Journal of
Sensor and
Actuator Networks

Article

Secure and Connected Wearable Intelligence for Content Delivery at a Mass Event: A Case Study

Aleksandr Ometov [1,*], Dmitrii Solomitckii [1], Thomas Olsson [1], Sergey Bezzateev [2], Anna Shchesniak [2], Sergey Andreev [1], Jarmo Harju [1] and Yevgeni Koucheryavy [1]

[1] Departments of Electronics and Communications Engineering, and Pervasive Computing, Tampere University of Technology, FI-33720 Tampere, Finland; dmitrii.solomitckii@tut.fi (D.S.); thomas.olsson@tut.fi (T.O.); sergey.andreev@tut.fi (S.A.); jarmo.harju@tut.fi (J.H.); evgeni.kucheryavy@tut.fi (Y.K.)

[2] Departments of Cyber Physical Systems Security, and Wireless Telecommunications, ITMO University, 197101 Kronverksky pr., 49, St. Petersburg, Russia; bsv@aanet.ru (S.B.); anna.schesnyak@scaegroup.com (A.S.)

* Correspondence: aleksandr.ometov@tut.fi

Academic Editor: Hakima Chaouchi
Received: 31 January 2017; Accepted: 11 May 2017; Published: 22 May 2017

Abstract: Presently, smart and connected wearable systems, such as on-body sensors and head-mounted displays, as well as other small form factor but powerful personal computers are rapidly pervading all areas of our life. Motivated by the opportunities that next-generation wearable intelligence is expected to provide, the goal of this work is to build a comprehensive understanding around some of the user-centric security and trust aspects of the emerging wearable and close-to-body wireless systems operating in mass events and under heterogeneous conditions. The paper thus intends to bring the attention of the research community to this emerging paradigm and discuss the pressing security and connectivity challenges within a popular consumer context. Our selected target scenario is that of a sports match, where wearable-equipped users may receive their preferred data over various radio access protocols. We also propose an authentication framework that allows for delivery of the desired content securely within the considered ecosystem.

Keywords: wearables; security; authentication; WiGig; mass event; wireless; challenges

1. Introduction and Scope

Today, smart and connected wearable systems, such as on-body sensors, head-mounted displays and other small form factor capable personal computers are rapidly pervading all areas of our life as a more personal part of the Internet of Things (IoT) paradigm [1,2]. Such emerging wearables open new avenues for fundamentally different forms of both user-centric contextual services and interactive multi-user applications based on sharing data and resources locally [3]. This trend provides immense opportunities but, on the other hand, constitutes a vast unexplored area, riddled with numerous research challenges for both academia and industry [4]. One of the key challenges relates to the 'big three': security, privacy, and trust [5], i.e., *how to ensure that wearable-specific information is produced and consumed appropriately by a multitude of devices and users* [6].

Wearables are developing rapidly to become the next major information and communications technology paradigm, while manifesting ubiquitous computing and intelligent information technology on the most personal level [7]. Wearable devices are the pinnacle of miniaturized computation and communication technology for tracking, storing, processing, and reporting important human activity, such as physiological parameters, social interactions, and events [8]. They enable the next generation of wearable intelligence, where the communications chain may interconnect not only the user smartphones (acting as gateways) but also a wide range of new services (see Figure 1).

Particularly in urban environments, the proliferation of mobile wearable technology [9], as well as the rise of smart and automated cities are opening up new opportunities for improved public safety and security [10]. Even though there has been significant deployment experience of diverse IoT systems, the understanding behind these systems and the corresponding implications in the context of safety and security have only just scratched the surface [11].

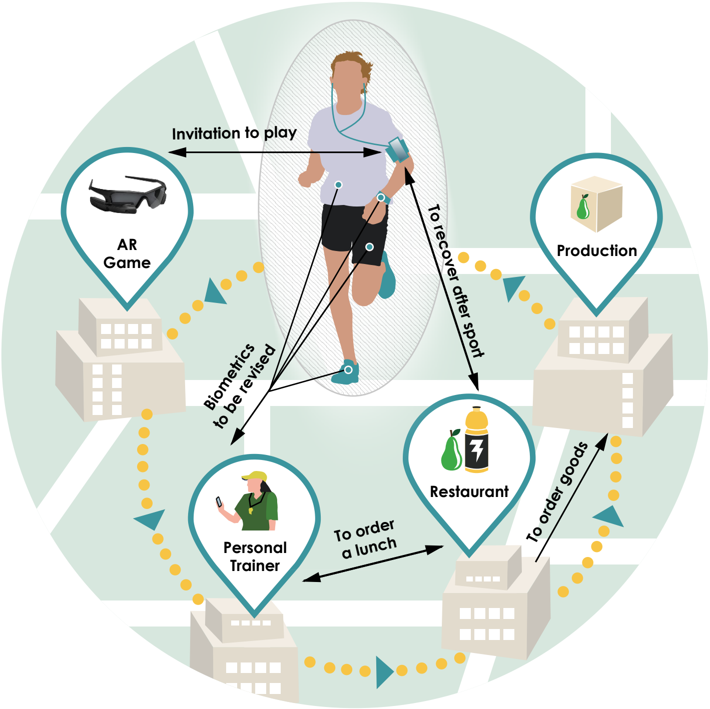


Figure 1. User-centric applications and services enabled by next-generation wearable intelligence.

1.1. Applications of Wearables

Wearables have become a decisive innovation offered by a plethora of accessories and clothes (smart glasses, smart watches, fitness bands, augmented reality glasses, cameras, gadget gloves, etc.), which dramatically augment human capabilities [12]. Underpinning the topicality of this area, large international business around wearables is now in turbulence, which is evident from, for example, recent acquisitions of corresponding start-ups by larger companies like Intel (Recon Instruments, Replay Technologies, etc.) as well as fascinating new releases, such as Samsung brainBAND [13], to measure specific health aspects in mass sports events. As a result, wearable devices are already taking over the market with an increase in shipments of over 40% in 2016 as compared to the previous year, while the total shipments are expected to exceed 200 million units by 2019 [14]. While wearable technology clearly demonstrates much promise for novel exciting innovations, a lot remains to be studied and understood before the full potential of large-scale wearable ecosystems can be harnessed beyond individual user applications [15]. The key challenges to address relate to information management within the device ecosystem, as well as the user-centric security, privacy, and trust aspects therein [16]. The rapid adoption rate of the paradigmatically new wearable technology poses multiple novel challenges along the lines of its security and privacy [17]. The sheer diversity of the devices leads to increased dynamics and complexity in terms of user management of the access rights and accentuates the need for wireless 5G-grade connectivity within the user's "personal cloud" [18].

The breadth of the kinds of wearable devices available to an individual person is steadily increasing, which calls for new solutions for managing the "personal cloud" security [19]. The wearable devices of one user being in physical proximity to each other creates opportunities for establishing trusted networks between smart devices and building meta-level intelligent services based on multiple devices operated by different users [20]. Additionally, the constraints of wearables in terms of, for example, their battery life, connectivity range, and computation power increase the complexity of management as the user's personal ecosystem remains constantly in a state of change [21]. To date, these aspects of future wearables have remained largely unexplored from the end user perspective. As most security threats are difficult for a consumer to understand or even identify, and the users should be allowed to focus on their desired activities in the real world, it is unclear how the management of security and, for example, access to information in the personal cloud should occur [22]. In what follows, we provide a concrete example of what the ecosystem of intelligent wearables could look like and what kind of security and privacy challenges the aspects of proximity, dynamics, and constraints of wearables bring about in this vision.

Considering the use cases of wearables, much of the prior research has focused on facilitating automation, healthcare, and other applications with pragmatic business prospects [23] and a clear return-on-investment [24]. From the research viewpoint, such contexts can often be readily modeled and controlled, since the tasks as well as the contextual factors are often well-understood, whereas handling mass contexts remains challenging to predict due to their behavior. This can lead to solutions that function satisfactorily in a specific context but cannot be generalized or transferred to other contexts, like Augmented and Virtual Reality (AR/VR) cases [25].

In stark contrast, the focus of this paper is on highly dynamic and complex contexts related to mass consumer applications in the leisurely use of wearables [26,27]. This emerging area sets unprecedentedly high requirements to: (1) understand the privacy- and security-related threats; and (2) develop scalable connectivity solutions that are acceptable for mass consumer markets. Indeed, consumers are particularly interested in knowing that their communicated data are protected and privacy is maintained. As of today, the information security ecosystem for such a wide range of intelligent wearables has not yet been established.

1.2. Structure of This Manuscript

The structure of this work is as follows. The future of wearable devices in the context of a mass event is discussed in the next section. A survey on possible market-available and next-generation wireless technologies with respect to AR/VR limitations is offered in Section 3. Further, our developed simulation framework allowing for improvement of the connectivity planning and security assessment, including the focus on the use of higher communication frequencies (such as 60 GHz bands), is outlined in Section 4. The produced results based on ray-based pass loss modeling within the characteristic scenario of a hockey match are given in Section 5. Further, in Section 6 we propose an authentication framework that secures the mass content delivery in the target scenario, and conduct a brief security analysis of the framework. The last section concludes the manuscript.

2. Background and Motivation

2.1. Related Historical Overview

For years now, sports players have been wearing tracking devices in training, so that the coaches could see who is in adequate condition and who has been "burning the candle at both ends" [28]. So far, such devices have not been allowed during competitive play [29]. In football, the only wearable that is permitted as of today is the referee's watch that buzzes to let them know whenever a goal has been scored [30].

