Unified Testing and Security Framework for Wireless Network-on-Chip Enabled Multi-Core Chips

ABHISHEK VASHIST, Rochester Institute of Technology, USA
ANDREW KEATS, Rochester Institute of Technology, USA
SAI MANOJ PUDUKOTAI DINAKARRAO, George Mason University, USA
AMLAN GANGULY, Rochester Institute of Technology, USA

On-chip wireless interconnects have been demonstrated to improve the performance and energy consumption of data communication in Network-on-Chips (NoCs). However, the wireless interfaces (WIs) can be defective, rendering these broken links severely affect the performance. This makes manufacturing test of the WIs critical. While analog testing of the transceivers is possible, such methodologies are impractical in a Wireless NoC (WiNoC) due to large overheads. In addition to testing, security is another prominent challenge in WiNoCs, as the security breach can happen due to embedded hardware Trojans or through external attacker exploiting the wireless medium. The typical security measures used in general wireless networks are not practical in a WiNoC due to unique network architectures and performance requirements of such a system. However, both testing and security defense can potentially leverage a basic monitoring framework which, can detect malfunctions or anomalies. Based on this idea, we propose a unified architecture for testing and attack detection and protection of on-chip wireless interconnects. We adopt a Built-In-Self Test (BIST) methodology to enable online monitoring of the wireless interconnects which can also be reused for monitoring the security threats. We focus on manufacturing defects of the WIs for testing and persistent jamming attack for the security measures, as this kind of attack is most likely on wireless communication systems. The BIST methodology is capable of detecting faults in the wireless links with a low aliasing probability of 2.32×10^{-10}. Additionally, the proposed unified architecture is able to detect the persistent jamming with an accuracy of 99.87% and suffer < 3% communication bandwidth degradation even in the presence of attacks from either internal or external sources.

CCS Concepts: • **Security and privacy** → **Embedded systems security**; **Denial-of-service attacks**; *Hardware-based security protocols*;

Additional Key Words and Phrases: Network-on-Chip, Wireless Interconnect, Security, DoS, Jamming, Machine learning

ACM Reference Format:
Abhishek Vashist, Andrew Keats, Sai Manoj Pudukotai Dinakarrao, and Amlan Ganguly. 2019. Unified Testing and Security Framework for Wireless Network-on-Chip Enabled Multi-Core Chips. *ACM Trans. Embedd. Comput. Syst.* 37, 4, Article PP (November 2019), 20 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Authors' addresses: Abhishek Vashist, av8911@rit.edu, Rochester Institute of Technology, 83 Lomb Memorial Drive, Rochester, New York, 14623, USA; Andrew Keats, axk7655@rit.edu, Rochester Institute of Technology, 83 Lomb Memorial Drive, Rochester, New York, 14623, USA; Sai Manoj Pudukotai Dinakarrao, spudukot@gmu.edu, George Mason University, 4400 University Drive, Fairfax, Virginia, 22030, USA; Amlan Ganguly, axgeec@rit.edu, Rochester Institute of Technology, 83 Lomb Memorial Drive, Rochester, New York, 14623, USA.

This article appears as part of the ESWEEK-TECS special issue and was presented in the International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), 2019.

1539-9087/2019/11-ARTPP $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

To meet the computational requirements, multi or many-core systems are introduced. In such systems, traditional bus-based interconnect mechanisms were found to be non-scalable from the design perspective. This led to the adoption of the Network-on-Chip (NoC) [2, 8, 25] paradigm for interconnecting tens to hundreds of cores on the same die. Mesh or torus topologies are widely adopted in the NoC architectures due to the ease of design, efficacy and reduced time-to-market benefits [31]. The data transfer over such a conventional NoC requires multi-hop communication over the metal interconnects. Other emerging interconnects such as silicon photonics [6] and Through-Silicon-Vias (TSVs) [5, 9] are investigated as alternatives. However, adopting these techniques need to address some challenges such as electrical-to-optical signal conversion [7] and heat dissipation [28, 45] will add significant silicon and performance overheads. Research in the recent years has demonstrated that on-chip wireless interconnects are capable of establishing radio communications between cores in multi-core chips. Wireless data communication links with multi GigaHertz (GHz) bandwidths in millimeter-wave (mm-wave) bands are fabricated and demonstrated [30]. Using such on-chip antennas embedded in the chip, Wireless Network-on-Chip (WiNoC) architectures [4] are shown to improve energy efficiency and latency of on-chip data communication manifold in multi-core chips [10, 39, 40].

Extensive amount of research has been carried out on enhancing the performance (such as high throughput and lower energy dissipation) of WIs or WiNoCs [15, 25, 29] and the design of WiNoCs. However, relatively little attention has been given to the information integrity and security or privacy and testing aspects of the WiNoCs, which are some of the prominent challenges to be addressed in the present day computing systems.

While security of traditional wired NoCs against various kinds of attacks such as hardware trojans (HT), eavesdropping or spoofing has resulted in appropriate defense mechanisms, the additional threats that unguided wireless interconnects can engender have not received the necessary attention. Wireless interconnects over unguided medium are vulnerable to similar security threats as any other wireless networks such as persistent jamming DoS attacks. HT inserted into the multi-core chip or an external attacker can attack the WIs or the on-chip wireless medium. As the amount of available resources on a NoC are limited, deploying the traditional security mechanism deployed on a macro-scale wireless networks such as [48] is not a viable solution. Therefore, without a security and privacy measure, a WiNoC is not a practical interconnection platform for current and future embedded multi-core systems.

Many different security attacks such as Denial-of-Service (DoS), eavesdropping, and spoofing are possible in a WiNoC, where the communication happens over a shared wireless medium, with each attack requiring its own detection and defense mechanism. Due to the presence of the on-chip wireless medium jamming and eavesdropping become more viable in WiNoCs as compared to a traditional wired NoC. In this work, we focus on DoS attacks that jams the wireless medium, as a case study for illustrating the proposed secure mechanisms. Furthermore, DoS attack is one of the most formidable attacks in wireless communication systems. For this purpose, we consider an external attacker that produces a high energy electromagnetic (EM) radiation that causes interference in the wireless medium used by the WiNoC. Moreover, it is also possible that a HT planted in the multi-core system from a vulnerable design and manufacturing process can cause a WI to transmit jamming signals to cause DoS for the other WIs. In this case, one of the WIs infected by a HT will transmit the data over wireless channel irrespective of whether it is enabled by the adopted Medium Access Control (MAC) protocol of the WiNoC. This will cause contention or interference with legitimate transmissions causing DoS on the remaining WIs. Hence, we consider and propose solution to detect DoS attacks. However, unlike traditional wireless networks, a WiNoC is severely resource-constrained while requiring high-speed operations. Our solutions are highly effective while requiring extremely low power consumption making them suitable to this particular environment.

On the other hand, the probability of manufacturing defects in Integrated Circuits (ICs) are increasing with the aggressive scaling of technology nodes due to shrinking form factors and higher process variations [3]. This makes post-manufacturing testing of multi-core System-on-Chips (SoCs) challenging and yet a non-trivial aspect to be addressed. The deployment of wireless interconnects in WiNoCs further exacerbates this problem with an additional point of failure due to fault in analog circuits and antennas which can manifest as broken communication links in the WiNoC. Therefore, testing of the WIs which enables NoC routers to access the on-chip wireless medium, becomes necessary.

Permanent faults in the WIs as well as security attacks both cause anomalous or unexpected behavior and therefore, can be potentially detected using a unified monitoring framework. The work in [42] proposes reusing existing P1500 testing infrastructure to realize a security gateway in SoCs. However, an external testing infrastructure such as JTAG or P1500 can not support online, on-die monitor during normal operations by itself. To address these shortcomings, in this work, we design a unified Built-In-Self-Test (BIST) based protection engine capable of detecting manufacturing faults as well as detecting and protecting the wireless interconnects from security threats. The rationale for selection of a BIST based mechanism rather than other forms of Design for Testability (DFT) mechanisms such as using an external Automatic Test Equipment (ATE) is driven by the fact that the data rate for these WIs operate at multi Gigabits per second (Gbps) making it impractical to perform at-speed testing using external data sources. At-speed testing is necessary, as achieving the target data rates is key to delivering the benefits of the wireless interconnects to the WiNoC.

The contributions of this work can be outlined as follows:

- To the best of our knowledge, this is the first work that proposes a unified architecture for testing as well as security of WiNoCs.
- Based on a digital equivalent fault model to represent the permanent faults expected in WIs, the BIST mechanism is developed and then modified to also be capable of detecting persistent jamming attacks.
- We propose a machine learning (ML)-based mechanism to detect and recover from persistent jamming-based DoS attacks that can disable the wireless interconnections in the WiNoC and trigger alternate routing algorithms in response to such an attack.

