Spoofing Prevention via RF Power Profiling in Wireless Network-on-Chip

Brian Lebiednik
Army Cyber Institute
West Point, NY, USA

Sergi Abadal
Universitat Politècnica de Catalunya
Barcelona, Spain

Hyouk Jun Kwon
Georgia Institute of Technology
Atlanta, GA, USA

Tushar Krishna
Georgia Institute of Technology
Atlanta, GA, USA

ABSTRACT

With increasing integration in SoCs, the Network-on-Chip (NoC) connecting of cores and accelerators is of paramount importance to provide low-latency and high-throughput communication. Due to limits of scaling of electrical wires, especially for long multi-mm distances on-chip, alternate technologies such as Wireless NoC (WNoC) have shown promise. Since WNoCs can provide low-latency one-hop transfers across the entire chip, there has been a recent surge in research demonstrating their performance and energy benefits. However, little to no work has studied the additional security challenges that are unique to WNoCs. In this work, we study the potential threat of spoofing attacks in WNoCs due to malicious hardware trojans. We introduce Veritas, a drop-in solution aimed at detecting and correcting such spoofing attacks. To this end, our solution exploits the static propagation environment of WNoCs to associate each node to a power profile. We demonstrate that, with small area and power overheads, Veritas works well in a variety of settings.

1 INTRODUCTION

Network-on-Chip (NoC) is currently the paradigm of choice to interconnect the different components of System-on-Chips (SoCs) or Chip Multiprocessors (CMPs). As the levels of integration continue to grow, however, current NoCs face significant scalability limitations, and have prompted research in novel interconnect technologies. Among these, wireless on-chip communications have garnered considerable attention due to their low latency, architectural flexibility, and inherent broadcast capabilities [2, 7, 13]. Architecting manycore systems with Wireless Network-on-Chips (WNoCs) is an active area of research [3] since low-latency broadcasts can facilitate scalable coherence and consistency.

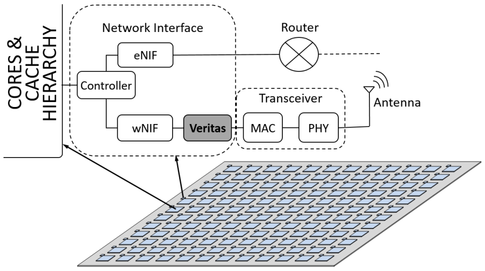

Figure 1: Schematic representation of Veritas within a wired-wireless NoC architecture.

The adoption of the WNoC paradigm brings up many new challenges. Among them, security is one that has not received much attention from the community. The broadcast nature of the wireless transmissions introduces new points of entry for an attacker to compromise the chip, as we describe in this work. If accesses to the wireless medium are not protected, smart Hardware Trojans (HTs) placed in the network or in third-party components can degrade the system performance, write corrupt data in memory, or steal sensitive information.

This paper focuses on one of the potential threats to a WNoC, spoofing, or impersonating another entity to gain unauthorized access. We build on the observation that WNoCs are different from both wired NoCs and traditional wireless networks in terms of their communication mechanism and latency thresholds, which renders solutions from both domains inapplicable and drives the need for novel fast and light-weight solutions.

The main contribution of this paper is Veritas, a light-weight solution that can detect a spoofing attack caused by a HT inside of a WNoC. Spoofing attacks are remediated opportunistically by comparing the reception power profiles of the presumed and actual source of a message. Through performance and cost analysis, we show that Veritas can protect a WNoC from advanced HTs with small overheads.

This paper is set forth as follows. First, we provide some background on WNoC in Sec. 2. Next, we discuss the threat model in Sec. 3 and our proposed architecture solution in Sec. 4. Then, we evaluate our proposal in Sec. 5, discuss related work in Sec. 6, and conclude the paper in Sec. 7.

2 BACKGROUND

As exemplified in Figure 1, the WNoC paradigm basically comprises a co-integration of antennas and transceivers with

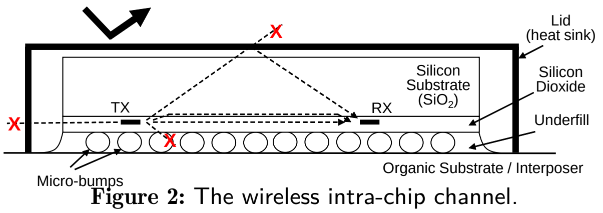

Figure 2: The wireless intra-chip channel.

cores, complementing the wired NoC. Information is first modulated by the transceiver at a frequency much higher than the processor clock, e.g. 60 GHz [3], and then radiated by the local antenna. Signals propagate within the chip package and are received by all the tuned-in antennas.

