International Journal of Wireless Information Networks (2018) 25:117–129
https://doi.org/10.1007/s10776-018-0391-6

A ReRAM Physically Unclonable Function (ReRAM PUF)-Based Approach to Enhance Authentication Security in Software Defined Wireless Networks

Fatemeh Afghah[1] · Bertrand Cambou[1] · Masih Abedini[2] · Sherali Zeadally[3]

Received: 13 March 2017 / Accepted: 12 January 2018 / Published online: 22 January 2018

Abstract
The exponentially increasing number of ubiquitous wireless devices connected to the Internet in Internet of Things (IoT) networks highlights the need for a new paradigm of data flow management in such large-scale networks under software defined wireless networking (SDWN). The limited power and computation capability available at IoT devices as well as the centralized management and decision making approach in SDWN introduce a whole new set of security threats to the networks. In particular, the authentication mechanism between the controllers and the forwarding devices in SDWNs is a key challenge from both secrecy and integrity aspects. Conventional authentication protocols based on public key infrastructure (PKI) are no longer sufficient for these networks considering the large-scale and heterogeneity nature of the networks as well as their deployment cost, and security vulnerabilities due to key distribution and storage. We propose a novel security protocol based on physical unclonable functions (PUFs) known as hardware security primitives to enhance the authentication security in SDWNs. In this approach, digital PUFs are developed using the inherent randomness of the nanomaterials of Resistive Random Access Memory (ReRAM) that are embedded in most IoT devices to enable a secure authentication and access control in these networks. These PUFs are developed based on a novel approach of multi states, in which the natural drifts due to the physical variations in the environment are predicted to reduce the potential errors in challenge-response pairs of PUFs being tested in different situations. We also proposed a PUF-based PKI protocol to secure the controller in SDWNs. The performance of the developed ReRAM-based PUFs are evaluated in the experimental results. Moreover, the effectiveness of the proposed multi-state machine learning technique to predict the drifts of the PUFs' responses in different temperature and biased conditions is presented.

Keywords Authentication · Hardware security · Internet of Things · Physically unclonable functions · Resistive RAM · Software defined wireless networking

This work was partially supported by Arizona Board of Regents, Grant Numbers: 1003073 & 1003074.

✉ Fatemeh Afghah
fatemeh.afghah@nau.edu

Bertrand Cambou
bertrand.cambou@nau.edu

Masih Abedini
masih@ieee.org

Sherali Zeadally
szeadally@uky.edu

[1] School of Informatics, Computing and Cyber Systems, Northern Arizona University, Flagstaff, AZ 86011, USA

[2] Isfahan, Iran

[3] College of Communication and Information, University of Kentucky, Lexington, KY 40506-0224, USA

1 Introduction

With the ever-growing number of devices connected to the Internet and the development of Internet of Things (IoT) networks, security of such large-scale heterogeneous networks has become a key challenge in cyber physical systems. Software defined networking (SDN) provides several benefits toward control and management of IoT networks. In traditional infrastructure-based networks, the control and data planes are tightly coupled together to process packets according to the protocols defined individually in the control plane. The tight coupling of the data and control planes hinders flexibility and performance of such networks. In these networks, whenever the network administrators need to change or update a parameter of

the protocols, they may need to re-configure all related devices (i.e. routers, switches, and firewalls) throughout the network. Depending on the size of the network, it can be a burdensome and time-consuming process.

The recently developed SDN technology aims at addressing the aforementioned challenges by separating the control and data planes. In the SDN paradigm, instead of designating the decision making to every active components in the network, this will be handled by a centralized controller called the *network operating system* (*NOS*). For instance, when a switch receives a packet, it chooses the proper action (forward, drop, modify, sending to the controller, etc.) based on the rules (flow table), which are defined by the programmable network applications at the centralized controller that rely on the NOS [38]. The communication between the NOS and the forwarding layer or the data plane is established by some protocols such as OpenFlow [48]. In contrast to the predecessor distributed architectures, this programmability leads to easy evolvable networks because the switches no longer need to interpret multiple protocols to make decisions individually. Rather, the network manager can manage and update the rules centrally. Moreover, OpenFlow offers a standardized interface that enables the integration of various heterogeneous devices from different vendors that can significantly simplify the operation of multi-vendor networks.

Since the emergence of SDN, most researchers have been focusing on wired networks. However, the emergence of next generation of mobile communication networks (5G) and IoT networks need effective resource allocation and interference management techniques which makes SDN a good paradigm to adopt for these wireless networks [22]. Before applying SDN to wireless networks, also called *software defined wireless networking (SDWN)*, several challenges such as the nature of wireless channels, dynamic network topology, heterogeneity of devices, and shortage of resources need to be further investigated. However, the SDN-enabled wireless networks can offer key advantages for both users and providers because of their centralized network management approach. Some of the main advantages of the SDN model in infrastructure-based, non-infrastructure-based, and hybrid networks are summarized as followed [22, 50].

- *Network Slicing (network virtualization)* In general, providing different services through a single physical infrastructure is a challenging task. With SDN, the infrastructure provider can slice the physical infrastructure into distinct virtual networks to handle different services or providers [22].
- *Effective Traffic Offloading* A global view of the networks and a centralized management approach in SDN enables the service providers to offload the traffic on the right locations and devices in the network [50].
- *Intelligent Routing* The forwarding devices in the SDN-enabled networks send the status of the traffic load to the control layer, so that the controller can balance the traffic efficiently because it is aware of the traffic status of the other devices in the network [50].
- *Security Enhancement* The rules in the flow tables that are regularly updated by the controller allow the network operator to define and assign new security roles to every SDN-enabled nodes in the network in a response to the network status [15].

While SDWN can offer the aforementioned advantages, the nature of centralized and software-based control of the network can introduce new security threats to the system [23, 32, 38, 56]. These threats are even more critical in large-scale and heterogeneous SDWN-based IoT networks. It is anticipated that, by 2020, about 21 billion things will be connected to the Internet [20]. These ubiquitous devices present specific security concerns due to their limited power, computing capability, and physical accessibility. Similar to other wireless networks, in an SDWN-based IoT network, the programmable devices can play a new role in packet forwarding, in addition to their traditional roles of sensing, monitoring and controlling [2, 3, 55]. As a result, the ramifications of attacks can intensify and propagate to the entire network very rapidly. Therefore, conventional security solutions such as transport layer security (TLS), secure sockets layer (SSL), and other public key infrastructure (PKI)-based protocols are no longer effective for large-scale IoT networks with billions of active devices [27].

In this paper, we propose an anti-piracy protection mechanism based on development of resistive random access memory (ReRAM)-based PUFs to protect both the network and IoT hardware intellectual properties (IPs) from potential code-injection and rogue node injection attacks. A key advantage of PUF-based IP protection is that it can prevent the malicious entities from copying the hardware components by noting the unclonable properties of PUFs. While in common crypto-based solutions, an attacker can easily replicate the system components when it got access to one device, in a PUF-based method, even if an adversary has a physical access to some devices, cloning the intrinsic characteristics of the chips and emulating them to forge the identity of the things is very difficult or almost impossible. By using the embedded memory in devices to generate the PUFs, we can also reduce the cost of manufacturing sensors and devices, because keeping the secrets on the chips does not need nonvolatile memory (NVM) and an always-on power source [25].