At the same time, hockey is one of the most dynamic global sports [31]. However, it still has not caught on to the technology boom that is changing the ways that teams track the progress of their players (like in football). The hockey teams are thus not yet producing the data to be processed and, therefore, the mass consumer cannot obtain them through the conventional channels (TVs, radio, etc.) nor with the next-generation AR/VR equipment. However, this may soon change as new wearable devices have been in the development process for a long time [32–34] and are currently being released into the market [35].

In the "2015 All Star game", the National Hockey League (NHL) placed tracking devices on the players' jerseys and inside the puck [36]. Putting technology on ice allowed coaches and players alike to focus on the game-play performance. Some teams are also considering various hockey stick add-ons that measure the power and the speed of slap shots, or the amplitude and execution speed of each swing [37]. With these advancements, it is not expected to be long until we see comprehensive tracking technology enter the NHL, providing the mass consumers with a completely new level of experience.

Technology has profoundly altered the way we do sports by capturing the attention of spectators for hours. With today's technology, we are now able to make grounded conclusions on the team's performance based on statistics made available to the audience through broadcasting [38]. Today, the data obtained from players, coaches, etc., are only available to a very limited circle of people. However, in the world of tomorrow, a hockey match spectator may enjoy a range of different services based e.g., on the type (level) of the purchased ticket, fan club membership, and/or the place on the tribune [39].

2.2. Market-Available Professional Products

Since wearable technology is becoming increasingly integrated into professional sports, various metrics can now be taken into account and utilized throughout training, thus allowing for real-time decisions to be made subsequently. Many known tech and clothing companies are attempting to bridge the gap between the state-of-the-art technology and the pace of the evolution. We hence list some of the professional wearable equipment already employed in sports training:

Adidas miCoach [40] is an ecosystem of connected wireless sensors with gear or apparel that is capable of quantifying athletic performance, including acceleration, speed, distance, power, heart rate, etc. After collection, all of the essential data are sent to the coach instantly, so that the performance of an individual could be monitored to make conclusions on potential concussions and injuries.

Viper Pod is a device widely utilized in the sports world by more than 10 globally-known teams, such as the football teams of Barcelona, Arsenal, and Manchester United, as well as the rugby team England National [41]. With a weight of under 50 g, this chest-mounted device is equipped with a Global Positioning System (GPS) module, accelerometer, gyroscope, digital compass, and heart rate monitor. The corresponding metrics are then transferred to other devices, thus enabling the coach to conduct real-time analysis depending on the team performance. Similarly to football, the National Hockey League (NHL) has embarked onto the Viper Pod with teams such as the Chicago Bulls, the Cincinnati Bengals, and the Carolina Panthers, all making use of this innovative technology.

Catapult OptimEye G5 is a piece of equipment suitable for goalkeepers [42]. The device in question allows the coach to track goalkeeper's movements together with a host of other statistics [43]. It is equipped with a set of sensitive accelerometers, a heart rate monitor, and a wireless module, thus providing close to real-time bio-mechanical and tactical analysis. The lifetime of the device is 5 h and the post-game analysis is also available as one of the features. The company also offers a variety of devices for the NHL, National Basketball Association (NBA), and National Collegiate Athletic Association (NCAA).

The E39 performance shirt by Armour is a high-tech T-shirt equipped with a removable computer that features a triaxial accelerometer, processor, and 2 GB of storage supplied with additional monitors to measure the wearer's heart rate and breathing [44].

ShotTracker is a basketball wearable consisting of the wrist and net sensors, which intends to improve the statistics of the players during the game [45]. This device was the first to be adopted by the basketball league with increasing intensity.

These are but a few of the professional sports wearables used by the leagues and the international teams across the globe. Some of the monitoring devices were also developed not for the public market but for the professional-targeted training, including the ones presented in [46–48]. The use of wearable technology is undeniably a major game-changer, while increased adoption of professional sports wearables during the games becomes another testament of this effective technology.

2.3. Proposed Model

Our envisioned service could be included with the initial game ticket and/or enabled by utilizing micro-transactions during the match itself. We further provide a non-exhaustive list of possible applications within this context:

- Obtaining video content made available by the proprietary sources (team players, opponents, referees, hockey gates, main cameras, etc.);
- Accessing general information related to the club (history, events, players, etc.);
- Monitoring critical information (warnings, evacuation plans, etc.);
- Advertisements and promotions (closest fast-food venue, order of a drink, taxi, etc.).

Complementing the above avenues of available monetization opportunities, the game organizers (owners of the stadium) may also acquire anonymized data related to the actual number of seats taken, distribution of spectators, amount of specific requests, and necessary feedback. The collected statistics could be utilized e.g., to improve the general levels of physical security as well as increase the effectiveness of future event planning. To this end, Figure 2 details our characteristic scenario depicting a wearable-enhanced **ice hockey** match, where we can differentiate between the following categories of participants (named here 'roles'):

- *Mass spectators* (purchased their personal ticket; have access to a personalized set of AR-based services; are main producers and consumers of data; have the possibility for on-demand content acquisition; engage into direct interactions);
- *Support personnel* (broadly includes technical, medical, maintenance, advertising, and other specialists with access to their specific and AR-based data; access detailed information on players/spectators);
- *Competing teams* (including players and coaches with data possibly affecting tactics and strategy of the team; the requirement of long-term protection against misuse of such more dynamic and context-oriented information).

Summarizing, the main target here is to benefit the following stakeholders: regular audience (spectators, fans, etc.), event venue (e.g., sports stadium), competing teams (coalitions) or their owners/sponsors, first responders and maintenance personnel, and other services (advertising companies, wearable equipment vendors, etc.).

The pragmatic example output that we assume when considering the ice hockey business setting is a *secure, wearable-aware data streaming system*. As players carry around multiple wearable devices and sensors, such as heart rate monitors, lung capacity, metabolism, and location monitors, collision sensors and cameras [49], this equipment streams relevant data, where more sensitive information is only delivered to the authorized nodes, while game-oriented data is made available to the mass public. Moreover, we may consider an "intelligent puck" system that tracks the puck location in the ring and communicates it to e.g., the ice hockey arena's public node.

The league organizing the games may have its own dedicated node and, depending on the agreement between the team and the league, the data might be aggregated and abstracted away before delivery by means of masking [50,51]. This can therefore fuel third-party services running on the spectator's smart display [52] (AR glasses or mobile on-demand TV screen). In this context, specific security demands arise for: (1) signatures to prove the origin and the authenticity of all data; (2) encryption for improved confidentiality while accessing the parts of data in transit; (3) randomized inspection protocols for data validity assessment; (4) restricted Application Programming Interfaces (APIs) to develop applications that perform computations over private data, where the application owner does not have the actual data but only the result; and (5) mechanisms to prevent from covert channels or to limit their bandwidth. The following section sheds light on the scenario-related security concerns.

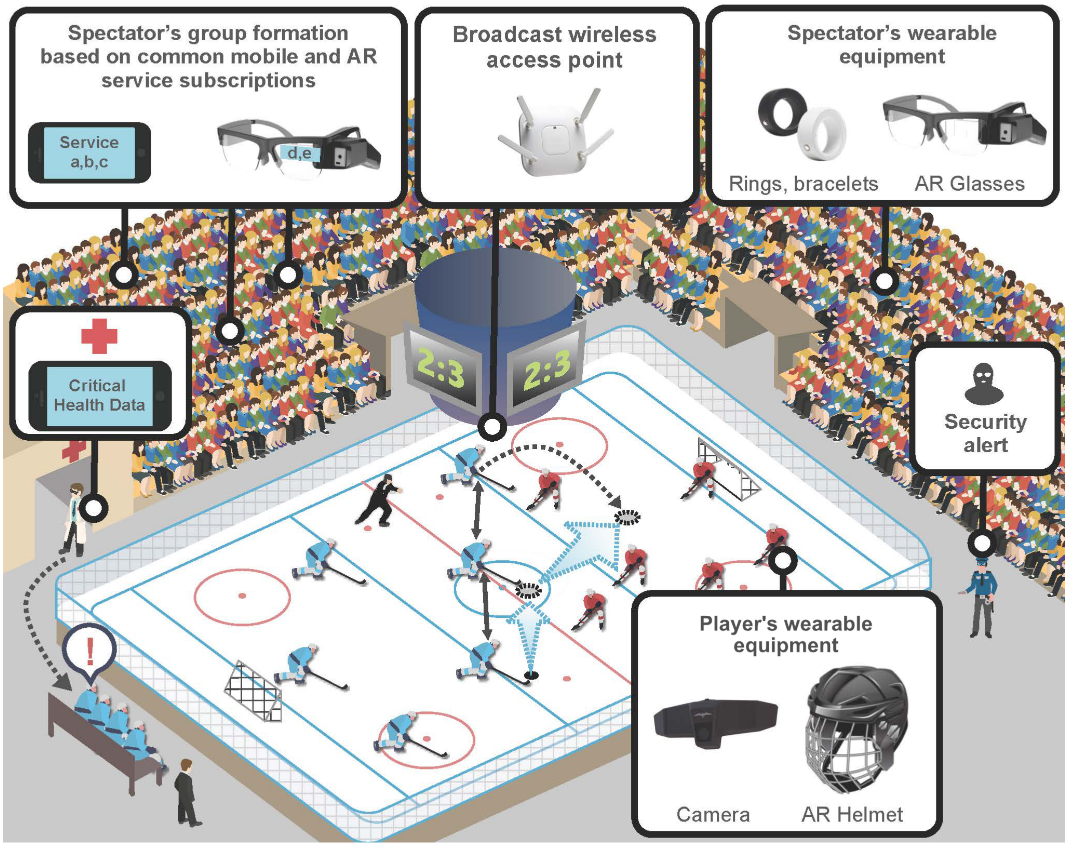

Spectator's group formation based on common mobile and AR service subscriptions
Service a,b,c
d,e
Broadcast wireless access point
Spectator's wearable equipment
Rings, bracelets
AR Glasses
Critical Health Data
2:3
2:3
Security alert
!
Player's wearable equipment
Camera
AR Helmet

Figure 2. Representative scenario: a wearable-enhanced ice hockey match. AR: Augmented Reality; VR: Virtual Reality.