We evaluate the test time, quality and overhead of the BIST based testing mechanism. We present the performance of the unified architecture in detecting, isolating and protecting against a persistent jamming attack on the WiNoC.

Rest of this paper is organized as follows. Section 2 reviews the existing works on WiNoC testing and security. The architecture of adopted WiNoC is described in Section 3. Fault and persistent DoS security threat model utilized in this work is presented in Section 4 with the proposed unified architecture described in Section 5. The evaluation of proposed unified testing and security framework and the overhead incurred is discussed in Section 6 with conclusions drawn in Section 7.

2 RELATED WORK

Here, we discuss the existing works pertaining to two aspects, namely, testing of NoCs in general and WiNoCs in particular and security of WiNoCs respectively.

As NoC paradigm emerged as the SoC interconnection backbone, various researchers proposed the idea of reusing the NoC interconnection as a Test Access Mechanism (TAM) [35]. In [41] the authors assumed NoC as fault free and used it for delivering the test vectors to the functional cores. However, assuming the interconnection fabric as fault free is not a realistic assumption. For testing the wired inter-switch link a BIST approach is presented in [21], where a high-level fault model is used that targets the crosstalk effects between the links. In [20] authors presented a unicast and multicast based approach for testing of NoC components, where, in multicast mode, the test packets have multiple destinations and improved test time compared to unicast messaging. In [22] authors use the regularity in the NoC switches to send test packets. Test vectors are sent simultaneously to all identical ports, and for all identical routers. In [49] authors presented a RF based wireless test network to test SoCs. In that work authors only presented wireless network to transmit control signals. However, in that work actual test data was not delivered using the wireless interconnects, thereby limiting the potential benefits. Authors in [50] proposes test scheduling based on [49].

WiNoCs have been shown to outperform wired NoCs and provide energy-efficient on-chip communication fabrics [10]. However, one of the main hurdles for large-scale adoption of WiNoCs is the fact that WiNoCs are enabled by wireless transceivers operating in the Radio Frequency (RF), Ultra Wide Band (UWB), millimeter wave (mm-wave) or Terahertz (THz), which are essentially high-speed analog circuits. The manufacturing testing of such circuits is challenging as typically, analog testing is performed to characterize the transceivers [16]. However, analog testing is impractical in a WiNoC with multiple transceivers due to large test times. Analog BIST would require several high-speed Digital-to-Analog Converters (DAC) and Analog-to-Digital Converters (ADC) to create analog test signals such as chirp or saw-tooth signals for testing multiple transceivers deployed across the WiNoC [37]. Consequently, the area overhead of such an analog BIST system will make this approach impractical in a WiNoC scenario. To alleviate these problems a digital BIST for digital equivalent fault models of on-chip wireless interconnects is proposed in [38]. In addition to the testing challenges, on-chip wireless interconnects expose the interconnection fabric to various security threats. While securing wired NoCs have received attention from researchers in recent years [17], mechanisms to secure WiNoCs have not been well developed.

In [19], a small-world graph based WiNoC architecture was proposed to mitigate DoS attacks, but small-world irregular topologies have negative implications on design and verification effort. On the other hand, hash based authentication to prevent eavesdropping has been proposed in [33]. However, detecting and defending against jamming attacks in WiNoCs have not been addressed. In [27] a secure WiNoC architecture has been proposed that can protect against DoS, eavesdropping and spoofing. However, this work does not address the issue of jamming attack from an external attacker assuming that the packaging will protect against such attacks. This may not be true for all kinds of chips or packaging materials. Additionally, the solution is too naive to detect complex and sophisticated DoS attacks.

On other hand, although machine learning (ML) has been used in the context of NoC systems for congestion-aware routing [24], but not used for securing NoC, especially against DoS attacks due to the resource constraints. However, there exist works on detecting DoS attacks on cloud or IoT systems. We review some of them to draw analogy and outline the differences here. In [48], a decision tree (DT) based algorithm is devised for detecting DoS attacks in cloud environment. Further, it is combined with signature detection techniques for improving efficiency. Similar works using radial basis function (RBF) neural networks (RBFNNs) [26], artificial NNs (ANNs) [34], probabilistic neural network [1] are proposed, and [13] presents a comparison of different ML algorithms when detecting Distributed DOS (DDoS) attacks in cloud and IoT devices. However, due to the considered features such as signal-to-noise ratio (SNR), transmission power and energy and the involved complex computations, the resource constraints prohibit straighforward plug-and-play adoption of those techniques on WiNoCs.

Furthermore, the existing architectures designed for testing lack security features and the secure designs do not address the testing needs. Therefore, in this work we propose a unified architecture that can be used as a BIST for the wireless interconnects while also protecting against persistent jamming DoS attacks.

3 ADOPTED WINOC PLATFORM

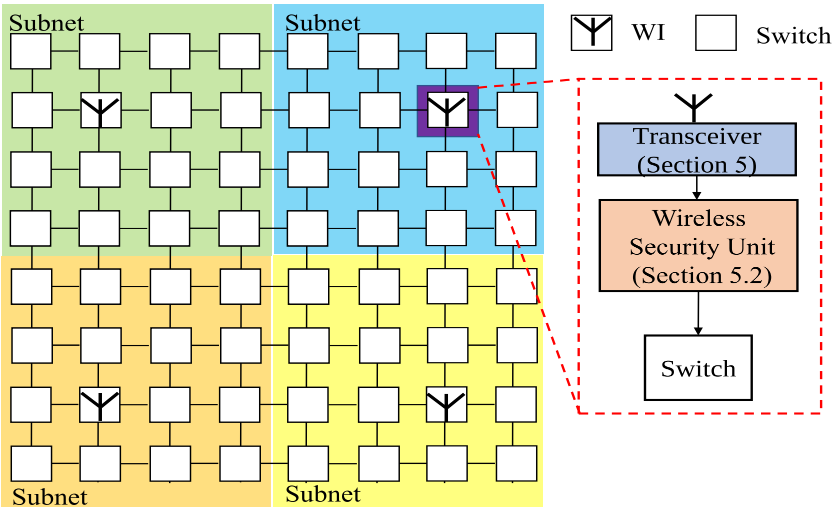

Fig. 1. System architecture of proposed secure WiNoC

Several WiNoC architectures have been proposed over the past few years [10]. While any of those architectures can be adopted to design the unified test and security architecture, we adopt a hybrid wired and wireless NoC, which has been proposed and studied extensively in the recent years [11, 12]. In this architecture, the topology is a wireline NoC overlaid with wireless interconnects. We adopt a mesh architecture for the wired NoC topology due to its low-complex design feasibility, verify and manufacture due to uniformity of link lengths as shown in Figure 1.

Inspired by previous works such as [10], we divide the mesh into multiple subnets to deploy the WIs among NoC switches. A central switch in each subnet is then equipped with a WI to