1.1 Contributions of the Paper

The key contributions of this paper are summarized as followed:

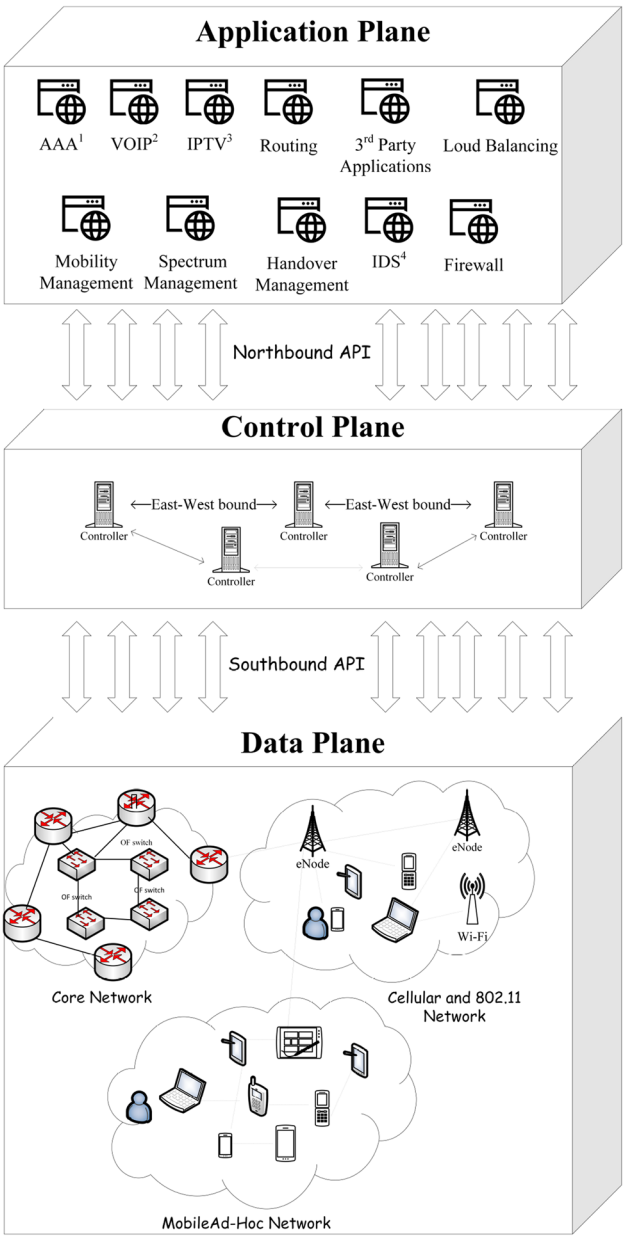
- A novel hardware security mechanism for IoT networks using ReRAM-based PUFs is proposed that utilizes the embedded memory of the devices.
- Multi-state strong PUFs are developed, in which the natural drifts of PUFs' responses in different network conditions are predicted to reduce the error in challenge-response pairs of PUFs.
- A new PUF-based PKI protocol is proposed to secure the controller in SDWN.

The rest of the paper is organized as follows: Section 2 provides an overview of the architecture of SDWN. We review recent security threats for SDWN and IoT, and the corresponding countermeasures in Sect. 3. An introduction to PUFs and their applications in security is provided in Sect. 4. We present the proposed security protocol for IoT networks using ReRAM-based PUFs with multi-state design. The experimental results are presented in Sect. 5 followed by some concluding remarks in Sect. 6.

2 SDWN Architecture and Components

As mentioned before, in the SDN paradigm the control plane makes decisions about traffic independent of the data plane which handles forwarding traffic to the target destinations. A general architecture for SDWN based on 3GPP evolved packet system is described in [7]. As shown in Fig. 1, SDWNs consist of three layers:

1. *Data Plane (Infrastructure Layer)* Recent wireless networks (infrastructure-based or infrastructure-less) have become increasingly heterogeneous. Hence, several heterogeneous radio access networks (RANs) such as Wi-Fi, 3G, LTE, LTE-A, and 5G can co-exist in this layer. In addition, the core networks (CNs) handle the communications among the users or servers. In mobile networks or wireless sensors networks, mobile terminals or wireless sensors also are included the data plane.
2. *Control Plane* The NOS or mobile network SDN controller resides in this layer. The controllers receive rules and commands from the network applications and send them to the data forwarding devices in the data layer.
3. *Network Applications* The operators or service providers use application program interfaces (APIs) to manage the controllers in the control plane. By using the network applications (e.g., mobility management, authentication, accounting, intrusion detection), the operators have access to network resources and manage them in an all-inclusive vision.



[1] Authentication, Authorization, and Accounting
[2] Voice over IP
[3] Internet Protocol Television
[4] Intrusion Detection System

Fig. 1 General architecture of SDWN

The communications interfaces among these three layers can be divided to three categories:

- *Northbound Interface* An interface to the operators, the service providers, or the application developers can be offered by NOS. The operators can dynamically manage the shared network resources between the virtual networks in one physical infrastructure. Furthermore, the service and application providers with different levels of access can influence on and change the network behavior using the authorized interfaces.
- *Southbound Interface* The way packets are forwarded between the forwarding devices is defined by the southbound application programming interfaces (APIs). An interface to the physical user plane network in the CN, RAN, or mobile node allows the network providers to set new policies and protocols or modify the old ones.
- *East–West bound Interface* Although in SDWN, the controller is logically centralized, but to improve the scalability and robustness, it can be physically distributed. Therefore, east/westbound interface is responsible for data exchange among the distributed controllers.

3 Background and Related Work

In this section, we present a summary of state-of-the-art research on security issues related to IoT networks and software defined networks.

3.1 Security Threats in IoT Networks

The emergence of IoT networks raise a new set of security challenges due to the large number of devices connected to the Internet, the ad hoc nature of such networks as well as the energy constraints and limited computational capability at these devices [6, 49, 65]. Moreover, the heterogeneity of IoT networks consist of various deceives with diverse set of security capabilities further threat the security of the network as a whole. Therefore, the existing cryptographic protocols that commonly involve intensive key generation, and key sharing process can not be utilized in such large scale networks. Several common security threats for IoT networks include: (i) denial of service attack, (ii) routing threats, (iii) replay attacks, (iv) fake node attack, (v) side channel attack, (vi) node capture, and (vii) mass node authentication problem [61, 65]. As we describe in Sect. 4, the proposed memory-based PUF technology can offer an affordable mechanism to protect the IoT networks from several of these attacks such as mass node authentication problem, and fake node attack.

3.2 Security Threats and Countermeasures in SDWN

While the SDN paradigm can enhance the scalability and performance of traditional networks as well as strengthen the current security mechanisms because of its reprogrammable and reconfigurable properties, it can also introduce new security threats to the network [28, 30, 31]. Due to recent emergence of SDWN, there are a few reported work in the literature to study the security issues of SDWN. In [12], the authors reviewed and classified the security threats in software defined mobile networking (SDMN) such as spoofing, tampering, repudiation, information disclosure, denial of service, elevation known as STRIDE. The authors in [59] compare the performance of several communication protocols in SDWNs including border gateway protocol (BGP), NETCONF when facing STRIDE security threat. In [23], the authors provide a comprehensive survey of security threats of SDWNs related to a centralized controller as well as the separation of the control and data planes.

Here, we present an overview of the security attacks and their countermeasures in SDN and SDWN [5, 12, 23, 28, 37].

