Securing a Wireless Network-on-Chip against Jamming based Denial-of-Service Attacks

Abhishek Vashist*, Andrew Keats*, Sai Manoj Pudukotai Dinakarrao†, Amlan Ganguly*
*Rochester Institute of Technology, Rochester, USA
{av8911, axk7655, amlan.ganguly}@rit.edu
†George Mason University, Fairfax, USA
{spudukot}@gmu.edu

Abstract*—Wireless Networks-on-Chips (NoCs) have emerged as a panacea to the non-scalable multi-hop data transmission paths in traditional wired NoC architectures. Using low-power transceivers in NoC switches, novel Wireless NoC (WiNoC) architectures have been shown to achieve higher energy efficiency with improved peak bandwidth and reduced on-chip data transfer latency. However, using wireless interconnects for data transfer within a chip makes the on-chip communications vulnerable to various security threats from either external attackers or internal hardware Trojans (HTs). In this work, we propose a mechanism to make the wireless communication in a WiNoC secure against persistent jamming based Denial-of-Service attacks from both external and internal attackers. Persistent jamming attacks on the on-chip wireless medium will cause interference in data transfer over the duration of the attack resulting in errors in contiguous bits, known as burst errors. Therefore, we use a burst error correction code to monitor the rate of burst errors received over the wireless medium and deploy a machine learning (ML) classifier to detect the persistent jamming attack and distinguish it from random burst errors. In the event of persistent jamming attack, alternate routing strategies are proposed to avoid the DoS attack over the wireless medium, so that a secure data transfer can be sustained even in the presence of jamming. We evaluate the proposed technique on a secure WiNoC in the presence of DoS attacks. It has been observed that with the proposed defense mechanisms, WiNoC can outperform a wired NoC even in presence of attacks in terms of performance and security. On an average, 99.87% attack detection was achieved with the chosen ML Classifiers. A bandwidth degradation of <3% is experienced in the event of internal attack, while the wireless interconnects are disabled in the presence of an external attacker.

I. Introduction

With the advent of the multi or many-core paradigm for increasing processing throughput of processors, traditional bus-based interconnect mechanisms were found to be non-scalable from a design perspective. This led to the adoption of the Network-on-Chip (NoC) paradigm for interconnecting tens to hundreds of cores on the same die. Regular NoC architectures such as mesh or torus-based ones proved to be relatively easy to design and replicate, and reduce time-to-market constraints. However, such regular architectures resulted in non-scalable performance with increase in number of cores due to long multi-hop paths over wired links. Along with other emerging interconnect technologies such as silicon photonics or Through-Silicon-Vias (TSVs) [1], [2] for 3D NoCs, wireless interconnects were envisioned to enable scalable communication fabrics in multi-core chips [3]. Low-power millimeter-wave wireless transceivers, efficient on-die miniature antennas, and smart designs of hybrid architectures with wired as well as single-hop wireless links resulted in lower packet latency and energy consumption in on-chip communication of wireless NoCs (WiNoCs). A simple experiment to compare a wired NoC and a WiNoC is performed for a 64 core system with wireless interfaces (WIs) overlaid on a mesh. The size of each packet is set to 2Kb. More details on simulation setup is presented in Section VI-A. One can observe from Figure 1 that the WiNoC improves the bandwidth per core and energy per packet by 15% and 39% respectively.

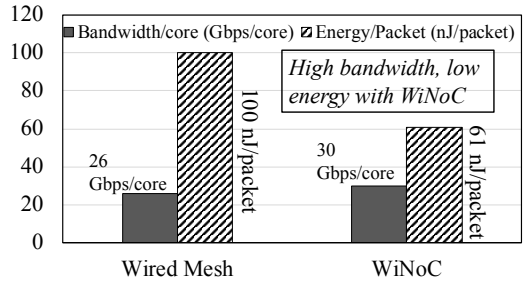

Fig. 1: Comparison of Wireless vs Wired NoC in terms of bandwidth and energy consumption