3. Security Context in Public Events with Wearable Intelligence

In this section, we bring the reader's attention to the key dimensions that we argue as underpinning the most crucial challenges pertaining to the security aspects of wearable intelligence:

- The notion of close proximity between several wearable and carriable devices, which can be mobile;
- Higher dynamics of personal user environment, where the components in the user "personal cloud" depend on the situation and where particular devices may often (de-)associate in real time;
- Tighter constraints on the available processing capabilities and energy supply of contemporary wearables as a result of their reduced form-factor and functionality.

These dimensions comprise a solid foundation that allows for a rapid advancement toward next-generation wearable intelligence, which has to be made secure, privacy-friendly, and trustworthy.

3.1. Proximity

The rapidly diversifying ecosystem of wearable devices that reside geographically close to each other–either belonging to one or to several users–opens new opportunities for developing secure connectivity solutions based on physical proximity [53,54]. For example, in the aforementioned scenario, proximity-based networking can be used to form data dissemination channels that are only available at the mass event. Additionally, wearable technology could be utilized by other users as a neighboring resource: various sensors on a user's smart jacket could provide him/her with customized and personalized service, while they could also accommodate other people nearby (proximate users), possibly with limited quality of service.

However, there are critical challenges that are required to be resolved before these applications can truly take off. The utilization of proximity as a security feature is vulnerable to some extent against attackers using specialized equipment [55]. Attackers can also spoof their presence using sybil attacks, particularly if radio resources or other physical resources are not attested [56]. However, whenever proximity can be guaranteed through the use of distance-bounding protocols [57], it could also be utilized to set-up security sensitive boundaries. Furthermore, the possible social and collective use of "personal clouds" of the neighboring users broadens these challenges from an individual user's perspective to that involving several users.

3.2. Dynamics

This dimension relates to unpredictable mobility of human users in real time as well as the highly-dynamic composition of their respective personal networks even though the actual movement could generally be tracked [58]. The research field is suffering from a significant lack of activities in the area of dynamic privacy and trust management. Earlier research focused on industrial solutions for hospitals [59] or controlled body-area networks (BANs) [60], where devices are assumed to always have stable connectivity to the control unit. Many new challenges arise in light of mobility, where privacy of the device location is one of the important requirements [61].

Besides the issues in defining initial trust anchors, trust relationships evolve continuously [62]. Hence, trust management could become a burden for the end-user equipment unless these tasks can be largely automated through the use of authorization protocols. Changes in device management transform physical device ownership more toward a responsibility and a liability, rather than absolute control over the device. This means that an understandable security model is needed for distributed management functions, in order to, for example, maintain dynamic user privacy. Furthermore, trust decisions of humans as well as relations between physical devices and their hosts have to be supported in verifiable ways. This requires identity management frameworks that support identities beyond these of only users and wearable devices (e.g., virtualization and sandboxing).

3.3. Constraints

Limitations of small form-factor and battery-powered wearable devices constitute one more, "internal" dimension, which imposes constrains on the respective complexity of cryptographic protocols suitable for next-generation wearables [63]. First, constraints in the device's user interfaces create challenges for the provisioning of the devices and communicating the security status together with the current trust relationships. In addition to verifying the configuration of wearable devices, detection of potentially malicious applications and actors in the "personal cloud" environment needs to be supported. Second, the coordination takes place on the lower levels of hardware. Hence, the real challenge is how to coordinate the actual hardware resources of each platform.

Developers require new programming frameworks and open-source platforms that help "get the most out of" hardware. Moreover, the corresponding security procedures are not standardized for the connectivity between the device and the gateway, and should be studied in more detail [64]. Further, the challenges of authenticating and authorizing wearable devices become pronounced, as their average densities around a user grow. Mutual authentication of wearables becomes therefore a glaring problem, including the risk of mismatch (accidental or premeditated). Finally, most of the wearables of today are optimized based on their energy consumption [65]. To this end, utilizing the conventional RSA-like information security solutions may be unacceptable for battery-constrained devices and thus new lightweight primitives should be proposed and developed.

4. Implementation of the Target Scenario

This section details the mass sports event within our selected target scenario, together with the delivery method (AR/VR) application requirements, potential wireless solutions, and the corresponding setup implementation. We have chosen the 20,000-seat hockey stadium as our reference design case. As with any high-density venue, specific deployments may have slightly different requirements. However, the principles outlined here are generally applicable for the venue of any size. The application type is mainly downlink data (video) streaming to the mass consumers. The goodput of the studied wireless technologies is not considered in this manuscript due to the static broadcast-like behavior. We base our research on the assumptions adopted from the industrial works by Ericsson [66,67]. Our custom simulator utilized in this work was previously calibrated with the real-life measurements in [68].

4.1. General Application Requirements

First, consider the data delivery though the smart glasses or portable televisions, where AR adds (computer-generated) supplemental elements to the user's viewpoint, whereas solid VR recreates the entire scene that the user sees based on multiple sensory sources (e.g., cameras and other sensors). Both technologies operate in real time, and the main requirements of these applications are throughput (up to 1.5 Gbps total or 6 Mbps per stream), latency that ranges from the sub-millisecond level to tens of milliseconds, and jitter of below 1 ms [69]. Importantly, in our scenario the challenges of mobility are not discussed due to nearly static behavior of spectators. The application range is limited by the dimensions of the arena. Power consumption requirements do not appear to be a major issue, since the deployment scenarios allow the equipment to be either powered or recharged in a timely manner due to the limited duration of the event.

One of the major issues in our scenario is, however, scalability [21]. Both capturing and viewing equipment are deployed at high density, and the actual numbers will depend on the complexity of the scene e.g., the size of population as well as the numbers of cameras/sensors in order to acquire/transmit all aspects of the match. At the same time, recent academic activity demonstrates that the actual user density within the stadium scenario is 200,000 users/km^2 on average [70]. In this work, we solve the scalability challenge by applying a solution from the field of information security, which allows for dynamic and secure content delivery. The proposed technique is discussed in the latter part of this manuscript.

The following subsection overviews the potential solutions that satisfy the requirements of the mass content delivery scenario.

4.2. Candidate Connectivity Solutions

Today, communications technology researchers and vendors are competing to fulfill the requirements of efficiency, flexibility, and simplicity of coexistence [71]. This subsection briefly surveys a number of widely adopted wireless protocols that are suitable for the utilization in cases of a highly dense environment.

We first focus on the market-available solutions that satisfy the above listed requirements. The most adopted and widespread technology is represented by Institute of Electrical and Electronics Engineers (IEEE) 802.11 protocols, or WiFi. As a prominent example, IEEE 802.11ac-based devices are offering high data rates acceptable for the AR connectivity of today. A conventional WiFi medium access protocol (MAC) was designed to efficiently support up to around 25 nodes communicating their bursty content simultaneously, due to its characteristic operation based on the random channel access i.e., the binary exponential backoff (BEB) protocol. Ultimately, it can offer up to 90% of spectral efficiency for as many as 5–10 devices [72]. In the scope of this research, conventional operation of WiFi does not fulfill the requirement of a high number of nodes from the efficiency or from the interference points of view [73].

Since we focus primarily on the AR/VR as a demanding wearable-based application, one of the key performance requirements is to provide at least tens of Mbps per client. Hence, Bluetooth (up to 20 Mbps, 15 m, and 8 clients per host) and WiFi technologies (up to 400 Mbps for IEEE 802.11ac, 50 m, and 15 clients per host), which are currently deployed on most consumer devices, need to scale by several orders of magnitude. As one of the possible market-ready options, a solution by Wireless Gigabit Alliance (WiGig) may be utilized to employ the specifics of millimeter-wave (mmWave) communications [74].

Practically, conventional radio technologies that serve up to 25 demanding devices have a considerable probability of receiving low quality of service (QoS) levels, while doubling this number may degrade the performance altogether. The reasoning behind this is that WiFi has been designed for private indoor use, where the number of served users per access point varies below 10. Any increase in this number would dramatically impact the collision probability. However, the standards do not specify the exact BEB parameters and such a setup is left entirely at the discretion of vendors, which may cause faulty operation of the devices. Similar situations could be observed for the upcoming generation of short-range wireless technologies [75].

The second group of connectivity solutions considered here can be referred to as "the next generation". Today, a large portion of wireless research and development is targeting the use of extremely high frequency bands in the range of 60 GHz. A brief overview of such technologies is given below.

The first considered solution was presented in 2008 and named Wireless HD [76]. Its target utilization is in home theaters and media centers. The main feature brought along by this standard is the use of both random and scheduled channel access, where one controller has a complete picture of the served nodes in its coverage. The main issue here is the lack of knowledge between the neighboring networks, which brings challenges of uncontrollable interference and hidden node problems [77] that primarily affect scheduled transmissions.

