Modeling and Analysis of Thermal Covert Channel Attacks in Many-core Systems

Shengjie Wang, Xiaohang Wang, *Member, IEEE,* Yingtao Jiang, Amit Kumar Singh, *Member, IEEE*, Mei Yang, and Letian Huang, *Member, IEEE*

Abstract—In a many-core chip, thermal flux and thermal correlation among the cores can be explored to create a thermal covert channel (TCC). In this paper, we provide an analytical model to quickly determine the key TCC performance metrics, in terms of bit error rate (BER), signal to noise ratio (SNR), and channel capacity, without going through lengthy computer simulation and/or physical experiments that are normally needed in current TCC performance studies. According to our model, the TCC's BER is proportional to the square root of the transmission frequency, which can be explored quantitatively to boost the TCC's transmission efficiency by letting the TCC's thermal signal be transmitted at a higher frequency. In addition, our proposed model also links the jamming noise and application of Dynamic Voltage Frequency Scaling (DVFS) to TCC's BER performance, a feature that can be explored to design/optimize the countermeasures against the TCC attacks. The TCC performance predicted by the proposed theoretical model is found in a good agreement with that obtained from computer simulations, with an average error lower than 7%.

Index Terms—Manycore Systems, Thermal Covert Channel, Analytical Model.

1 Introduction

More than ever before, security of individual many-core chips has been so critical to ensure the security of modern information system infrastructure and platforms, ranging from cloud system [1] to end point mobile devices [2]. Unfortunately, many-core chips face escalating multiple threats, among which the covert channel attacks enabled by many possible covert channels media [3], [4], [5] happen to be among the most notorious and dangerous ones.

Of many possible covert channels that may exist in many-core chips, the thermal covert channel (TCC) that exploits high thermal correlation among processor cores can do a great harm. In the literature, various thermal covert channels have been demonstrated and studied [6], [7], [8], [9], [10]. Transmitted over a thermal covert channel in the form of temperature signals, secret data (*e.g.*, passwords) originated from one core in the secure zone can be leaked to another core in the unsecured zone [9]. A thermal covert channel can be established as a program or core in the secure zone which is compromised by malware software, backdoor, or even hardware Trojan (HT) [11].

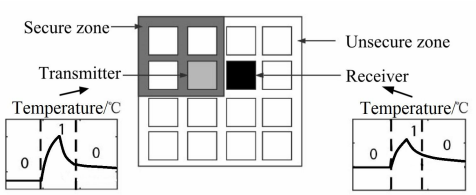

Fig. 1. Illustration of thermal covert channel attack.

Fig. 1 illustrates an attack scenario over a thermal covert channel [9]. In this example, the compromised core in the secure zone (referred to as the transmitter) loses control to turn itself on or off. When the core is forced ON to consume power, there is a direct consequence to bring up the core's temperature. On the other hand, the core's temperature drops when it is turned off. A password can be encoded and then transmitted as thermal signals by setting the ON/OFF intervals of the core. The malicious core in the unsecured zone (referred to as the receiver) reads its local thermal sensor to collect the thermal signal and decodes it to recover the data. A simple thermal covert channel can be made more robust and resilient to countermeasures, and thus more dangerous, if it can dynamically change its transmission frequency, as indicated in [9].

Performance of TCCs has been studied through lengthy computer simulations and/or time-consuming experimentation with special hardware setup. Simulation or experiments on real machine are time-consuming, or require well-craft design. In this paper, we explore to derive a model based approach to predict the attack effects of TCCs under various configurations in a fast manner. Design of countermeasures against TCCs can benefit greatly from using the analytical models for quick turnout when evaluating various design options and tradeoffs. To this end, we present

- *S. Wang is with the School of Software Engineering, South China University of Technology, Guangzhou 510006, China. E-mail: 201921043708@mail.scut.edu.cn.*
- *X. Wang is with the School of Software Engineering, South China University of Technology, Guangzhou 510006, China, Zhejiang Lab, and State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences. X. Wang is the corresponding author. E-mail: xiaohangwang@scut.edu.cn.*
- *Y. Jiang and M. Yang are with the Department of Electrical and Computer Engineering, University of Nevada, Las Vegas, USA. E-mail: yingtao@egr.unlv.edu, mei.yang@unlv.edu.*
- *A.K. Singh is with the School of Computer Science and Electronic Engineer, University of Essex, CO4 3SQ Colchester, United Kingdom. E-mail: a.k.singh@essex.ac.uk*
- *L. Huang is with the School of Communication and Information Engineering, Electronic Science and Technology of China, Chengdu 610054, China. E-mail: huanglt@uestc.edu.cn.*

in this paper a theoretical model that quantifies the power spectral density, noise characteristics, channel capacity, signal to noise ratio (SNR), and the bit error rate (BER) of thermal covert channel. The results predicted by the proposed theoretical model are found in a good agreement with those obtained from computer simulations, with a difference of lower than 7%.