Although extensive research has been carried out towards high performance and lower energy dissipation in WiNoCs, relatively little attention has been given to the information integrity and security or privacy aspects of WiNoCs. While security of traditional wired NoCs against various kinds of attacks such as hardware Trojans (HTs), eavesdropping or spoofing has resulted in appropriate defense mechanisms, the additional threats that unguided wireless interconnects can engender has not received the necessary attention. Wireless interconnects in WiNoCs are vulnerable to attacks, similar to those encountered in other wireless networks such as sensor networks or mobile networks. Furthermore, conventional defenses against persistent jamming attacks such as frequency or channel hopping [4] are not applicable in a WiNoC as the WIs have access to a single shared channel and limited resources. This calls for an embedded defense mechanism for current and future WiNoC based 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. In this work, we focus on DoS attacks that jams the wireless medium, as this is the most common attack on wireless communication systems. We consider an external attacker who produces a high energy electromagnetic

radiation that causes interference in the wireless medium used by the WiNoC. Moreover, it is also possible that a HT planted in the system from a vulnerable design and manufacturing process can cause a WI to transmit persistent jamming signals to cause DoS for the other WIs. In this case, one of the WIs infected by a HT will send data over the wireless channel irrespective of whether it is enabled by the adopted Medium Access Control (MAC) of the WiNoC. This will cause contention or interference with legitimate transmissions causing DoS on the remaining WIs. While well-known defenses exist against DoS attacks in large-scale wireless networks [4], those techniques are not directly applicable to the WiNoC scenario due to specific architecture and MAC constraints in WiNoCs.

In this work, we propose a mechanism to detect and recover from persistent jamming based DoS attacks that can disable the wireless interconnections in the WiNoC. We present and evaluate the design of a detection unit that monitors the number of interference generated errors in the received data, and employs a Machine Learning (ML) classifier to distinguish between random errors and those due to an attack and a defense unit that aids the WiNoC recover based on whether the attacker is internal or external. We propose to equip every wireless transceiver in the WiNoC with the proposed defense unit. We use a thorough simulation framework using tools at various levels of abstraction to evaluate the WiNoC with the proposed DoS detection and defense mechanism.

II. Related Work

Considerable research has been done to secure conventional NoC based multi-core processors [5]. However, these security measures are confined to wired NoCs and not scalable to wireless NoCs. However, the envisioning of on-chip wireless interconnects [6], [7] led to additional vulnerabilities in the WiNoCs. Very little attention has been dedicated to this important problem of securing on-chip wireless communication although it has been identified as an important challenge to be overcome to make WiNoCs a reality [8]. In [9], a small-world graph based WiNoC architecture was proposed to mitigate DoS attacks. In [10] a secure WiNoC architecture has been proposed that can protect against DoS, eavesdropping and spoofing but engages the Operating System to block DoS attacks in a WiNoC with contention-free channel access, which is the type of WiNoC considered in this work. In this work, detecting and defending against jamming attacks in WiNoCs have been addressed in the NoC itself.

On the other hand, although machine learning (ML) has been used in the context of NoC systems for congestion-aware routing [11], but not used for securing NoC, especially against DoS attacks due to resource constraints. However, there exist works on detecting DoS attacks on cloud or IoT systems. We review some of them and outline the differences here.

In [12], 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 artificial NNs (ANNs) [13], are proposed, and [14] presents a comparison of different ML algorithms when detecting Distributed DOS (DDoS) attacks in cloud and IoT devices. The work in [15] employs 23 features to detect the DDoS attacks using different ML classifiers. Despite having the similar objective of detecting DoS/DDoS attacks, the constraints, protocols and traffic flow are different for miniature NoC systems.

Thus, the main differences and challenges compared to existing works using ML for security against DoS attacks can be outlined as follows: in the existing works, the detection is carried out in a cloud or resource-ample environment, where complex computations can be afforded. However, on a NoC like miniature system that is considered in this work, the overhead and processing resources are limited and play a pivotal role. As such, a direct adoption is inefficient and leads to large overhead and performance penalties.

III. System Description

A. Wireless NoC (WiNoC) System Architecture

In the adopted WiNoC architecture, each core in the multi-core chip is connected to a NoC switch via a Network Interface (NI). The switches are then connected by wired links forming a mesh topology. We adopt a mesh architecture for the wired NoC topology due to its low complexity, ease to verify and manufacture due to uniformity of link lengths. However, other topologies such as torus or small-world can be chosen if required by the system design constraints. In addition to the wired links, a few NoC switches are equipped with an additional port connected to the WI to access to the mm-wave channel, thus forming a hybrid WiNoC architecture.