3.2.1 Data Plane Security Issues

In attacks regarding the data plane, the attackers can target different network elements including the forwarding components such as the OpenFlow switches, the mobile terminals or the sensors in IoT or the radio access elements. The various threats on the forwarding components can be classified as follows:

- *Sniffing* a passive attacker can sniff the traffic at the forwarding components for use in future attacks.
- *Forged Traffic Flows* the compromised nodes or even malfunctioning or mis-configured devices can generate forged traffic flow and send it to the controller. An active attacker can force to send false flow information to the controller to deceive it.
- *Flow Tables Overflow* an attacker can continuously send a series of flows which are slightly different from each other. As a result, the switch is forced to send the information of the new flows to the controller and receive related entries updates. Since the flow table on the OpenFlow-enabled devices can only accept a limited number of entries, this process can cause the flow table to become full very quickly and slow down that impacts the forwarding of regular flows [12].
- *Selfishness* some mobile nodes in mobile ad-hoc networks (MANET)s or wireless sensor networks (WSNs) may tend to act selfishly to preserve their resources (such as power and computing). As a result they may refuse to forward and relay the packets received from other users or devices.
- *Spoofing* (*forged identity of authorized components*) in this threat, the attackers want to conceal their malicious activities behind a legitimate entity in the network. Hence

they try to forge the identity of authorized terminals or switches to achieve their goals. The infrastructure-less environment exacerbates the frequency of this attack due to the easy access to the communication media.

Several methods have been proposed to mitigate these attacks including (i) encryption of data and sensitive parameters at the forwarding elements which is the first line of defense against adversaries to sniff or steal credential data, (ii) using intrusion detection systems (IDSs) or intrusion prevention systems (IPSs) to detect or prevent anomalous behaviors of the components, (iii) mutual authentication between the controller and the forwarding components which can prevent the unauthorized access as well as forging the identity of legitimate users.

In addition to the forwarding components' threats, the RANs can also suffer from a wide variety of attacks such as sniffing and denial of service attacks (DoS), mainly due to the co-existence of multiple standards and mobile networking technologies at the data plane layer. These threats can be thwarted by different encryption and mutual authentication mechanisms.

3.2.2 Control Plane Security Threats

The centralized nature of network management in SDN-enabled networks make them prone to several attacks that threaten the centralized controller. Hence, failure of the centralized controller called as "single point of failure" has been the main concern in these networks [23]. The implementation of a distributed controllers' architecture for SDN-enabled IoT mitigates the risk of single point of failure and also enhances the security level of the network by using hierarchical controllers in multiple domains [16]. Other major threats to the control plane include: (i) Distributed denial of service (DDoS) attacks or flood attacks, in which the control plane is overwhelmed by dummy flow traffic from the attackers and it has to respond to these unknown flows for making decisions, and (ii) Data leakage, where an adversary can discover the policy of the controller about special flows by using packet processing timing analysis [57].

3.2.3 Application Plane Security Issues

If an attacker takes over control of the clients remotely or physically by means of viruses, trojans, and etc., the attacker can insert fraudulent flow rules into the forwarding components and potentially control the network. To prevent these threats, the admin terminals can be protected by traditional mechanisms such as anti-virus and IDS. Moreover, the likelihood of these attacks can be reduced by using two-factor authentication mechanisms when accessing the applications and the clients as well as by choosing strong access control policies. In addition to these client-based threats, the network application threats refer to attacks that implement network functions in applications running on the application plane which can potentially disturb the performance of the entire network [4]. Regular penetration testing and strong authentication(e.g. Kerberos [52]) and authorization management techniques can prevent unauthorized access by applications executed by the controllers [23, 57].

3.2.4 Communication Protocols Security Issues

The attacker can exploit the vulnerabilities in the protocols that control the communication between the controllers, network applications, switches, base stations, and users devices to launch DoS attacks on the entire network or sniff important information. In [12], the authors presented three well-known threats and discussed countermeasures to mitigate them:

- *IP Spoofing* the lack of the IP layer security (such as internet protocol security (IPsec)) among backhaul of RANs can lead to this attack.
- *Transport Layer Security/Secure Socket Layer (TLS/SSL) Vulnerabilities* recently many flaws have been found in these security protocols such as SYN DoS that can be launched by the attackers.
- *Man-in-the-Middle Attack* in this attack, the adversary intercepts the communication channel and exchanges the authorized parties messages in a way that they are not aware of the existence of any adversary.

Mutual authentication mechanisms together with the key distribution algorithms can be applied for securing the channel. Additionally, we can use improved protocols such as the host identity protocol (HIP) and IPsec tunneling to secure the channels between the controllers and the forwarding components [12, 43].

4 Proposed Security Protocol Using Memory-Based Physical Unclonable Functions (PUFs)

PUF is a generic technology used for creating cryptographic primitives that can be integrated in cyber physical systems (CPS) to strengthen security [25, 29, 44, 46, 53]. The concept was introduced 15 years ago, and has been commercialized quite successfully recently. During manufacturing, electric components encounter random variations that are due to small local changes in the chemical composition, physical dimensions, density, and other physical elements [11, 17, 21]. These variations make each device unique. The idea behind a PUF is to identify these differences in order to be

able to differentiate each component from the others so that we can achieve a secure authentication of the components in the CPS.

The basic protocol is initiated by generating PUF "challenges", the reference patterns of the components that can act as digital finger prints. These challenges are usually stored in a secure server for future use. When queried by the secure server, which is the case during an authentication cycle, the PUF generates "responses" in a way similar to the challenges generated upfront. The authentication is thus, completed by analyzing the challenge-response-pairs (CRPs), and the resulting matching error rate. This methodology is not different from what is done to authenticate users in biometric methods using their finger-prints, images of their iris, veins, or biometric characteristics. Two important figures of merit for PUFs include: i) the ability to be clearly identifiable in spite of natural drifts, or noisy conditions, and ii) the existence of secret properties that make them hard to extract through side channel analysis often used by the hackers. These two benefits are often in conflict with each other, and fuzzy PUFs that are hard to extract by the hackers could also be erratic under noisy conditions.

In this work, we utilize the embedded ReRAM in IoT devices to generate strong PUFs. Since these elements operate at very low voltage and low power, they are hard to analyze through side channel attacks. We also propose a multi-state and machine learning based technique that greatly strengthens the PUFs by reducing CRP error rates. This involves developing novel hardware design and computational mechanisms to create a PUF with multi-state memory, where the measurements of a physical parameter are saved in multiple states format rather than the conventional binary style [9]. To do so, we propose a novel design for the CRP generation process that captures the specific "personality" of the physical elements underlying the PUFs under various conditions (such as ambient temperature). This can substantially improve the accuracy of the challenge and response evaluation and hence reduce the error in the challenge and response comparison.

4.1 Memory PUFs Compared with Legacy PUFs, and Why ReRAM?

The early PUF technology was based on ring oscillators and gate delays [58, 60]. The authentication protocol of such PUFs uses the result of "in situ" matching of the challenges with the responses. The secure server sends the challenge to the PUF, the PUF responds with a positive or negative authentication of whether the frequency or delay matches or not. Such a protocol is very interesting because there is no need for complex key distribution protocols, as there are no keys stored on the PUF, therefore the crypto-analyst cannot easily find the cryptographic primitives, and the authentication process can be quick.

PUF technology is not easy to achieve in practice however, because the physical elements can vary when subject to temperature changes, parameter drifts, bias effects, electromagnetic interferences, and aging [24, 47, 54]. Drifting responses produce higher CRP error rates, and can create false negative authentications. The attackers, through side channel analysis and fault injection, can extract the responses from PUFs defeating their purpose.

Memory-based PUFs are now becoming increasingly important as a cryptographic primitive to protect IoT devices [10, 13, 14, 26, 39, 45, 63, 66]. Embedded memories are widely available in IoT devices as cache memory, or non-volatile storage. The density needed for PUF CRP generation is extremely small, i.e. 128–256 bits, compared with the memory needed in IoT devices, which is typically in the 1–8 Mbit range. The low memory requirement of PUFs can be easily achieved by IoT devices making them hard to extract through side channel attacks.

