by the corresponding TC, in this case TC SmartBAN.

The TS for associate service models, ontology and enabler extension, which is linked to already published TS 103 378 [6] is ready to be published soon. The work towards higher open system interconnection (OSI) layer specifications has started for the data scanner agent specifications, but this work is not ready, yet.

The latest PHY layer studies have focused on implant communications and especially utilizing ultra wideband (UWB) technology in localizing and communicating with wireless capsule endoscope (WCE). Under ETSI, medical applications which are utilizing UWB are not covered by other TCs, but SmartBAN is collaborating with the corresponding technical bodies, such as TC UWB [12], to maintain harmonized technology approaches.

As SmartBAN is dealing with health and wellness related information, it is mandatory to achieve high trustworthiness at all the levels, including data collection and transmission, data analytics, and data storage. SmartBAN has a dedicated work item (WI) to define respective security features and it is collaborating with ETSI TC CYBER [13].

TABLE I
PUBLISHED ETSI SMARTBAN STANDARDS

Topic	**Document ID**
System description and use-cases	TR 103 394 [7], TR 103 711 [14]
PHY layer	TS 103 326 [8]
MAC layer	TS 103 325 [5]
Interoperability management	TS 103 327 [15]
Radio frequency environment	TR 103 395 [9]
Data formats and semantics	TS 103 378 [6]
Implant communications	TR 103 751 [16]

V. CURRENT WORK

As the work towards the European WBAN standard has progressed well, the TC has incorporated and complemented with topics the evolving SmartBAN standard will include. As the original network topology was based on one-hop star network, the covered area will be extended by introducing a two-hop relay functionality. This feature removes the isolated node problem, which might prevent the connectivity between the hub and a node locating on the other side of a torso, for example. The definition work for a new, enhanced MAC features has been done and the complementary TS document is almost ready to be published. In addition to a relay option, also neighbouring SmartBAN networks can be connected using, so called, hub-to-hub communications. Soon, the TS describing this feature will also be published. The final revisions are also ongoing in the definition of unified data representation formats, semantics and open data model.

A. Data representation formats, Semantic and open data model

To enable low complexity, SmartBAN is utilizing a modular, open data model, which is divided in three domains: WBAN

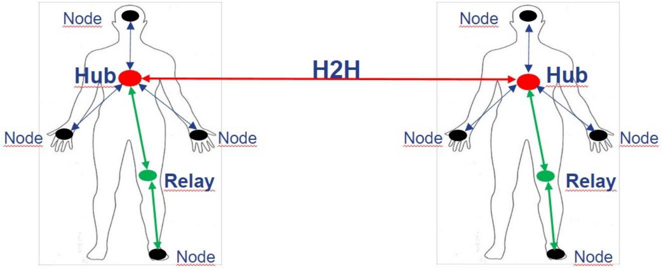

Fig. 3. Relay and hub-to-hub links in the SmartBAN context.

itself; nodes (hub, sensors, actuators and corresponding peripheral devices); and processes and measurements. Well-defined parameters are important, especially in the case of health or assisted living related applications, when, e.g., the lifetime of a device should be long and the fault tolerance need to be extremely small. Independently of the application, the accuracy of the measurements should be high. Harmonized ontology enables vendor independent interoperability between the devices.

B. *Relay functionality*

To enable longer distances between the nodes and the hub as well as connections to isolated nodes, new SmartBAN specification will introduce a two-hop relaying feature, which is extending the original one-hop MAC specification [5], and will be published in TS 103 805 technical specification as an amendment to the original MAC specification. According to the new specifications, connections between the nodes around a relay node will be initiated as a joint effort by the hub and the isolated node. An isolated node willing to remain in connection to the hub, but temporarily out of the range due to distance and/or poor channel conditions, can then reach the hub via the relay node.

C. *Hub-to-hub communications*

To serve multiple SmartBANs, TC has defined a hub-to-hub (H2H) communication specification at MAC level in TS 103 806 document, which is also an amendment to the original MAC specification [5]. This new feature enables communications between the neighbouring hubs, thus between two adjacent SmartBANs. This kind of H2H connectivity can also be established between a medical device and a person's SmartBAN.

The TSs for relay and hub-to-hub functionalities are currently in the final edition phase. New amendments requires also edition to be done to the original MAC specification [5]. The relay and H2H links under discussion are visualised in Fig. 3.

