New Directions: Proof-Carrying Sensing – Towards Real-World Authentication in Cyber-Physical Systems

Min Wu
University of Maryland, College Park
minwu@umd.edu

Fernando M. Quintão Pereira
UFMG, Brazil
fernando@dcc.ufmg.br

Jie Liu
Microsoft Research
jie.liu@microsoft.com

Heitor S. Ramos
UFAL, Brazil
heitor@ic.ufal.br

Mário S. Alvim
UFMG, Brazil
msalvim@dcc.ufmg.br

Leonardo B. Oliveira
UFMG, Brazil
leob@dcc.ufmg.br

ABSTRACT

It is paramount to ensure secure and trustworthy operations in Cyber-Physical Systems (CPSs), guaranteeing the integrity of sensing data, enabling access control, and safeguarding system-level operations. In this paper, we address trustworthy operations of next generation CPSs. Our idea is inspired by a trustworthy computing framework known as *Proof-Carrying Code*, in which foreign executables carry a model to prove that they have not been tampered with and they function as expected. In our context, we leverage the physical world–a channel that encapsulates properties impossible to tamper with remotely, such as proximity and causality–to create a challenge-response function. We call it *Proof-Carrying Sensing* and use it to help authenticate devices, collected data, and locations. A unique advantage of this approach, vis-à-vis traditional multi-factor or out-of-band authentication mechanisms, is that authentication proofs are embedded in sensor data and can be continuously validated over time and space without resorting to complicated cryptographic algorithms. This, in turn, makes it fit particularly well to CPSs where mobility and resource constraints are common.

CCS CONCEPTS

• **Security and privacy** → **Authentication**; • **Computer systems organization** → *Embedded and cyber-physical systems*;

KEYWORDS

Cyber-Physical Systems, Security, Information Forensics

ACM Reference format:
Min Wu, Fernando M. Quintão Pereira, Jie Liu, Heitor S. Ramos, Mário S. Alvim, and Leonardo B. Oliveira. 2017. New Directions: Proof-Carrying Sensing – Towards Real-World Authentication in Cyber-Physical Systems. In *Proceedings of SenSys '17, Delft, Netherlands, Nov. 6–8, 2017,* 6 pages.
DOI: 10.1145/3131672.3131700

1 INTRODUCTION

Cyber-Physical Systems (CPSs) [1–3] are becoming part of our daily life and have the potential to redefine human capabilities. As sensors and actuators, potentially belonging to different people and organizations, are connected and orchestrated to create increasingly complex and autonomous behaviors, the trustworthiness of remote data and commands directly contribute to the safety and correctness of the overall system.

CPSs call for tailor-made authentication schemes [4, 5]. Current CPS authentication schemes are typically borrowed from human-machine authentication paradigms originated from user access control. Examples are username/password pairs, biometrics, or their combinations to create multi-factor authentications. Once the user is authenticated, all their actions are considered legitimate. These schemes have two fundamental problems. The first is password management. CPS involves machine-machine interactions at large scale and in mobile environments, potentially over many administrative domains. Robots, autonomous vehicles, and wearable devices may discover new devices in their journey that they must collaborate with. A smart environment must authenticate the occupants it encounters. Dealing with cross domain authentication mechanisms and policies is a major scalability challenge. The second and more challenging problem is data integrity. Traditional authentication is primarily a cyber-space activity. Authorized data access does not provide any proof of the correctness of the data. Even if a device is physically moved, a compromised sensor produces wrong data, or a compromised actuator ignores remote commands, there is no way for the authentication system to validate.

As a new research direction, we propose the investigation of novel authentication mechanisms to address the challenges of machine-machine authentication in CPS. Our view stems from two main facts. First, the behavior of CPSs heavily depends on the veracity and timeliness of data collected by sensors belonging to different administrative domains. Second, the physical world connects sensors, actuators, and background noise; and encapsulates properties virtually impossible to be replicated exactly or tampered with remotely (e.g. proximity and causality). We believe that it is possible to leverage the physical world and transform the sensing process itself into a challenge-response function, as opposed to performing primarily cyber domain challenge-response and authentication as in the past. We call it *Proof-Carrying Sensing* (PCS) as it uses sensing data to authenticate the sensor, time, and place of the collection. Figure 1 provides a general view of our idea.