The only operations available with memory devices are: program, erase, and read. Hence it is not possible to follow the protocol described above with ring oscillators and gate delays to match "in situ" challenges and responses. During authentication cycles, it is then necessary to extract the responses away from the memory array, and to perform the CRP matching separately. Two protocols emerge, the first is to send the response to the secure server which analyzes the CRPs matching. In the second method, the analysis of the CRP matching is directly performed in the IoT device. In both cases the communication between the secure server and the IoT device has to be encrypted to protect the PUFs cryptographic primitives, challenges or responses. For this purpose, a crypto-processor has to be incorporated as part of the design of the IoT device, and cryptographic protocols such as public key infrastructure (PKI) need to be in place. The deployment of PKI requires the distribution of private keys to the IoT devices. These keys can be stored in the embedded memory.

ReRAM is an emerging technology for IoT that has the potential to replace EEPROM and flash as a non-volatile memory [18, 19, 34–36, 51, 62]. ReRAMs operate at very low power compared with flash, have low access time, and are very fast to program. These properties are extremely desirable for secure operations. Differential power analysis (DPA), and electro-magnetic interference analysis coupled with fault injections are not effective in extracting the secret keys that are stored in ReRAMs. This is because their operating power is orders of magnitude lower than flash. Hence, ReRAMs operate below the noise level present in the system [1, 8–10, 64]. Electron beams created by secondary electron microscopy (SEM) can be deflected by the electrons trapped in flash memory thereby exposing the content of the

stored information. In contrast, the chargeless ReRAMs are immune to this type of attack. Therefore, both metal-oxide ReRAM, and conductive bridge ReRAM technologies are appropriate candidates for the purpose of PUF CRP generation in IoT networks [8–10, 33].

4.2 Proposed Memory-Based PUFs with Multi-state and Machine Learning

In the proposed multi-state PUF design, the challenges or responses are generated based on the measurements of a physical parameter such as temperature or bias voltage, V_{set}, and are saved in multiple states format rather than the conventional binary style, as depicted in depicted in Fig. 2. In the conventional binary notation, a "0" refers to the case where the measured parameter of a memory cell is below the threshold located in the middle of the distribution, while a "1" is programmed in the cells measured above the threshold.

In our proposed multi-state method, the cells are organized in *n multiple states* by sorting out the value of the physical parameters underlining each cell of the memory, as shown in Figure 2. This multi-state method can more accurately capture the specific "personality" of the physical elements underlying the PUFs in a challenge or response generation process. A PUF of N bits is to be sorted into n states, either during challenge generation, or response generation. Each state i has n_i cells such that $\sum_{i=0}^{n} n_i = N$. The PUF responses are generated in the same way as the challenges as often as needed. CRPs errors are to be expected because the measurement of the physical parameters of the PUFs is changing over time.

For a given cell k that is part of the PUF, the CRP error between the challenge C_k and the response R_k is given by $\Delta CRP_k = |R_k - C_k|$, where ΔCRP_k is the CRP error rate of the cell. For the populations of n_i cells that are part of the state i, the average CRP error rate is given by:

$$E_i = \frac{1}{n_i} \sum_{k=1}^{k=n_i} |R_k - C_k| \tag{1}$$

The average error rates E_0 to E_n (as calculated with (1)) for the n states result in a Vector of Errors (VE) that is characteristic of a particular response: $VE = (E_0, E_1, \ldots, E_i, \ldots, E_n)$. This process is summarized in Fig. 3.

These VEs are used to complete the authentication process using a machine learning engine (MLE) that predicts the expected drifts of the responses for a given physical parameter (such as temperature), and adjust the results accordingly. When the server sends a challenge to the MLE, a fresh response is generated by the PUF. The MLE gathers the response, as well as all available data to compute a secure authentication. The MLE integrated in the micro-controller handles the communication between the secure server and the PUF. For the authentication j, $VE_j = (E_0, E_1, \ldots, E_i, \ldots, E_n)_j$ and the vector of input $I_j = (I_0, I_1, \ldots, I_i, \ldots, I_m)_j$, where m denotes the number of input parameters, are fed into the MLE. The vector of input includes the physical parameters of interest such as operating temperature, and biased conditions. Then the MLE completes the authentication process by considering the available learning data based on a record of prior responses with the predictive models of the laws for the PUF parameters. It is worth mentioning that noting the limited size of input history dataset, this process does not impose a considerable computational load to the IoT devices. The block diagram of this authentication protocol is shown in Fig. 4.

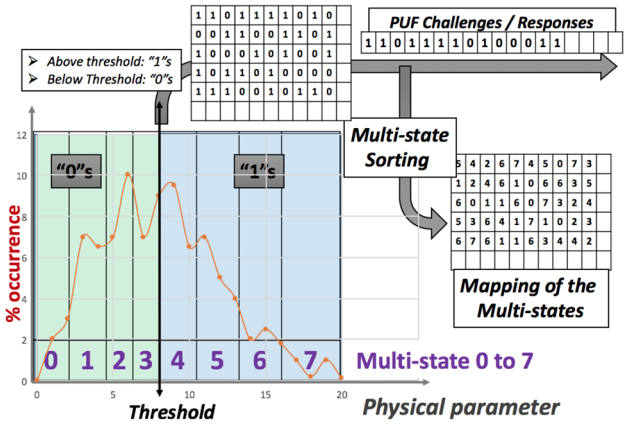


Fig. 2 challenge/response generation in the proposed PUFs with multi-states

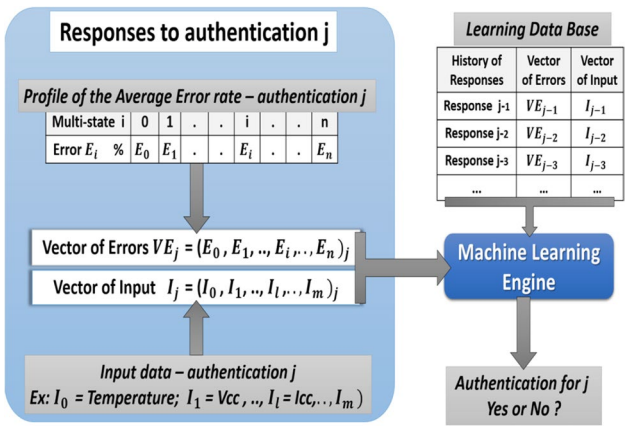


Fig. 3 CRPs error rates in multi-state PUFs

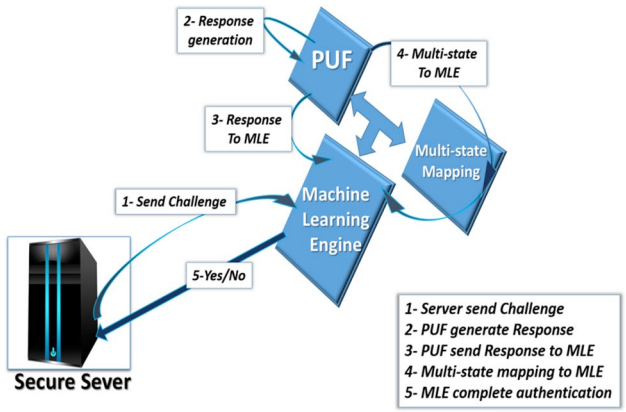


Fig. 4 Authentication protocol for memory-based PUFs with a machine learning engine (MLE)

4.3 Proposed Security Protocols for SDWN-based IoT Networks

We propose a security protocol based on the developed memory-based PUFs to significantly enhance the security in SDWN-based IoT networks. Public key infrastructure (PKI) is known to be a powerful and commonly-used infrastructure to protect software defined wireless networks with a large quantity of IoT devices, and peripherals. When the PKI security protocol is utilized in SWDNs, each node needs to have a pair of public and private keys to allow two-way encrypted communication between the IoT devices and the secure controller as depicted in Fig. 5. The private keys can be downloaded during the post manufacturing operations of secure elements; these operations are also called personalization If the non-volatile memory of the secure element is made with ReRAM rather than flash, the private keys can be adequately protected from an attack.