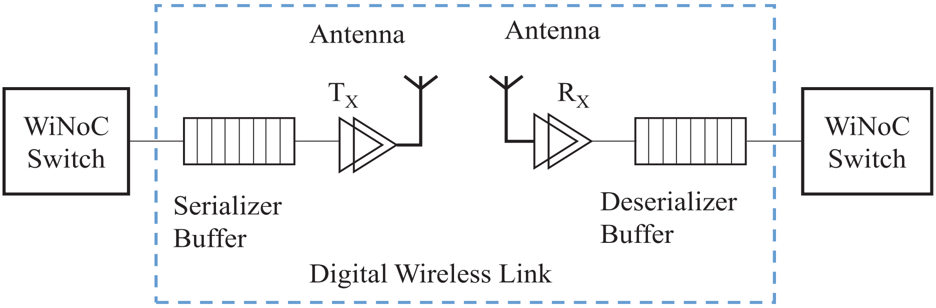

Fig. 2. Wireless link modeled as a digital link

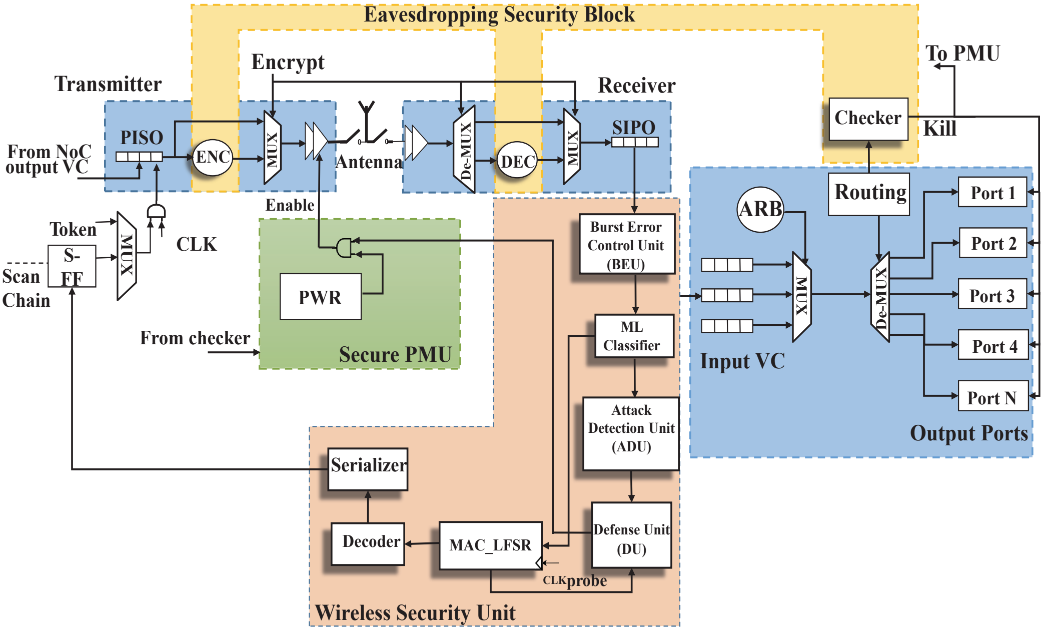

Fig. 3. Proposed unified BIST and security architecture. Color coding shows how the test flit is created and received by the LFSRs. BIST and security components shown in bold

facilitate data communication using the wireless medium. We propose the use of on-chip embedded miniature antennas operating in the unlicensed 60 GHz mm-wave band, which can establish direct communication channels between the WIs. We have adopted mm-wave zig-zag on-chip antennas, which have a bandwidth of 16GHz for intra-chip communications through typical on-chip dielectric materials [36].

To ensure high throughput and energy efficiency, we adopt the transceiver design from [46, 47], where low power design considerations are taken into account. Non-coherent On-Off Keying (OOK) modulation is chosen, as it allows relatively simple and low-power circuit implementation without the need for power-hungry carrier recovery and high-frequency synchronization circuitry. The wireless link model is depicted in Figure 2.

Due to the chosen antennas being non-directional and tuned to the 60GHz channel, the wireless channel is a shared medium, requiring a contention free Medium Access Control (MAC) protocol. To avoid non-scalable central arbitrations and power-hungry synchronization across the chip we adopt a distributed wireless token passing mechanism to grant access of the shared wireless channel to the WIs. Each WI can only occupy the token for a pre-determined maximum time that can be optimized based on application traffic.

We adopt a Virtual Channel (VC) based wormhole switching protocol for routing data where packets are broken into smaller flow control units or flits [14]. A forwarding-table based routing over pre-computed shortest paths is adopted to minimize the test time. Only the header flits of the message packets are routed using the forwarding table to determine the next hop reducing both computational complexity and eliminating the need for maintenance of global routing information. The routing tree is constructed using Dijkstra’s algorithm, which extracts a Minimum Spanning Tree (MST) providing the shortest path between any pair of nodes in a graph. Consequently, deadlock is avoided by transferring packets along the shortest path routing tree, as it is inherently free of cyclic dependencies. The unified architecture for testing and security in illustrated in Figure 3 with more details in Section 5.

4 FAULT AND ATTACK MODEL

Before presenting the details of proposed framework, we introduce the fault and attack models that the proposed wireless test and security measure can detect.

4.1 Fault Model

The wireless interconnects transmit both data signal and control signals. The data signals are flits that are transferred between the transmitters and receivers whereas the control signals are the MAC signals which determine which transmitter has access over the channel to send the data. We propose fault models for both and develop testing methods for both types of faults. Here, we focus only on faults that result from physical manufacturing defects.

Faults of the data signals can be caused by failures at transceiver such as out-of-tune antennas. Process variations and manufacturing faults can distort the shape of metallic structures in an IC [3]. The antenna elements being fabricated as metallic structures in the CMOS process can suffer from such distortions. This in turn results in loss of tuning of the antenna element to the specific carrier frequency. Such a loss of tuning essentially makes the antenna unable to communicate using the wireless channel resulting in permanently broken wireless links. A permanent failure of an antenna will disable its WI. The oscillators, modulators, drive amplifiers of the transceivers and the Low Noise Amplifiers (LNA) and demodulators of the receiver at RF and mm-wave frequencies consist of inductors responsible for impedance matching and signal coupling. As these inductors are also fabricated out of metal spirals in the IC, they are also susceptible to the same fault scenarios. All these factors can cause transceiver failure resulting in permanent failure of a transceiver to either transmit or receive data over the wireless channel. Although the transceivers are analog circuits, we model these faults as data stuck-at faults. This because the wireless link can be modeled as a digital link as shown in Figure 2. This is feasible as the analog transceivers are ultimately responsible for transmitting digital bits after modulation. As diagnosis of the root-cause of the fault is not the goal in this paper, digital fault model is effective and efficient. This is because, the goal of the transceivers is to transmit and receive from the digital NoC switch buffers and therefore, if the digital bits are not transmitted and received properly, it does not matter, which part of the transmitter is faulty. Therefore, we model the wireless link including the digital buffers of the NoC switch as a digital link and model its faults digitally to simplify the fault model and testing methodology.

In particular, in an OOK transceiver scenario, if a transmitter is unable to send data, it results in a stuck-at-0 (if not transmitting the carrier is considered a logic '0') fault for the transmitter. Conversely, if the switching transistor in the modulator is always stuck-short, then the transmitter will always send out the carrier signal causing a stuck-at-1 fault. An analogous scenario may arise in the receiver when it fails to receive signal resulting in a stuck-at-0 data fault. Therefore, data faults can be stuck-at-0 or stuck-at-1 between the transceivers. If a transmitter or receiver has a stuck-at fault, multiple wireless links connected to that transmitter or receiver will have the same stuck-at fault. This is analogous to a fan-out or fan-in scenario in digital testing. Therefore, we model the analog transceiver circuit failures as digital data stuck-at faults at the WIs. This enables us to simplify the testing infrastructure. Moreover, it must be noted that each wireless link is a serial interconnect. Therefore, a stuck-at fault at a transceiver means all bits transmitted or received at that WI will be stuck-at. However, the serializer/deserializer buffers are also parts of the WIs, and those maybe faulty as well. In case of serializer/deserializer buffer faults, only bits corresponding to the faulty buffer locations will have stuck-at faults. The proposed BIST method can test for single or multiple stuck-at faults at the serializer/deserializer or the transceivers.

In addition to the stuck-at faults we also test for delay faults of the transceivers. Due to the defects in the transceivers such as a reduced bandwidth of the amplifiers, antennas or the mixer data may be transferred correctly, but not at the designed speed. Moreover, due to defects in capacitors, inductors or transformers in the transceivers, data dependent delay faults can happen. For example, in the case of the wireless links, due to the limitations in speed of the transmitter or receiver, it may happen that the response to a ”lone-pulse” data, where there is a single ’1’ (or ’0’) in a long train of ’0’s (or ’1’s) is not correct. The long train of ’0’s stabilize the transceivers and then a short single bit ’1’ can cause capacitors and inductors in the analog transceivers need full charging or discharging, causing a slower than expected response time. Similar effects can cause unexpected behavior from partial (or full) charge (or discharge scenarios) in the analog transceivers. In general, these faults are due to inter-symbol interference, caused by a slow transceiver. This makes the delay faults in the wireless interconnects data dependent, similar to crosstalk/delay faults in wired interconnects. Therefore, for data signals we consider both stuck-at and delay faults.

The MAC enables a particular transmitter to send data over the wireless medium. We model the MAC control of the transmitters analogous to a tri-state buffer circuit. Therefore, we model possible faults of the MAC circuit as either stuck-enabled or stuck-disabled. This implies that due to manufacturing defects, the MAC circuit loses the controllability and manifests the defect by either always enabling or disabling a particular transmitter. In the testing methodology, a single stuck-enable or single stuck-disable fault is assumed.

4.2 Attack Model

From the security perspective, several security and privacy attacks are possible on electronic systems such as multi-core processors, especially with wireless interconnects. In this work, we consider persistent jamming based DoS attacks on the wireless interconnections of a WiNoC. While such attacks have been studied in the context of wireless networks, the available protection methods are not applicable to the WiNoC platform due to the resource constraints and other aforementioned concerns. The most common approach to neutralize jamming attacks is frequency or channel hopping [44] in macro-scale networks. However, this method cannot be used in a WiNoC, as typically the WiNoCs operate on a single or a few shared channels on the chip. In the presence of such a persistent DoS jamming attack either from an external or internal attacker, there will be interference among the attacker and the legitimate transmitter. This interference will cause high error rates due to interference noise. Moreover, as the attack is persistent, it will cause errors in contiguous bits of flits resulting in burst errors. Over the duration of the attack, these errors will span multiple flits and therefore, cause burst errors in multiple consecutive flits of a packet.

