Research Article

Using Physical Context-Based Authentication against External Attacks: Models and Protocols

Wilson S. Melo Jr. ¹, **Raphael C. S. Machado** ^{1,2} and **Luiz F. R. C. Carmo**^{1,3}

¹National Institute of Metrology, Quality and Technology, Rio de Janeiro, RJ, Brazil

²Federal Center for Technological Education, Rio de Janeiro, RJ, Brazil

³Federal University of Rio de Janeiro, Rio de Janeiro, RJ, Brazil

Correspondence should be addressed to Wilson S. Melo Jr.; wsjunior@inmetro.gov.br

Received 25 August 2017; Revised 17 December 2017; Accepted 21 January 2018; Published 25 February 2018

Academic Editor: Indrakshi Ray

Copyright © 2018 Wilson S. Melo Jr. et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Modern systems are increasingly dependent on the integration of physical processes and information technologies. This trend is remarkable in applications involving sensor networks, cyberphysical systems, and Internet of Things. Despite its complexity, such integration results in physical context information that can be used to improve security, especially authentication. In this paper, we show that entities sharing the same physical context can use it for establishing a secure communication channel and protecting each other against external attacks. We present such approach proposing a theoretical model for generating unique bitstreams. Two different protocols are suggested. Each one is evaluated using probabilistic analysis and simulation. In the end, we implement the authentication mechanism in a case study using networks radio signal as physical event generator. The results demonstrate the performance of each of the protocols and their suitability for applications in real world.

1. Introduction

Authentication is the process of identifying an entity and reliably granting authorization to a resource. Although it is a widely discussed and studied topic, authentication remains a crucial security issue [1–4]. Nowadays, technologies such as sensor networks, smart systems, cyberphysical systems (CPS), and Internet of Things (IoT) depend on small building blocks like sensors, actuators, measuring instruments, and smart devices. These building blocks also become system entities and can require specific authentication mechanisms, as evidenced in applications related to manufacturing [5], transportation [6–8], energy management [9, 10], smart cities and smart homes [11], and electronic healthcare [12], among others. On the other hand, the same ubiquitous components also introduce a new asset: the *physical context* information amount, resulting from the integration of physical processes and information technologies [3, 13].

Context-aware computing has constituted a well-studied topic for the last two decades [14]. Recently, a renewed interest in this area has emerged due to ubiquitous technologies

that expand the idea of context to the physical world [13]. Physical context can provide information about a system and its entities, *where* they are, *what* they do, and *when* they do it. Different features in systems with ubiquitous technologies already take advantage of physical context information (e.g., energy saving based on environmental sensors). However, that seldom happens with security mechanisms.

We work with the hypothesis that physical context information can be used to improve cybersecurity, especially authentication processes. For example, a person walking down a street can use the physical context related to her pace for authenticating personal devices, such as smartphones or any wearable smart device that has an accelerometer. There are several works where authentication demands that entities share the same physical context [8, 10, 12, 15–18]. Although this is a very particular authentication case, it finds application in several practical scenarios related to systems with ubiquitous technologies. Manufacturing systems [5], for instance, can authenticate products based on their position in an assembly line, validating specific steps in manufacturing processes and quality assurance. Cooperative

vehicular applications, such as collision avoidance and platooning [7, 8], usually need to restrict communication to authenticated vehicles which are close to each other. Relay attacks against mobile and wireless networks can be avoided using environmental sensing to determine the proximity among entities before authenticating them [12, 15, 19]. Furthermore, two-factor authentication (2FA) mechanism using physical patterns to enforce identification [20] suggests that security can be remarkably improved when physical context information is part of the authentication process.

In this paper, we provide a formal framework for studying and implementing *physical context-based authentication* mechanisms. Firstly, we analyze related works in literature that use physical context for enhancing authentication processes. We show that such strategy depends on the existence of a secure communication channel; otherwise, authentication becomes vulnerable. Most works assume that a secure channel is established using preshared secret keys [15, 17, 19] or traditional key agreement protocols (e.g., Diffie-Hellman, TLS) [12, 16, 20–22]. However, these methods have drawbacks associated with the management of preshared keys [23] and traditional protocols complexity [24]. Then, we evaluate a less explored alternative that uses the physical context information for establishing secret keys. That results in an authentication mechanism which is very robust against passive and active external attackers.

This paper brings the following main contributions:

- (i) We formalize the idea of *physical context-based authentication* and describe distinct attacks according to the communication channel security properties.
- (ii) We define the problem of using *physical events* to generate *unique bitstreams* with high probability. We also discuss probabilistic models to the problem and how to use them to perform physical context-based authentication.
- (iii) We propose *two protocols* to generate *unique bitstreams* from physical context information. These protocols have the advantage of *not disclosing information about the physical context* during the handshake. We analyze and compare both methods using *probabilistic analysis, simulation, and real world data*.
- (iv) We implement a case study using local Wi-Fi network signal as physical events generator, showing that *our method achieves fair accuracy rates and is suitable for practical applications*.

The paper is organized as follows. In Section 2, we revise the literature related to physical context-based authentication, and we present the concepts and terminology necessary to the proper understanding of the remainder of the paper. In Section 3, we provide a formal definition of the authentication problem as well as the attack model considered in this paper, describing two realistic scenarios according to the communication channel security properties. In Section 4, we consider the particular and more effective scenario where two parties must generate the same bitstreams by observing a set of physical events. We describe formal models to the

problem and obtain theoretical results that are corroborated by simulation experiments in Section 5. Section 6 describes a case study for physical context-based authentication using network radio signals as physical events generator. Section 7 contains final considerations about our results and provides future directions for researching the theme.

2. Preliminaries

2.1. Physical Context-Based Authentication in a Nutshell. The idea of *physical context-based authentication* is showed in Figure 1. Alice and Bob are entities in any system that interacts with the *physical world*, being able to *observe* and *describe* a specific *physical context*. They do that by measuring *physical quantities* such as speed, temperature, electromagnetic spectrum, or any other sensing information. Bob wants to *prove* to Alice that they *share the same physical context*. Bob's strategy is to show Alice that he can *observe* the same *physical events* as her. The intuitive way that Bob can do that is by sending a message describing the physical events in a given period. Alice then compares the description in Bob's message with those physical events observed by her. Naturally, one can expect to find differences between the event descriptions. The precise entities position, noise, synchronization errors, and sensors physical properties are some of the factors that can affect the physical event observation. If Bob is a legitimate entity, then *event descriptions are quite similar*. By using appropriate tools, Alice can eventually be convinced that Bob describes the same physical context.