The second step made by the wireless industry is IEEE 802.11ad standard, widely known as WiGig [78]. The main requirement here is to enable the throughputs of at least 1 Gbps on top of the MAC layer. It offers a number of flexible protocol solutions, especially for low-cost devices. The scheduling is implemented similarly to that in Wireless HD, thus bringing along the same interference and management issues–the number of possible networks that may coexist in space and time is four. Another solution is ECMA 387 [79], which provides mobility support by dynamically resolving the cross-cloud collisions with a novel approach: soft channel switch and coordination. Basically, whenever a collision is detected, the communication channel is switched, hence reducing the subsequent collision probability. If there are no free channels left to utilize, the beaconing time is reassigned by keeping the networks operational, so that the beacons of neighboring clusters would be transmitted one after another. Unfortunately, there are no vendors supporting this standard as of today.

Summarizing, we can conclude that the best practical option to be utilized today is WiGig technology due to its desirable properties and market support. The general challenge here is radio propagation due to the inability of 60 GHz wireless signals to penetrate almost any material at such high frequencies. On the other hand, this construction allows to assume that the receivers are mounted as part of the AR/VR heads-on devices [80] and thus the line-of-sight communication is delivered. An inherent feature of the 60-GHz solution is to adopt beam-forming that increases e.g., the levels of security while delivering the user-specific content at high rates. Further in Section 5, we compare the results of its utilization with the conventional IEEE 802.11n and .11ac operation.

4.3. Scenario Details and Simulation Description

To study wireless propagation in our characteristic scenario, we consider a 3D stadium grid presented in Figure 3a. A large number of receiving nodes (RXs) are located on the tribunes according to the mass user positions. This considered layout is common for any large sports event [81]. In this work, we first assess the conventional WiFi-like solutions provided, for example, by Cisco and then extend the evaluation to embrace the next-generation mmWave technology. The geometrical parameters of the scenario in question are summarized in Table 1.

Table 1. Geometrical properties of the scenario.

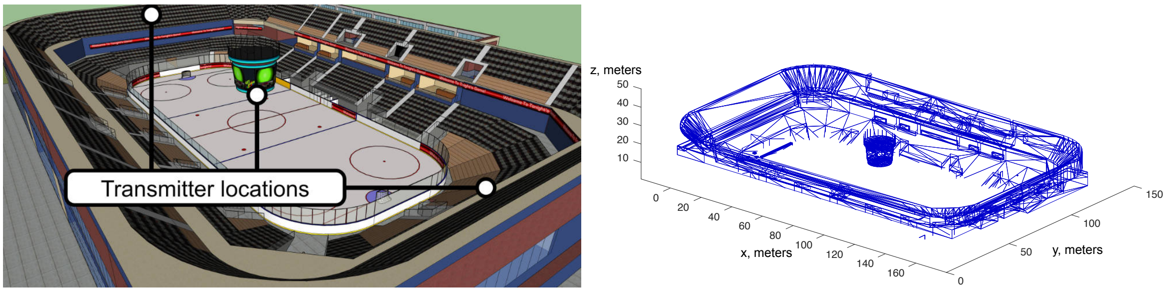
Parameter	Value
Overall scenario size	200 m × 160 m
Scenario height	40 m
Ice ring size	61 m × 37 m
Number of receivers	515
Number of transmitters	1–3

The site-specific deterministic Ray-Launcher (RL) tool was utilized in this work, which models the multi-path propagation of a wavefront within the wireless medium [82]. This principle is implemented in the geometrical engine of the RL tool, which is based on the ray-casting methods, where the continuous wavefront is replaced with the discrete one. Multiple 3D rays (or beams) outgoing from the transmitting (TX) node propagate to the RX through the line-of-sight links and on the reflected paths. At the same time, the physical engine of the RL tool is based on the geometrical optics (GO) and the uniform theory of diffraction (UTD) techniques [83].

In this work, we concentrate on a first-order evaluation and thus disregard the relatively small objects due to several reasons. First, simulation of a highly detailed scenario requires powerful computing resources and significant computation time. Second, diffuse scattering produced by the objects that are electrically small with respect to the wavelength does not offer a considerable impact in terms of power. Based on that, only bulky and electrically large objects feature in our 3D reconstruction of the stadium, which are presented in Figure 3. Here, Figure 3a is an original model with the high level of details, while Figure 3b is a preprocessed and simplified model acceptable for the purposes of our intended evaluation. The 3D simplification utilized in our work is to reduce the number of vertices on a mesh by lowering the maximum angle to 15°.

Further, the RXs are carefully positioned to cover the entire area of interest. As the RXs are located around the hockey arena, an empirical consideration to place the TX below the tableau was applied. We then assumed that the TX and the wearable devices (i.e., RXs) of the spectators are vertically polarized, that is, the polarization mismatch is insufficient. To avoid additional complexity at the MAC-layer, an isotropic radiator was selected as the reference antenna design for both the TX and RX, which has a uniform gain in the spherical coordinate system. Thereby, each RX observes the signal combined by summing up different rays that propagate on the various paths and with different power levels.

In this paper, we study three representative broadcast scenarios: (1) one TX placed in the middle of the stadium below the tableau; (2) two TXs on the opposite sides of the stadium; and (3) a combined scenario with all three TXs, whereas the locations are marked in Figure 3a.



(a) Three-dimensional original

(b) Preprocessed representation

Figure 3. Model utilized for calculation.

4.4. Key Performance Metrics

In this study, we evaluate to what extent the utilization of different wireless technologies could support the broadcast data delivery during a mass event (e.g., a hockey match). More specifically, we focus on the coverage optimization target [84]; hence, our main metric of interest is the path loss (PL). It can be obtained as follows:

$$PL = P_{TX} - P_{RX}, \tag{1}$$

where P_{TX} is the radiated power from the TX and P_{RX} is the total received power at the RX.

In this work, each of the RXs collects its own portion of power after multi-path radio propagation. Taking into account the carrier frequency, which leads to the corresponding attenuation per distance, each P_{RX} must be different at 2.4 GHz, 5 GHz, and 60 GHz.

5. Selected Numerical Results

Evaluating the most widely utilized radio technologies that operate in unlicensed spectrum (IEEE 802.11n at 2.4 GHz and IEEE 802.11ac at 5 GHz bands), we also address the benefits brought along by the potential use of mmWave communications technology (IEEE 802.11ad or WiGig at 60 GHz). We emphasize that both the RXs and TXs have zero antenna gains. The calculation error at the RX side is within the -3dB range, while the calculation time for our model with 8000 faces takes approximately 4 h with 1 GB RAM. The resulting PL maps are collected in Figure 4.

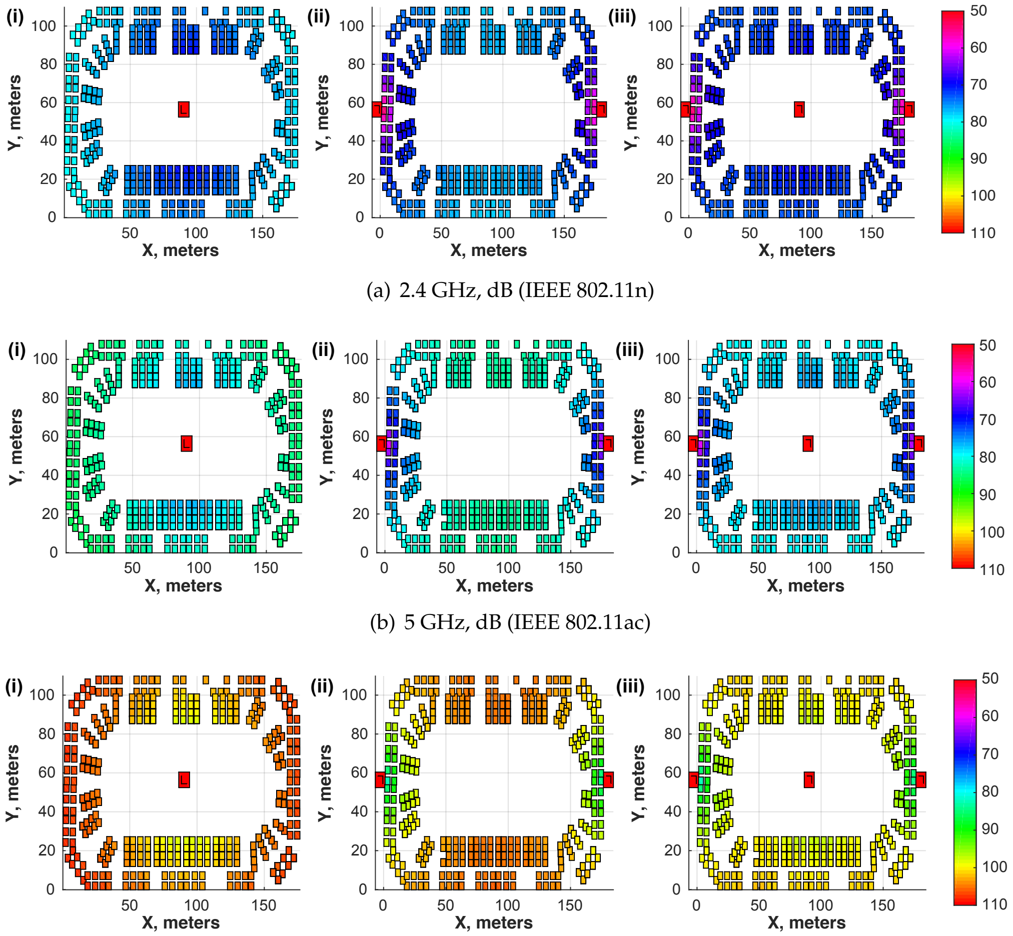
In order to validate our simulation results, we also compared these with the free-space PL model at each frequency:

$$FSPL = 20log_{10}(d) + 20log_{10}(f) + 20log_{10}\left(\frac{4\pi}{c}\right) - G_t - G_r, \tag{2}$$

where d is the average distance from the TX to RX, f is the frequency, c is the speed of light, and G_t, G_r are the RX and TX gains that are set to 0, respectively. All of the simulation data fell within the acceptable bounds of $+/-5\%$ compared to the analytical results across the three scenarios of interest. Reporting on the results of our evaluation in Figure 4, we provide the average theoretical Signal-to-Noise Ratio (SNR) values for all the scenarios: (a) for 2.4 GHz this is 72.0854 dB; (b) for 5 GHz this is 78.4606 dB; and (c) for 60 GHz this is 100.0442 dB. It could be observed in the color map of the plots that the theoretical values fit well within the bounds of the simulated results. The main thinking behind the utilization of the RL techniques for our study is the fact that the pseudo-random paths of rays would provide similar picture independently of the frequency. However, the received power figure should vary based on the TX, as can be seen in the plots, for example, by considering a set of Figure 4a. This allows us to utilize our custom framework for the analysis of different scenarios by consuming less time and fewer computation resources.

Importantly, from the information security perspective, these obtained results offer useful functionality by aiming to avoid a number of threats. We further list some of the applications to be considered during the mass event at the network planning phase:

- The PL map allows for predicting the levels of transmit power required for the path-based denial-of-service attacks, such as jamming [85]. By doing so, the detection of potential malicious activity becomes more straightforward.
- The users with the lowest RX power are also vulnerable to the distributed denial-of-service attack. The PL value allows for deriving a lower bound on the throughput, which can compromise such (edge) nodes [86].
- Even though general mobility levels in this mass system are considered to remain low, the PL map allows for addressing the moments of a possible handover between the access points, thus outlining the risk zone of rogue access points [87].



(a) 2.4 GHz, dB (IEEE 802.11n)

(b) 5 GHz, dB (IEEE 802.11ac)

(c) 60 GHz, dB (IEEE 802.11ad)

Figure 4. Receiving node (RX) path loss for the selected technologies: (1) Transmitting node (TX) placed in the middle; (2) Two TXs on the opposite sides; (3) Three TXs: one in the middle, and two on the opposite sides.

In summary, the utilized RL technique may be employed at the network planning phase, thus allowing for not only solving the conventional scenario-related connectivity challenges but also understanding the security issues pertaining to it.

6. Authentication Methods for Massive Content Delivery

In the previous section, we modeled the broadcast system operation suitable for content delivery at a mass event of a hockey match e.g., when the spectators are willing to access information encoded as the broadcast data stream. Typically, users attending such an event segregate not only based on the teams that they follow, but also subject to the ticket price, which directly transforms into the event observation quality, that is, better experience at higher price. Based on this fact, we further propose an authentication mechanism that may be utilized to offer the next-generation services that incorporate the AR/VR content delivery based on the subscription, which could be resolved with a dynamic authentication mechanism.

Generally, authentication protocols may be classified into three main groups [88]: (1) based on symmetric cryptosystems; (2) based on asymmetric cryptosystems; and (3) hybrid. The majority of those utilize hash functions as their basis, thus allowing to combine the secret information "shares" into one specific secret key. As the most trivial and well-known example, we may recall the exclusive disjunction (XOR) function that makes it possible to group a set of identifiers ID_i:

$$ID = ID_1 \oplus ID_2 \oplus \cdots \oplus ID_n. \tag{3}$$

The possible utilization of the public key infrastructure (PKI) is an example of applying the asymmetric cryptosystems [89]. It allows for implementation of flexible authentication frameworks suitable for serving higher numbers of active users with a variety of access control mechanisms and features.

For our target scenario, the first requirement of the appropriate authentication protocol is to consider a set of simultaneously available secret shares i.e., unique identifiers that depend on the seat number, ticket number, etc. The second important requirement is the association of the secret/public keys with each specific content-consuming user that could thus be verified. The simultaneous provision of the set of required shares within a specified time interval is a solution to prevent reuse of the same identifiers by different users. One of the well-known solutions that enables such a functionality is the hybrid Yoking–Proof protocol [90,91]. Our proposed example is given in what follows.

6.1. Proposed Authentication Method for the Mass Event

We propose an adequate technological solution based on the stadium equipment availability: (1) both seats and tickets are supplied with the radio-frequency identification (RFID) tags [92]; (2) the spectator has a smartphone equipped with the near field communication (NFC) technology. The required identification data are obtained based on the simultaneous verification of both the ticket and the seat by utilizing the broadband access deployed at the stadium.

In order to provide with the needed functionality, the following requirements are to be satisfied: (1) each seat is numbered (equipped with a one-time sticker containing its unique identifier), all of the tickets have the corresponding unique identifier; and (2) each spectator has a smartphone. In this simple setup, the authentication code may be delivered through a trusted cellular network via the SMS code.

By doing so, the company responsible for the event in question has an opportunity to obtain the following information from each attendee: (1) the seat identifier ($ID(s)_k$); (2) the main ticket identifier ($ID(t)_i$); and (3) an additional subscription identifier ($ID(a)_j$). The level of service (S_i) provided to the ith user could thus be estimated based on the received information. The system would need to provide a unique result of the hashing function:

$$h = H(ID(s)_k||ID(t)_i||ID(a)_j||...||ID(a)_m||A_c), \tag{4}$$

where k, i, j are the counters for different components, m is the maximum value for the counter j, and A_c is the authentication code. The result is further signed with the unique user's (ID_i) secret key (SK_i) as:

$$s_v = sign(h_z, SK_i), \tag{5}$$

where h is obtained by the Equation (4) corresponding to zth result of the function, and SK_i is a unique user's secret key.

Therefore, each vth subscription level acquires the corresponding unique pair of the secret SK_i and the public PK_i keys. Hence, each user has an anonymized (from the third-party perspective) *ticket*,

$$t_i = (i||h_z||s_v), \tag{6}$$

where h_z is produced by the Equation (4) and s_v is given by the Equation (5).

Based on the above, each ticket is composed of a unique sequence including the specific seat, the level of service provided, and the signature that allows to validate the previous fields based on the public key stored in the service provider cloud. The event-organizing company is assumed to act as a trusted certificate authority. In our scenario, there may be two cases of interest:

- The organizer provides its services to the customers in an anonymized way. To achieve anonymity in relation to the service provider (stadium administration), the following addition to the authentication protocol could be utilized:
  - Conventional PKI authentication and integrity protocols need to be replaced with ID-based formulations [93,94];
  - Certificate authority in the modified scheme is represented by the private key generator (PKG);
  - The secret key SK_i is not directly "connected" to a unique user ID_i, but rather links with the ticket number and/or the seat number, and the event parameters (name, date, time, etc.). The SK_i is to be obtained by the PKG with the use of any ID-based key generation protocol.
- At the signature verification stage s_v, the event-organizing company requires only the ticket number and the event parameters. Therefore, it is not necessary for a user to provide any personal information (for realizing the verification procedure) directly to the event organizers. However, the authority may still obtain these data if necessary.
- In cases of, for example, Public Protection and Disaster Relief (PPDR) [95] or mass riots during the event, the administration has an opportunity to acquire the data on each user and forward it to the dedicated security units.

6.2. Framework Security Analysis

The main challenge behind the proposed solution lies in the very structure of the Yoking–Proof protocol and is related to the timeouts [96]. Generally, during simultaneous verification, the main device utilizes a preset timer to enable the said check. This is mainly due to the inability of scanning two or more sources at the exact same time. Therefore, a threshold value is defined and an attack could be executed if it provides, for example, a too-long validation interval not related to the actual source reading times.

Further, we briefly elaborate on the security analysis of the proposed solution. In our framework, security is based on the RSA assumptions, similarly to [97]. It utilizes primitive arithmetic operations at the user equipment (UE) side, such as the *Add* function, *XOR* operation, random number generator, and hash function. Therefore, the container data can be *XOR*-ed with the random values to prevent private data leakage.

Tag anonymity in the proposed solution is not considered by this work, since the tags are distributed across a publicly available area and thus could be temporarily accessed by an eavesdropping user. The IDs are accessible in plaintext and each of them is associated with the corresponding secret key on the owner's side to perform meaningful computation. Note that the plain IDs can be eavesdropped but the security robustness of the meaningful data in the transmitted messages will not be compromised, and thus confidentiality can be guaranteed [98].

Another important issue to solve for the Yoking–Proof protocol is a replay attack [99]. At the stage of querying the smartphone tags, each of them responds with its corresponding message. An attacker can eavesdrop on the transmitted information over an insecure channel and store the messages locally. Next, the attacker may utilize the intercepted messages to complete the reader's authentication. One of the solutions to overcome this threat is to utilize timestamps [100] and/or pseudo-random numbers [101] along with every communicated message, in exchange for additional space and connectivity requirements. Generally, this makes the replay attack more cumbersome for the attackers.