However, burst errors in both wired and wireless NoC links can happen as a random event as well such as, power source fluctuations, ground bounce or crosstalk [18]. However, the burst errors due to random events such as crosstalk will be relatively short lived, due to the data transition pattern in that cycle. On the other hand, burst errors resulting from jamming could be sustained for longer duration as a short DoS attack is not an effective attack. A few burst errors caused by a short-lived DoS can be corrected/detected by a burst error correction/detection (BEC) code depending on its correction capability. In the absence of such a BEC mechanism, a request for retransmission can be sent in case of erroneous flits from the upper layers of the NoC protocol stack. Therefore, to be truly effective as an attack, the jamming has to be persistent to cause enough flits to be in error such that the existing BEC mechanism either cannot correct it or retransmission requests are prohibitively expensive due to a potentially large number of requests. Hence, we consider persistent jamming attacks either from a single external attacker or a single internal HT which affect the WIs in the WiNoC.

5 UNIFIED WINOC TEST AND SECURITY ARCHITECTURE

For manufacturing testing of the WIs, we adopt a BIST approach that enables a periodic in-field testing. The same BIST infrastructure can be adapted to be reused for probing the WiNoC and securing against persistent jamming attacks. The architecture of the proposed unified framework is shown in Figure 3. Here, we discuss the architecture along with the test and attack detection methodology.

5.1 BIST-based Test of the Wireless Interconnects

In the proposed architecture, there is a Probe Control Unit (PCU) that can receive an assert signal from a Primary Input (PI) of the chip which is identical to the Test Mode Select (TMS) of a JTAG/P1500 standard. When TMS is asserted, the PCU will suspend the normal operation of the WiNoC and enable a Linear Feedback Shift Register (LFSR) called MAC-LFSR that will grant access of the on-chip wireless medium to the WIs in a pseudo-random sequence. Each WI is equipped with a Data-LFSR. On being enabled by the MAC-LFSR the Data-LFSR creates a packet with pseudo-random bits to be sent from the WI. This data includes the destination address of the target WI making the selection of the destination pseudo-random as well. Data padding is done to embed the source address of the sending WI in the packet. The Data-LFSR creates pseudo-random bits necessary for testing the stuck-at faults as well as the delay faults in the data signals. Moreover, as the BIST tests only the wireless links between the WIs, errors in the header flit does not cause mis-routing and we do not cover faults in the routing logic blocks in this paper.

The sequence generated by the MAC-LFSR is first passed into a decoder, which will convert the LFSR output sequence into a one-hot encoded sequence. This one-hot encoded sequence is then passed through a parallel load-shift register into the scan flip-flops, which form a scan chain. This scan chain will be used to set the token possession register, T at the WiNoC switches. Therefore, the length of scan chain is same as the number of WIs in the WiNoC. The scan chain, setting up the test vectors for the token registers, is interconnected between WIs with wired links which maybe pipelined if the wire length between the WIs cannot be traversed in one clock cycle. The clock of the serializer buffer of the transmitter in the WIs are gated with the content of the token register. Therefore, the MAC-LFSR sequence converted into one-hot sequence will enable a single WI to transmit the data generated by its Data-LFSR. All the receivers will receive this data packet and pass it to their respective Multiple Input Signature Register (MISRs). The Data-LFSRs in all the WIs are constructed using the same characteristic polynomial. This would make test data transmission from any sequence of WIs indistinguishable from another. However, the test packet has the source address of the WI randomly chosen by the MAC-LFSR. Therefore, the MISR captures not only, the pseudo-random test data from the Data-LFSR but also that of the MAC-LFSR requiring the MISR length to be same as that of the sum of the lengths of the Data and MAC LFSRs. The MAC-LFSR operates on a slower clock CLK_{pkt} while the Data-LFSRs operate at the faster clock CLK_{data} that operates at the data rate of the transceivers.

In this way, if any WI is stuck-disabled, then that fault will be captured as that WI will not transmit when the MAC-LFSR enables it and the BIST mechanism is able to test both data and control concurrently. To test for any WI being stuck-enabled, in addition to the random testing by the MAC-LFSR, the WIs will be tested with a special sequence, which is all zeros in the beginning of the test sequence. This will disable all the WIs and ideally no receiver should receive any data. However, if any WI is stuck-enabled, the receivers will receive the packets generated by the Data-LFSR of that WI declaring a single stuck-enabled fault. If multiple WIs are stuck-enabled, they will transmit all at the same time and their transmissions can not be individually recognized. For this reason, only a single stuck-enabled fault can be reliably diagnosed. Multiple such faults can be detected but the faulty WIs can not be diagnosed with this design. However, due to the sequential checking for stuck-disabled faults, multiple stuck-disabled faults can be detected and the faulty WIs can be diagnosed.

5.2 Attack Detection Methodology

In addition to the BIST-based test elements mentioned above, we equip the receivers of WIs with Wireless Security Unit (WSU) that will enable detection of persistent jamming from both internal HTs as well as external attacker. The WSU consist of a Burst Error Control Unit (BEU), an ML Classifier, an Attacker Detection Unit (ADU), and a Defense Unit (DU), as shown in the Figure 3. The Parallel-In-Serial-Out (PISO) buffer represents the output buffer on the transmitter side same as the serializer buffer in Figure 2. Similarly, the Serial-In-Parallel-Out (SIPO) buffer represents the deserializer buffer on the receiver side in Figure 2. Other elements are added to the basic wireless link model in Figure 2 to enable the testing and security mechanisms as discussed next.

5.2.1 Architecture of Wireless Secure Unit. In the normal mode of operation, the data flits are received at the deserializer buffer of a NoC switch equipped with a WI. Upon reception of flits at the receiver's buffer, flits are sent to the Burst Error Unit (BEU). The BEU employs the BEC proposed in [18] to detect burst errors. The corrected flits after burst error correction are sent to the input VCs of the NoC switch to be routed downstream in parallel to the error related information as discussed in the next subsection, being sent to the ML Classifier, to remove the DoS detection mechanism from the critical path of the data transfer. The ADU further comprises of an intelligent unit which uses an ML classifier, and an attacker detection unit. The ML classifier is responsible for detecting if the system is under attack based on the input it receives from the BEU. More details of the ML classifier is presented in the next subsection. If the ML classifier detects an attack as opposed to a random burst error, it asserts a flag to the ADU. The ADU receives the input from the ML classifier and determines if the attack is internal or external as discussed in Section 5.2.3.

5.2.2 Machine Learning for Attack Detection. As aforementioned, the considered attacks in this work primarily result in causing continuous sustained burst errors in the flits (data corruption). This can be detected by observing the number of flits in error. In the proposed WiNoC, the output of BEU, which is the number of burst errors within a block, is fed to an ML classifier to detect and differentiate attacks. We experimented with multiple ML classifiers to evaluate the robustness and efficiency of attack detection in the proposed system. The different ML classifiers considered here are: multi-layer perceptron (MLP), support vector machine (SVM), k-nearest neighbors (KNN), and Decision tree (DT) classifiers. For the MLP, we considered a single hidden layer with 10 nodes is utilized, with two neurons in the output layer. We utilize a polynomial kernel based SVM in this work, as it considers the combination of the input features as well as input features for classification. Similarly, we experimented with k-nearest neighbors with k=1 and 3 in this work. In addition, we consider decision classifier namely DT. The rationale for experimenting with different classifiers are: a) there exist no unique classifier that has 'perfect' yield; b) different classifiers have different resource requirements and performance (accuracy, and latency) and c) the chosen classifiers represent different branch of ML, thus representing a wide spectrum of ML classifiers. The important factor to note is that the decision depends not only on the detection of the error in the current received flit but also on the past flits.

In order to train the ML classifier, the attacks aforementioned in Section 4 are deployed on a WiNoC (shown in Figure 1) with no security mechanisms deployed. A cycle accurate NoC simulator was modeled to operate in one of the three modes: normal, random burst errors and attack. In the normal mode, the wireless interconnects are assumed to work with the reliability level determined by the operation of the transceiver and their operating thermal noise. This type of noise is shown to result in a random Bit Error Rate (BER) of 10^{-10} or less [46]. The second mode (random burst errors) is modeled with higher BERs as the burst errors are contiguous bits of flits. BERs of 10^{-5} is used in this case [18]. Lastly, under DoS attack, a high BER of 0.5 is assumed as for identically and independently distributed (iid) data bits even a very high power jamming signal can cause errors only half of the time on an average. This is because the adopted modulation mechanism in these wireless interconnects is OOK, where on an average the data bits are represented as presence or absence of transmission. Therefore, a jamming signal will only cause errors when the transmission is supposed to be absent, which can be assumed to be half of the time for iid data.