However, one drawback of this method is the public-private key pair of the secure controller. Attackers can focus their efforts to break this single node, and compromise the entire group of IoT devices connected to the controller. Another threat, although with potentially limited impact, is the loss of a public-private key pair of one IoT device to some third party.

Here, we propose a novel PUF-based protocol that can drastically reduce the exposure to these cyber-attacks. In this protocol, two challenges of $C1$ and $C2$ are generated from two distinct parts of the array at every IoT node in the network, and these challenges are stored in the secure network. We describe the protocol below.

1. The first step of the protocol is initiated by the secure server; an encrypted challenge $C1$ is sent to the corresponding IoT device. Then IoT device decrypts $C1$, generates a response $R1$ from the part of the array that generated $C1$, then checks whether the CRPs match. This step authenticates the secure network.
2. The second step of the protocol is initiated by the IoT device; a response $R2$ is generated from the part of the array that generated $C2$, $R2$ is then encrypted and sent to the secure server. The secure server compares $C2$, and $R2$ to authenticate the IoT device.

Figure 6 presents a block diagram of the proposed PUF-based PKI protocol.

If an attacker breaks the public-private key pair of the server, it should not be able to authenticate itself by the IoT device, unless the hacker also finds a way to uncover $C1$. If this were to happen, other IoT devices would not be exposed to the breach, thereby protecting the network from a large scale attack. Conversely, if an attacker breaks the public-private key of the IoT device, it should not be able

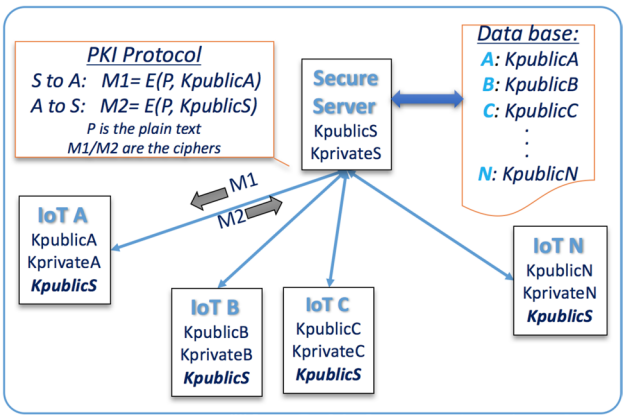


Fig. 5 Block diagram of a public key infrastructure protocol to secure the network with IoTs. The two-way communications between the server and the IoT are encrypted with public keys

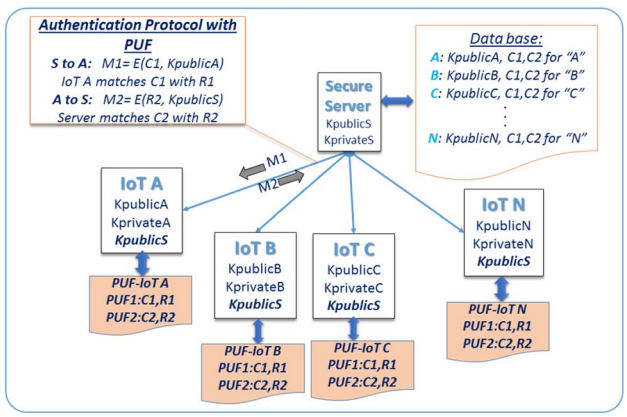


Fig. 6 Block diagram of the proposed PKI protocol with PUF authentication. The two-way communication is also encrypted with public keys. Two PUFs per IoT device provide two-way authentication

to be authenticated by the secure server, unless the attacker also finds a way to uncover $C2$. Our proposed PUF protocol therefore provides an important second level of protection in addition to the protection offered by PKI. The protocol presented in this section can be extended to a larger number of PUFs by a memory array. This protocol could be used for hierarchical level of security, with additional PUFs needed for highly sensitive parts of the network.

5 Experimental Results

In this section, we present the experimental results obtained to generate PUFs using ReRAM based on metal oxide with oxygen vacancies is presented. For this purpose, Cu/TaOx/Pt resistive devices have been fabricated, and characterized at Virginia Tech in a crossbar array on a thermally oxidized silicon wafer [18, 40–42]. Figure 7 shows the cumulative V_{set} probability distribution within a typical sample of ReRAM memory array, containing a large number of cells. The mean of this distribution is $\mu = 2.1$ V, as indicated by the dashed line, and the standard deviation is $\sigma = 0.54$ V. The variation of standard deviation (σ) of all cells are extrapolated as shown in Fig. 8.

The challenges and responses on each cell of the array are generated based on the value of V_{set}, the voltage necessary to create a conductive bridge within the solid electrolyte separating two conductive electrodes. In order to study the quality of the PUF, the samples were submitted to repetitive program erase cycles. When a progressive positive voltage sweep is applied to the cell, the programming step, the voltage reaches V_{set} when a conductive filament is created, which reduces the resistance by two or three orders of magnitude. With a negative voltage sweep, the erase step, has the reverse effect; when the voltage exceeds V_{reset} the

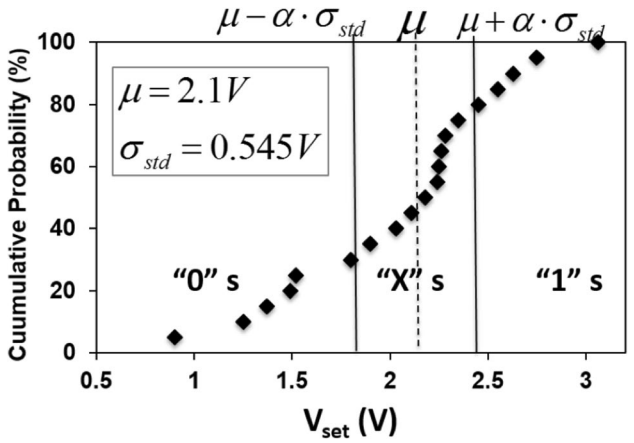


Fig. 7 Cumulative V_{set} probability distribution for the entire array of cells

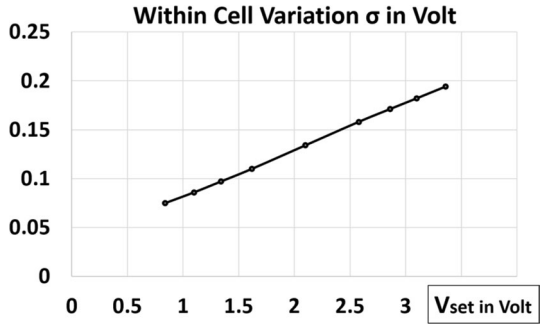


Fig. 8 Variation of σ within cell versus the average V_{set}

conductive filament is partially dissolved, and the resistance increases by several orders of magnitude. Based on the experimental data presented in Fig. 7, the drift between the challenges and the responses is modeled by using a normal distribution.

Here, we applied a *ternary states* methodology, with a threshold value T which is close to the median value of the V_{set}. When a cell has a V_{set} clearly below T, the cell is considered as a "0" state; when a cell has a V_{set} clearly above T, the cell is considered as a "1" state; and when a cell has a V_{set} close to T or one that varies randomly around T, the cell is considered as a "X" state. As a result, the challenge-response-pair CRP error rate is reduced when the proportion of X states is higher, leaving only solid "0" and "1" states.