Figure 2 illustrates the typical structure of a flip-chip package, which is crucial to understand wave propagation in a WNoC. The chip consists of a set of metal layers within an insulator (SiO_2) placed on a silicon substrate. This structure is flipped, connected to the system via an array of metallic micro-bumps, and covered with a metallic heat sink. In this configuration, signals reach the receivers possibly after multiple reflections [6], but cannot scatter outside the package. Note that, around 60 GHz, the micro-bumps and subsequent metallizations obstruct the signals because their pitch (∼100 µm) is much lower than the wavelength of the radio waves (∼1 mm) [6]. Thus, in such a controlled environment, humidity effects on propagation are negligible and signals cannot leak to or come from outside the package.

The transceiver interfaces the antenna with three modules. The physical layer (PHY) modulates and amplifies the signals to a known, controlled power level minimizing transmission errors. Then, the Medium Access Control layer (MAC) ensures that all nodes can access the medium reliably, either by completely avoiding collisions [13] or by managing then in schemes where nodes contend for the channel [14]. Finally, the Network Interface (NIF), located between the core and the transceiver, performs address translation and admission control tasks. A unique trait of WNoC is that its static and quasi-deterministic propagation allows to design PHY/MAC/NIF solutions to fine-tune transmitted power [15], detect collisions [14] and, as we propose in this work, protect nodes from spoofing attacks.

3 THREAT MODEL: SPOOFING

Since the WNoC naturally acts as a shared medium [2], any node can broadcast information. This can be leveraged by malicious cores to cause system-level problems by manipulating the source address of flits. Hence, it is important to have a mechanism to detect these anomalies in a timely manner to prevent application or data corruption.

Spoofing could be employed to respond to legitimate requests originally intended for a given node x. Before x can answer with the requested information, another rogue node r responds with false information, causing the application to crash. A more complex r might respond with incorrect data that does not lead to a crash, but rather to incorrect outputs or loss in performance. In both cases, insecure WNoCs may be an entry point for spoofed messages.

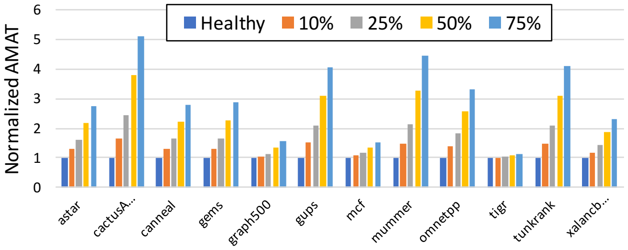

Figure 3: Potential Spoof Attack: Average Memory Access Time (AMAT) of workloads as a function of probability of spoof invalidations to the L1 from a rogue Directory.

To quantify the harm of a potential form of spoofing attack, we modeled a scenario where the malicious node r spoofs the directory ID and continually asks x to invalidate lines in its L1 cache with some probability relative to requests. We simulated this across a suite of cloud workloads. Figure 3 demonstrates that even with 10% spoof invalidations, the performance can drop by 27% on average, especially if the workloads have high L1 hit rates in the healthy scenario. An aggressive spoofer that broadcasts invalidates at 75% can make the average performance drop by 2.8×. This is an attack that could be disguised since a drop in L1 hit rate is a performance issue, but will not make the program crash.

In this work, we consider that spoofing attacks can only be performed from inside the system because signals cannot pass through the chip package, as discussed in Sec. 2. Besides this, it is common practice to assume that the HT is placed in a digital circuit due to the complexity of RF design. Therefore, HTs cannot alter the PHY layer and, more specifically, the amplifier that determines the RF power profile. Another common assumption we make is that Veritas, our solution, cannot be compromised [5].

4 SECURE ANTI-SPOOFING MICROARCHITECTURE: VERITAS

We design Veritas, a hardware solution that leverages the uniquenesses of WNoC to address spoofing attacks. We cannot guarantee authenticity using asymmetric keys, which is a widespread technique in wireless networks, because it requires a large amount of resources. Asymmetric encryption can be orders of magnitude slower than symmetric encryption, which even in the best case requires several cycles per byte [18], thus becoming a huge bottleneck in the processor. Fast and lightweight alternatives are required instead.