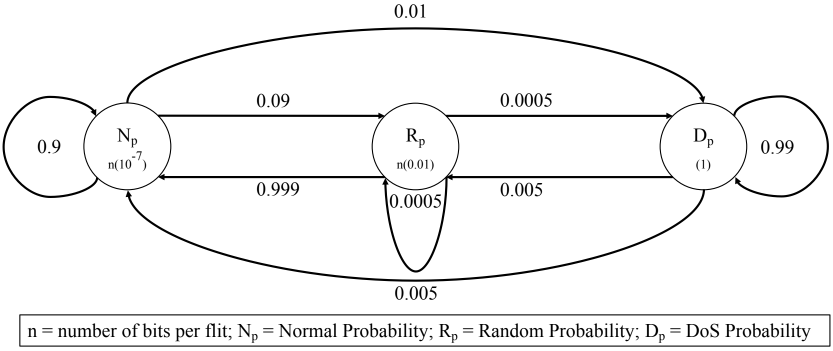
0.01
0.09
0.0005
0.9
N_p
$n(10^{-7})$
R_p
n(0.01)
D_p
(1)
0.99
0.999
0.0005
0.005
0.005
n = number of bits per flit; N_p = Normal Probability; R_p = Random Probability; D_p = DoS Probability

Fig. 4. Markov Chain to generate training and test data

The simulator is modeled to create flit errors based on these BERs, which are then assumed to be detected by the BEU. The simulator is made to operate in one of the three modes dynamically by using a Markov Chain driven process, as shown in Figure 4. The probability of staying in the attack mode, when already under attack is considered high, as a jamming attack is effective only when it is sustained for sufficiently long duration. The probability of staying in a random burst error mode when already in it is modeled low, as random burst errors are short-lived phenomena. The probability of transition into normal mode from a random burst error mode is therefore high. The specific probability values can be altered to model any particular scenario. This observed data (number of flit errors) along with the operating mode (attack class i.e., random or burst) is used to train ML classifiers.

During the inference i.e., attack detection, the ML classifiers are fed runtime information such as, whether a flit is received and whether a burst error is detected for the ML classifier to detect the mode of operation of the system. The simulation data for a hundred thousand cycles was used to train each of the ML Classifiers.

5.2.3 Attacker Detection Unit. The jamming signal can be caused by an external source equipped with an RF transmitter tuned to the spectral band used in the WiNoC, though unlikely to happen due to packaging and encasement precautions. Another likely scenario is when a particular WI is affected by a HT which forces the WI to ignore the MAC protocol and continue to inject traffic from the transmitter of the WI. This constitutes an internal attack. In this section, we discuss the logic block that is designed to distinguish an external attacker from an internal one in the proposed secure WiNoC, ensuring different defense mechanisms are activated.

The detector takes as an input the signal from the ML classifier that detects the occurrence of a jamming based DoS attack. On the detection of an attack, the ADU activates the probe mode, in which all the WIs operate according to the token based MAC mechanism controlled by the

MAC-LFSR. The MAC-LFSR is enabled when the ML classifiers of any of the WIs detects an attack. They send this single-bit signal to the MAC-LFSR. We consider the MAC-LFSR to be located in a secure part of the chip and it is reasonable to assume that it is not affected by the wireless jamming attack model assumed here. The MAC-LFSR then grants access to the wireless medium to each WI in a pseudo-random pattern. A probe-clock (CLK_{probe}) triggers the MAC-LFSR to generate the encoded GRANT signal which is decoded to create a one-hot signal which is sent over pipelined link to the transmitters of all the WIs. A parallel-load shift register is used to serialize this one-hot signal.

The token register in each WI is converted into a scan Flip-Flop. At each transmitter this signal is ANDed with the power supply routed from a secure Power Management Unit (PMU) [23] to regulate the power supply to the transmitter. Thus, only one transmitter transmits data flits over the WI in one instance. The very first signal is initialized as an all-zero signal to disable all WIs from transmitting. In this case, if any of the WIs still receives wireless transmission, it implies that the jamming source is an external attacker as none of the internal transmitters are powered on. The probe mode is then terminated and the decision is send to the defense block for appropriate action. However, if in this case, there is no RF transmissions received, the MAC-LFSR progresses to further probing by cycling through the MAC-LFSR where, only one transmitter is powered on in each cycle. In these cases, where the enabled WI is not the internal attacker, there will be interference in received flits at the WIs due to continuous jamming from the attacker. Only in the case where the MAC-LFSR enables the attacker there will be no interference and correct reception will be received at the WIs. So, the algorithm declares the WI that is enabled by the MAC-LFSR in which case there is no interference, as the internal attacker. The ID of this WI is then passed to the defense block discussed next. The algorithm of ADU to classify the attack source is illustrated in Figure 5.

5.2.4 Defense for Security. The ADU passes the address of the WI that is determined to be the attacker to the DU. In case the attacker is an external agent, the address is an all-zero string. If the address received indicates an external attacker, the DU sends a signal to the secure PMU to shut down all the WIs and also update the routing tables of the WIs such that the wireless links are not used for data routing. This updates of the routing tables can be done without hardware overhead as these alternative values can be pre-computed for each WI for the alternative shortest path routing when the WIs are not available and stored in the operating system. Therefore, in this case, all the WIs are disabled and data is routed via the wired links, eliminating the advantage of the wireless interconnections.

The routing tables are updated only at the WIs disabling the use of the port connected to the wireless transceiver. Therefore, this does not require propagating the update information to all the switches in the WiNoC saving the complexity of convergence of the network. So, packets that would normally use the wireless links, arrive at the WIs and then get detoured via the alternate wired paths and a field in their header is set to denote no further routing or usage of wireless links to avoid further deadlock. This would cause a performance loss in case of such packets that are forced to take the detour which is captured in our performance analysis in the next section. In order to benefit from the wireless interconnection, the probe mode is periodically activated by the ADU to check if the attack has stopped. In this case the use of the WIs can be resumed by using the secure PMU and by updating the routing tables.

If the address passed on to the DU indicates the address of an internal attacker, the DU sends a signal to disable only the power supply to the indicated WI and updates the routing table of its NoC switch to not use the WI. In this way, only the HT infected WI is disabled and the rest of the WIs continue to use the wireless medium. Unlike the previous case, as the attacker is an internal

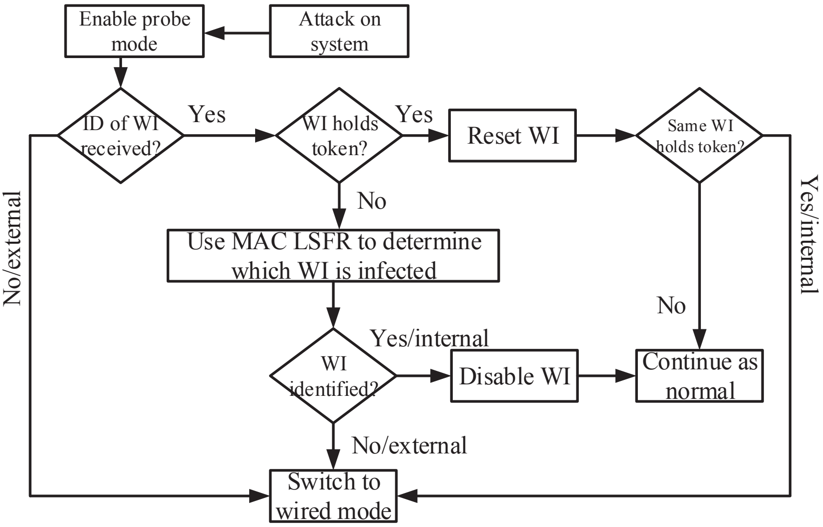

Fig. 5. Algorithm design for reaction to jamming attack

HT, the associated WI may never be safe to use again and therefore will be permanently disabled using the secure PMU and quarantined.

6 RESULTS AND ANALYSIS

Here, we evaluate the performance of the proposed unified test and security of WiNoCs under different attack scenarios.

6.1 Simulation Setup

Simulation of wireless interconnection requires a combination of multiple simulation tools. We use ASIC design flows with Synopsys Design Compiler with 65nm CMP standard cell libraries (https://mycmp.fr/) to model the digital parts of the WiNoC such as NoC switches and the WSU. The BEU encoder and decoder is implemented as two pipelined stages in the WIs to accommodate their delay [18] thereby maintaining the pipelined communication of the WiNoC. Each switch has three pipeline stages implementing backpressure flow control [32]. We consider each input and output port of a switch including those with the wireless transceivers to have 8 VCs with a buffer depth of 4 flits for all the architectures considered in this work. We consider a packet size of 64 flits with a flit size of 32 bits in our experiments. All the digital components are driven by a 2.5GHz clock and 1V power supply. The delay and energy dissipation on the wireline links is obtained through Cadence simulations considering the specific lengths of each link based on the NoC topology assuming a 20mm×20mm chip.