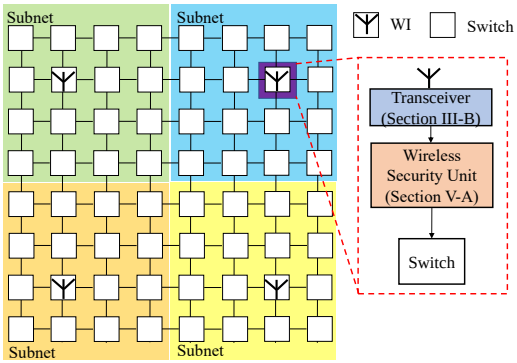

Fig. 2: System architecture of proposed secure WiNoC

Based on several previous works such as [16], we partition the mesh into multiple subnets to deploy the WIs among the NoC switches, as shown in Figure 2. A central switch in each subnet is equipped with a WI to facilitate on-chip communication using the wireless medium. The selection of subnet size (or the number of WIs) offers a trade-off between performance of the WiNoC and area overhead of the WIs which can be designed with system-level simulations. The underlying cores are not shown for the purpose of brevity. In this work, we propose to equip the WIs with a Wireless Security Unit (WSU), which can detect and protect against persistent jamming attacks from both internal and external attackers. The WSU is located between the wireless transceiver and the NoC switch so that it can process the data and detect the attack before the data passes into the NoC switch.

B. Wireless Interconnections

We propose the use of on-chip embedded miniature antennas operating in the 60 GHz mm-wave band unlicensed by Federal Communications Commission, which can establish direct communication channels between the WIs. We intend

that the chosen antenna to be compact as well as non-directional, so that they can communicate with other WIs in all directions in the WiNoC. We adopt the 60GHz zig-zag antenna with these characteristics from [16].

To ensure high bandwidth and energy efficiency, we adopt a transceiver design where low power design considerations are taken into account [17], [18]. 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. Each WI is a combined transceiver with a single antenna enabling half-duplex communication. Parallel data from a NoC switch is serialized using a Parallel In Serial Out (PISO) register before transmission and vice-versa after reception, where they are received into a Serial In Parallel Out (SIPO) buffer. The PISO buffer receives data from the output virtual channel (VC) of the transmitting WI while the SIPO sends the received data to the input VCs of the receiving WI.

To avoid non-scalable central arbitrations and power-hungry synchronization across the chip and facilitate wireless contention-free channel access, we adopt a distributed wireless token passing mechanism to grant access of the shared wireless channel to only the WI possessing the token. Each WI can only occupy the token for a pre-determined maximum time that is optimized based on system-level simulations.

We use a forwarding-table based routing algorithm over pre-computed shortest paths along a Minimum Spanning Tree (MST) determined by Dijkstra's algorithm. Consequently, deadlock is avoided by transferring flits along the extracted shortest path routing tree. The routing decisions are made locally based on the forwarding table for determining the next hop and is done only for the header flit, reducing computing requirements and maintaining global routing information.

IV. Attack Model

In this work, we consider only persistent jamming based DoS attacks on the wireless interconnections of a WiNoC due to aforementioned arguments. In the presence of 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 over a relatively long period of time, 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. Burst errors can also be a result of power source fluctuations, ground bounce or crosstalk [19]. The burst errors due to random events such as crosstalk will be relatively short lived, typically, a single clock cycle, due to the data transition pattern in that cycle. On the other hand, burst errors resulting from persistent 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 last for relatively long duration 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 need a mechanism to detect jamming based DoS attacks and distinguish it from a random burst error. In this work, we consider attacks either from a single external attacker or a single internal HT based attacker which affect one or more WIs in the WiNoC.

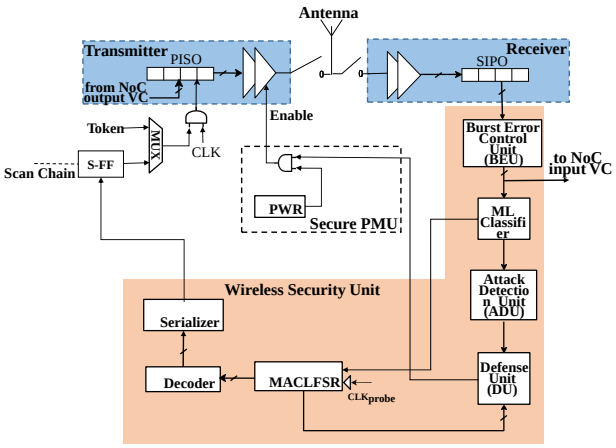

Fig. 3: Wireless security unit architecture in a WI

V. Secure Wireless NoC

To enable the proposed secure WiNoC, each WI is equipped with an attack detector and a defense mechanism to sustain functionality of the interconnection fabric even under attack.