However, the communication between Alice and Bob affects authentication effectiveness. Alice and Bob need mechanisms for establishing a *secure communication channel*. Otherwise, any authentication protocol will be vulnerable to eavesdropping and active attacks.

2.2. Related Works. Context-aware computing is an extensive knowledge area that explores the use of complementary information to characterize an entity situation [14]. Context-aware authentication mechanisms can be projected for taking advantage of information related to the users' role and behavior or even properties from the environment where system entities are immersed. Different works proposing context-aware authentication techniques for IoT are surveyed by Habib and Leister [13]. Although the authors use the term *physical context* to designate a specific context type, just a few works related to authentication using physical or environmental sensing are mentioned. Despite that, Habib and Leister [13] emphasize that physical context-based mechanisms are suitable for ubiquitous computing applications (e.g., sensor networks, IoT, and CPS). The reasons are their dynamic and heterogeneous environment as well as the amount of context information from physical world gathered by sensors and smart devices.

Physical context information is often associated with a physical location, position, or proximity [16, 17, 25]. Authentication mechanisms based on physical proximity explore the colocation of devices as a countermeasure against relay and impersonation attacks [17]. The concept of ambient multi-sensing authentication in Shrestha et al. [19], for instance,

makes use of physical quantities such as temperature, humidity, and pressure for composing location identifiers which are robust against relay attacks. In Miettinen et al. [16] context information related to positioning is used for pairing colocated and wearable IoT devices. Another example is *Convoy* [8], an authentication system for vehicle platoon admission based on the vehicle's position, using sensors such as accelerometers to estimate trajectories and road conditions. STASH [17] is also an authentication system that uses the estimated trajectory of mobile devices for providing proximity verification as a countermeasure against relay attacks. Proximity also works in 2FA schemes. Karapanos et al. [20] use ambient sound for providing 2FA authenticating entities. Gu and Liu [26] also explore ambient sound for implementing group authentication of IoT devices.

Physical context information can also be used for identifying patterns related to an entity. An example is energy load signature [27], where electrical load patterns are associated with individual appliances in a house, enabling their identification. Behavioral biometrics [28, 29] also make use of patterns for identifying biological entities based on their physical actions (eyes blink, keystrokes, and gestures, among others). An interesting example is the "cyberphysical handshake" in Wu et al. [22], where two persons wearing watch-like smart devices equipped with accelerometers shake their hands, generating a physical event for mutual identification. Human voluntary actions can also be used for authenticating smart devices. In Mayrhofer and Gellersen [21] two devices with accelerometers are paired by shaking them together. Other approaches make use of involuntary behavioral actions for identification. Heart-to-Heart (H2H) authentication scheme, proposed by Rostami et al. [12], uses time-varying randomness from the heart beating signal for granting remote access to an implantable medical device.

One can also find ideas related to physical context-based authentication in works using events from physical layer in communication networks. Scannell et al. [30] use radio environment traces for generating identifiers attesting that two entities are physically close to each other. Mathur et al. [31] explore physical properties which assure that the radio channel between two entities is unique, introducing the concept of channel-based authentication. Zhang et al. [18] present a comprehensive study about alternatives for securing wireless communication of IoT devices using context information from network physical layer.

An important aspect of physical context-based authentication is the security of the communication channel. Most of the approaches rely on preexisting protection mechanisms assumed as secure. The use of a secret key shared previously is the mechanism adopted in [15, 17, 19] for establishing encrypted sessions. In turn, key agreement protocols like Diffie-Hellman and TLS (Transport Layer Security) are protection measures used in [12, 16, 20–22]. Such trend is expected since protection mechanisms related to cryptographic premises are cornerstones for implementing secure systems [32]. However, the management of shared secret keys can be complex and expensive in practical scenarios [23]. Furthermore, key agreement protocols also have their limitations, as is the case of possible problems related to

the Diffie-Hellman implementation and TLS recent security flaws [24].

An alternative approach consists of using physical context information for establishing a secret key between two entities. This concept is revealed in works related to physical layer-based security in communication networks, using an information-theoretic approach [33, 34]. One can expect that two entities observing the same physical context will get similar (although not equal) descriptions. So a *reconciliation* method can be used to change different physical context descriptions into the same secret key. The main reconciliation methods are based on *error correction codes* (ECCs) [34]. Although ECC is a reliable solution for communication errors, its use in key agreement protocols implies a handshake that discloses information about the key. A channel subject to a high error rate requires more information redundancy and consequently discloses more information, compromising the key's secrecy. Apart from works related to network physical layer-based security, we have found just a few studies proposing reconciliation protocols in physical context-based authentication. One can mention Gu and Liu [26], who use BCH, Reed-Muller, Golay, and Reed-Solomon codes, and Han et al. [8] using Reed-Solomon.

2.3. What We Do Different. In this paper, we revisit the main concepts related to physical context-based authentication. We believe that this theme lacks a formal model for study and implementation. Thus we propose a comprehensive model that can be instantiated in practical applications involving interactions with the physical world. Besides, our work differs from previous ones in two main aspects:

- (i) We demonstrate that physical context information is more than just a proximity evidence. The first reason is because we glimpse cases where the physical context consists of information about a physical phenomenon that implies *connectivity* and not necessarily proximity. For instance, the energy flow in a smart grid can generate a physical context shared by devices which are connected to the same grid segment, although they are not close to each other. The second reason is because physical context information also includes *simultaneity evidence*, a property that results in natural protection against replay attacks.
- (ii) We emphasize the use of physical context information for *establishing secret keys* among the entities. Furthermore, we propose two key agreement algorithms that do not disclose information about the secret key. That constitutes a significant improvement when compared to solutions using error correction codes. To the best of our knowledge, we are the first to propose such methods in physical context-based authentication.

2.4. Potential Applications. In this section, we describe some potential applications for the industry that can be abstracted from our authentication mechanism. All the cases involve well-known cyberphysical systems with high demand for security solutions.

2.4.1. Manufacturing Industry. Critical concerns about the security in manufacturing processes have been addressed in the literature [3, 5]. Physical context information from industrial processes environment can improve products identification and authentication. Products embedding sensors and smart components able to store data can gather information from physical events related to any physical process. Such information can attest that a specific product was submitted to specific manufacturing steps and quality assessment procedures. As an example, one can consider a product using accelerometers for measuring its movement into an industrial conveyor belt. The continuous start/stop movement on an assembly line produces a “kinetic fingerprint” which can confirm that this product has passed by the specific manufacturing process. Besides improving identification and traceability of products after production, such approach can also be explored in quality control. One can implement authentication checkpoints in the manufacturing line, avoiding defects related to wrong steps sequences or even the absence of specific manufacturing steps and tests. That solution could have a remarkable impact on conformity assessment and quality control in industrial processes.