The adopted wireless transceiver circuits consume 2.075pJ/bit at 16Gbps in 65nm technology, similar to that in [46, 47]. The adopted antenna has a 3-dB bandwidth of 16GHz [10]. The characteristics of the transceivers, routers and wired links are annotated into a system-level cycle-accurate simulator to evaluate the performance of the WiNoC in presence of DoS attacks and the proposed defense mechanism. The simulator monitors the progression of flits on a cycle-by-cycle basis accounting for all flits that move or are stalled. We evaluate the proposed system in terms of average packet latency, peak bandwidth per core and average packet energy. *Average packet latency* is defined as the number of cycles required for a packet to reach its final destination after being injected on an average. Peak bandwidth per core is defined as the number of bits received per core of the WiNoC per second with full injection load. *Average packet energy* is the energy dissipated by a packet to be transferred to the final destination over the WiNoC fabric through switches, wired and wireless links on an average. Next, we present the evaluation of testing and the security achieved by employing the ML classifiers and the incurred overheads.

Table 1. Test time (in cycles of CLK_{data}) for WUTs for different WiNoCs with varying number of WIs

WiNoC	Number of WIs								
size	4	8	16	32	64	128	256	512	1024
64 cores	24	48	96	192	384	-	-	-	-
256 cores	24	48	96	192	384	768	1536	-	-
1024 cores	24	48	96	192	384	768	1536	3072	6144

6.2 Wireless Interconnect Test

We evaluate the proposed test methodology in terms of test time, probability of aliasing and the area overhead.

6.2.1 Test Time. For an individual WI Under Test (WUT) the test time, T_{WUT}, will include scan-chain latency to set up the token registers, $L_{Scan-Chain}$, the test generation time of the Data-LFSR, $T_{Data-LFSR}$, and the wireless link latency of the test data packet, L_{WI}. The scan chain latency is due to the fact that each new one-hot test vector decoded from the MAC-LFSR needs to be passed to the token registers of all the WIs before a testing cycle for a WI can begin. As the vectors are one-hot, the entire previous vector needs to be flushed out increasing this latency. The MISR response compaction time is masked by the test data generation time except for the last flit. Receiving the last flit may take multiple cycles of CLK_{data} if the LFSR/MISR length is less than that of the flit width. Therefore, T_{WUT} in cycles of the CLK_{data} is given by,

$$T_{WUT} = L_{scan-chain} + T_{Data-LFSR} + S_{pkt} \cdot L_{WI} + m \tag{1}$$

Where, m is the number of CLK_{data} cycles necessary to generate a flit from the LFSR or conversely, the number of cycles necessary to receive a flit at the MISR. All the timing parameters in equation (1) are expressed in terms of number of CLK_{data} cycles. As the wireless links cannot be pipelined, its latency, L_{WI}, is incurred by every transmitted flit separately and is therefore multiplied by the packet size, S_{pkt} in equation (1). The total time required to test all WIs in the network is given by,

$$T_{WI} = (N + 1)T_{WUT} \tag{2}$$

This is because, the total test time comprises of testing N stuck-disabled faults of WUTs while, testing stuck-enabled fault for all the WUTs requires testing with only one additional pre-determined test vector (logic '0's) for all the WUTs. Table 1 shows the test time of the WIs in a WiNoC with varying size and varying number of WIs for each system size evaluated according to equation (2). It can be observed that the test time is same for systems with different number of cores if they have the same number of WIs.

6.2.2 Aliasing and Area Overhead. BIST based testing suffers from the problem of aliasing of the syndrome of a faulty Circuit-Under-Test (CUT) to the syndrome of a fault-free CUT. As each wireless link is modeled as a digital communication link including the serializer/deserializer buffers, the probability of any bit position to be faulty can be assumed to be independent of each other because a fault in one serializer/deserializer buffer location does not necessarily imply a fault in another. This assumption would not be valid if the wireless link only has the serial wireless transceivers. Assuming the probability of fault of each bit exchanged between the WUTs to be independent of each other, the probability that a particular syndrome in response to a particular fault will suffer from aliasing, P_{alias} is given by [43]

$$P_{alias} = \frac{1}{2^k} \tag{3}$$

Where, k is the length of the MISR used in response compaction. Therefore, longer MISRs with higher k will reduce the possibility of aliasing. For an aliasing probability of 2.32×10^{-10} corresponding to a Data-LFSR of length 32 bits, the power consumption and area overhead per WI will be 0.19mW and 0.0015 mm^2 respectively in the 65nm technology. The area and power consumption of the BIST hardware is obtained from post-synthesis RTL models using 65nm standard cell libraries (https://mycmp.fr/). The transceivers consume around 32mW thereby making the BIST power overhead about 0.56% of the transceiver power when the test mode is asserted.

6.3 Evaluation of WiNoC Security

We evaluate the security mechanism of WiNoC in terms of attack detection performance by employing ML and the performance of WiNoC in presence of attacks and defense mechanisms.

6.3.1 Performance of Attack Detection. Table 2 presents the accuracy and robustness of different ML classifiers when deployed to detect the DoS attacks. To compare the ML classifiers with a heuristic method as proposed in [27], we consider a similar threshold-based approach. For the neural network (MLP) a single hidden layer with 10 nodes is utilized. One can observe from Table 2, among different classifiers, KNN achieves high attack detection accuracy of nearly 99.87%, higher than other techniques. We anticipate this behavior, as no assumptions are made regarding the data during the training phase of KNN. We have experimented with $k = 1, 3$ for KNN and have observed a similar performance, hence considered $k = 1$ in this work due to its reduced complexity. Although SVM showed high accuracy, it is observed in experiments that it is not able to detect sporadic variations such as spontaneous random errors, and is hence not the best option. It can be argued that the hyper-parameters of other ML classifiers can be tuned to improve the performance, however optimizing the ML classifiers is not the focus nor contribution of this work.

During the runtime for the attack detection, the KNN classifier is fed with the information whether a flit is received or not and whether a burst error is detected or not, to detect the mode of operation of the system. The simulation data for a hundred thousand cycles was used to train each of the ML Classifiers and is then tested on a new hundred thousand cycles of simulation which were not used in training. The KNN classifier achieves a detection accuracy of 99.87% accuracy. Also, it has a Recall, F-score and Area Under the Curve (AUC) of 0.99, 0.99 and 0.99 respectively, showing high robustness. Furthermore, as shown in Table 2, the threshold based mechanism is not as accurate as the chosen machine learning (KNN) approach. In this threshold-based approach, two thresholds are necessary, to separate between the attack mode, burst error mode and normal mode. The thresholds are computed based on the same data that was used to train the machine learning algorithms. The threshold between the attack mode and burst error mode is chosen to be equidistant from the average number of erroneous flits in burst errors and jamming induced errors. Likewise, the threshold to separate the burst error mode from the normal mode is chosen to be equidistant from the average number of flit errors in burst mode and normal mode.

In addition to the performance benefits, ML classifiers also incur silicon and resource overheads. To obtain these metrics, the post-synthesis models of the ML classifiers with 65nm standard cell libraries (https://mycmp.fr/) are carried out. Table 3 presents the incurred overhead in terms of area, power and delay of the deployed ML Classifiers. In addition to KNN performing a good attack detection, KNN also incurs lowest area and power consumption, hence, we adopt the KNN Classifier for the evaluation of overall system. It can be argued that the delay of the KNN classifier is not the optimal, however, we choose KNN for attack detection, as the ML Classifier is not in the path of data transmission of the WiNoC, as shown in the proposed secure wireless architecture in Figure 3. Despite having low latency, threshold-based approach has higher area and power consumption due to the involved floating point computations and comparisons, as shown in Table 3.