A. System Architecture of Proposed WSU

The proposed WSU shown in Figure 3 consists of a Linear Feedback Shift Register (LFSR) called MAC-LFSR, a Burst Error Control Unit (BEU), an Attack Detection Unit (ADU), and a Defense Unit (DU). In the normal mode of operation, the data flits are received at the SIPO buffer of a NoC switch equipped with a WI. Upon reception of flits at the receiver's SIPO buffer, flits are sent to the BEU. The BEU then detects a burst error and sends its output to the ADU. The BEU employs the BEC proposed in [19] 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 V-C.

B. Machine Learning for Attack Detection

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: artificial neural network (ANN), support vector machine (SVM), k-nearest neighbors (KNN), and Decision tree (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 covering a wide spectrum of ML.

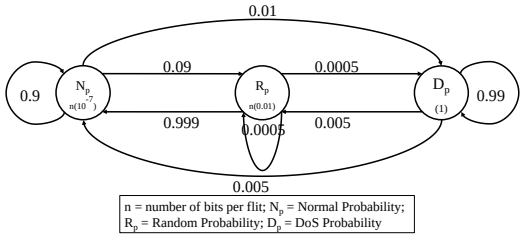

Fig. 4: Markov Chain to control system operating state

In order to train the ML classifier, the attacks aforementioned in Section IV are deployed on a WiNoC (shown in Figure 2) 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 [18]. 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 [19]. 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 persistent 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.

The simulator is modeled to create flit errors based on these BER information, 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 persistent jamming attack is effective only when it is sustained for a long duration. The probability of staying in a random burst error mode when already in it, is modeled as 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. This observed data (number of errors, flits transmitted and received) along with the operating mode (attack class) is used to train the ML classifiers. As the duration of the individual states are determined by the Markov Chain randomly, each specific instance of the states have varying duration, resulting in a diverse training data set.

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

C. Attacker Detection Unit

The jamming signal can be caused by an external source equipped with a 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 WI transmitter. This constitutes an internal attack. Here, 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 signal from the ML classifier that detects the occurrence of a jamming based DoS attack as an input. 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) [20] 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 sent to the defense block for appropriate action. However, if 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 as the internal attacker. The ID of this WI is then passed to the DSU. The algorithm of ADU to detect the attack source is in Figure 5.

D. 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

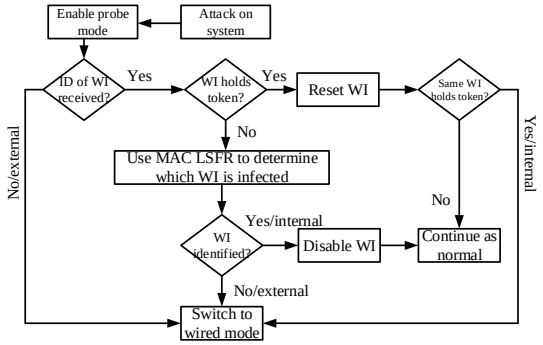

Fig. 5: Algorithm design for reaction to jamming attack

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. 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 HT, the associated WI may never be safe to use again and therefore will be permanently disabled using the Secure PMU and quarantined. The core or cores attached to the infected WI will continue to route their packets over wired links using the NoC switch as the HT does not influence the wired part of the NoC in the threat model that we have considered in this work.

VI. Experimental Evaluation

A. 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 [19] thereby maintaining the pipelined communication of the WiNoC. Each switch has three pipeline stages implementing backpressure flow control [21]. 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$\times$20mm chip. The adopted wireless transceiver circuits consume 2.075pJ/bit at 16Gbps in 65nm technology [17], [18]. The adopted antenna has a 3-dB bandwidth of 16GHz [16]. 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 ML classifiers' performance for detecting the DoS attacks and system-level performance.