SenSys '17, Delft, Netherlands
© 2017 ACM. 978-1-4503-5459-2/17/11…$15.00
DOI: 10.1145/3131672.3131700

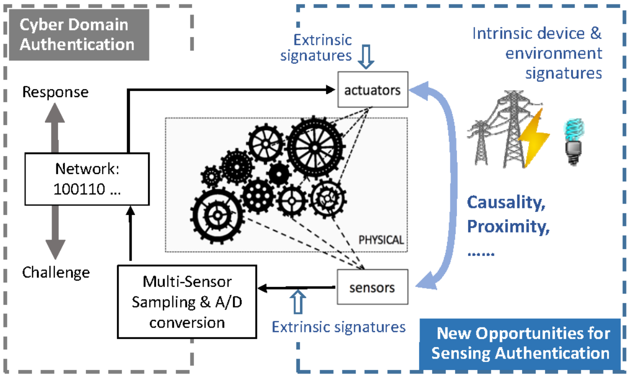

Cyber Domain Authentication
Response
Network: 100110 ...
Challenge
Multi-Sensor Sampling & A/D conversion
Extrinsic signatures
actuators
PHYSICAL
sensors
Extrinsic signatures
Intrinsic device & environment signatures
Causality, Proximity, ...
New Opportunities for Sensing Authentication

Figure 1: The proposed Proof-Carrying Sensing framework and new opportunities for sensing authentication in CPSs.

Our PCS idea draws inspiration from the concept of *Proof-Carrying Code* [6]. As its name suggests, Proof-Carrying-Code is a technique by which a program (code) carries proof of its own trustworthiness. The technique enables safe execution of arbitrary code, i.e., the code whose origin is potentially untrusted. Proof-Carrying Code has been fundamental to the construction of trustworthy agents in the distributed systems world [6]. Here, we take this idea one step further, transposing its basic principles to the physical world.

After explaining the basic principles behind Proof-Carrying-Sensing in Section 3, we describe representative scenarios in Section 4 and the many challenges involved in the implementation of the PCS framework in Section 5. These challenges include practical and theoretical problems. On the practical side, we need to choose and manipulate physical data that can be used to build reliable challenge-response systems. On the theoretical side, it remains to formalize PCS, for instance, determining acceptable bounds within which physical data can be reliably used.

In terms of related work, physical data has already been used for authentication. The field of biometrics, for instance, relies on an individual's certain physical attributes being difficult to reproduce artificially. Likewise, previous work demonstrated that the same applies to electronic devices [7–11]. However, the past research has not fully benefited from a self-evident observation: individuals and devices are immersed in a sea of physical data, which varies in time and space. Such data provides unique information, which can potentially be used as proof of legitimacy across very different scenarios. Our ideas diverge from the past work in that our proposed authentication proofs are embedded in sensor data, and analog signals are leveraged to authenticate not only senders and data, but also other aspects of the sensing context, such as the location and the occasion when an event happens. This approach can be relatively lightweight and fits well into CPSs, where mobility and resource constraints are common.

2 THE NEED FOR NEW APPROACHES

At present, most perceived need for authentication methods tailored to CPSs relies on cryptographic techniques. Even though they are necessary to secure CPSs, cryptographic schemes alone have limitations in several aspects, including i) providing a holistic authentication mechanism to address the authentication of user, content, and time/location aspects; and ii) performing lightweight operations enough to be run on top of severely limited devices.

Typically, cryptosystems consider two primary classes of authentication: source and data [12]. Source authentication guarantees a receiver that the message indeed originated from the claimed sender. Data authentication, in turn, ensures integrity plus liveness and hence prevents in-transit message violations and replay-attacks, respectively. Nonetheless, it is worth noting that, when it comes to CPSs, mechanisms for source and data authentication–when used without further support–are unable to fulfill a complete set of security requirements.