Another attack to be considered is the so-called *counterfeit-proof attack* [102]. Similarly to the method used against the replay attack, a timeout mechanism may be utilized to ensure that all of the proof-involved tags coexist for a specific and limited time period.

Finally, the notorious person-in-the-middle attack may also take place [103]. Here, an attacker can eavesdrop on the messages transmitted between the tag and the smartphone, and then modify the information to counterfeit a legitimate role. This challenge is solved by utilizing secure cellular assistance mechanisms by means of an extra *SMS verification code*, which solves most of the pressing authentication issues. To this end, the operation of our proposed protocol primarily relies on the assumption of a secure cellular channel. Since security-centric analysis is not the main goal of this paper, the proposed protocol may require a deeper evaluation and testing in field scenarios.

7. Conclusions

Today, the rapidly expanding deployments of wearable technology as well as the rise of smart cities are underpinning new opportunities for wearable paradigm adoption. While there have been multiple attempts to deploy different IoT systems, our understanding of those and the corresponding implications in the context of safety and security have only scratched the surface, especially in wearable scenarios.

Particularly, we surveyed wireless technologies suitable for wearable-equipped consumers with the emphasis on the AR/VR applications as well as the corresponding security challenges in case of a mass sports event (e.g., a hockey match). Then, we utilized our developed ray-based simulator employing the ray-launching principles to study some of those technologies at various frequencies to conclude that WiGig (a 60-GHz solution) is the most appropriate choice for the broadcast content delivery in terms of its achieved path loss. We also elaborated on how the utilization of our study may improve security within the target scenario at the network planning phase. The proposed tool could be further utilized for both indoor and outdoor radio network planning.

Further, we also proposed an authentication technique based on the Yoking–Proof protocol that allows for secure content dissemination in the presence of simultaneous access to multiple unique identifiers, such as the ticket, seat, SMS, etc., therefore enabling a secure ecosystem within our representative scenario of interest.

The ultimate goal of this work is not to answer all of the pressing questions, but rather to bring the community's attention to the challenges of mass wearable scenarios. The state-of-the-art in wearables is just at the beginning of a long journey, but there is already a lot to consider before making the next step.

Acknowledgments: The described research was partially supported by the Foundation for Assistance to Small Innovative Enterprises (FASIE) within the program "UMNIK" under grant 8268GU2015 (02.12.2015).

Author Contributions: A.O., D.S., and S.B. conceived and designed the experiments; A.O. and D.S. performed the experiments; A.S. and D.S. analyzed the data; T.O., S.B., S.A., J.H., and Y.K. contributed analysis tools; A.O., D.S., T.O., S.B., and A.S. wrote the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Barfield, W. *Fundamentals of Wearable Computers and Augmented Reality*; CRC Press: Boca Raton, FL, USA, 2015; ISBN 9781138749313.
2. Billinghurst, M.; Busse, D. Rapid Prototyping for Wearables: Concept Design and Development for head-and wrist-mounted Wearables (Smart Watches and Google Glass). In Proceedings of the 9th International Conference on Tangible, Embedded, and Embodied Interaction, Stanford, CA, USA, 16–19 January 2015; ACM: New York, NY, USA, 2015; pp. 505–508.
3. Xu, C.; Zhao, F.; Guan, J.; Zhang, H.; Muntean, G.M. QoE-driven user-centric VoD services in urban multihomed P2P-based vehicular networks. *IEEE Trans. Veh. Technol.* **2013**, *62*, 2273–2289.
4. Chaouchi, H.; Laurent-Maknavicius, M. *Wireless and Mobile Networks Security*; John Wiley & Sons: Hoboken, NJ, USA, 2013; ISBN 9780470611883; doi:10.1002/9780470611883.
5. Malina, L.; Hajny, J.; Fujdiak, R.; Hosek, J. On perspective of security and privacy-preserving solutions in the Internet of Things. *Comput. Netw.* **2016**, *102*, 83–95.
6. Wearable.com. Wearables Are Only Secure until They Become Worthwhile Hacking. Available online: http://www.wareable.com/wearable-tech/ (accessed on 15 May 2017).
7. Wearable Technologies. On Perspective of Security and Privacy-Preserving Solutions in the Internet of Things. Available online: https://www.wearable-technologies.com/2016/06/the-new-wave-of-wearables-is-transforming-the-world-of-soccer/ (accessed on 15 May 2017).

8. Case, M.A.; Burwick, H.A.; Volpp, K.G.; Patel, M.S. Accuracy of smartphone applications and wearable devices for tracking physical activity data. *JAMA* **2015**, *313*, 625–626, doi:10.1001/jama.2014.17841.
9. Motorola, Connected Law Enforcement Officer. Available online: https://www.motorolasolutions.com/en_us/solutions/law-enforcement/connected-law-enforcement-officer.html (accessed on 15 May 2017).
10. Arbia, D.B.; Alam, M.M.; Attia, R.; Hamida, E.B. Behavior of wireless body-to-body networks routing strategies for public protection and disaster relief. In Proceedings of the 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, UAE, 19–21 October 2015; pp. 117–124.
11. Chaouchi, H. *The Internet of Things: Connecting Objects*; John Wiley & Sons: Hoboken, NJ, USA, 2013; ISBN 9781118600146; doi:10.1002/9781118600146.
12. LifeHack. 10 Ways that Wearable Technology Can Positively Change the World. Available online: http://www.lifehack.org/509376/preventing-unwanted-intrusions-your-mobile-devices (accessed on 13 April 2017).
13. Samsung Newsroom. Samsung Australia Introduces brainBAND to Help Tackle Concussion Head on. Available online: https://news.samsung.com/global/samsung-australia-introduces-brainband-to-help-tackle-concussion-head-on (accessed on 15 May 2017).
14. IDC Research. IDC Forecasts Worldwide Shipments of Wearables to Surpass 200 Million in 2019, Driven by Strong Smartwatch Growth. Available online: https://www.idc.com/getdoc.jsp?containerId=prUS40846515 (accessed on 15 May 2017).
15. Castellet, A. What If Devices Take Command: Content Innovation Perspectives for Smart Wearables in the Mobile Ecosystem. *Int. J. Handheld Comput. Res. (IJHCR)* **2016**, *7*, 16–33, doi:10.4018/IJHCR.2016040102.
16. Zhou, J.; Cao, Z.; Dong, X.; Lin, X. Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions. *IEEE Wirel. Commun.* **2015**, *22*, 136–144, doi:10.1109/MWC.2015.7096296.
17. Alam, M.M.; Hamida, E.B. Surveying wearable human assistive technology for life and safety critical applications: Standards, challenges and opportunities. *Sensors* **2014**, *14*, 9153–9209, doi:10.3390/s140509153.
18. Hasan, R.; Khan, R. A Cloud You Can Wear: Towards a Mobile and Wearable Personal Cloud. In Proceedings of the 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 10–14 June 2016; Volume 1, pp. 823–828.
19. Small Business Trends. Can Wearable Technology Threaten the Cyber Security of Your Business? Available online: https://www.idc.com/getdoc.jsp?containerId=prUS40846515 (accessed on 15 May 2017).
20. Ometov, A.; Orsino, A.; Militano, L.; Araniti, G.; Moltchanov, D.; Andreev, S. A novel security-centric framework for D2D connectivity based on spatial and social proximity. *Comput. Netw.* **2016**, *107*, 327–338, doi:10.1016/j.comnet.2016.03.013.
21. Galinina, O.; Pyattaev, A.; Johnsson, K.; Turlikov, A.; Andreev, S.; Koucheryavy, Y. Assessing system-level energy efficiency of mmwave-based wearable networks. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 923–937, doi:10.1109/JSAC.2016.2544539.
22. Kerr, D.; Butler-Henderson, K.; Sahama, T. Security, Privacy, and Ownership Issues with the Use of Wearable Health Technologies. In *Managing Security Issues and the Hidden Dangers of Wearable Technologies*; IGI Global: Hershey, PA, USA, 2016; p. 161, doi:10.4018/978-1-5225-1016-1.ch007.
23. Islam, S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The Internet of Things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708, doi:10.1109/ACCESS.2015.2437951.
24. Levine, J.A. The Baetylus Theorem—The central disconnect driving consumer behavior and investment returns in Wearable Technologies. *Technol. Invest.* **2016**, *7*, 59, doi:10.4236/ti.2016.73008.
25. Simsek, M.; Aijaz, A.; Dohler, M.; Sachs, J.; Fettweis, G. 5G-enabled tactile internet. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 460–473, doi:10.1109/JSAC.2016.2525398.
26. Moor Insights & Strategy. Wearables Have a Long Way to Go to Be Mass Consumer Markets. Available online: http://www.moorinsightsstrategy.com/wearables-have-a-long-way-to-go-to-be-mass-consumer-markets/ (accessed on 15 May 2017).
27. Schneegass, S.; Olsson, T.; Mayer, S.; van Laerhoven, K. Mobile Interactions Augmented by Wearable Computing: A Design Space and Vision. *Int. J. of Mob. Hum. Comput. Interact. (IJMHCI)* **2016**, *8*, 104–114, doi:10.4018/IJMHCI.2016100106.