B. Attack Detection Performance by ML Classifier

Table I presents the accuracy and robustness (in terms of precision, recall, and the area-under-curve (AUC) metrics) of different ML classifiers when deployed to detect the DoS attacks. Higher the value of accuracy and robustness metrics, better will be performance.

One can observe from Table I, 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. For the KNN, a Euclidean distance function is employed with k=1 due to its lower complexity and best performance achieved over different experimented k values. Therefore, KNN is deployed in this ADU for attack detection. SVM though shown high accuracy, is observed in experiments that it is not able to detect sporadic variations such as spontaneous random errors, hence not the best option. For the neural network (ANN) a single hidden layer with 20 nodes is utilized. It can be argued that the hyper-parameters of the ML classifiers can be tuned to improve the performance, however optimizing the ML classifiers is not the focus of this work. For all the employed ML classifiers, the inputs (flits received, flits at error and flit error ratio) and output classes (normal, random error, DoS error) are same.

TABLE I: Attack detection performance of ML classifiers

ML classifier	Accuracy (%)	Recall	F-score	AUC
ANN	47.86	0.48	0.65	0.47
SVM	98.96	0.98	0.98	0.99
KNN	99.87	0.99	0.99	0.99
DT	52.46	0.52	0.69	0.53

TABLE II: Overhead analysis for different ML classifiers

Classifier	Area (μm^2)	Power (μW)	Timing (ns)
ANN	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

Table II presents the incurred overhead in terms of area, power and delay of the deployed ML Classifiers. The char-

TABLE III: System performance under attacks

	Wired mesh	WiNoC with 4 WIs	WiNoC with external attack	WiNoC with internal attack
Bandwidth per core (Gbs/core)	26.4	30.4	26.4	29.5
Average packet latency (Cycles)	395.96	286.80	395.96	319.00
Average packet energy (pJ)	100	61	101	78

acteristics of the various classifiers are obtained from post-synthesis RTL models are synthesized using 65nm standard cell libraries, as mentioned earlier. As the KNN Classifier has the highest accuracy and lowest area and power consumption, we adopt the KNN Classifier for the evaluation of overall system. Although, the delay of the KNN classifier is not the optimal, 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 WiNoC in Figure 3.

C. Secure WiNoC Performance in Presence of Attacks

Here, we evaluate the performance of the proposed WiNoC in presence of DoS attacks from internal and external attackers. We consider a WiNoC with 64 cores in a 20mm$\times$20mm die interconnected with a wired mesh and overlaid with 4 WIs at the central node of each subnet of 16 cores. The WiNoC with embedded security is also compared with an equivalent 64 core wired mesh for performance. From Table III, it is clear that the WiNoC outperforms the wired mesh in terms of peak bandwidth, latency and packet energy due to the wireless shortcuts between cores, which reduce the average path length and also a low power wireless medium for communication. This performance can change depending on the number of subnets and WIs deployed on the WiNoC [16], The security measures developed in this work, will be effective irrespective of the number of WIs for the assumed attack model.

Next, it can be seen that in presence of an external attack, the performance of the WiNoC is similar to that of the wired mesh. This is expected, as on detecting an external attacker, the WSU deactivates all the WIs leaving wired links as the only medium of communication for the purpose of security. On the other hand, when the attacker in an internal agent, only the infected WI is disabled, retaining the advantage due to the presence of the rest of the WIs. Thus, in the case of internal attack, $<$3% degradation in communication bandwidth compared to WiNoC without any attack is achieved.

D. System Overhead Analysis

As noted in Figure 3 each WI is equipped with the BEU, ML Classifier based ADU and Defense Units. The adopted KNN Classifier occupies an area of 105.3μm^2. The BEU [19] occupies an area of 4357.5μm^2. The scan FF for the token register is 15μm^2. The area of the Attack Detector and Defense Unit logic blocks is negligible. Therefore, the total area overhead for each WI is 0.0044mm^2. The area of the WIs is 0.2mm^2, making this overhead 0.2% per WI in the system. The area of the single MAC-LFSR and its decoder is 41μm^2 and 38μm^2. As observed, the area overhead incurred by embedding proposed secure mechanism is negligible compared to the die size of 400 mm^2 (considered in this work).