The remainder of the paper is organized as follows. Section 2 reviews related work. Section 3 introduces the preliminary of thermal covert channel. Modeling TCC is presented in Section 4, and the model is validated with various configurations experimentally in Section 5. Finally, Section 6 concludes the paper.

2 Related Work

Covert channel attacks have been studied for cloud systems [1], operating system [12], and many-core chips [3], [4] *etc.* To attack a many-core chip, a variety of thermal covert channel designs have been proposed. They differ from each other in terms of line coding schemes adopted and their application areas.

Masti *et al.* [6] proposed a thermal covert channel with a simple binary coding scheme, where bits '1' and '0' are respectively represented by high and low temperature levels. So far, they have achieved a throughput of 1.33 bits per second (bps) and a BER of 11% on an Intel Xeon-based sever. A more sophisticated coding scheme was adopted in [7] and achieved an even lower bit error rate of 0.1% at 8 bps on a real machine, where bit '1' is encoded as a state transition from active to sleep, and bit '0' is encoded as a state transition from sleep to active. Another thermal covert channel was demonstrated in a package-on-package system [8]. In this case, sensitive data are able to be transmitted between the CPU and the DRAM by measuring the number of bit flips in the DRAM which is affected by temperature variation. A related but different cover channel is power management covert channel [5], where the transmitter and receiver running on different cores use operating frequency and/or voltage as a transmission medium, which is fundamentally different from TCC.

There are two countermeasures that can be applied to thwart TCC attacks. In [9], a jamming noise whose transmission frequency matches any detected TCC is emitted to block the TCC transmission. In [10], DVFS is applied on cores running TCC transceiver to make TCC transmission impossible.

Bartolini *et al.* [7] proposed a model to estimate the channel capacity. However, this work does not model the channel signal, BER, and SNR of TCC. By far, no analytical models of BER and SNR of TCC are found in the literature. In this paper, we model the signal, noise, power spectral density, BER, and bandwidth. Moreover, we explore the theoretical bound of maximally allowed data transmission rate. Furthermore, the models are validated by comparing the results of simulation experiments with the values obtained by modeling.

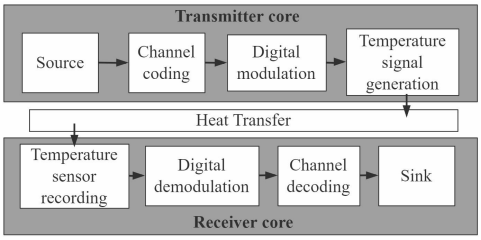

Fig. 2. The baseline of the thermal covert channel.

3 The Thermal Covert Channel

3.1 Overview

In the thermal covert channel, the bit streams of the passwords are encoded in the form of temperature variations. The baseline of the thermal covert channel includes a transmitter and a receiver, as shown in Fig. 2. The compromised core sending the passwords is referred to as the transmitter, and the malicious core receiving passwords is referred to as the receiver. We assume that each core has a thermal sensor [13], which is prevalent in modern many-core chips for thermal management and fine-grain power budgeting purposes [14].

The transmitter controls its ON/OFF status to consume high or low power consumption. The lengths of the time intervals of the ON or OFF period correspond to the data transmission rate. The temperature of a core varies according to its power consumption.

The thermal covert channel includes two components: a physical system for data transmission and a communication protocol to establish and sustain a data communication session.

3.2 Transmitting the Bit Streams

A covert channel is built on a communication system that transmits encoded thermal signals. The coding scheme includes level coding scheme (*i.e.*, bits '1' and '0' are encoded by high and low temperatures) and return-to-zero (RZ) line coding scheme. However, the level coding can cause overheating when multiple bits '1' are sent continuously. Thus, the RZ encoding scheme in [10] is adopted to encode the bit streams. Bit '1' is encoded by turning the transmitter ON and then turning it OFF, and bit '0' by keeping it OFF for sufficient amount of time. By controlling the length of the time period of the temperature variation, the frequency components of the temperature variations can vary. The noise power of a TCC is mostly concentrated at low frequencies, as demonstrated in [15]. As a result, by setting the frequency of temperature signal higher than that dominated by noise, the data transmission over such a covert channel can be of little or no interference from noise. The digital modulation modulates the bit streams via OOK (On-Off Keying). The signal in the time domain can be expressed as follows.