28. Wearable.com. From Pigeons to Pebbles: How Wearable Tech Has Evolved over the Centuries. Available online: http://www.moorinsightsstrategy.com/wearables-have-a-long-way-to-go-to-be-mass-consumer-markets/ (accessed on 15 May 2017).
29. Gastin, P.B.; McLean, O.; Spittle, M.; Breed, R.V. Quantification of tackling demands in professional Australian football using integrated wearable athlete tracking technology. *J. Sci. Med. Sport* **2013**, *16*, 589–593, doi:10.1016/j.jsams.2013.01.007.
30. Coutts, A.J. Evolution of football match analysis research. *J. Sports Sci.* **2014**, *32*, 1829–1830, doi:10.1080/02640414.2014.985450.
31. Alhonsuo, M.; Hapuli, J.; Virtanen, L.; Colley, A.; Häkkilä, J. Concepting wearables for ice-hockey youth. In Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct, Copenhagen, Denmark, 24–27 August 2015; ACM: New York, NY, USA; 2015, pp. 944–946.
32. Honey, S.K.; Cavallaro, R.H.; Hill, D.B.; Heinzmann, F.J.; Phillips, A.C.; Guthart, H.; Burns, A.A.; Rino, C.L.; Evans, P.C. Electromagnetic Transmitting Hockey Puck. U.S. Patent 5,564,698, 15 October 1996.
33. Lerer, S.J.; Tieniber, E.B.; Smith, J.M. *Building a Wireless Ice Hockey Personnel Management System*; Senior Design Project: Philadelphia, PA, USA; 2010.
34. Cavallaro, R. The FoxTrax hockey puck tracking system. *IEEE Comput. Graph. Appl.* **1997**, *17*, 6–12, doi:10.1109/38.574652.
35. Wearable Technologies Magazine. Wearables for Icehockey. Available online: https://www.wearable-technologies.com/2016/09/wearables-for-icehockey/ (accessed on 15 May 2017).
36. NHL, Player, Puck Tracking Coming to World Cup. Available online: https://www.nhl.com/news/nhl-to-use-player-puck-tracking-at-world-cup/c-281359780/ (accessed on 15 May 2017).
37. FWD. The World's First Advanced Sensor for Hockey sticks. Available online: http://www.quattriuum.com/en/powershot (accessed on 15 May 2017).
38. Huffpost. Wearing to Win: Wearable Technology in Sport. Available online: http://www.huffingtonpost.com/advertising-week/wearing-to-win-wearable-t_b_12455882.html (accessed on 15 May 2017).
39. Engadget. How Fox Sports Is Bringing Augmented Reality to NFL Games. Available online: https://www.engadget.com/2016/09/26/how-fox-sports-is-bringing-augmented-reality-to-nfl-games/ (accessed on 15 May 2017).
40. Adidas. Let's Get Fit in a Smart Way. Available online: http://www.micoach.com/start (accessed on 15 May 2017).
41. Statsports. Delighted to Work with 10 International Clients at EURO 2016. Available online: http://statsports.com (accessed on 15 May 2017).
42. PerformBetter. Catapult OptimEye G5 Goalkeeper Monitoring System. Available online: http://performbetter.co.uk/product/catapult-optimeye-g5-goalkeeper-monitoring-system/ (accessed on 15 May 2017).
43. Gastin, P.B.; Mclean, O.C.; Breed, R.V.; Spittle, M. Tackle and impact detection in elite Australian football using wearable microsensor technology. *J. Sports Sci.* **2014**, *32*, 947–953, doi:10.1080/02640414.2013.868920.
44. Ecouterre. Under Armour's Biometric Compression Shirt. Available online: http://www.ecouterre.com/under-armours-biometric-compression-shirt-tracks-broadcasts-athletic-performance-video/zephyr-under-armour-e39-shirt-2/ (accessed on 15 May 2017).
45. ShotTracker. Unleash Your Game. Available online: http://shottracker.com (accessed on 15 May 2017).
46. Lapinski, M.; Berkson, E.; Gill, T.; Reinold, M.; Paradiso, J.A. A distributed wearable, wireless sensor system for evaluating professional baseball pitchers and batters. In Proceedings of the International Symposium on Wearable Computers (ISWC), Linz, Austria, 4–7 September 2009, pp. 131–138.
47. Michahelles, F.; Schiele, B. Sensing and monitoring professional skiers. *IEEE Pervasive Comput.* **2005**, *4*, 40–45, doi:10.1109/MPRV.2005.66.
48. Ghasemzadeh, H.; Loseu, V.; Jafari, R. Wearable coach for sport training: A quantitative model to evaluate wrist-rotation in golf. *J. Ambient Intell. Smart Environ.* **2009**, *1*, 173–184, doi:10.3233/AIS-2009-0021.
49. Ozcan, K.; Mahabalagiri, A.K.; Casares, M.; Velipasalar, S. Automatic fall detection and activity classification by a wearable embedded smart camera. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2013**, *3*, 125–136, doi:10.1007/978-1-4614-7705-1_7.

50. Oracle Corporation. Data Masking Best Practices. Available online: http://www.oracle.com/us/products/database/data-masking-best-practices-161213.pdf (accessed on 15 May 2017).
51. Olshannikova, E.; Ometov, A.; Koucheryavy, Y.; Olsson, T. Visualizing Big Data with augmented and virtual reality: challenges and research agenda. *J. Big Data* **2015**, *2*, 22, doi:10.1186/s40537-015-0031-2.
52. Hathaway, D.H.; Meyer, P.J. Video Image Stabilization and Registration. U.S. Patent 6,459,822, 29 May 2002.
53. Cernea, D.; Mora, S.; Perez, A.; Ebert, A.; Kerren, A.; Divitini, M.; de La Iglesia, D.G.; Otero, N. Tangible and wearable user interfaces for supporting collaboration among emergency workers. In Proceedings of the International Conference on Collaboration and Technology, Raesfeld, Germany, 16–19 September 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 192–199.
54. Billinghurst, M.; Kato, H. Collaborative mixed reality. In Proceedings of the First International Symposium on Mixed Reality, Berlin, Germany, 9–11 March 1999; pp. 261–284.
55. Kfir, Z.; Wool, A. Picking virtual pockets using relay attacks on contactless smartcard. In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Athens, Greece, 5–9 September 2005; pp. 47–58.
56. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The sybil attack in sensor networks: Analysis & defenses. In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 27–27 April 2004; pp. 259–268.
57. Cremers, C.; Rasmussen, K.B.; Schmidt, B.; Capkun, S. Distance hijacking attacks on distance bounding protocols. In Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05) Symposium on Security and Privacy, San Francisco, CA, USA, 20–23 May 2012; pp. 113–127.
58. Orsino, A.; Moltchanov, D.; Gapeyenko, M.; Samuylov, A.; Andreev, S.; Militano, L.; Araniti, G.; Koucheryavy, Y. Direct Connection on the Move: Characterization of User Mobility in Cellular-Assisted D2D Systems. *IEEE Veh. Technol. Mag.* **2016**, *11*, 38–48, doi:10.1109/MVT. 2016.2550002.
59. Leister, W.; Hamdi, M.; Abie, H.; Poslad, S. An evaluation scenario for adaptive security in eHealth. In Proceedings of the Fourth International Conference on Performance, Safety and Robustness in Complex Systems and Applications, Nice, France, 23–27 February 2014; Volume 2327.
60. Li, M.; Yu, S.; Guttman, J.D.; Lou, W.; Ren, K. Secure ad hoc trust initialization and key management in wireless body area networks. *ACM Trans. Sens. Netw. (TOSN)* **2013**, *9*, 18, doi:10.1145/2422966.2422975.
61. Singelée, D.; Preneel, B. Location privacy in wireless personal area networks. In Proceedings of the 5th ACM Workshop on Wireless Security, Los Angeles, CA, USA, 29 September 2006; ACM: New York, NY, USA, 2006; pp. 11–18.
62. Militano, L.; Orsino, A.; Araniti, G.; Nitti, M.; Atzori, L.; Iera, A. Trust-based and social-aware coalition formation game for multihop data uploading in 5G systems. *Comput. Netw.* **2016**, *111*, 141–151, doi:10.1016/j.comnet.2016.08.001.
63. Wei, J. How Wearables Intersect with the Cloud and the Internet of Things: Considerations for the developers of wearables. *IEEE Consum. Electron. Mag.* **2014**, *3*, 53–56, doi:10.1109/MCE. 2014.2317895.
64. Paul, G.; Irvine, J. Privacy implications of wearable health devices. In Proceedings of the 7th International Conference on Security of Information and Networks, Glasgow, Scotland, UK, 9–11 September 2014; ACM: New York, NY, USA, 2014; p. 117.
65. Krause, A.; Ihmig, M.; Rankin, E.; Leong, D.; Gupta, S.; Siewiorek, D.; Smailagic, A.; Deisher, M.; Sengupta, U. Trading off prediction accuracy and power consumption for context-aware wearable computing. In Proceedings of the 9th IEEE International Symposium on Wearable Computers (ISWC'05), Osaka, Japan, 18–21 October 2005; pp. 20–26.
66. Yilmaz, O.N.; Wang, Y.P.E.; Johansson, N.A.; Brahmi, N.; Ashraf, S.A.; Sachs, J. Analysis of ultra-reliable and low-latency 5G communication for a factory automation use case. In Proceedings of the International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 1190–1195.
67. Brahmi, N.; Yilmaz, O.N.; Helmersson, K.W.; Ashraf, S.A.; Torsner, J. Deployment Strategies for Ultra-Reliable and Low-Latency Communication in Factory Automation. In Proceedings of the Globecom Workshops (GC Wkshps), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
68. Semkin, V.; Solomitckii, D.; Naderpour, R.; Andreev, S.; Koucheryavy, Y.; Raisanen, A.V. Characterization of Radio Links at 60 GHz Using Simple Geometrical and Highly Accurate 3D Models. *IEEE Trans. Veh. Technol.* **2016**, doi:10.1109/TVT.2016.2617919.