One metric to evaluate the performance of PUFs is the amount of entropy, and therefore the number of independent CRPs that can be generated which is limited by the number of elements used to construct the PUFs. Because the traditional PUF generation mechanisms have certain limitations in this regard, several mapping methods have been proposed to produce stronger PUFs. In [47], the authors proposed an identity-mapping function to expand the set of challenge-response pairs for ring-oscillator PUFs, where a group of ring-oscillator frequencies is utilized to generate the PUFs. Because generating stronger PUFs of this type comes with higher area cost, this proposed method can generate stronger ring-oscillator PUFs with lower cost using an identity-mapping function that results in a larger set of CRPs. While the new sets of CRPs are not information-theoretic independent, the statistical tests confirmed that the generated lower-cost PUFs with the identity-mapping function are strong. Noting the fact that the PUFs usually need only 128–256 bits to ensure an acceptable level of security in different applications, while commercial memory arrays that are integrated within micro-controllers, ordinarily have memory densities in the mega-byte range, we can easily generate a large set of CRP for our proposed memory-based PUFs. As shown in Figs. 7 and 8, this value follows a normal distribution with mean value of μ, where its standard

deviation varies cell to cell. This concludes the uniformity of the responses. Furthermore, considering the scale of available memory, the readings can be done over different cells in a way that there is no overlap between the challenges (or the responses) that confirms the inter-response dependency.

Moreover, we enhance the reliability of the developed PUFs by predicting their response variations for different environmental conditions (e.g. temperature) as presented in Figs. 7 and 8. In memory-based PUFs, this criteria means to have enough random variations, cell to cell, in order to obtain strong cryptographic entropy, while the measurements of each cell should be reproducible when responding to successive queries. This can be satisfied when the standard deviation of cell to cell (mainly due to manufacturing variations) is much higher than the standard deviation of each cell (mainly due to noise, and measurement variations).

In this experimental validation we also utilized the aforementioned learning approach to predict the natural drifts in the responses of a PUF in different situations. The V_{set} of ReRAMs is sensitive to temperature, and biased conditions. When the temperature increases, the mobility of the positive ions, oxygen vacancies, is higher, and conductive filaments are created at lower voltages, hence the V_{set} is lower. If the generation of the challenges, and responses is done under different conditions this could increase CRP error rates. Considering this fact, the drifts that are due to temperature changes, or different biased conditions are largely predictable by the laws of physics and are tracked by the learning approach.

An analysis of the results shown in Fig. 9 reveals, the impact of the drift of the response on the CRP error rates, by state. In this Figure M_i denotes the state i for the proposed multi-state PUF. The population of the ReRAM array with 8 multi-states of 0–7 with equal probability of 12.5% has been considered. The VE_i vectors are calculated by state from 0 to 7 for the base, where the resulting base vector of error has a

Mi	Median Vset Volt	Median σ Volt	VE_i % Neg Drift (1.8V)	VE_i % Neg Drift (1.95V)	VE_i % Base (2.1V)	VE_i % Pos Drift (2.25V)	VE_i % Pos Drift (2.4V)
0	1.285	0.099	0	0	0	0	0
1	1.615	0.110	5	0.1	0	0	0
2	1.840	0.125	62	19	2	0.1	0
3	2.015	0.132	95	69	26	4	0.2
4	2.185	0.138	0.2	4	26	68	95
5	2.374	0.151	0	0.3	4	23	60
6	2.579	0.160	0	0	0	2	13
7	2.928	0.175	0	0	0	0	0.2

Fig. 9 Statistical analysis for the impact of the drift of the responses on the CRP error rate

Mi	σ_D/σ_{Mi} Tighter -20%	σ_D/σ_{Mi} Base ---	σ_D/σ_{Mi} Wider +20%	VE_i % Tighter (0.8σ_D)	VE_i % Base (σ_D)	VE_i % Wider (1.2σ_D)
0	4.54	5.45	6.83	0	0	0
1	4.09	4.91	6.14	0	0	0
2	3.60	4.32	5.40	4	2	0
3	3.42	4.09	5.09	30	26	21
4	3.25	3.91	4.91	30	26	22
5	2.98	3.58	4.46	7	4	1
6	2.81	3.37	4.21	1	0	0
7	2.57	3.09	3.86	0	0	0

Fig. 10 Variations of standard deviation for the entire population versus the standard deviation of each cell

mean of V_{set} of 2.1 V. When the responses drift in a positive direction, respectively to 2.25 and 2.4 V, the CRP error rates of the first four states decrease, while the CRP error rates of the last four states increase. The effects are reversed for negative drifts (1.95 and 1.8 V). In Fig. 10, the analysis is related to the respective change of the standard deviation of the entire population versus the standard variation of each cells. In this figure, σ_D denotes the standard deviation of the entire distribution for all cells, and σ_{M_i} is the standard variation of the distribution of all cells with state M_i. If the spread of the general population of responses to the PUF is getting tighter compared with the spread of responses to an individual cell, the average error rates across the 8 states will go up. Conversely, if the spread is relatively wider, the average defect rates will decrease.

This proposed method to capture the profile of the physical parameters underlying a PUF with multi-states can result in a tracking of the PUFs drifts over time that are predictable. As we mentioned earlier, the modeling of the effect of the external parameters such as temperature and bias conditions can decrease the probability of false negatives when authenticating a PUF-based IoT device under various conditions.

6 Conclusions

One of the key challenges facing implementation of IoT networks is security. This is even more critical in SDWN-based IoT network noting the vulnerability of the network to the central controller failure due to malicious attacks. In this paper, we propose a novel ReRAM-based PUFs that can function as digital fingerprints to secure SDWN-based IoT networks. In order to enhance the performance of these PUFs in terms of reducing the error rate between the challenge and response pairs (CRPs) in different network condition, we

proposed a multi-state machine learning technique. In this method, the potential drifts in the PUFs' responses due to various physical parameters such as temperature, and biased conditions are predicted and utilized to reduce the CRP error rates. The effectiveness of this method in reducing the CRP errors is confirmed in the numerical results. Furthermore, we proposed a PUF-based PKI protocol to establish a two-way authentication in SDWN-based IoT networks that protects both the server and IoT devices. This method adds another level of security comparing with common PKI protocols in a way that the attackers cannot authenticate themselves in the network by finding the public-private key pair, unless they can get access to the challenge. This can significantly enhance the security of the network specifically against the central controller attacks, because even if an attacker breaks the public-private key pair and the challenge of the server for one IoT device, other IoT devices would not be exposed to this attack, thereby protecting the network from a large scale attack.

Acknowledgements This project has been partially supported by Arizona Board of Regents under Grants 1003074 and 1003074. The authors would like to thank their colleagues from the pilot manufacturing facility at Virginia Tech that allowed us to produce quality samples for this work. We thank the anonymous reviewers for their valuable comments which helped us improve the quality and presentation of this paper.