Highly resource-constrained devices may not be able to rely on cryptography for protection [13]. Although lightweight cryptography (such as Elliptic Curve Cryptography) can be used to add security properties onto resource-poor systems, there are a broad spectrum of devices, such as light bulbs, which are still unguarded by these schemes. This vulnerability exists because many devices often cannot afford to run cryptography operations appropriately such as for cases in [14]. At the first glance, we could embed more processing power or built-in hardware-based security on those devices as a workaround for this problem. This extra capacity, however, may impact their retail price or their energy footprint. Thus it is essential to develop an authentication mechanism that is feasible by the most resource constrained hardware while at the same time preserving its low-cost and dependability.

Furthermore, the security of current authentication schemes is at stake in the long-run [15]. Traditional cryptosystems have been scrutinized by industry and academia for a while. Yet, cryptanalytic advances (e.g., the work of Barbulescu *et al.* [16]) continue to point out vulnerabilities of existing cryptosystems. Hence, it is imperative to develop authentication mechanisms that can complement what is widely deployed today.

In short, it is paramount to propose solutions that can effectively satisfy the CPS requirements. More specifically, it is necessary to encompass more aspects of the CPS context and, thus, authenticate information like time and location of the data processed. Also, it is important to develop a solution well-suited for resource constrained devices, i.e., devices that are not solely dependent on time-consuming operations as those present in some cryptographic schemes. It is our view that such actions will ensure the long-term security of CPS authentication schemes.

3 PROOF-CARRY SENSING FRAMEWORK

Our notion of PCS authentication mechanism for CPS is that two or more devices closely located can use physical data available locally to establish a mutual trust. As we shall see, these data can be intrinsic to the physical environment (e.g., temperature, luminosity, noise, electrical frequency), or extrinsic to it, in the sense that they are actively injected by the device into the physical world. By monitoring the propagation of intrinsic or extrinsic data, a device can confirm its reception by other devices located within its vicinity. The design and secure implementation of such protocols involves the orchestration of combined expertises such as signal processing, statistical detection and learning, cryptography, software engineering, and electronics. Next, we present the apparatus (Section 3.1) and the vision (Section 3.2) of our PCS framework.

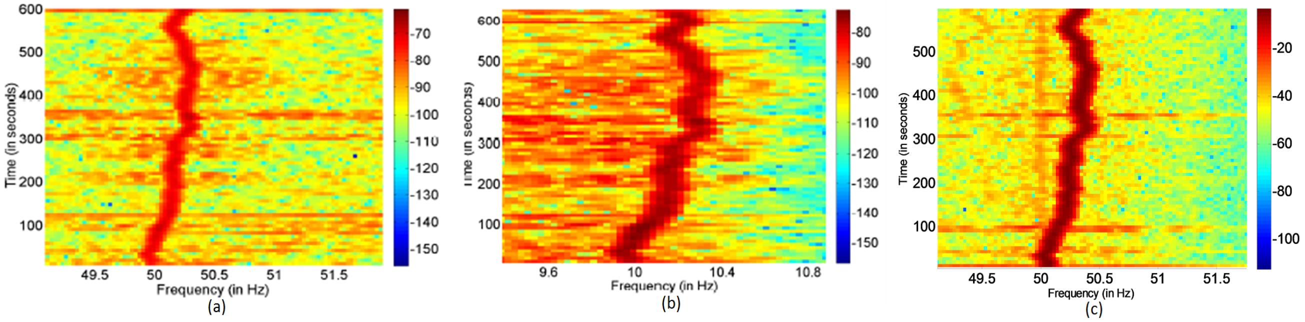


Figure 2: Spectrogram showing ENF signals in concurrent recordings of (a) audio, (b) visual, and (c) power main. Cross-correlation study can show similarity between media and power line reference at different time lags, where a strong peak appears at the temporal alignment of the matching grid.

3.1 Intrinsic and Extrinsic Signatures

Intrinsic Signatures. Intrinsic Signatures are signatures inherent to devices, channels, and sensing environments in the physical world. Some past research (e.g.,[17]) has exploited those invisible but detectable signatures on images, video, and sound recordings. We envision that intrinsic signatures can be applied to much broader sensing scenarios and form a strong basis to develop novel authentication mechanisms in machine-to-machine and human-to-machine interactions and, ultimately, our PCS framework. For instance, we can exploit intrinsic signatures to discover characteristics of the capturing devices and processing channels, and use such characteristics for authentication.