VII. Conclusions

In this work, we present a detection and defense mechanism for WiNoCs against jamming based DoS attacks originating from either an internal HT or an external attacker. We use burst error correction codes to estimate the number of burst errors in received packets over the wireless interconnects. This is then used in an ML Classifier to distinguish DoS attacks from random transient burst errors. In the event of attack detection by ML classifier, a logic block will analyze the attacker as either internal or external and enact a defense mechanism accordingly. Using this proposed mechanism, data transfer over the WiNoC is sustained even in the presence of DoS jamming. In presence of an external attacker the wireless interconnects are disabled and data is routed using the wired NoC only. However, in presence of an internal attack the performance is still better than a wired NoC.

References

[1] P. D. S. Manoj *et al.*, "Reliable 3-D clock-tree synthesis considering nonlinear capacitive TSV model with electrical-thermal-mechanical coupling," *IEEE Trans. CAD*, vol. 32, no. 11, pp. 1734–1747, Nov 2013.

[2] P. D. S. Manoj *et al.*, "A scalable network-on-chip microprocessor with 2.5D integrated memory and accelerator," *IEEE Trans. on CAS-I*, vol. 64, no. 6, pp. 1432–1443, June 2017.

[3] L. P. Carloni, P. Pande, and Y. Xie, "Networks-on-chip in emerging interconnect paradigms: Advantages and challenges," in *ACM/IEEE Int. Symp. on Networks-on-Chip*, 2009.

[4] B. Wu *et al.*, *A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks*, 2007, pp. 103–135.

[5] J. Sepúlveda *et al.*, "Dynamic NoC buffer allocation for MPSoC timing side channel attack protection," in *IEEE Latin American Symp. on Circuits Systems*, 2016.

[6] D. Zhao and Y. Wang, "SD-MAC: Design and synthesis of a hardware-efficient collision-free QoS-aware MAC protocol for wireless network-on-chip," *IEEE Trans. Comp.*, vol. 57, no. 9, pp. 1230–1245, Sept 2008.

[7] A. Ganguly *et al.*, "Scalable hybrid wireless network-on-chip architectures for multicore systems," *IEEE Trans. on Computers*, vol. 60, no. 10, pp. 1485–1502, Oct 2011.

[8] A. Ganguly *et al.*, "Intra-chip wireless interconnect: The road ahead," in *Int. W. on Network on Chip Architectures*, 2017.

[9] A. Ganguly, M. Y. Ahmed, and A. Vidapalapati, "A denial-of-service resilient wireless NoC architecture," in *ACM GLSVLSI*, 2012.

[10] B. Lebiednik *et al.*, "Architecting a secure wireless network-on-chip," in *IEEE/ACM International Symposium on Networks-on-Chip*, 2018.

[11] E. Kakoulli, V. Soteriou, and T. Theocharides, "Intelligent hotspot prediction for network-on-chip-based multicore systems," *IEEE Trans. on CAD*, vol. 31, no. 3, pp. 418–431, March 2012.

[12] M. Zekri *et al.*, "DDoS attack detection using machine learning techniques in cloud computing environments," in *Int. Conf. of Cloud Computing Technologies and Applications (CloudTech)*, 2017.

[13] P. A. Raj Kumar and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier," *Comput. Commun.*, vol. 34, no. 11, pp. 1328–1341, July 2011.

[14] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," *CoRR*, vol. abs/1804.04159, 2018.

[15] M. Suresh and R. Anitha, "Evaluating machine learning algorithms for detecting DDoS attacks," in *Advances in Network Security and Applications*, 2011.

[16] S. Deb *et al.*, "Design of an energy-efficient CMOS-compatible NoC architecture with millimeter-wave wireless interconnects," *IEEE Trans. Comput.*, vol. 62, no. 12, pp. 2382–2396, Dec 2013.

[17] X. Yu *et al.*, "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.*, vol. 62, no. 10, pp. 2357–2369, Oct 2014.

[18] X. Yu *et al.*, "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*, vol. 62, no. 3, pp. 799–806, March 2015.

[19] B. Fu and P. Ampadu, "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*, 2009.

[20] R. JayashankaraShridevi *et al.*, "Catching the flu: Emerging threats from a third party power management unit," in *ACM/IEEE DAC*, 2016.

[21] P. P. Pande *et al.*, "Performance evaluation and design trade-offs for network-on-chip interconnect architectures," *IEEE Trans. on Computers*, vol. 54, no. 8, pp. 1025–1040, Aug 2005.