Table 2. Attack detection performance of ML classifiers

ML classifier	Accuracy (%)	Recall	F-score
MLP	47.86	0.48	0.65
SVM	98.96	0.98	0.98
KNN	99.87	0.99	0.99
DT	52.46	0.52	0.69
Thresh	94.55	0.92	0.92

Table 3. Overhead analysis for different ML classifiers

Classifier	Area (μm^2)	Power (μW)	Timing (ns)
MLP	34448.79	6299.3	0.41
SVM	5412.01	8076.1	0.37
KNN	105.28	27.075	0.56
DT	127.32	41.12	0.23
Thresh	24262.63	22515.2	0.07

Table 4. Component configuration for simulation

Component	**Configuration**
System size	64 cores
NoC router	3 stage pipelined 5 ports, 0.078pJ/bit (except wireless)
Total VC	4, each 8 flits deep
Flit width	32 bits
Wired NoC links	32-bit flits, single cycle latency, 0.2pJ/bit/mm
OOK wireless transceiver	16Gbps, 2.07pJ/bit, OOK modulated at 60GHz
Technology node	65nm, 1V supply 1GHz system clock
Number of WIs	4
Traffic pattern	Uniform random

6.3.2 Performance of WiNoC in Presence of Attacks. Here, we evaluate the bandwidth per core, average packet latency and average packet energy consumption of the WiNoC in presence of persistent jamming attacks. A system with 64 cores is considered here (similar to that in Figure

Table 5. Performance of WiNoC in presence of attacks

	Bandwdith per core (Gbps/core)	Packet latency (Cycles)	Packet energy (pJ)
Wired mesh	26.4	396	100
WiNoC	30.4	257	61
WiNoC with internal HT	29.5	319	78
WiNoC with external attacker	26.4	396	101

1). The WiNoC is considered to be designed as a wired mesh overlaid with 4 WIs deployed in the central switch of 4 subnets. The WiNoC outperforms a wired mesh NoC when operating under normal mode even with the proposed unified BIST and security measures. The power consumption and delay of the test and security measures were considered along with that of post-synthesis RTL models of the NoC routers and physical design of wire segments of the NoC links based on the layout in a 20mm×20mm die. The transceivers in the WI consume an energy of 2.06pJ/bit [46, 47], while operating at 16Gbps data rate over the 60GHz on-chip wireless channel. The energy consumption of the wired links are obtained by parasitic extraction from layout models of global wires depending upon the lengths of links necessary to realize the wired mesh topology. The relevant details about the various components of the WiNoC and the security architecture is listed in Table 4. The cycle-accurate simulator used to model the attack scenarios was annotated with these simulation parameters from Table 4 to evalaute the WiNoC in presence of attacks. A uniform random traffic pattern is considered in our experiments at full load which evaluate the NoCs when the packet transfer has reached saturation in steady-state. We evaluate the performance of the WiNoCs when an attack has been detected and the packets are being rerouted as per the defense mechanism for each of the attack scenarios.

It can be seen from Table 5 that in the presence of persistent jamming due to an internal HT the bandwidth, latency and energy are worse compared to the WiNoC with no attack, but better than the wired mesh NoC as only the infected WI is quarantined while the remaining WIs contribute to improve the performance. However, in the presence of persistent jamming from an external attacker all the WIs are bypassed in data communication and therefore the performance is similar to that of the wired NoC but the packet energy increases by 1% due to the additional power overhead of the security unit consisting of the BEC, LFSRs, ML classifiers, ADUs and DUs. While these performance metrics are measured at steady-state, in the transient phase, when the WIs detect an attack, they transmit flits to the NoC switches in their subnets to update routing tables.

The time required for the transfer of this single-flit packet from the WIs to the Noc switches farthest away, which is at a distance of 4 hops away (in a subnet of 16 cores) is 16 cycles as the delay of each switch is 3 cycles and that of each link is 1 cycle. This is because any WI is 4 hops away from the NoC switch which is farthest from the WI within the same subnet. Each hop consist of 4 clock cycles due to the 3-stage switch architecture adopted and the wired links within the subnet having a delay budget of 400ps from the 2.5GHz clock used for design synthesis. However, this is a one-time delay which is needed to send the update signal from the affected WIs to all the NoC switches and does not affect the steady state performance for either internal or external attacks. The overheads can be further reduced if the security monitoring engaging the BEU, ML Classifier, ADU and DU is employed only at some intervals of time on assertion of the TMS similar to the testing mode. While this will reduce and amortize the overheads furhter, it will also reduce the response time of the WINoC in case of an attack. Given the negligible overheads, we have seen in Table 5 in the absence of attacks, we choose to place the security architecture in constant probe mode engaging the BEU and ML classifier at all times.

6.4 Overall Area Overhead

In the previous sections we have observed the area overheads incurred by the BIST and the security blocks. Here, we first summarize and provide the overall overhead impact on the system. Based on post-synthesis RTL models in the 65nm technology node, the area overheads of the BIST is 0.0015 mm^2 per WI. The area overhead of the jamming protection hardware is 0.0044 mm^2 per WI [46, 47]. Therefore, collectively they occupy 0.0059 mm^2 per WI while the transceivers occupy an area of around 0.2 mm^2, making the overhead only 2.95% of the transceivers and making the verification and security feasible.

7 CONCLUSIONS

In this work we propose a unified architecture for test and security of on-chip wireless interconnects used in WiNoCs. While on-chip wireless interconnects can improve the performance of the NoCs they need to be tested for proper functioning. Moreover, on-chip wireless interconnects make the WiNoC vulnerable to jamming based DoS attacks. Monitoring security threats requires online probing of the WiNoC to detect anomalous behavior. Therefore, the same hardware architecture can be used for testing the wireless interconnects as well. We show that the wireless BIST can test the wireless interconnects with very low probability of aliasing of 2.32×10^{-10} and provide protection against jamming attacks with 99.87% accuracy of detection while sustaining the functionality of the WiNoC even in the presence of attacks. Even in the presence of persistent jamming from an HT the secure WiNoC outperforms a wired mesh NoC while, in the presence of an external attacker the energy overhead of the secure WiNoC is 1% with no impact on performance in the steady state.

REFERENCES

[1] V. Akilandeswari and S. M. Shalinie. 2012. Probabilistic Neural Network based attack traffic classification. In *Int. Conf. on Advanced Computing.*

[2] Luca Benini and Giovanni De Micheli. 2002. Networks on Chips: A New SoC Paradigm. *Computer* 35, 1 (Jan 2002), 70–78.

[3] M. Bühler, J. Koehl, J. Bickford, J. Hibbeler, U. Schlichtmann, R. Sommer, M. Pronath, and A. Ripp. 2006. DFM/DFY Design for Manufacturability and Yield - Influence of Process Variations in Digital, Analog and Mixed-signal Circuit Design. In *Design, Automation and Test in Europe.*

[4] Kevin Chang, Sujay Deb, Amlan Ganguly, Xinmin Yu, Suman Prasad Sah, Partha Pratim Pande, Benjamin Belzer, and Deukhyoun Heo. 2012. Performance Evaluation and Design Trade-offs for Wireless Network-on-chip Architectures. *J. Emerg. Technol. Comput. Syst.* 8, 3 (Aug 2012), 23:1–23:25.

[5] Kyungwook Chang, Sai Pentapati, Da Eun Shim, and Sung Kyu Lim. 2018. Road to High-Performance 3D ICs: Performance Optimization Methodologies for Monolithic 3D ICs. In *International Symposium on Low Power Electronics and Design.*

[6] Sai Vineel Reddy Chittamuru, Dharanidhar Dang, Sudeep Pasricha, and Rabi N. Mahapatra. 2018. BiGNoC: Accelerating Big Data Computing with Application-Specific Photonic Network-on-Chip Architectures. *IEEE Trans. Parallel Distrib. Syst.* 29, 11 (2018), 2402–2415.

[7] S. V. R. Chittamuru, I. G. Thakkar, and S. Pasricha. 2018. HYDRA: Heterodyne Crosstalk Mitigation With Double Microring Resonators and Data Encoding for Photonic NoCs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 26, 1 (Jan 2018), 168–181.

[8] Sai Mano P D, J. Lin, S. Zhu, Y. Yin, X. Liu, X. Huang, C. Song, W. Zhang, M. Yan, Z. Yu, and H. Yu. 2017. A Scalable Network-on-Chip Microprocessor With 2.5D Integrated Memory and Accelerator. *IEEE Transactions on Circuits and Systems I: Regular Papers* 64, 6 (June 2017), 1432–1443.

[9] Sai Manoj P D, H. Yu, Y. Shang, C. S. Tan, and S. K. Lim. 2013. Reliable 3-D Clock-Tree Synthesis Considering Nonlinear Capacitive TSV Model With Electrical-Thermal-Mechanical Coupling. *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems* 32, 11 (Nov 2013), 1734–1747.

[10] Sujay Deb, Kevin Chang, Xinmin Yu, Suman Prasad Sah, Miralem Cosic, Amlan Ganguly, Partha Pratim Pande, Benjamin Belzer, and Deukhyoun Heo. 2013. Design of an Energy-Efficient CMOS-Compatible NoC Architecture with Millimeter-Wave Wireless Interconnects. *IEEE Trans. Comput.* 62, 12 (Dec 2013), 2382–2396.

[11] S. Deb, A. Ganguly, P. P. Pande, B. Belzer, and D. Heo. 2012. Wireless NoC as Interconnection Backbone for Multicore Chips: Promises and Challenges. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 2, 2 (June 2012), 228–239.