Consider, for example, an intrinsic signature of power grids. The electric network frequency (ENF) is the supply frequency of power distribution grids; it has a nominal value of 60 Hz (North America) or 50 Hz (Europe). The instantaneous ENF usually fluctuates around its nominal value due to the dynamic interplay between load variations and control mechanisms for power generation in the grid. These variations are nearly identical in all locations of the same grid at a given time due to the interconnected nature of the grid. We refer to the changing values of instantaneous ENF over time as an ENF signal. The ENF signal can be intrinsically captured by audio/visual recordings (Figure 2) or other sensors [18]. This has led to several emerging forensic applications based on the use of ENF signals, such as validating the time-of-recording of an ENF-containing multimedia signal and estimating its recording location using concurrent reference signals from power grids.

In addition to the micro-signal signatures associated with the sensing environment, sensing devices also carry unique intrinsic traces. These may be in the form of inherent noise in the sensors that can be learned, such as physical or electronic randomness as a form of Physical Unclonable Functions (PUFs); or as some ensemble properties that can be verified, such as color handling in image sensors, and various statistical properties of sensing noises [19].

Extrinsic signatures. Extrinsic signatures are signals and data that can be injected and monitored by a system. These signatures can be in the form of physical-layer watermarks, of physical- or digital-layer pilot sequences, or of challenges. Extrinsic signatures can have their injection guided by a cross-layer system modeling or cryptographically random number generation [20]. Figure 3 shows an example how extrinsic signatures identify the malicious behavior of relay nodes.

We can inject extrinsic signatures with known values into a CPS. Either by design or by proactive learning, we would establish and verify the expected outcome of these signatures. A deviation from such an outcome indicates a potential abnormality. A primary research challenge is how to efficiently characterize the expected outcome of extrinsic signatures, and to assess the capability to discriminate between normal and abnormal behaviors vis-à-vis different locations and forms of injection.

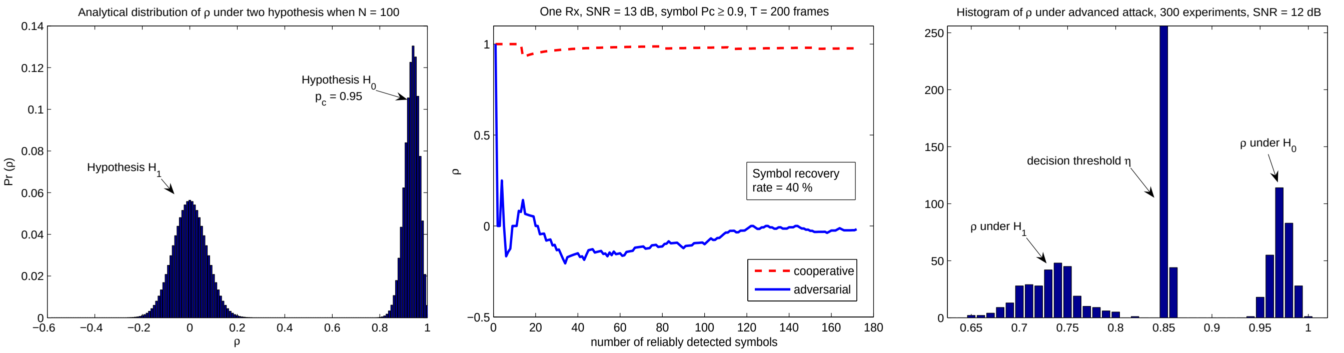
By way of example, consider the recent work by Satchidanandan and Kumar [21]. They developed a notion of watermarking in a cyber-physical system, which can be viewed as a class of extrinsic signatures. If an actuator injects into the system a properly designed probing signal that is unknown *a priori* to other nodes in the system, then based on the knowledge of the cyber-physical system's dynamics and other properties, the actuator can examine the sensors' report about the signals at various points, and can potentially infer whether there is malicious activity in the system or not, and if so, where and how.