Overview. The WNoC paradigm offers a unique possibility of using the received RF power levels to determine the identity of the source of a given packet. In conventional wireless communications, propagation is modeled as a stochastic process as it depends on many random factors such as the environment, mobility, blocking, and so on. On the contrary, the WNoC scenario is static and can be explored thoroughly. In fact, the path loss between any two antennas can be measured beforehand via an accurate channel characterization.

Building on this observation, Veritas converts the received power into an effective source address and compares it with the ID contained in the packet header. A mismatch raises

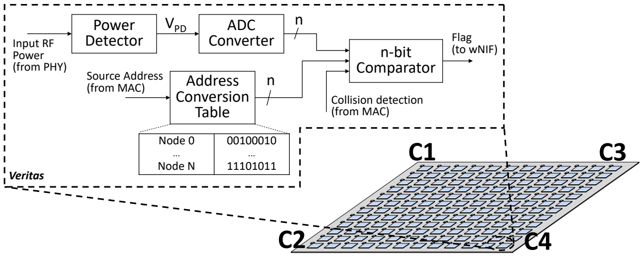

Figure 4: Schematic representation of the Veritas module integrated in the chip corners C1–C4.

a spoofing alert. The challenge with the power profile is that nodes equidistant from the transmitter may receive very similar powers, making it hard to detect a spoofer if it happens to lie on the same contour as the expected sender. To handle potential false positives, we propose to place the Veritas modules at the cores located at the corners of the chip (C1–C4) and detect spoofers with trilateration. We validate this in our evaluations and demonstrate that this placement is sufficient to uniquely distinguish between every sender[1].

Microarchitecture. Figure 4 depicts the microarchitecture of the Veritas module. In a setup phase, each and every node of the network is prompted to send an initialization message in order. This needs to be done only once and it is used by the nodes equipped with Veritas to fill an address conversion table with *{source address, voltage level}* pairs.

During runtime, for every received message, the power from the MAC is probed by a Power Detector (PD), for which designs exist for on-chip and millimeter-wave (mmWave) applications [19]. The PD translates the power level at the output of the receiver's low-noise amplifier (LNA) into a voltage level V_{PD}, which is later converted into a digital quantity using a n-bit Analog-to-Digital Converter (ADC). The MAC module also provides the source address of the packet, which is translated into a digital representation of a voltage level using the address conversion table. Finally, the two voltages are compared only when the MAC module confirms no collision. A mismatch is broadcast by Veritas, forcing all nodes to ignore all wireless messages until the OS solves the issue. The OS can either power gate the wireless NIF of the rogue node or preempt the rogue thread.

Design Issues. Without loss of generality, let us assume that all nodes are allocated with the same RF power. Since equidistant cores may reach some corner nodes with very similar power levels, two entries of the conversion table may contain the same voltage value. To address this, all duplicate entries are set to zero and the comparator is designed to not raise the flag when one of the operands is zero. Then, the PD and the ADC are carefully designed to avoid the same duplicate entries in the four corners, ensuring that all nodes can be unequivocally identified using the received power.

To evaluate the dynamic range of the PD, the wireless channel needs to be characterized to determine the maximum and minimum power expected at the corners. Even within the dynamic range, PDs may incur into a linearity error. Another source of uncertainty is the ADC, which only allows to distinguish between 2^n voltage levels for an n-bit implementation. Finally, thermal noise can also introduce variations in the received signal. However, the impact of noise is low since the error rate requirements of the scenario force to have very large signal-to-noise ratios. As we will see next, Veritas takes all these issues into consideration.

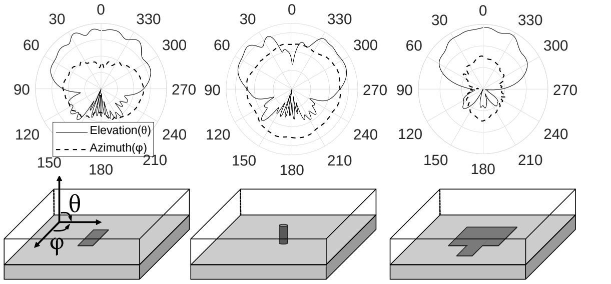

Figure 5: Radiation pattern of evaluated antennas: aperture (left), monopole (center), and patch (right).