References

1. F. Afghah and B. Cambou. Multi-state unclonable functions and related systems, November 2016.
2. F. Afghah, M. Costa, A. Razi, A. Abedi, and A. Ephremides. A reputation-based stackelberg game approach for spectrum sharing with cognitive cooperation. In *2013 IEEE 52nd Annual Conference on Decision and Control (CDC)*, pages 3287–3292, 2013.
3. F. Afghah, A. Razi and A. Abedi, Stochastic game theoretical model for packet forwarding in relay networks, *Springer Telecommunication Systems Journal, Special Issue on Mobile Computing and Networking Technologies*, Vol. 54, No. 2, pp. 1877–1893, 2013.
4. I. Ahmad, S. Namal, M. Ylianttila and A. Gurtov, Security in software defined networks: A survey, *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 4, pp. 2317–2346, 2015.
5. S. T. Ali, V. Sivaraman, A. Radford and S. Jha, A survey of securing networks using software defined networking, *IEEE Transactions on Reliability*, Vol. 64, No. 3, pp. 1086–1097, 2015.
6. F. Ayotunde Alaba, M. Othman, I. A. T. Hashem and F. Alotaibi, Internet of things security: A survey, *Journal of Network and Computer Applications*, Vol. 88, No. Supplement C, pp. 10–28, 2017.
7. C. J. Bernardos, A. de la Oliva, P. Serrano, A. Banchs, L. M. Contreras, H. Jin and J. C. Zuniga, An architecture for software defined wireless networking, *IEEE Wireless Communications*, Vol. 21, No. 3, pp. 52–61, 2014.
8. B. Cambou and F. Afghah. Physically unclonable functions with multi-states and machine learning. In *14th International Workshop on Cryptographic Architectures Embedded in Logic Devices (CryptArchi)*, 2016.
9. B. Cambou and M. Orlowski. Puf designed with reram and ternary states. In *Proceedings of the 11th Annual Cyber and Information Security Research Conference*, 2016.
10. B. Cambou, F. Afghah, D. Sonderegger, J. Taggart, H. Barnaby, and M. Kozicki. Ag conductive bridge rams for physical unclonable functions. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 151–151, 2017.
11. B. Cambou. Physically unclonable function generating systems and related methods, 08 2015.
12. M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang. Software-defined mobile networks security. *Mobile Networks and Applications*, Vol. 21, No. 5, pp. 729–743, 2016.
13. A. Chen. Comprehensive assessment of rram-based puf for hardware security applications. In *2015 IEEE International Electron Devices Meeting (IEDM)*, pages 10.7.1–10.7.4, 2015.
14. T. A. Christensen and J. E. Sheets II. Implementing puf utilizing edram memory cell capacitance variation, 10 2012.
15. A. Y. Ding, J. Crowcroft, S. Tarkoma and H. Flinck, Software defined networking for security enhancement in wireless mobile networks, *Computer Networks*, Vol. 66, pp. 94–101, 2014.
16. O. Flauzac, C. Gonz, A. Hachani, and F. Nolot. SDN based architecture for IoT and improvement of the security. In *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 688–693, 2015.
17. Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, Emerging physical unclonable functions with nanotechnology, *IEEE Access*, Vol. 4, pp. 61–80, 2016.
18. G. Ghosh and M. Orlowski, Write and erase threshold voltage interdependence in resistive switching memory cells, *IEEE Transactions on Electron Devices*, Vol. 62, No. 9, pp. 2850–2856, 2015.
19. N. Gilbert, Y. Zhang, J. Dinh, B. Calhoun, and S. Hollmer. A 0.6v 8 pj/write non-volatile cbram macro embedded in a body sensor node for ultra low energy applications. In *2013 Symposium on VLSI Circuits*, pages C204–C205, 2013.
20. Granter Inc. Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015. Available: http://www.gartner.com/newsroom/id/3165317, 2015.
21. J. Guajardo, S. S. Kumar, G.-J. Schrijen and P. Tuyls, Fpga intrinsic pufs and their use for ip protection, *Cryptographic Hardware and Embedded Systems - CHES*, Vol. 2007, pp. 63–80, 2007.
22. I. T. Haque and N. Abu-Ghazaleh, Wireless software defined networking: A survey and taxonomy, *IEEE Communications Surveys & Tutorials*, Vol. PP, No. 99, p. 1, 2016.
23. D. He, S. Chan and M. Guizani, Securing software defined wireless networks, *IEEE Communications Magazine*, Vol. 54, No. 1, pp. 20–25, 2016.
24. C. Helfmeier, C. Boit, , and S. S. J. Tajik. Physical vulnerabilities of physically unclonable functions. In *Proceedings of the conference on Design, Automation & Test (DARE'14)*, 2014.
25. C. Herder, M. Yu, F. Koushanfar, and S. Devadas. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, 102(8), 2014.
26. D. E. Holcomb, W. P. Burleson, and K. Fu. Power-up sram state as an identifying fingerprint and source of true random numbers. *IEEE Transactions on Computing*, Vol. 58, No. 9, pp. 1198–1210, 2009. https://doi.org/10.1109/TC.2008.212.
27. R. Holz, T. Riedmaier, N. Kammenhuber and G. Carle, *X.509 Forensics Detecting and Localising the SSL/TLS Men-in-the-Middle*, SpringerBerlin, 2012. pp. 217–234.
28. N. A. Jagadeesan and B. Krishnamachari, Software-defined networking paradigms in wireless networks: A survey, *ACM Computer Survey*, Vol. 47, No. 2, pp. 27:1–27:11, 2014.
29. Y. Jin, Introduction to hardware security, *Electronics*, Vol. 4, pp. 763–784, 2015.