Next, we present our vision of a new framework by orchestrating digital, extrinsic, and intrinsic signatures.

3.2 Vision

Proof-Carrying Sensing (PCS) is an innovative authentication framework for CPSs. As we mentioned in Section 2, one of the motivations for our PCS is the lack of validations in the time and location of data generation. So far, there is insufficient information to answer such questions as "is the sensing data coming from where it is claimed to be," or "was the sensing data collected when it is declared to be?" Tracing IP addresses and routing can be relatively easily circumvented by anonymization and proxies; and GPS-based localization is not always available, especially in indoor settings. The ability to provide some form of the location proof, even at a coarse level, can be helpful in detecting fraud and mitigating attacks.

Our key insight is to use the concept of *Proof-Carrying Code* [6] as inspiration for our solution, where a program (code) carries proof of its trustworthiness. Proof-Carrying Code has been fundamental to the construction of trustworthy agents in the distributed system



(a) (b) (c)

Figure 3: An example of injecting pseudo-random tracing symbols for relay-node authentication in cooperative wireless communications [20]. (a) The distribution of detection statistic ρ for N = 100 tracing symbols measuring the normalized similarity between observed tracing symbols and the ground truth, where the expected value of ρ is zero under adversarial relay (H1 hypothesis) and approaches one for cooperative relay (H0 hypothesis); (b) One realization of sequentially computed ρ as the number of reliably detected symbols grows; (c) histogram of ρ under partial-corruption attack by a sophisticated adversarial relay node, leading to an increased mean ρ value under attack.

world. In order to take this idea one step further to transpose its basic principles to the physical world, we have carried out preliminary studies discussed in the previous subsection, which suggest the benefit of utilizing intrinsic, extrinsic, and digital signatures in designing PCS. An important step along the new direction is to investigate these three mechanisms, with their pros and cons compared qualitatively and quantitatively, and synergies explored.

We envision a PCS framework that strategically uses the digital, extrinsic, and intrinsic signatures with the right mix in the authentication process. For instance, lightweight digital signatures will provide access control, protection against malicious outsiders, and source plus data authentication. Extrinsic signatures will serve as an alternative or complement to digital signatures, especially for nodes that cannot afford to compute cryptographic primitives. And intrinsic signatures will supply the network with ways of authenticating not only source and data but also time and location of data collection. A unique advantage of this approach, in comparison to traditional multi-factor or out-of-band authentication mechanisms today, is that the authentication proofs are embedded in sensor data. The data, in turn, can be continuously validated over time and space without resorting to complex and resource-consuming cryptographic operations. We believe this combination fits particularly well for CPS where mobility and resource constraints are typical.

A PCS modus operandi is as follows, utilizing major components shown earlier in Figure 1. The cyber system generates both digital and extrinsic signatures, uses them to secure outgoing messages, and sends the messages to its physical counterpart via actuators. The same physical system supplies the cyber one with sensing data containing inherent, intrinsic signature(s). Next, the cyber system verifies all classes of signatures, cross-check results, and then based on the application's needs and set-up, provides decision-making information to the human users as appropriate. Last, users reason about the information and decide whether they should take action.

4 REPRESENTATIVE SCENARIOS

Our proposed PCS framework can be used in a varied range of scenarios in which data from the physical world is available as an authentication mechanism. We describe in this Section three representative situations in which our proposed idea could improve security: namely, e-voting, transportation, and shopping. These scenarios provide compelling illustrations of our ideas, although there are many other scenarios that can benefit from PCS.

e-Voting. Electronic elections are becoming more common in many democracies in the world. In 2004, 28.9% of the registered voters in the United States used some type of direct recording electronic voting system, up from 7.7% in 1996. In Brazil, 100% of all the votes are collected electronically, using the device seen in Figure 4. Given the current scale of such elections, and the increasing adoption of electronic voting, it is essential to ensure the dependability of this process. Today, electronic election systems typically require a voter to be physically close to the voting machine to participate in the ballot. Usually, the identity of voters is checked by human referees. However, a combination of biometric and physical data could be used for the same purpose. Biometric information ensures the identity of electors, and physical data, such as the ambient sound or luminosity, provide a further guarantee that they are present at the voting site. To implement the authentication procedure, a micro-chip in the elector's ID can send physical data that it reads on-site to a verification hardware in the voting machine.