69. National Science Foundation. NSF Follow-on Workshop on Ultra-Low Latency Wireless Networks. Available online: http://inlab.lab.asu.edu/nsf/files/WorkshopReport-2.pdf (accessed on 15 May 2017).
70. Vannithamby, R.; Talwar, S. *Towards 5G: Applications, Requirements and Candidate Technologies*; John Wiley & Sons: Chichester, UK, 2016, ISBN 978-1-118-97983-9.
71. Scopelliti, P.; Araniti, G.; Muntean, G.M.; Iera, A. Mobility-aware energy-quality trade-off for video delivery in dense heterogeneous networks. In Proceedings of the International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Nara, Japan, 1–3 June 2016; pp. 1–6.
72. Andreev, S.; Pyattaev, A.; Johnsson, K.; Galinina, O.; Koucheryavy, Y. Cellular traffic offloading onto network-assisted device-to-device connections. *IEEE Commun. Mag.* **2014**, *52*, 20–31, doi:10.1109/MCOM.2014.6807943.
73. Daneshgaran, F.; Laddomada, M.; Mesiti, F.; Mondin, M.; Zanolo, M. Saturation throughput analysis of IEEE 802.11 in the presence of non ideal transmission channel and capture effects. *IEEE Trans. Commun.* **2008**, *56*, 1178–1188, doi:10.1109/TCOMM. 2008.060397.
74. Chang, W.C.; Tseng, M.Y.; Iok-Kan, C.; Tseng, W.J.; Wu, J.L. Virtual Reality System and Method for Controlling Operation Modes of Virtual Reality System. U.S. Patent App. 14/943,721, 9 June 2016.
75. Park, C.; Rappaport, T.S. Short-range wireless communications for next-generation networks: UWB, 60 GHz millimeter-wave WPAN, and ZigBee. *IEEE Wirel. Commun.* **2007**, *14*, 70–78, doi:10.1109/MWC.2007.4300986.
76. Lawton, G. Wireless HD video heats up. *Computer* **2008**, *12*, 18–20.
77. Takinami, K.; Motozuka, H.; Urushihara, T.; Kobayashi, M.; Takahashi, H.; Masataka, I.; Sakamoto, T.; Morishita, Y.; Miyanaga, K.; Tsukizawa, T.; et al. A 60 GHz Hybrid Analog/Digital Beamforming Receiver with Interference Suppression for Multiuser Gigabit/s Radio Access. *IEICE Trans. Electron.* **2016**, *99*, 856–865, doi:10.1587/transele.E99.C.856.
78. Perahia, E.; Cordeiro, C.; Park, M.; Yang, L.L. IEEE 802.11ad: Defining the next generation multi-Gbps Wi-Fi. In Proceedings of the 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 9–12 January 2010; pp. 1–5.
79. Daniels, R.C.; Murdock, J.N.; Rappaport, T.S.; Heath, R.W. 60 GHz wireless: Up close and personal. *IEEE Microw. Mag.* **2010**, *11*, 44–50, doi:10.1109/MMM.2010.938581.
80. Alipour, S.; Parvaresh, F.; Ghajari, H.; Donald, F.K. Propagation characteristics for a 60 GHz wireless body area network (WBAN). In Proceedings of the Military Communications Conference (MILCOM), San Jose, CA, USA, 31 October–3 November 2010; pp. 719–723.
81. Cisco. Connected Stadium Wi-Fi Solution. Available online: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/sports/c78-675063_dSheet.pdf (accessed on 15 May 2017).
82. Durgin, G.; Patwari, N.; Rappaport, T.S. An advanced 3D ray launching method for wireless propagation prediction. In Proceedings of the 47th Vehicular Technology Conference, Phoenix, AZ, USA, 4–7 May 1997; Volume 2, pp. 785–789.
83. Peter, M.; Wisotzki, M.; Raceala-Motoc, M.; Keusgen, W.; Felbecker, R.; Jacob, M.; Priebe, S.; Kürner, T. Analyzing human body shadowing at 60 GHz: Systematic wideband MIMO measurements and modeling approaches. In Proceedings of the 6th European Conference on Antennas and Propagation (EUCAP), Prague, Czech Republic, 26–30 March 2012; pp. 468–472.
84. RUCKUS Wireless, Inc. *Deploying Very High Density Wi-Fi: Design and Configuration Guide for Stadiums*; Best Practicies v1.0; RUCKUS Wireless, Inc.: Sunnyvale, CA, USA, 2012; p. 51.
85. Anwar, R.W.; Bakhtiari, M.; Zainal, A.; Abdullah, A.H.; Qureshi, K.N. Security issues and attacks in wireless sensor network. *World Appl. Sci. J.* **2014**, *30*, 1224–1227, doi:10.5829/idosi.wasj.2014.30.10.334.
86. Abdullah, N.F.; Goulianos, A.A.; Barratt, T.H.; Freire, A.G.; Berraki, D.E.; Armour, S.M.; Nix, A.R.; Beach, M.A. Path-loss and throughput prediction of IEEE 802.11ad systems. In Proceedings of the 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May 2015; pp. 1–5.
87. Robert, J.M.; Barbeau, M. Rogue Access Point Detection in Wireless Networks. U.S. Patent 7,962,958, 14 June 2011.
88. Chandra, S.; Paira, S.; Alam, S.S.; Sanyal, G. A comparative survey of symmetric and asymmetric key cryptography. In Proceedings of the International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, India, 17–18 November 2014; pp. 83–93.
89. Gordon, S.D.; Katz, J.; Kumaresan, R.; Yerukhimovich, A. Authenticated broadcast with a partially compromised public-key infrastructure. *Inf. Comput.* **2014**, *234*, 17–25, doi:10.1145/357172.357176.

90. Liu, W.; Liu, H.; Wan, Y.; Kong, H.; Ning, H. The yoking-proof-based authentication protocol for cloud-assisted wearable devices. *Pers. Ubiquitous Comput.* **2016**, *20*, 469–479, doi:10.1007/s00779-016-0926-8.
91. Prudanov, A.; Tkachev, S.; Golos, N.; Masek, P.; Hosek, J.; Fujdiak, R.; Zeman, K.; Ometov, A.; Bezzateev, S.; Voloshina, N.; et al. A Trial of Yoking-proof Protocol in RFID-based Smart-Home Environment. In Proceedings of the Distributed Computer and Communication Networks: Control, Computation, Communications (DCCN), Moscow, Russia, 21–25 November 2016.
92. Papapostolou, A.; Chaouchi, H. Integrating RFID and WLAN for indoor positioning and IP movement detection. *Wirel. Netw.* **2012**, *18*, 861–879, doi:10.1007/s11276-012-0439-y.
93. Chen, H.M.; Lo, J.W.; Yeh, C.K. An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. *J. Med. Syst.* **2012**, *36*, 3907–3915, doi:10.1007/s10916-012-9862-y.
94. He, D.; Zeadally, S.; Kumar, N.; Lee, J.H. Anonymous authentication for wireless body area networks with provable security. *IEEE Syst. J.* **2016**, doi:10.1109/JSYST.2016.2544805.
95. Fodor, G.; Parkvall, S.; Sorrentino, S.; Wallentin, P.; Lu, Q.; Brahmi, N. Device-to-device communications for national security and public safety. *IEEE Access* **2014**, *2*, 1510–1520, doi:10.1109/ACCESS.2014.2379938.
96. Juels, A. "Yoking-proofs" for RFID tags. In Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, Orlando, FL, USA, 14–17 March 2004; pp. 138–143.
97. Scott, M.; Costigan, N.; Abdulwahab, W. Implementing cryptographic pairings on smartcards. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Yokohama, Japan, 10–13 October 2006; Springer: Berlin, Germany, 2006; pp. 134–147.
98. Lo, N.W.; Yeh, K.H. Anonymous coexistence proofs for RFID tags. *J. Inf. Sci. Eng.* **2010**, *26*, 1213–1230, doi:10.1.1.429.9815.
99. Burmester, M.; De Medeiros, B.; Motta, R. Provably secure grouping-proofs for RFID tags. In Proceedings of the International Conference on Smart Card Research and Advanced Applications, London, UK, 8–11 September 2008; Springer: Berlin, Germany, 2008; pp. 176–190.
100. Saito, J.; Sakurai, K. Grouping proof for RFID tags. In Proceedings of the 19th International Conference on Advanced Information Networking and Applications, Taipei, Taiwan, 28–30 March 2005; Volume 2, pp. 621–624.
101. Weis, S.A.; Sarma, S.E.; Rivest, R.L.; Engels, D.W. Security and privacy aspects of low-cost radio frequency identification systems. In *Security in Pervasive Computing*; Springer: Berlin, Germany, 2004; pp. 201–212, doi:10.1007/978-3-540-39881-3_18.
102. Liu, Y.; Qin, X.; Li, B.; Liu, L. Cryptanalysis of a Scalable Grouping-proof Protocol for RFID Tags. *Int. J. Digit. Content Technol. its Appl.* **2012**, *6*, 247, doi:10.4156/jdcta.vol6.issue21.28.
103. Chen, C.L.; Wu, C.Y. Using RFID yoking proof protocol to enhance inpatient medication safety. *J. Med. Syst.* **2012**, *36*, 2849–2864, doi:10.1007/s10916-011-9763-5.