30. K. Kalkan and S. Zeadally. Securing internet of things (iot) with software defined networking. *IEEE Communications Magazine, in press*, 2017.
31. D. Klingel, R. Khondoker, R. Marx, and K. Bayarou. Security analysis of software defined networking architectures: PCE, 4D and SANE. In *Proceedings of the AINTEC 2014 on Asian Internet Engineering Conference*, AINTEC '14, pages 15:15–15:22, New York, NY, USA, 2014. ACM.
32. R. Klti, V. Kotronis, and P. Smith. Openflow: A security analysis. In *2013 21st IEEE International Conference on Network Protocols (ICNP)*, pages 1–6, 2013.
33. M. N. Kozicki, M. Balakrishnan, C. Gopalan, C. Ratnakumar and M. Mitkova, Programmable metallization cell memory based on ag-ge-s and cu-ge-s solid electrolytes. In *ProcNon-Volatile Memory Technology Symposium*, 2005.
34. M. N. Kozicki, C. Gopalan, M. Balakrishnan, M. Park, and r M. Mitkova. Nonvolatile memory based on solid electrolytes. In *Proc. IEEE Non-Volatile Memory Technol. Symp.*, 2004.
35. M. N. Kozicki and M. Mitkova, Mass transport in chalcogenide electrolyte films ? Materials and applications, *Journal of Non-Crystalline Solids*, Vol. 352, pp. 567–577, 2006.
36. M. N. Kozicki, M. Park and M. Mitkova, Nanoscale memory elements based on solid-state electrolytes, *IEEE Transactions on Nanotechnology*, Vol. 4, No. 3, pp. 331–338, 2005.
37. D. Kreutz, F. Ramos, and P. Verissimo. Towards secure and dependable software-defined networks. In *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, pages 55–60. ACM, 2013.
38. D. Kreutz, F. M. V. Ramos, P. E. Ver, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, Software-defined networking: A comprehensive survey, *Proceedings of the IEEE*, Vol. 103, No. 1, pp. 14–76, 2015.
39. C. Krutzik. Solid state drive physical unclonable function erase verification device and method, 01 2015.
40. T. Liu, T. Verma, Y. Kang and M. Orlowski, Coexistance of bipolar and unipolar switching in Cu/TaOx/Pt resistive devices for Cu and oxygen vacancy nanofilaments, *ECS Transactions*, Vol. 45, No. 3, pp. 279–285, 2012.
41. T. Liu, T. Verma, Y. Kang and M. Orlowski, Volatile resistive switching in Cu/TaOx/-Cu/Pt devices, *Applied Physics Letter*, Vol. 101, p. 073510, 2012.
42. T. Liu, Y. Kang, S. El-Helw, T. Potnis and M. Orlowski, Physics of the voltage constant in multilevel switching of conductive bridge memory, *JJAP*, Vol. 52, p. 084202, 2013.
43. M. Liyanage, I. Ahmed, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, Uriarte O. Edgardo M. de Itzazelaia, M., A. Valtierra, and C. Jimenez. Security for future software defined mobile networks. In *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, pages 256–264. IEEE, 9 2015.
44. R. Maes and I. Verbauwhede, Physically unclonable functions: A study on the state of the art and future research directions. In *Towards Hardware-Intrinsic Security Part of the series Information Security and Cryptography*, Springer, Berlin, 2010.
45. R. Maes, P. Tuyls, and I. Verbauwhede. A soft decision helper data algorithm for sram pufs. In *2009 IEEE International Symposium on Information Theory*, 2009.
46. R. Maes, *Physically Unclonable Functions: Constructions Properties and Applications*, SpringerBerlin, 2015.
47. A. Maiti, I. Kim and P. Schaumont, A robust physical unclonable function with enhanced challenge-response set, *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 1, pp. 333–345, 2012.
48. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, OpenFlow: Enabling innovation in campus networks, *ACM SIGCOMM Computer Communication Review*, Vol. 38, No. 2, pp. 69–74, 2008.
49. D. M. Mendez, I. Papapanagiotou, and B.Yang. Internet of things: Survey on security and privacy. *CoRR*, abs/1707.01879, 2017.
50. M. Mendonca, K. Obraczka, and T. Turletti. The case for software-defined networking in heterogeneous networked environments. In *Proceedings of the 2012 ACM conference on CoNEXT student workshop*, pages 59–60. ACM, 2012.
51. P. R. Mickel, A. J. Lohn, B. J. Choi, J. J. Yang, M.-X. Zhang, M. J. Marinella, C. D. James and R. S. Williams, A physical model of switching dynamics in tantalum oxide memristive devices, *Applied Physics Letters*, Vol. 102, p. 223502, 2013.
52. B. C. Neuman and T. Ts'o, Kerberos: An authentication service for computer networks, *IEEE Communications Magazine*, Vol. 32, No. 9, pp. 33–38, 1994.
53. R. Pappu, B. Recht, J. Taylor and N. Gershenfield, Physical one-way functions, *Science*, Vol. 297, pp. 2026–2030, 2002.
54. M. Potkonjak and V. Goudar, Public physical unclonable functions, *Proceedings of the IEEE*, Vol. 102, No. 8, pp. 1142–1156, 2014.
55. A. Razi, F. Afghah and A. Abedi, Power optimized DSTBC assisted DMF relaying in wireless sensor networks with redundant super nodes, *IEEE Transactions on Wireless Communications*, Vol. 12, No. 2, pp. 636–645, 2013.
56. L. Schehlmann, S. Abt, and H. Baier. Blessing or curse? Revisiting security aspects of software-defined networking. In *10th International Conference on Network and Service Management (CNSM) and Workshop*, pages 382–387, 2014.
57. S. Scott-Hayward, S. Natarajan and S. Sezer, A survey of security in software defined networks, *IEEE Communications Surveys & Tutorials*, Vol. 18, No. 1, pp. 623–654, 2016.
58. G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *Design Automation Conference (DAC)*, 2007.
59. A. I. Swapna, M. R. Huda, and M. K. Aion. Comparative security analysis of software defined wireless networking (sdwn)-bgp and netconf protocols. In *2016 19th International Conference on Computer and Information Technology (ICCIT)*, pages 282–287, 2016.
60. P. Tuyls, G. Schrijen, B. Skoric, J. van Geloven, N. Verhaegh, and R. Wolters. Read-proof hardware from protective coatings. In *8th Int. Workshop on Cryptographic Hardware and Embedded Systems(CHES)*, 2006.
61. J. D. Tygar, V. Wen, A. Perrig, R. Szewczyk and D. Culler, Spins: Security protocols for sensor networks, *Wireless Network*, Vol. 8, p. 521534, 2002.
62. L. Valov, R. Waser, J. R. Jameson and M. N. Kozicki, Electrochemical metallization memories–fundamentals, applications, prospects, *Nanotechnology*, Vol. 22, p. 254003, 2011.
63. E. I. Vatajelu, G. D. Natale, M. Barbareschi, L. Torres, M. Indaco and P. Prinetto, STT-mram-based PUF architecture exploiting magnetic tunnel junction fabrication-induced variability, *ACM Journal on Emerging Technologies in Computing Systems*, Vol. 13, No. 1, p. 5, 2016.
64. Y. Yoshimoto, Y. Katoh, S. Ogasahara, Z. Wei, and K. Kouno. A reram-based physically unclonable function with bit error rate lt; 0.5 In *2016 IEEE Symposium on VLSI Technology*, pages 1–2, 2016.
65. K. Zhao and L. Ge. A survey on the internet of things security. In *2013 Ninth International Conference on Computational Intelligence and Security*, pages 663–667, 2013.
66. X. Zhu, S. Millendorf, X. Guo, D. M. Jacobson, K. Lee, M. M. Nowak S. H. Kang, and D. Fazla. Pufs based on resistivity of mram magnetic tunnel junctions, 03 2015.

Fatemeh Afghah received the B.Sc. and M.Sc. degrees (with Hons.) in Electrical Engineering from Khajeh Nassir Toosi University of Technology (K.N.T.U), Tehran, Iran, and the Ph.D. degree in Electrical & Computer Engineering from the University of Maine (UMaine), Orono, ME, USA, in 2005, 2008, and 2013, respectively. She was a Visiting Student with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD, USA, from 2011 to 2012. Currently, she is an Assistant Professor with the School of Informatics, Computing and Cyber Systems, Northern Arizona University (NAU), Flagstaff, AZ, USA, where she is the Director of Wireless Networking and Information Processing (WiNIP) Laboratory. Prior to joining NAU, she was an Assistant Professor with the Electrical and Computer Engineering Department, North Carolina A&T State University, Greensboro, NC, USA, from 2013 to 2015. Her research interests include wireless communication networks, decision making in multi-agent systems, radio spectrum management, game theoretical optimization, and biomedical signal processing.

Bertrand Cambou is a Professor of Practice at Northern Arizona University where his primary areas of research are in cybersecurity and how to apply nanotechnologies to strengthen hardware security. Dr. Cambou was selected by the American Association for the Advancement of Science (AAAS), and the Lemelson Foundation as one of their Inventor Ambassadors for 2016/2017. He has previously worked as a CEO in Silicon Valley in nanotechnologies where his organization won a contract with IARPA with applications related to quantum cryptography. He worked in the smartcard industry at Gemplus (now part of Gemalto) as COO, and in the POS/secure payment industry at Ingenico USA as the CEO. He was an Executive VP at AMD in charge of the Memory Group, and spent 15 years at Motorola Semiconductor (now part of NXP), where he was CTO for 5 years and was named Distinguished Innovator and scientific advisor of the BOD. He is the author or co-author of 50 US patents pending or granted in microelectronics and cybersecurity, and has published scientific and technical papers with more than 1100 citations. Dr. Cambou holds a Doctorate degree from Paris-South University, an Engineering degree from Supelec, and an undergraduate degree from Toulouse University.

Masih Abedini was born in 1986 in Iran. He received his M.Sc. degree in Electrical Engineering (Telecommunication Network) from Isfahan University of Technology in 2012. His research interests include Mobile Ad-Hoc Networks, Software Defined Networks, and Intrusion Detection Systems. He is a graduate student member of IEEE.

Sherali Zeadally is an associate professor at the University of Kentucky. He received his Bachelor and Doctoral degrees in computer science from the University of Cambridge, England, and the University of Buckingham, England, respectively. He is a Fellow of the British Computer Society and a Fellow of the Institution of Engineering Technology, England.