D. *Implant communications*

In addition to on-body communications, which is defined in [8], SmartBAN is also covering in-body communications, e.g., relating to information transfer between on-body node and a WCE, which is located inside a gastrointestinal tract (GI), such as a small device in the intestines of a human body. Additionally, locating the WCE inside a GI is another key issue for in-body and implant communications. The same technology can be utilized in the links between two implanted devices or WCEs. In this case, the physical layer is not following the generic SmartBAN approach, narrowband signaling at 2.4 GHz ISM band, but the wireless part is implemented using impulse radio based UWB operating around 4 GHz. The use of UWB in the implant communications enables to realize high-resolution image/video data transmission with higher data rate and reliability, as compared with medical implant communication service (MICS) at 400 MHz band. UWB communications also allows precise WCE localization because of its high distance resolution. Currently, implant communication studies have produced only a TR document. This part of the work is carried out in collaboration with ETSI TC UWB [12] and ETSI EMC and Radio Spectrum Matters (ERM) [17].

E. *Smart Coordinator*

Future healthcare and well-being systems will extend mobile services into a new vertical application domain with a specific requirement for healthcare and well-being services.

Such new domain applications come with demanding requirements, such as high availability, high reliability, low latency, and seamless integration into infrastructure.

The smart coordinator (SC) represents the next step to bridge uncoordinated SmartBAN networks to infrastructure like Wi-Fi or cellular network while adding support to other personal technologies, like Bluetooth. Hence, the SC intends to support the following:

- Define the convergence function between the Link layer (L2) of SmartBAN and the corresponding entity at the infrastructure side.
- Support high reliability and dependable quality of service (QoS) across networks in the communications path by bridging via the time sensitive networking (TSN) infrastructure.
- Definition of a new vertical for 5G/6G that enables a wide range of personal applications, from general health indicators to medical-grade devices.
- Coexistence mechanisms that support operation with other SmartBANs and wireless technologies operating sharing the same spectrum.
- Define the security protocol for operation with infrastructure or standalone. Cyber-security has become essential for the protection of information data and privacy.

F. *Security*

One of the major starting points in the SmartBAN standardization has been a high-level trustworthiness at all levels of operation. In this work, TC SmartBAN is collaborating with ETSI TC CYBER [13] under the security framework.

SmartBANs are networks of wearable or implantable devices that monitor and collect physiological and biomedical data of an individual in real-time. The main challenge in body area networks is to ensure security and privacy of the sensitive data being collected and transmitted. To achieve this, various security mechanisms have been proposed, such as encryption of data, authentication of devices and users, and secure communications protocols. Additionally, physical security mechanisms, such as tamper-resistant packaging and anti-tampering techniques, can also be implemented to prevent unauthorized access. It is important to consider both the confidentiality and integrity of data, as well as the availability of the SmartBAN system, to ensure its effectiveness and reliability. Overall, ensuring the security of SmartBANs is critical to protect the privacy and safety of individuals, and it requires a multi-layered approach that includes both technical and physical security measures.

The TC CYBER security requirements and specifications document [18] is related to IoT networks, and not specifically for body area networks, even more not for the specific architecture of SmartBAN. The TC CYBER approach focuses on three main security approaches: authentication, confidentiality, and integrity. Authentication is achieved through the use of unique identifiers and secure key exchange protocols, which enable devices to verify the identity of each other before any data transfer occurs. Confidentiality is ensured through data encryption techniques, which prevent unauthorized access and eavesdropping of the data in transit. Integrity is maintained through digital signatures and message authentication codes, which ensure that the data has not been tampered with or altered in transit. In addition to these security measures, the SmartBAN standard will also specify specific network management procedures and protocols to mitigate security risks, such as denial-of-service attacks, packet replay attacks, and unauthorized access to network resources.

As described earlier, SmartBAN aims to establish a European standard for a smart body area network (BAN) by comprehensively defining system aspects from lower to higher OSI layers, including end-to-end, to support applications such as health, wellness, leisure, and sports. SmartBAN employs small, low-power devices and a star topology comprising two types of devices, namely an information source device (node), such as a medical sensor, and a coordinator device (hub). At least one node on the body should communicate directly with the hub. Security mechanisms and algorithms, either modified traditional or new, should be considered in defining security solutions for SmartBAN. A trade-off analysis should be performed based on specific applications, taking into account the target security level, complexity, resource usage, power consumption, and cost.