2.4.2. Vehicular Transportation. Transportation implies the movement of vehicles into a physical environment. Consequently, vehicles can make use of rich physical context information for providing more sophisticated services. Several emerging applications involving smart autonomous vehicles and vehicular networks can employ physical context-based authentication to increase security. For instance, vehicles implementing vehicle-to-vehicle communication (V2V) [6] can authenticate each other using physical context information that describes their environment and trajectory. In a V2V environment, vehicles are usually close to each other and consequently can describe the same physical context [8]. Signals from environmental sensors (temperature, humidity, and air pressure) and movement sensors (accelerometers, compass, and GPS) can be used for obtaining a “context fingerprint.” A similar strategy could protect a moving vehicle against external attacks which aim to get access to the Control Area Network (CAN) bus [7, 35]. In such situation, the vehicle’s Electronic Control Units (ECUs) can authenticate each other by asking for credentials which also describe the vehicle’s physical context, including dynamic attributes related to its trajectory and environment. Again, movement and environmental sensors can be used for composing a context identifier which only ECUs embedded in the vehicle can determine. The attacker, placed outside the vehicle, cannot guess or describe the respective physical context.

2.4.3. Smart Grids. One of the basic features provided by smart grids consists of telemetry, which enables the reading of end-users’ consumption from a remote place [36]. Due to privacy reasons, some solutions propose the existence of a gateway to aggregate information from a group of smart meters (end-users) in the same neighborhood. In turn, gateway and smart meters need to authenticate each other before exchanging any consumption information. Physical context information can improve this process by providing

FIGURE 1: The physical context authentication problem.

evidence that gateway and smart meters are in the same power grid segment, thus avoiding external attacks. That can be done by measuring physical events from the power grid. One possibility is to explore the variations in voltage levels. The Volt/VAR Control (VVC) [37] is the system that keeps a stable voltage profile in the power grid. However, slight voltage variations can be observed along a grid segment. They result from different energy loads supported in each specific grid segment. Such phenomenon becomes even more dynamic in energy microgeneration scenarios, creating a singular case of physical context given by the energy flow in a grid. Thus gateway and smart meters placed in the same grid segment can use such context for authenticating each other.

3. Physical Context and Secure Channels

3.1. Defining Physical Context. It is time to return to our authentication problem (Figure 1). Alice must authenticate Bob before starting any communication. Furthermore, Bob needs to prove to Alice that they are *sharing the same physical context*. If that is true, then Alice and Bob also fulfill two important conditions:

- (i) *Colocation*: Alice and Bob are in the same physical location, or relatively close to each other, or connected to an environment where the physical phenomenon occurs.
- (ii) *Simultaneity*: Alice and Bob are observing their physical context at the same time.

One should note that our definition implies that *colocation* is more than physical proximity. For instance, two smart meters connected to the same smart grid segment can describe the same physical context related to the grid energy flows, even while being placed far away from each other. Indeed, colocation can indicate a relative idea of proximity.

Colocation and simultaneity are desirable properties to enforce security policies in situations where entities location and synchronism matter. Usually, this information is obtained using additional infrastructures such as positioning systems (geographic or indoor) and timestamps services. However, colocation and simultaneity also can be evidenced

by physical events and physical context information, without the need for any additional infrastructure. That happens when Alice and Bob can describe the same physical events, something expected when they share the same physical context. Besides that, in the described scenario, neither Alice nor Bob needs to interact with the physical world actively. They could be just passive entities, gathering information from the physical world.

3.2. Attack Model. We assume that the attacker is a malicious external entity (Marley) with total access to the communication channel used by Alice and Bob. Marley can listen to this channel and intercept authentication messages. Moreover, Marley can send fake messages, performing man-in-the-middle attacks. His primary intention is to impersonate Bob, fooling Alice and so getting nonauthorized access to information and services. However, once Marley is an external entity, he does not have access to Alice and Bob's physical context. Consequently, Marley cannot capture the same physical events observed by them. Despite that, he can try to find out physical context information from Alice and Bob, eavesdropping on their communication channel.

Marley's attack capabilities must be evaluated considering the two following scenarios:

- (1) *Secure communication scenario*: we assume the existence of a reliable mechanism that delivers the same secret key to Alice and Bob. This key can be used to establish an encrypted communication channel using any reliable cryptographic protocol. We also assume that Marley cannot steal that secret key. Thus Marley's capabilities are restricted to relay attacks by forwarding messages of legitimate entities, something that does not represent any threat once all the messages are encrypted.
- (2) *Nonsecure communication scenario*: we assume that the messages are sent in plain text. In this case, Marley has the following capabilities:
 - (i) Steal information, eavesdropping on the communication between Alice and Bob.
 - (ii) Impersonate Bob, using intercepted information from a legitimate entity in a relay attack.
 - (iii) Impersonate Bob, using authentication tokens from previous sessions in a replay attack.

Since Marley has total control over the communication channel, he can launch a diversity of attacks targeting availability (e.g., injection attacks, Denial-of-Service attacks). Such situation requires defense-in-depth strategies (e.g., a previous authentication layer that prevents Marley from getting control over the communication channel [38]). Although that is a relevant concern, we do not consider such attacks in this study. Thus we assume that Marley has no interest in attacks against system availability.

3.3. Authentication Mechanism Using Physical Context. Physical context-based authentication can work in different ways for each described attack scenario. On one hand, physical

context can be used only as evidence of colocation and simultaneity between Alice and Bob. That is the approach followed by most of the works related to physical context-based authentication (see Section 2.2). On the other hand, when we consider a nonsecure communication scenario, things become more interesting: physical context can also work as an exclusive channel for secret key distribution.

Suppose that Alice and Bob share the same physical context. So they know that their physical context description is quite similar, although not equal. We call these descriptions as *physical event identifiers*. All Alice and Bob need is a *reconciliation protocol* that can convert both identifiers in the same secret key. Such protocol must disclose just a minimal information amount about the physical context description and the respective identifiers. Consequently, Marley cannot figure out the physical context or deduce the secret key. Once Alice and Bob have a shared secret key, they can establish a secure channel, reducing the attacker capabilities to the first attack scenario.

We formalized the idea expressed above in the following protocol. If Alice and Bob are represented by A and B , respectively, and P is a proper reconciliation function, we have the following:

- (1) A observes physical event E and extracts ID_A .
- (2) B observes physical event E and extracts $ID_B \approx ID_A$.
- (3) A computes $k = P(ID_A)$.
- (4) B computes $k = P(ID_B) = P(ID_A)$.
- (5) A and B can communicate using cryptographic protocols over the secret key k .