Transportation. The second area that could greatly benefit from PCS is the design and implementation of dependable vehicular systems. Physical data can be used to make autonomous transportation safer from adversaries. For instance, Miller and Valasek recently demonstrated that attackers could hijack control from a moving car [22]. Physical data, such as temperature or vibration in the direct vicinity of a vehicle, could be used to prevent this kind of exploitation, ensuring that only the driver–who is inside the vehicle–

Figure 4: 112,683,879 Brazilians in 2014 used a Direct-Recording Electronic Voting Machine in the second round of presidential elections. (Image Source: WikiCommons).

Figure 5: Self-checkout systems are becoming a common trend. PCS can be used–in a cashier-less shop–to grant users access into restricted areas. Physical data available locally might be used as the authentication key. The origin of this data can be natural, or artificial, such as low-frequency noise or infra-red radiation. (Image Source: WikiCommons).

has enough credentials to steer it. Therefore, PCS techniques raise the bar for attacks such as those performed by Miller and Valasek, because it forces attackers to either be physically close to a moving target, or be able to emulate environment conditions in the vicinities of that target.

Shopping. Automatic retail, such as the recent pilot of Amazon Go[1], is another example in which PCS is appealing. Such a cashier-less grab-and-go retail paradigm offers users a fully automated shopping experience. This kind of automated shopping requires users to be physically inside the store, and we can use environment data, such as sound, luminosity or temperature, to ensure that the owner of the electronic ID is on site. This can help shield both the client's and the shopkeeper's interests from fraudulent buying/selling activities.

As an example, consider the following scenario: a shopper wants to access an age-limited area that sells alcohol. There is a barcode at the door that the shopper needs to scan using the store app to gain authentication in the cloud. A database in the cloud validates the user's age; hence, opening the door. Assume a particular shopper physically present at the store is underage, but has a remote, malicious, friend who has installed the same app and owns an account with the appropriate age for access to alcohol. The in-store shopper can take a picture of the barcode and send it to his remote friend, who has it displayed on one device and uses the store app to scan the image. Without a proper authentication mechanism, the door in the store will open, giving the under-aged shopper access to alcohol. It is our vision that such attacks as this one can be prevented by using the physical world as an authentication channel. In this case, PCS can use such signals as background noise or luminosity, which are unique to that environment, to enforce authentication. PCS can also be actively created at the store. Similar its intrinsic counterparts, this extrinsic signal can be captured only if the sensor is present in the actual location and at the right time.

5 CHALLENGES AHEAD

The development of PCS will require both solid theoretical foundations and effective implementation via appropriate software methodologies. This section addresses theses challenges.

Suitable Physical Signatures. A key research problem is to characterize suitable intrinsic and extrinsic signatures, to support the construction of reliable challenge-response functions to authenticate sensing data in CPS. Although some qualitative properties of such signatures are known, it is important to develop quantitative models to characterize the normal and abnormal behavior of CPS. The exploration of physical models might yield analytic approximations of such properties. And data-driven learning approaches can be used to gather statistical data characterizing normal and abnormal behaviors. From this data and its statistics, a natural step is to develop metrics to assess the appropriateness of a given signature in authenticating CPS. For example, we can use probabilistic characterizations to compute the corresponding entropy or entropy rate to provide a solid ground on the posterior uncertainties, thus inferring the trustworthiness in authentication.

Formal Model and Certification. The implementation of any expressive method to formalize PCS will require the expertise of theoreticians and engineers. In particular, researchers must ensure that authentication mechanisms based on local physical information are sound. A natural implementation of PCS compares the attributes of the physical world to what is known about incoming certificates. Since we are dealing with physical, continuous information, small variations between the expected and received certificates should be accepted, as long as they fit within a given threshold of trust. Determining the degree of tolerance and the thresholds that such degrees imply are a major challenge that must be solved when implementing PCS. Probability theory and algebra techniques can be useful tools to address these questions. For instance, similar to the design of robust hash in other context [23], we can describe a *physical data vector* as a set of ordered data from the natural world, such as sound, light and temperature. Beneficial insights may also be taken from the robust hashing techniques of multimedia [23].