5 EVALUATION

Simulation Methodology. We evaluate Veritas by performing the power profiling of a typical chip. We use CST MWS [1], a full-wave electromagnetic simulation tool, to model a 20×20 mm^2 die within a realistic flip-chip package. Antennas and circuits are placed within a 13-μm thick SiO$_2$ (loss-free, ε_r = 3.9), which has a 500 μm-thick layer of bulk silicon (ρ = 10 Ω-cm, ε_r = 11.9) and a metallic heat sink on top, and rests over an array of solder bumps with 100-μm pitch and a ceramic carrier. We divide the chip into 4×4 tiles and place an integrated 60-GHz antenna in each tile. Note that the methodology is amenable not only to multiprocessors, but to any application involving a WNoC [4].

To demonstrate the validity of Veritas in different WNoC designs, we consider three types of antennas. The antennas are sketched in Fig. 5 together with their on-chip radiation patterns[2]. The aperture is a slot cut out of a metallic plane within the SiO$_2$, small enough to generate a quasi-isotropic radiation at 60 GHz. Due to chip package effects, the aperture tends to radiate towards the heat sink. The monopole antenna is a vertical, single-ended TSV, that radiates almost omnidirectionally in the co-planar direction. Finally, the patch antenna is a metallic sheet placed in the first layers of the metal stack. Fed from the side, the patch radiates mostly upwards with a dipole-like behavior in the azimuth. See [12] for more details on the different antennas.

For all node pairs and antenna types, we evaluate $|S_{ij}|^2 = P_{r,i} \ / \ P_{t,j}$, this is, the fraction of signal transmitted from node j that is received by node i. The S matrix is enough to obtain the power profile within the chip because the RF power allocation strategy ($P_{t,j}$ for all j) is known.

Results. After obtaining the S matrix for the different antennas, we determine the resolution required to avoid having

[1] Three locations are enough, but more robustness can be added by placing Veritas at multiple cores at the cost of higher area and power.

[2] Radiation patterns are typically evaluated in the far field, which is not necessarily the case here. However, they still help to understand the RF power profile.

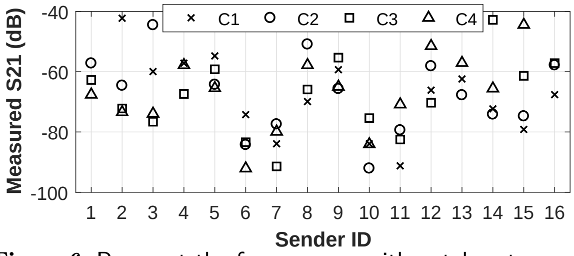

Figure 6: Power at the four corners with patch antennas.

the same duplicated entries in the four corners. Figure 6 exemplifies this process for the patch antenna: the max-min power distance, which determines the dynamic range of the PD, is ∼49 dB. After checking all combinations, we identify nodes 5 and 9 as the worst case. Those nodes reach all corners with similar power; the ambiguity, however, is resolved by C1 and C3, whose received powers differ by ∼4.6 dB. Thus, if noise and PD-ADC errors are less than 4.6 dB, then Veritas unequivocally identifies all nodes. With the dynamic range of 49 dB, this resolution is achieved with $n = 5$ bits.

Since each antenna has a distinct radiation pattern, different results are obtained (see Table 1). Due to their almost omnidirectional radiation in the chip plane, the monopole and the aperture have lower dynamic range requirements. Also, the attenuation of signals over distance is more predictable at all directions, reducing the amount of ambiguous cases. As a result, the resolution requirements are relaxed.

Overhead. Veritas would incur minimal area and power overheads. PDs as small as 0.006 mm^2 consuming less than 1 mW could meet the requirements set above [19]. Moreover, an ADC operating at ∼100 MS/s (enough to allow spoofing protection on a per-packet basis) with 9-bit resolution has been reported to occupy 0.028 mm^2 and consume less than 1 mW [11]. Since the anti-spoof module is only placed in four locations, the cost is also scalable.

6 RELATED WORK

Secure Wireless Networks-on-Chip. Using small world topologies, researchers have found ways of relieving single-node DoS attacks in a NoC, but do not address spoofing attacks [9]. To prevent eavesdropping and spoofing, one solution proposes a hash-based authentication with secret key [16] which incurs a huge latency cost of several hundreds of cycles per validation. To the best of our knowledge, no other work has addressed spoofing attacks in a WNoC and, in this context, Veritas represents a cost-effective solution.