Two aspects must be properly addressed to confirm the protocol security. The first one is the P function. P has to be chosen in such manner that the differences between identifiers ID_A and ID_B are suppressed. Otherwise, the k value will not be the same for A and B . The second aspect is related to the interpretation of E . Since k is proposed for cryptographic use, one expects that k presents random properties. So the physical context (and consequently each physical event) must be associated with nondeterministic processes.

To point out a solution and make the security analysis clearer, we propose a *Unique Bitstream Generator* model that can be implemented using physical context information. The idea will be formally exposed and discussed in the next section.

4. Generation of Unique Bitstream from Physical Events

4.1. Probabilistic Theoretic Model. We formalize the *Unique Bitstream Generator* based on a discrete probabilistic model. We assume the existence of a random bit generator G whose generated bitstream is accessible to any party that is located in a given environment. The goal is to use these bitstreams to generate cryptographic keys that will allow the secure communication between the parties in this environment. However, the communication between G and the parties

FIGURE 2: The Unique Bitstream Generator G description.

inserts errors in the bits generated by G . Therefore, the parties receive related but distinct bitstreams that will need to be somehow processed before generating cryptographic keys. The diagram in Figure 2 depicts the model.

We denote by *time unit* the minimum amount of time observed by the parties. Each time unit corresponds to a unique bit generated by G . Note that this bit is sent via a communication channel that introduces errors. So the parties will not necessarily receive the bit generated by G . A *time slot* is a set of subsequent time units and the *size* of the time slot is the size of the set.

4.2. Clock Errors and Transmission Delays. One important aspect for the Unique Bitstream problem is whether the parties can refer precisely to each time unit or whether clock error and delays on the transmission of physical events can impact the synchronization between the parties. “Absolute synchronization” allows the development of more powerful protocols, but in general, it is not a reasonable assumption for most real world applications. In practice, we assume that synchronization errors lead to bit transmission errors. A bit associated with a time unit can be interpreted differently by A and B since the precise instants where the time unit begins and finishes are not the same for A and B .

4.3. Counting Events: The Binomial Distribution Model. We consider that the following strategy generates a unique key k from the bitstream generated by G . We partition the bitstream into time slots and count the number of bits 1 (i.e., we compute the sum of the bits in the time units in each time slot). Then, we define a bit associated with each slot according to this sum. Assuming the *equiprobability* of bits 0 and 1, and considering that the number of bits 1 in each slot follows a binomial distribution, a typical choice is to associate bit 0 with a slot whose sum is less than half the number of time units of this slot. Formally, we represent a time slot T with k time units

FIGURE 3: The Unique Bitstream Generator counting events example.

as a k -tuple $(b_1, \dots, b_k)$ of binary digits. The sum S_T is given by

$$S_T = \sum_{i=1}^k b_i. \quad (1)$$

The bit N_T associated with slot T is 1 if $S_T < k/2$ and is 0 otherwise. Figure 3 depicts an example.

Consider a time slot $T = (b_1, \dots, b_k)$ transmitted to A and B and received by A as $T^A = (b_1^A, \dots, b_k^A)$ and by B as $T^B = (b_1^B, \dots, b_k^B)$. Recall that each bit b_i can be flipped with a given probability p_E , so that the probability that $b_i^A \neq b_i^B$ for each bit received by A and B is given by

$$p = 2p_E(1 - p_E). \quad (2)$$

Considering the possibility of error, it is possible that the total number of bits counted by A and B is not the same. So the associated bits are distinct.

An important aspect of our proposed model is that it takes advantage of classic probabilistic models and paradigms. As we saw, the model is strongly based on the so-called binomial distribution. Furthermore, the behavior observed in the simulation and the case study is properly explained by analyzing the scenarios defined over the binomial distribution function.

4.4. Naive Counting Protocol (NC). We start by considering the more simple protocol where the bit associated with a time slot is determined by the majority of the bits in this time slot. Formally, the protocol associates bit 0 with a time slot $T = (b_1, \dots, b_k)$ if $S_T < k/2$ and bit 1 otherwise.

In the above model, the probability of an error is the probability that one party, say A , receives a time slot whose majority is distinct to the majority in the time slot received by the other party B —this could happen due to transmission errors.

In the following subsection, we generalize the Naive Counting Protocol and derive bounds for the probability of errors.

4.5. The Band of Guard Protocol (BG). As we show in the previous section, the Naive Counting Protocol presents a nonnegligible probability that A and B associate distinct bits with a time slot. In the present section, we define an alternative protocol. The idea is to define a “band” that determines whether time slot presents a high probability of error. Intuitively, a time slot has a high probability of error if the number of 1s is close to half the number of time units of the slots. In practice, A and B agree about a number b if the number of bits 1 in a slot is between $k/2 - b$ and $k/2 + b$, where k is the number of time units in a time slot. If a slot T^A observed by A (resp., slot T^B observed by B) has a sum of bits that falls inside the band, that is, between $k/2 - b$ and $k/2 + b$, then T^A (resp., T^B) does not generate a bit. In other words, the bit associated with a slot can be bit 0 if the number of bits 1 is below $k/2 - b$, bit 1 if the number of bits 1 is above $k/2 + b$, and “undefined” if the sum of bits is between $k/2 - b$ and $k/2 + b$.

Note that the “band of guard” protocol is a generalization of the “naive counting” protocol, where the “naive counting” protocol has a band of guard $k = 0$.

The advantage of the above strategy is that the probability that a slot T gives origin to distinct bits for A and B is lower, as a larger number of bit flips would need to occur. On the other side, the bit production rate is lower due to the “undefined” bits. Besides, the parties should interact to inform which slots generated undefined bits (hence need to be discarded). Note that the fact that the parties indicate discarded slots does not allow an attacker to obtain any information about the generated bits.

One disadvantage of the “band of guard protocol” is the rapid decrease of throughput as a function of the size of the guard. Indeed, the binomial distribution leads to a strong concentration around the mean. Using Chernoff bounds [39], it can be proved that

$$\Pr\left(\left|X - \frac{n}{2}\right| \geq \frac{1}{2} \sqrt{6n \log_e(n)}\right) \leq \frac{2}{n}, \quad (3)$$

where X is the number of bits 1 in a time slot with n bits.

In practice, that means that the concentration on the number of bits 1 around the mean $n/2$ is very tight: most of the time, the deviation from this mean is on the order of $O(n \log(n))$.

Another way of using the Chernoff bound technique gives

$$\Pr\left(\left|X - \frac{n}{2}\right| \geq \frac{n}{4}\right) \leq 2e^{-n/24}. \quad (4)$$

which indicates exponential decrease on the size of the slot for the probability of the total number of bits 1 to be below $n/4$ or above $3n/4$. As a consequence, a small increase in the size of the band of guard leads to a relevant decrease in the percentage of valid time slots.