[12] D. DiTomaso, A. Kodi, D. Matolak, S. Kaya, S. Laha, and W. Rayess. 2013. Energy-efficient adaptive wireless NoCs architecture. In *IEEE/ACM Int. Symp. on Networks-on-Chip.*

[13] Rohan Doshi, Noah Apthorpe, and Nick Feamster. 2018. Machine Learning DDoS Detection for Consumer Internet of Things Devices. *CoRR* abs/1804.04159 (2018).

[14] Jose Duato, Sudhakar Yalamanchili, and Ni Lionel. 2002. *Interconnection Networks: An Engineering Approach.* Morgan Kaufmann Publishers Inc.

[15] K. Duraisamy and P. P. Pande. 2017. Enabling High-Performance SMART NoC Architectures Using On-Chip Wireless Links. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 25, 12 (Dec 2017), 3495–3508.

[16] E. S. Erdogan and S. Ozev. 2010. Detailed Characterization of Transceiver Parameters Through Loop-Back-Based BiST. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 18, 6 (2010), 901–911.

[17] S. Evain and J. . Diguet. 2005. From NoC security analysis to design solutions. In *IEEE Workshop on Signal Processing Systems Design and Implementation.*

[18] B. Fu and P. Ampadu. 2009. Burst Error Detection Hybrid ARQ with Crosstalk-Delay Reduction for Reliable On-chip Interconnects. In *IEEE Int. Symp. on Defect and Fault Tolerance in VLSI Systems.*

[19] Amlan Ganguly, Mohsin Yusuf Ahmed, and Anuroop Vidapalapati. 2012. A Denial-of-service Resilient Wireless NoC Architecture. In *Great Lakes Symp. on VLSI.*

[20] C. Grecu, A. Ivanov, R. Saleh, and P. P. Pande. 2007. Testing Network-on-Chip Communication Fabrics. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 26, 12 (Dec 2007), 2201–2214.

[21] C. Grecu, P. Pande, A. Ivanov, and R. Saleh. 2006. BIST for network-on-chip interconnect infrastructures. In *IEEE VLSI Test Symposium.*

[22] Mohammad Hosseinabady, Atefe Dalirsani, and Zainalabedin Navabi. 2007. Using the Inter- and Intra-switch Regularity in NoC Switch Testing. In *Design, Automation and Test in Europe.*

[23] R. JayashankaraShridevi, C. Rajamanikkam, K. Chakraborty, and S. Roy. 2016. Catching the Flu: Emerging threats from a third party power management unit. In *ACM/EDAC/IEEE Design Automation Conf.*

[24] E. Kakoulli, V. Soteriou, and T. Theocharides. 2012. Intelligent Hotspot Prediction for Network-on-Chip-Based Multicore Systems. *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems* 31, 3 (March 2012), 418–431.

[25] M. Kar and T. Krishna. 2017. A case for low frequency single cycle multi hop NoCs for energy efficiency and high performance. In *IEEE/ACM International Conference on Computer-Aided Design.*

[26] Reyhaneh Karimazad and Ahmad Faraahi. 2011. An Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks. In *Int. Conf. on Network and Electronics Engineering.*

[27] B. Lebiednik, S. Abadal, H. Kwon, and T. Krishna. 2018. Architecting a Secure Wireless Network-on-Chip. In *IEEE/ACM International Symposium on Networks-on-Chip (NOCS).*

[28] Y. Lee and S. K. Lim. 2011. Co-Optimization and Analysis of Signal, Power, and Thermal Interconnects in 3-D ICs. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 30, 11 (Nov 2011), 1635–1648.

[29] X. Li, K. Duraisamy, J. Baylon, T. Majumder, G. Wei, P. Bogdan, D. Heo, and P. P. Pande. 2017. A Reconfigurable Wireless NoC for Large Scale Microbiome Community Analysis. *IEEE Trans. Comput.* 66, 10 (Oct 2017), 1653–1666.

[30] J. Lin, H. Wu, Y. Su, L. Gao, A. Sugavanam, J. E. Brewer, and K. K. O. 2007. Communication Using Antennas Fabricated in Silicon Integrated Circuits. *IEEE J. of Solid-State Circuits* 42, 8 (Aug 2007), 1678–1687.

[31] J. Lin, S. Zhu, Z. Yu, D. Xu, Sai Manoj P D, and H. Yu. 2015. A scalable and reconfigurable 2.5D integrated multicore processor on silicon interposer. In *IEEE Custom Integrated Circuits Conf.*

[32] Partha Pratim Pande, C. Grecu, M. Jones, A. Ivanov, and R. Saleh. 2005. Performance evaluation and design trade-offs for network-on-chip interconnect architectures. *IEEE Trans. on Computers* 54, 8 (Aug 2005), 1025–1040.

[33] Fernando Pereñíguez García and José L. Abellán. 2017. Secure Communications in Wireless Network-on-chips. In *Int. W. on Advanced Interconnect Solutions and Technologies for Emerging Computing Systems.*

[34] P. Arun Raj Kumar and S. Selvakumar. 2011. Distributed Denial of Service Attack Detection Using an Ensemble of Neural Classifier. *Comput. Commun.* 34, 11 (July 2011), 1328–1341.

[35] M. Richter and K. Chakrabarty. 2012. Test pin count reduction for NoC-based Test delivery in multicore SOCs. In *Design, Automation Test in Europe Conference Exhibition (DATE).*

[36] M. S. Shamim, N. Mansoor, R. S. Narde, V. Kothandapani, A. Ganguly, and J. Venkataraman. 2017. A Wireless Interconnection Framework for Seamless Inter and Intra-Chip Communication in Multichip Systems. *IEEE Trans. Comput.* 66, 3 (Mar 2017), 389–402.

[37] C. Stroud, J. Morton, T. Islam, and H. Alassaly. 2003. A mixed-signal built-in self-test approach for analog circuits. In *Southwest Symposium on Mixed-Signal Design*.

[38] A. Vashist, A. Ganguly, and M. Indovina. 2018. Testing WiNoC-Enabled Multicore Chips with BIST for Wireless Interconnects. In *IEEE/ACM International Symposium on Networks-on-Chip (NOCS)*.

[39] A. Vashist, A. Keats, Sai Manoj P D, and A. Ganguly. 2019. Securing a Wireless Network-on-Chip against Jamming based Denial-of-Service and Eavesdropping Attacks. *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)* (2019).

[40] A. Vashist, A. Keats, Sai Manoj P D, and A. Ganguly. 2019. Securing a Wireless Network-on-Chip against Jamming based Denial-of-Service Attacks. In *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*.

[41] B. Vermeulen, J. Dielissen, K. Goossens, and C. Ciordas. 2003. Bringing communication networks on a chip: test and verification implications. *IEEE Communications Magazine* 41, 9 (Sep 2003), 74–81.

[42] X. Wang, Y. Zheng, A. Basak, and S. Bhunia. 2015. IIPS: Infrastructure IP for Secure SoC Design. *IEEE Trans. Comput.* 64, 8 (Aug 2015), 2226–2238.

[43] T. W. Williams and W. Daehn. 1989. Aliasing errors in multiple input signature analysis registers. In *European Test Conference*.

[44] Bing Wu, Jianmin Chen, Jie Wu, and Mihaela Cardei. 2007. *A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks*. Springer US, 103–135.

[45] S. S. Wu, K. Wang, Sai Manoj P D, T. Y. Ho, M. Yu, and H. Yu. 2014. A thermal resilient integration of many-core microprocessors and main memory by 2.5D TSI I/Os. In *Design, Automation Test in Europe Conference Exhibition (DATE)*.

[46] X. Yu, H. Rashtian, S. Mirabbasi, P. P. Pande, and D. Heo. 2015. An 18.7-Gb/s 60-GHz OOK Demodulator in 65-nm CMOS for Wireless Network-on-Chip. *IEEE Trans. on Circuits and Systems I* 62, 3 (March 2015), 799–806.

[47] X. Yu, S. P. Sah, H. Rashtian, S. Mirabbasi, P. P. Pande, and D. Heo. 2014. A 1.2-pJ/bit 16-Gb/s 60-GHz OOK Transmitter in 65-nm CMOS for Wireless Network-On-Chip. *IEEE Trans. on Microwave Theory and Tech.* 62, 10 (Oct 2014), 2357–2369.

[48] M. Zekri, S. E. Kafhali, N. Aboutabit, and Y. Saadi. 2017. DDoS attack detection using machine learning techniques in cloud computing environments. In *Int. Conf. of Cloud Computing Technologies and Applications (CloudTech)*.

[49] D. Zhao, S. Upadhyaya, and M. Margala. 2006. Design of a wireless test control network with radio-on-chip technology for nanometer system-on-a-chip. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 25, 7 (July 2006), 1411–1418.

[50] D. Zhao and Y. Wang. 2006. MTNET: Design and Optimization of a Wireless SOC Test Framework. In *IEEE International SOC Conference*.