Safeguarding Physical Data. A design of PCS must ensure that the physical data being utilized do not leak out from the network of trust; otherwise, an adversary who can read the physical data in real time from a target node would be equivalent to an adversary who can read a secret password stored in that node itself. Although the importance of securing passwords is well understood, physical data might be shared among the many devices that constitute a federation of sensors and may not be easy to safeguard. The software security community relies on the information flow framework [24]

[1] https://www.amazon.com/b?node=16008589011#

to preserve the confidentiality of data. In the mean time, we should recognize the new challenge in PCS in terms of the amount of data that must be secured and the real-time constraints of such systems. For instance, a formalization of PCS must be aware of time, because old physical data might not need to be secured, depending on system requirements. In this regard, the Temporal Logic [25] can be a starting point towards the formalization of PCS.

Computational Complexity. The performance of PCS also demands the support of formal methods. It is desirable that researchers be able to establish complexity results for the certification, schemes, or mechanisms that shall constitute this authentication framework. These analytical results should be expressive enough to model the execution time, storage space and energy consumption. This line of investigation faces important challenges because it deals with distributed algorithms meant to run in low-power devices. Furthermore, these algorithms have an online and adaptive behavior by nature, and certification is only possible when sufficient physical data becomes available and communicating devices are sufficiently close. To deal with said issues, researchers can have recourse to a rich literature on on-line [26] and real-time [27] algorithms.

Dependable Software Engineering. The immediate question that must be addressed along this path is which tools developers should use to implement, test, and deploy this certification mechanism. The current CPS networks are usually programmed in more than one language–a phenomenon known as *polyglot programming*. A common setup involves, for instance, *C* together with such scripting language as Lua or Python. Should we provide libraries in different languages, or should we create a domain specific language to address this problem? Furthermore, given that such systems are meant to be widely deployed and used, we expect tools that make it possible for ordinary programmers, not necessarily experts in software security, to use them. This "democratization" is possible only in the presence of a suitable infrastructure for implementing, testing and deploying certifications based on physical data. In particular, we believe that simulators should be implemented to ease the effort of testing this kind of certification protocol.

6 CONCLUDING REMARKS

In this paper, we reviewed pressing challenges regarding the trustworthiness of CPSs; in particular, the severe limitations of current authentication schemes regarding resource consumption, usability, and scalability. Using the scenarios from e-voting, transportation, and automatic retail, we illustrated the need for alternative schemes to the current password- and biometric-based authentication.

We proposed the framework of Proof-Carrying Sensing (PCS) for authentication on CPSs. The PCS' main premise is that signals from the physical environment of a system can serve as signatures to validate devices, collected data, and locations. PCS has two main advantages over existing approaches: (i) physical signatures are virtually impossible to fake; and (ii) it may require less computational resources. We presented a general PCS framework, discussing key challenges we envision for its implementation, including determining whether a physical signal is suitable as a signature, avoiding leaks of sensitive information, and ensuring performance in low-resource devices. We also discussed ways to ensure PCS is an accessible, usable framework in practice.

The success of CPSs depends on innovative solutions to ensure their trustworthiness. The task is challenging, and demands expertise from diverse areas. We believe that the PCS framework outlined in this paper—together with the accompanying systematic identification of key challenges for its implementation—constitutes a promising innovative approach to the problem. We hope this new direction paper can motivate experts from diverse areas to engage in the search for PCS-based solutions for trustworthiness in CPSs.

ACKNOWLEDGMENTS

The work was partially funded by NSF, CNPq, CAPES, and FAPEMIG.