4.6. The Best Slots Protocol (BS). We describe a strategy to reduce the number of errors in the generation of bitstreams from physical events. Basically, instead of using time slots with predefined timeframes, that is, set of time units, we allow the beginning and the end of each slot to be dynamically

FIGURE 4: How the choosing best slots protocol works.

defined, so that the number of bits 1 or bits 0 is guaranteed to be above the desired threshold, therefore leading to an adequate error rate.

The idea is simple. Consider a time slot $T = (b_1, \dots, b_k)$ transmitted to A and B and received by A as $T^A = (b_1^A, \dots, b_k^A)$ and by B as $T^B = (b_1^B, \dots, b_k^B)$. Assume that A and B agreed about a value k for a threshold for the band of guard. If the number of bits 1 observed by A in T^A (resp., observed by B in T^B) is between $k/2 - b$ and $k/2 + b$, where k is the number of time units in a time slot, then A (resp., B) sinalizes that (s)he does not wish to use slot T as the generator of a bit. Then, each A and each B considers the “next slot” $T = (b_2, \dots, b_{k+1})$, that is; we slide right the time slot.

It is important to mention that the checksum update can be efficiently computed by considering only the values of bits b_1, b_k, b_{k+1} —there is no need to perform an additional counting of bits 1 in the new time slot $T = (b_2, \dots, b_{k+1})$.

The protocol works as follows (see Figure 4). We start like in BG protocol, selecting time slots $T = (b_1, \dots, b_k)$. Before accepting a new time slot T , one of the parties (the verifier) checks the sum of the bits S_T . If S_T is inside the band of guard, the first bit $b_1 \in T$ is discarded, and the bits are shifted doing $b_i = b_{i+1}$. The next bit will be again b_k and the procedure repeats until S_T generates 0 or 1. When it happens, the new time slot T is accepted, and the verifier informs the other part how many bits must be discarded to get T .

5. Simulation Results

The protocols proposed in the previous section were verified using simulation. We suppose that two entities A and B try to establish a secure communication channel using physical events. The experiment is set up as follows. We use a random binary stream generated by website www.random.org which was checked using the NIST Statistical Test Suite for Random and Pseudorandom Number Generators [40]. The binary stream works as an oracle of “virtual” physical events, just like in the Unique Bitstream Model previously described. We simulate A and B as entities that observe physical events and try to determine a secret key k implementing each one of the described protocols.

The simulation results show each protocol accuracy and throughput. By accuracy, we mean the rate of simulated cases where Alice and Bob are successful in establishing the same secret key k . In turn, the throughput is the rate of physical events (in our simulation, bits) which are effectively used on valid slots. Aiming to make the simulation more realistic, we define an error rate err which determines the probability which an entity can miss a described event. That means a physical event $E = 0$ can be observed as $E' = 1$ with a probability of err and vice versa.

TABLE 1: Theoretical NC and BG protocols simulation results.

Band	Accuracy (%)			Throughput
	err = 0.01	err = 0.02	err = 0.05	
0 (NC)	5.5	0.5	0.0	100
1	12.5	1.8	0.0	75.3
2	82.7	57.0	5.4	34.3
3	100	89.9	47.2	10.8
4	100	100	63.2	2.19

TABLE 2: Theoretical BS protocol simulation results.

Band	Accuracy (%)			Throughput
	err = 0.01	err = 0.02	err = 0.05	
0	21.7	5.7	0.3	97.6
1	94.8	81.3	35.3	93.8
2	99.87	99.1	91.8	91.9
3	100	99.49	94.9	24.1
4	100	100	100	1,34

For practical reasons, we fixed some parameters for determining the Unique Bitstream. We consider each bit as 1 time unit. The time slot is fixed as 10 time units, and we try to obtain 64-bit unique bitstreams, which means that each protocol will consume the binary stream until it finds 64 “good” slots.

Table 1 summarizes the results obtained for Naive Counting (NC) and Counting with Band of Guard (BG) protocols. The *Band* column indicates the band of guard size (in bits) adopted on each simulation. One can note that accuracy and throughput reach better rates when the band of guard value is increased. The gain in accuracy depends on the simulated error rate *err*, something already expected once the Unique Bitstream generation protocols shall work better with low error rates.

Table 2 describes the simulation results for best slots (BS) protocol. One shall observe that BS protocol presents a better performance when compared to NC and BG protocols. Besides the higher accuracy, its results show a significant gain in throughput. In practice, such performance implies a faster authentication process, once BS protocol requires less physical events to determine *k*.

6. Case Study: Using Radio Signal

6.1. Radio Signals as Physical Events. In this section, we present a practical case study, related to the activities of the National Institute of Metrology, Quality, and Technology (Inmetro), in Brazil. The Inmetro delegates notified bodies to inspect measurement instruments under legal regulation. Such activity, called metrological surveillance, is done in instruments already in use on the field (e.g., scales, fuel pumps). Albeit these measuring instruments are connected to the Internet, surveillance agents (i.e., notified bodies’ technicians) need to go to the instrument’s site for proceeding with a complete visual inspection. So the Inmetro wants to

check the suitability of using physical context to authenticate surveillance agents before granting access to the instrument.

Measuring instruments employed for regulating consumer relations are typically used in places such as supermarkets, stores, shops, and gas stations. Nowadays these places are surrounded by different radio-based communication infrastructures (e.g., WLANs). The radio signal propagation generates physical context information, creating an “electromagnetic fingerprint.” That can be used as evidence of colocation and simultaneity of measuring instruments and surveillance agents. In this case study, we use the signal generated by public IEEE 802.11 wireless (Wi-Fi) networks. The IEEE 802.11 is a well-disseminated network standard and can be easily found in practically any public place.

We see Wi-Fi network packets as physical events. They can be detected and measured by any device using a proper radio in monitoring mode. In our study, the Wi-Fi network is treated as a physical event generator, and not as a communication channel. Thus the authenticating devices are not connected to the Wi-Fi network. Instead, they just use their radios as sensors, receiving Wi-Fi packets as physical context information.

The study case contemplates a measuring instrument *A* and a surveillance agent *B*. Both entities are equipped with Wi-Fi radios and share the same physical context described by the electromagnetic fingerprint of a local Wi-Fi network (Figure 5). At the same time, *M* is a malicious surveillance agent who wants to counterfeit a visual inspection of *A*. The three entities are connected to the Internet, but *A* and *B* do not use their Wi-Fi radio for that. We also assume that *M* has all the capabilities and restrictions described in Section 3.2.