A layered approach can be adopted to identify potential solutions that meet the requirements of nodes and the hub. For nodes, physical-layer techniques, light cryptography, fast cipher key generation and exchange can be considered against eavesdropping, while active learning and intelligent monitoring, such as energy detection, can be used to cope with denial-of-service (DoS) attacks [19]. An example of a physical-layer technique that protects confidential data from eavesdroppers by leveraging the unique characteristics of thermal noise inside any electronic device is a noise-loop (NL) [20]. A NL has low hardware resource occupancy and low computational cost [21], making it suitable for secure cipher-key distribution or to directly protect short-range wireless communications in SmartBAN applications.

The SmartBAN approach to security and privacy is aiming to provide a framework for secure and reliable wireless communications between wearable or implantable devices in a WBAN environment. The work is still in progress, but it can be summarized as follows:

- Inherit the security requirements from ETSI TC CYBER.
- Add to those security requirements specifically for health-related devices/sensors.
- Identify the security threats specific for the SmartBAN architecture.
- Propose solutions for those threats in each level of the OSI layers.

It is important to point out, for example, that the SmartBAN security approach is based on the use of physical-layer security techniques for confidentiality, authentication and key exchange.

By following the security approaches outlined in the SmartBAN standard, BAN designers and developers can ensure that their systems provide secure, reliable, and trustworthy connectivity for medical, wellness, and sports applications.

VI. Conclusion and Future Work

As can be seen, ETSI TC SmartBAN has already produced four TS and four TR documents, new releases to be published soon. The main contributions relate to harmonized data formats and ontologies with other IoT devices, as well as standardized physical and MAC layer functionalities. The novel smart coordinator is distinguishing SmartBAN from other existing WBAN solutions. The other feature characteristic of SmartBAN is the multi-use channel access mechanism at MAC layer, which enables fast channel access for priority traffic and utilization of scheduled but unused time slots by secondary users. Our vision is that in the coming years, SmartBAN enabled devices can share the environment with other radio systems, especially coexisting with numerous IoT and IoMT devices. All the solutions included in the TS documents are targeted to enhance robustness, interoperability and trustworthiness of the low-power wearable devices.

Acknowledgment

Authors would like to thank all the SmartBAN contributors during the years as well as the associated ETSI Technical Officers who have greatly helped and made this work possible.

References

[1] IEEE Standards Association, “IEEE Standard for Local and Metropolitan Area Networks - Part 15.6: Wireless Body Area Networks.” IEEE Std 802.15.6™-2012.

[2] Bluetooth SIG, “Bluetooth Core Specification.” Bluetooth Specification v5.4, 2023.

[3] H. Viittala, L. Mucchi, M. Hämäläinen, T. Paso, ”ETSI SmartBAN System Performance and Coexistence Verification for Healthcare”, IEEE Access, Dec. 2017, Volume: 5, Issue: 1, Page(s): 8175-8182. DOI: 10.1109/ACCESS.2017.2697502.

[4] M. Hämäläinen et al., ”ETSI SmartBAN Architecture: The Global Vision for Smart Body Area Networks,” IEEE Access, vol. 8, pp. 150611-150625, 2020, doi: 10.1109/ACCESS.2020.3016705.

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

[6] Smart Body Area Networks (SmartBAN) Unified data representation formats, semantic and open data model. ETSI TS 103 378.

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

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

[9] Smart Body Area Networks (SmartBAN); Measurements and modelling of SmartBAN Radio Frequency (RF) environment. ETSI TR 103 395.

[10] L. Mucchi, et al., “Spectrum Occupancy and Interference Model based on Network Experimentations in Hospital”, IEEE Transactions on Wireless Communications, Print ISSN: 1536-1276, Online ISSN: 1558-2248, DOI: 10.1109/TWC.2020.2995116.

[11] https://www.etsi.org/committee/1413-smartban. Accessed Apr 12, 2023.

[12] https://www.etsi.org/technologies/ultra-wide-band. Accessed Apr 12, 2023.

[13] https://www.etsi.org/committee/cyber. Accessed Apr 12, 2023.

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

[15] Smart Body Area Networks (SmartBAN); Service and application standardized enablers and interfaces, APIs and infrastructure for interoperability management. ETSI TS 103 327.

[16] Smart Body Area Networks (SmartBAN); Implant communications. ETSI TR 103 751.

[17] https://www.etsi.org/committee/erm. Accessed Apr 12, 2023.

[18] CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI EN 303 645.

[19] 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.

[20] 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.

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