Other scenarios. NoC researchers have proposed to establish some standards for securing wired NoCs and the access rights to memory units [8]. These solutions use high overhead encryption and do not take into account effects on the network. Another proposal uses an AES-like symmetric key encryption combined with an asymmetric key (anti-Spoofing) encryption [10]. In wireless sensor networks, some proposals combat spoofing by using neighbor-specific asymmetric keys, which still causes delays unacceptable for WNoC [17]. Likewise, high-latency RC6 stream cipher are used in [20] to create key pairs out of master keys, making it prohibitive in a WNoC.

Table 1: Summary of results for different antennas.

Antenna	Dynamic Range	Resolution	Number of bits
Aperture	38.12 dB	8.9 dB	≥4
Monopole	40.03 dB	8.2 dB	≥4
Patch	48.98 dB	4.6 dB	≥5

7 CONCLUSION

Veritas is a new microarchitecture to secure WNoCs from the spoofing vulnerability associated with wireless communications. Using RF power profiles, Veritas can detect and reconcile HTs attempting to spoof the source address of another node in the system. Results have shown that, with small increases in power and area, Veritas works in a 4×4 WNoC assuming a variety of antennas. In denser networks, we anticipate that the requirements of Veritas will increase moderately. Future works will further explore scalability and ways to reduce the dynamic range.

ACKNOWLEDGMENT

This work has been supported by the Spanish MINECO under contract TEC2017-90034-C2-1-R (ALLIANCE project) that receives funding from FEDER. Brian Lebiednik accomplished this research while studying at Georgia Tech, but is now working for the Army Cyber Institute.

REFERENCES

[1] 2017. CST Microwave Studio. *http://www.cst.com* (2017).

[2] S. Abadal *et al.* 2016. Scalability of Broadcast Performance in Wireless Network-on-Chip. *IEEE TPDS* 27, 12 (2016), 3631–45.

[3] S. Abadal *et al.* 2016. WiSync: An Architecture for Fast Synchronization through On-Chip Wireless Communication. In *ASPLOS*.

[4] S. Abadal *et al.* 2017. Computing and Communications for the Software-Defined Metamaterial Paradigm: A Context Analysis. *IEEE Access* 5 (2017), 6225–6235.

[5] T. Boraten and A. Kodi. 2016. Mitigation of Denial of Service Attack with Hardware Trojans in NoC Architectures. In *IEEE IPDPS*.

[6] J. Branch *et al.* 2005. Wireless communication in a flip-chip package using integrated antennas on silicon substrates. *IEEE EDL* 26, 2 (2005), 115–117.

[7] S. Deb *et al.* 2012. Wireless NoC as Interconnection Backbone for Multicore Chips: Promises and Challenges. *IEEE JETCAS* 2, 2 (2012), 228–239.

[8] L. Fiorin *et al.* 2008. Secure Memory Accesses on Networks-on-Chip. In *IEEE TC*, Vol. 57. Issue 9.

[9] A. Ganguly and A. Vidapalapati. 2012. A Denial-of-Service Resilient Wireless NoC Architecture. In *GLSVLSI*.

[10] C. Gebotys and R. Gebotys. 2003. A Framework for Security on NoC Technologies. In *IEEE ISVLSI*.

[11] Y. Z. Lin *et al.* 2013. A 9-bit 150-MS/s subrange ADC based on SAR architecture in 90-nm CMOS. *TCAS-I* (2013).

[12] O. Markish *et al.* 2015. On-chip mmWave Antennas and Transceivers. In *IEEE/ACM NOCS*.

[13] D. Matolak *et al.* 2012. Wireless networks-on-chips: architecture, wireless channel, and devices. *IEEE Wirel. Comm.* (2012).

[14] A. Mestres *et al.* 2016. A MAC protocol for Reliable Broadcast Communications in Wireless Network-on-Chip. In *NoCArc*.

[15] A. Mineo *et al.* 2016. Runtime Tunable Transmitting Power Technique in mm-Wave WiNoC Architectures. *IEEE TVLSI* 24, 4 (2016), 1535–1545.

[16] F. Pereñíguez García and J. L. Abellán. 2017. Secure Communications in Wireless Network-on-Chips. In *AISTECS*.

[17] K. Ren *et al.* 2008. LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks. (2008), 585–598.

[18] J. Rott. 2012. Intel Advanced Encryption Standard (AES-NI). In *Intel Developer Zone*.

[19] A. Serhan *et al.* 2015. Common-Base/Common-Gate Millimeter Wave Power Detectors. *IEEE T-MTT* (2015).

[20] S. Slijepcevic *et al.* 2002. On Communications Security in Wireless Ad-Hoc Sensor Networks. In *WETICE*.