Wi-Fi radios can be configured in monitoring mode and work as sensors. They can “sense” all Wi-Fi traffic and identify different packets with their respective source and destination addresses. Such information constitutes our physical context. We use it for composing a physical event identifier that

FIGURE 5: Using Wi-Fi signals as physical event.

results from the interaction among several connected devices sending Wi-Fi packets in a given moment. Once the network coverage field is limited, only entities placed in this same area at the same time can obtain the event identifier.

6.2. The Physical Event Identifier. We associate the idea of physical context with the Wi-Fi network traffic. Each packet sent by any node in the network is considered a physical event. Since A and B have Wi-Fi radios, they can be configured for monitoring any specific Wi-Fi network channel. Thus they use the Wi-Fi tracing information to determine a physical event identifier.

Firstly, A and B process tracing information by extracting only packets source addresses and timestamps. Source addresses link a physical event with the location where it occurs. Wi-Fi networks are sharply distinguished by their nodes mobility. So one can expect that a public Wi-Fi network will present different nodes (and consequently different addresses) when we compare traces extracted at different moments. We use A and B local clocks to obtain the packets timestamps, which implies that the devices are not synchronized. Timestamps are necessary to know when each node is sending information to the network. Doing that, we can determine time slots by assigning zero when a node does not send any information and one when otherwise. The result is a physical context description that can be analyzed using the Unique Bitstream Generator model already described. Furthermore, such time slots present a nondeterministic pattern once it is hard to predict when a network node will send a packet. A problem emerges due to the *hidden node problem*: A can detect packages from a node which is hidden from B or vice versa. This condition can affect A and B physical event identifiers, compromising authentication. We avoid such problem proposing an additional message interchange which enables A and B to determine a common set of communicating node addresses for extracting their respective physical event identifiers ID_A and ID_B .

The authentication protocol is initiated by B asking A for authentication. After that, A challenges B to present the physical context proof. Both the entities start to collect network traces during a predefined time interval. After

collecting all the traces, A and B will have two similar sets of partial identifiers, given by the following equation:

$$ID_i = \{\langle s_1, t_1 \rangle, \dots, \langle s_k, t_k \rangle, \dots, \langle s_K, t_K \rangle\}, \quad (5)$$

where K is the number of different nodes identified in the Wi-Fi trace, s_k is the k th network node MAC (Media Access Control) address, and t_k is a L -bit binary string corresponding to the frequency distribution of the k th network node signal.

For security reasons, s_k could be obfuscated by any hash function, preventing the disclosure of private information about the Wi-Fi network node. Regardless, our experiment considers the use of a public Wi-Fi network, implying that MAC addresses are public as well.

In turn, t_k is given by the following algorithm:

- (1) Define L slots of time and compute a frequency distribution $F = \{f_1, f_2, \dots, f_L\}$ counting each packet, where the source address corresponds to s_k , using timestamp information.
- (2) Extract a binary L -bits representation, where for each class $l = 1, 2, \dots, L$ in F , the l th bit b_l is given by the Boolean operation $b_l = (f_l > 0)$.
- (3) Do $t_k = \langle b_1, b_2, \dots, b_L \rangle$.

Figure 6 illustrates the proposed algorithm with $L = 16$. Packets from the same source address are sampled in a frequency distribution histogram. One can observe that in subgraphs A and B . Finally, the binary representation showed in graph C is computed as a partial identifier t_k .

Once A and B have their respective partial identifiers ID_A and ID_B , they need to solve the hidden node problem determining the intersection among their known node addresses s_k . Supposing that $Addr_A$ and $Addr_B$ are the subsets containing $\{s_1, \dots, s_K\}$ of ID_A and ID_B , respectively, we propose the following sequence of messages:

$$B \rightarrow A : Addr_B$$

$$A : I = Addr_A \cap Addr_B$$

$$A : s_R \in I \mid R = \text{rand}() \quad (6)$$

$$A \rightarrow B : s_R$$

$$A, B : k = t_R.$$

Although the proposed messages reveal the node addresses chosen to determine the physical event identifier, they do not disclose any information about the selected frequency distribution of t_R . That keeps the authentication protocol secure against an attacker M with capabilities described at Section 3.2.

6.3. Experiment Description. Our experiment is implemented using two computers with different Wi-Fi adapters, simulating A and B devices, respectively. Both computers run Ubuntu 14.04 Linux operating system. Their Wi-Fi interfaces work as sensors, using monitoring mode to gather all Wi-Fi packages traffic.

TABLE 3: Experiment datasets generated for analyzing the proposed authentication mechanism.

Experiment location	Alias	Auth. tries	err
Federal University of Rio de Janeiro	FND	112	6.31%
Starbucks day 1	STB1	141	27.9%
Starbucks day 2	STB2	150	25.5%

FIGURE 6: How t_i is generated from packets tracing information.

An authentication script is triggered at the same time in both computers. The script is responsible for collecting network packets traces for approximately one minute. The trace is obtained invoking Linux `tcpdump` command. No particular filter is used, neither is the kernel modified to drop packets. The experiment does not make use of any mechanism for synchronizing A and B . That is purposeful since we aim to evaluate the method robustness against delays in processing and network signal propagation. After collecting the traces, a second script extracts timestamps and packets source addresses. It also determines each partial identifier t_k , performing the algorithm described in the previous section.

We run the experiment in two different testing environments: (1) a building of research labs at the Federal University of Rio de Janeiro and (2) a Starbucks Coffee located inside a crowded shopping mall at Rio de Janeiro downtown. In the second environment, we perform the simulation on two different days. Therefore we have three different simulation datasets whose details are shown at Table 3. For each one, we describe the number of authentication tries (Auth. tries) and the estimated sensing error err , which means the probability of A and B disagreeing about a physical event binary description (0 or 1).

Just like we did in Section 5, we fixed some parameters for determining the physical event identifiers. We consider the time unit as 0.02 seconds or 20 milliseconds. The time slot corresponds to 10 time units or 200 milliseconds. We obtain 64-bit identifiers ($L = 64$). We keep these values aiming to compare the theoretical simulation results with the practical

study case. In turn, we choose time unit trying to keep the authentication time below 30 seconds.

6.4. Experiment Results. We evaluated the experiment results for both attack scenarios described at Section 3.2. At the first one, k value has only the function of providing colocation and simultaneity evidence. We perform authentication following the same idea found in previous works. Once the communication channel is protected, B can just send his k_B value to A . A evaluates k_A and k_B similarity using a comparison function C and defining an acceptance threshold value Th . Such strategy can be described as follows:

$$C(k_A, k_B) \leq Th. \quad (7)$$

On the other hand, when one analyzes the nonsecure communication scenario, a protected channel can be established if and only if $k_A = k_B$. That imposes a more restrictive accuracy condition. So we evaluate the second scenario first, aiming to determine the accuracy and throughput rates of BG and BS protocols in each dataset.