REFERENCES

[1] E. A. Lee. Cyber physical systems: Design challenges. In *ISORC*, 2008.
[2] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic. Cyber-physical systems: The next computing revolution. In *Design Automation Conference*, pages 731–736, 2010.
[3] G. Schirner, D. Erdogmus, K. Chowdhury, and T. Padir. The future of human-in-the-loop cyber-physical systems. *Computer*, 46(1):36–45, 2013.
[4] Alvaro Cardenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, and Shankar Sastry. Challenges for securing cyber physical systems. In *Workshop on future directions in cyber-physical systems security*, page 5, 2009.
[5] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta. Ensuring safety, security, and sustainability of mission-critical cyber-physical systems. *Proceedings of the IEEE*, 100(1):283–299, 2012.
[6] George C. Necula. Proof-carrying code. In *POPL*, pages 106–119, 1997.
[7] Masoud Rostami, Ari Juels, and Farinaz Koushanfar. Heart-to-heart (h2h): authentication for implanted medical devices. In *CCS*, pages 1099–1112, 2013.
[8] J. Han, Y. Lin, A. Perrig, and F. Bai. MVSec: Secure and easy-to-use pairing of mobile devices with vehicles. In *WiSec*, pages 51–56, 2014.
[9] A. Das, N. Borisov, and M. Caesar. Do you hear what I hear?: Fingerprinting smart devices through embedded acoustic components. In *CCS*, pages 441–452, 2014.
[10] Lin Yang, Wei Wang, and Qian Zhang. Secret from muscle: Enabling secure pairing with electromyography. In *SenSys*, pages 28–41, 2016.
[11] L. Guan, J. Xu, S. Wang, X. Xing, L. Lin, H. Huang, P. Liu, and W. Lee. From physical to cyber: Escalating protection for personalized auto insurance. In *SenSys*, pages 42–55, 2016.
[12] Antonio L. Maia Neto, Artur L. F. Souza, Italo Cunha, Michele Nogueira, Ivan Oliveira Nunes, Leonardo Cotta, Nicolas Gentille, Antonio A. F. Loureiro, Diego F. Aranha, Harsh Patil, and Leonardo B. Oliveira. AoT: Authentication and access control for the entire iot device life-cycle. In *SenSys*, 2016.
[13] Eyal Ronen, Colin O'Flynn, Adi Shamir, and Achi-Or Weingarten. IoT goes nuclear: Creating a zigbee chain reaction. Cryptology ePrint Archive, 2016.
[14] Sindhu Karthikeyan and Mikhail Nesterenko. RFID security without extensive cryptography. In *SASN*, pages 63–67, 2005.
[15] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. *Post Quantum Cryptography*. Springer Publishing Company, Incorporated, 1st edition, 2008.
[16] R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *Eurocrypt*, volume 8441, pages 1–16, 2014.
[17] R. Garg, A. Hajj-Ahmad, and M. Wu. Geo-location estimation from electrical network frequency signals. In *ICASSP*, pages 2862–2866. IEEE, 2013.
[18] Catalin Grigoras. Applications of ENF analysis in forensic authentication of digital audio and video recordings. *Journal of the Audio Engineering Society*, 57(9):643–661, 2009.
[19] Matthew C Stamm, Min Wu, and KJ Ray Liu. Information forensics: An overview of the first decade. *IEEE Access*, 1:167–200, 2013.
[20] Yinian Mao and Min Wu. Tracing malicious relays in cooperative wireless communications. *TIFS*, 2(2):198–212, 2007.
[21] B Satchidanandan and PR Kumar. Dynamic watermarking: Active defense of networked cyber–physical systems. *Proceedings of the IEEE*, 105(2):219–240, 2017.
[22] Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. Technical report, UBER, 01 2015.
[23] A. Swaminathan, Y. Mao, and M. Wu. Robust and secure image hashing. *TIFS*, 1(2):215–230, June 2006.
[24] Dorothy E. Denning and Peter J. Denning. Certification of programs for secure information flow. *Communications of the ACM*, 20:504–513, 1977.
[25] Amir Pnueli. The temporal logic of programs. In *SFCS*, pages 46–57, 1977.
[26] Susanne Albers and Stefano Leonardi. On-line algorithms. *ACM Computing Surveys*, 31(3es), 1999.
[27] Sanjoy K. Baruah, Louis E. Rosier, and R. R. Howell. Algorithms and complexity concerning the preemptive scheduling of periodic, real-time tasks on one processor. *Real-Time Systems*, 2(4):301–324, 1990.