Table 4 summarizes accuracy (Acc%) and throughput (Thr%) rates for datasets FND, STB1, and STB2 when BG protocol is performed. One shall note that BG works better in FND physical context. Such behavior was expected due to the lower sensing error (err) observed in this dataset. The rates resulted from STB1 and STB2 datasets are low for authentication applications, even when the band of guard is increased in BG protocol. One can note a limit when a larger band of guard decreases accuracy rate. Such results point out

TABLE 4: Case study NC and BG protocols simulation results.

Band	FND dataset		STB1 dataset		STB2 dataset	
	Acc%	Thr%	Acc%	Thr%	Acc%	Thr%
0	62.5	100	15.6	100	16.6	100
1	68.7	96.4	16.3	94.8	18.0	94.9
2	80.3	89.2	31.9	83.6	32.6	83.5
3	91.0	83.3	43.9	70.4	42.6	69.6
4	95.5	68.4	51.0	50.1	48.0	49.4
5	97.3	61.9	46.0	40.2	50.0	38.2

TABLE 5: Case study BS protocol simulation results.

Band	FND dataset		STB1 dataset		STB2 dataset	
	Acc%	Thr%	Acc%	Thr%	Acc%	Thr%
1	69.6	99.6	20.5	99.4	20.6	99.5
2	84.8	99.0	31.9	98.4	39.3	98.5
3	92.8	98.3	52.4	97.2	52.6	97.4
4	95.5	80.0	51.7	75.9	56.6	79.4
5	96.4	67.8	43.9	48.3	50.6	48.1

the need for the best protocols to deal with situations when sensing error is increased.

In turn, Table 5 shows accuracy and throughput rates using BS protocol. One can observe a little increase in accuracy while the gain is expressive in throughput. That was already expected due to the discussed theoretical model properties. However, we found the same BG protocol weakness: accuracy rates are not good enough for authentication in physical contexts where sensing error is higher than 20%.

Now we investigate the authentication in a secure communication scenario. We define an acceptance threshold Th that should increase the proposed authentication mechanism accuracy. At the same time, Th introduces type I and type II errors in our statistical hypothesis testing, both represented by false acceptance rate (FAR) and false rejection rate (FRR). (FAR and FRR are error rates commonly used for evaluating identification algorithms in biometrics. They also can be referenced as false positive rate (FPR) and false negative rate (FNR).) We need to determine the confusion matrix for each specific situation, evaluating how it changes with Th value. We do that by creating fake pairs of identifiers, combining A and B identifiers generated at different moments. Such practice is interesting for analyzing because it also simulates a replay attack. We selected 20 pairs of identifiers generated by both BG and BS protocols from each collected dataset, performing a total of six test cases. For each one of the described tests we experiment different values of threshold Th , aiming to minimize FAR and FRR. For practical reasons, we analyze just the cases associated with BG and BS protocols' best results from nonsecure communication scenario. So we fixed band of guard $Band = 4$.

Figure 7 shows how FRR and FAR change with Th value in each one of the six proposed test cases. These results expose a weak aspect of the proposed mechanism: it presents a high FAR. Consequently, fake pairs of identifiers have a

high probability to be accepted as correct pairs. This behavior is notably in FND dataset tests. One can observe that FAR starts from 0.23 in BG protocol and 0.11 in BS protocol. The test cases related to STB1 and STB2 datasets present better boundary conditions. One can establish a reasonable tradeoff between FRR and FAR. Again, BS protocol presents better results than BG protocol. So we decided to estimate the accuracy increase just for BS, choosing a Th value that keeps FAR below 0.05 (except for FND dataset) and determining our best authentication results according to the metrics in Table 6.

Comparing the results in Table 5 (when $Band = 4$) and Table 6, one can note that the gain using acceptance threshold is not meaningful. Although we can increase accuracy while keeping a low FAR in STB1 and STB2 datasets, precision and recall rates indicate an enhancement no more than 10% in successful authentication cases.

7. Conclusions

This work presented a comprehensive study of physical context-based authentication. Such context information is usually available in ubiquitous modern systems due to the integration of physical processes and information technologies. We explored this asset proposing an authentication mechanism for entities that share the same physical context. We evaluated two different approaches, according to the assumptions about the communication channel. The main contributions are the model for generating a Unique Bitstream using physical events and the two key agreement protocols BG and BS. They can be used for establishing a secure communication channel and protecting authentication processes against external attackers. We also developed the probabilistic analysis, simulation and presented a practical case study. The results are promising since they

TABLE 6: Authentication performance rates for BS protocol with different Th values.

	FND/Th = 0		STB1/Th = 9		STB2/Th = 2	
	OK	NOK	OK	NOK	OK	NOK
Correct ID	17	3	13	7	11	9
Fake ID	21	169	9	181	8	182
FRR		0.15		0.35		0.45
FAR		0.11		0.047		0.042
Precision		0.447		0.59		0.578
Recall		0.85		0.65		0.55
Accuracy		88.5%		92.3%		91.9%

FIGURE 7: FRR and FAR for scenario RS attack with different Th values.

indicate that our contributions are suitable for practical applications.

We also point out two main weaknesses in our study. The first one is the need for a low error rate in physical context description. Simulation and practical experiments with an error rate around 5% showed good results. On the other hand, real datasets with an error rate higher than 20% resulted in insufficient accuracy for practical applications

in authentication. The second deficiency is the high false acceptance rate FAR. Such result suggests that the generated secret keys present low entropy. That raises the risk of collisions in key generation and consequently compromises security.

Our next steps will include new case studies as well as the development of new alternatives to deal with the drawbacks above. We intend to apply our authentication

mechanisms in different practical cases involving manufacturing, transportation, and smart grids; see Section 2.4. We also foresee some strategies for improving our Unique Bitstream protocols. They include the merge with some ECCs features and zero-interaction authentication approaches.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The present research was partially supported by FAPERJ (JCNE E-26/201.551/2014) and by CNPq (Universal 421007/2016-8).

References

- [1] M. A. Simplicio Jr., B. T. De Oliveira, C. B. Margi, P. S. L. M. Barreto, T. C. M. B. Carvalho, and M. Näslund, "Survey and comparison of message authentication solutions on wireless sensor networks," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1221–1236, 2013.
- [2] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *Institute of Electrical and Electronics Engineers Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.
- [3] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC '15)*, pp. 1–6, IEEE, San Francisco, Calif, USA, June 2015.
- [4] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and Privacy in Cyber-Physical Systems: A Survey of Surveys," *IEEE Design and Test*, vol. 34, no. 4, pp. 7–17, 2017.
- [5] K. Islam, W. Shen, and X. Wang, "Wireless sensor network reliability and security in factory automation: a survey," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 42, no. 6, pp. 1243–1256, 2012.
- [6] M. Durrezi, A. Durrezi, and L. Barolli, "Secure Inter Vehicle Communications," in *Proceedings of the 2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)*, pp. 177–183, Palermo, Italy, July 2012.
- [7] K. Han, S. D. Potluri, and K. G. Shin, "On authentication in a connected vehicle," in *Proceedings of the the ACM/IEEE 4th International Conference*, p. 160, Philadelphia, Pennsylvania, April 2013.
- [8] J. Han, M. Harishankar, X. Wang, A. J. Chung, and P. Tague, "Convoy: Physical context verification for vehicle platoon admission," in *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications, HotMobile 2017*, pp. 73–78, USA, February 2017.
- [9] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.
- [10] A. C.-F. Chan and J. Zhou, "Cyber-Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1509–1517, 2014.
- [11] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: issues, challenges and counter-measures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.
- [12] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-Heart (H2H): Authentication for Implanted Medical Devices," in *Proceedings of the 2013 ACM SIGSAC conference on Computer communications security - CCS 13*, pp. 1099–1112, 2013, <http://dl.acm.org/citation.cfm>.
- [13] K. Habib and W. Leister, "Context-Aware Authentication for the Internet of Things," in *Proceedings of the in International Conference on Autonomic and Autonomous Systems Context-Aware*, pp. 134–139, 2015.
- [14] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.
- [15] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, "Using contextual co-presence to strengthen Zero-Interaction Authentication: Design, integration and usability," *Pervasive and Mobile Computing*, vol. 16, pp. 187–204, 2015.
- [16] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani, "Context-based zero-interaction pairing and key evolution for advanced personal devices," in *Proceedings of the 21st ACM Conference on Computer and Communications Security, CCS 2014*, pp. 880–891, USA, November 2014.
- [17] M. Juuti, C. Vaas, I. Sluganovic, H. Liljestrand, N. Asokan, and I. Martinovic, "STASH: Securing Transparent Authentication Schemes Using Prover-Side Proximity Verification," in *Proceedings of the 14th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2017*, USA, June 2017.
- [18] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall, "Securing wireless communications of the internet of things from the physical layer, an overview," *Entropy*, vol. 19, no. 8, article no. 420, 2017.
- [19] B. Shrestha, N. Saxena, H. T. T. Truong, N. Asokan, and N. Asokan, "Drone to the rescue: Relay-resilient authentication using ambient multi-sensing," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 8437, pp. 349–364, 2014.
- [20] N. Karapanos, C. Marforio, C. Soriente, and S. Capkun, "Sound-proof: usable two-factor authentication based on ambient sound," in *Proceedings of the 24th USENIX Conference on Security Symposium (SEC '15)*, pp. 483–498, 2015, <http://dl.acm.org/citation.cfm>.
- [21] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Authentication Based on," in *Proceedings of the 5th International Conference, Pervasive 2007*, pp. 144–161, 2007.
- [22] F.-J. Wu, F.-I. Chu, and Y.-C. Tseng, "Cyber-physical handshake," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, p. 472, 2011.
- [23] L. C. Priya and S. D. Patil, "A Survey on Sensor Authentication in Dynamic Wireless Sensor Networks," in *Proceedings of the International Journal of Computer Science and Information Technology Research*, vol. 2, pp. 454–461, 2014.
- [24] D. Adrian, K. Bhargavan, Z. Durumeric et al., "Imperfect forward secrecy: How diffie-hellman fails in practice," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS 2015*, pp. 5–17, USA, October 2015.

- [25] J. E. Bandram, R. E. Kjær, and M. Ø. Pedersen, "Context-Aware User Authentication – Supporting Proximity-Based Login in Pervasive Computing," in *UbiComp 2003: Ubiquitous Computing*, vol. 2864 of *Lecture Notes in Computer Science*, pp. 107–123, Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.
- [26] Z.-L. Gu and Y. Liu, "Scalable group audio-based authentication scheme for IoT devices," in *Proceedings of the 12th International Conference on Computational Intelligence and Security, CIS 2016*, pp. 277–281, chn, December 2016.
- [27] A. Zoha, A. Gluhak, M. A. Imran, and S. Rajasegarar, "Non-intrusive load monitoring approaches for disaggregated energy sensing: a survey," *Sensors*, vol. 12, no. 12, pp. 16838–16866, 2012.
- [28] D. Gafurov, E. Snekenes, and P. Bours, "Gait authentication and identification using wearable accelerometer sensor," in *Proceedings of the 2007 IEEE Workshop on Automatic Identification Advanced Technologies, AUTOID 2007*, pp. 220–225, Italy, June 2007.
- [29] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and classification," *International Journal of Biometrics*, vol. 1, no. 1, pp. 81–113, 2008.
- [30] A. Scannell, A. Varshavsky, A. LaMarca, and E. de Lara, "Proximity-based authentication of mobile devices," *International Journal of Security and Networks*, vol. 4, no. 1-2, pp. 4–16, 2009.
- [31] S. Mathur, A. Reznik, C. Ye et al., "Exploiting the physical layer for enhanced security," *IEEE Wireless Communications Magazine*, vol. 17, no. 5, pp. 63–70, 2010.
- [32] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577–601, 2016.
- [33] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Security and Communication Networks*, vol. 8, no. 2, pp. 332–341, 2015.
- [34] C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, and T. Güneysu, "Information reconciliation schemes in physical-layer security: A survey," *Computer Networks*, vol. 109, pp. 84–104, 2016.
- [35] C. Miller and C. Valasek, "Adventures in Automotive Networks and Control Units," in *Proceedings of the DEF CON 21*, vol. 21, pp. 260–264.
- [36] W.-L. Chin, Y.-H. Lin, and H.-H. Chen, "A Framework of Machine-to-Machine Authentication in Smart Grid: A Two-Layer Approach," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 102–107, 2016.
- [37] R. W. Uluski, "VVC in the smart grid era," in *Proceedings of the IEEE PES General Meeting, PES 2010*, USA, July 2010.
- [38] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Computing Surveys*, vol. 39, no. 1, Article ID 1216373, 2007.
- [39] M. Mitzenmacher and E. Upfal, *Probability and computing*, Cambridge University Press, Cambridge, 2005.
- [40] A. Rukhin, J. Sota, J. Nechvatal et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Special Publication NIST 800-22, National Institute of Standards and Technology, 2010.