$$e_{OOK}(t) = s(t) \times c(t) \tag{1}$$

$$s(t) = \sum_{k} a_k g(t - kT_b) \tag{2}$$

where $c(t)$ is the carrier signal, T_b is the symbol width of one bit, $g(t)$ is the baseband pulse waveform with duration T_b, and a_k is the value of the k-th bit of the bit streams to be transmitted ('1' or '0'). The receiver uses a finite impulse response (FIR) [16] filter to extract the temperature information of the transmission frequency in the temperature signal. The receiver decodes the bit streams by checking the signal amplitude. If it is higher than a preset threshold, it is decoded as '1', otherwise it is '0'.

A communication protocol decides when to start and finish a communication session. In the baseline thermal covert channel, the communication protocol in [10] is used to initiate and terminate a transmission. A transmission starts by a REQ packet from the transmitter to the receiver. The transmitter keeps waiting until it receives an ACK replied from the receiver. Then the transmitter sends data (passwords) to the receiver. Once the transmitter finishes transmission, a specific END packet is sent to the receiver to inform it to terminate the transmission.

4 Modeling Thermal Covert Channel Attack

4.1 Modeling the Thermal Signal

According to [17], a heat flow is modelled by

$$\boldsymbol{A}\frac{d\boldsymbol{T}(\tau)}{d\tau} + \boldsymbol{D}\boldsymbol{T}(\tau) = \boldsymbol{P} + \boldsymbol{T_{amb}}\boldsymbol{G} \tag{3}$$

where $\boldsymbol{A}$ is the thermal capacitance matrix of the components in a multi-core system (routers, processors, etc), τ is the discrete time unit, $\boldsymbol{T}(\tau)$ is the temperature vector with $\boldsymbol{T}(\tau)[j]$ representing the temperature of the j-th component, $\boldsymbol{D}$ is the thermal conductance matrix which includes the thermal conductance between vertical and lateral neighboring nodes, and $\boldsymbol{P}$ is the power vector that take into account of both dynamic and leakage power, $\boldsymbol{T_{amb}}$ is the ambient temperature, and column vector $\boldsymbol{G}$ contains the thermal conductance between each node and the ambient.

Consider a simplified case that there are only two active cores (*i.e.*, the transmitter and the receiver) in the multi-core system. Every core is treated as a node in the proposed model; that is, the grid resolution is assumed to be 1×1 for every core. We assume that the two cores have the same configuration and designate core 1 transmitting and core 2 receiving. In this case, matrices $\boldsymbol{A}$, $\boldsymbol{D}$, and vectors $\boldsymbol{T}$, $\boldsymbol{P}$, and $\boldsymbol{G}$ in Eqn. 3 are given as:

$$\boldsymbol{A} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \boldsymbol{D} = \begin{bmatrix} b & c \\ c & b \end{bmatrix}, \boldsymbol{T} = \begin{bmatrix} T_1 \\ T_2 \end{bmatrix}, \boldsymbol{P} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}, \boldsymbol{G} = \begin{bmatrix} g_1 \\ g_2 \end{bmatrix} \tag{4}$$

where a is the thermal capacitance of the cores, b is the thermal conductance of the cores to the ground, c is the thermal conductance between the two cores, p_1 and p_2 are the respective power consumption values of core 1 and core 2, g_1 and g_2 are the respective thermal conductances between the ambient and core 1 and core 2, and T_1 and T_2 are the respective temperatures of core 1 and core 2.

Eqn. 3 then can be expressed as two differential equations below.

$$\begin{cases} aT_1' + bT_1 + cT_2 = p_1 + \boldsymbol{T_{amb}}g_1 \\ aT_2' + cT_1 + bT_2 = p_2 + \boldsymbol{T_{amb}}g_2 \end{cases} \tag{5}$$

where T_1' and T_2' account for the first derivatives of the temperatures of core 1 and core 2 with respect to time, respectively. Solving the differential equations given in Eqn. 5 yields

$$\begin{cases} T_1 = C_2 e^{\frac{-c-b}{a}\tau} - C_1 e^{\frac{c-b}{a}\tau} + bp_1 + b\boldsymbol{T_{amb}}g_1 - cp_2 \\ T_2 = C_1 e^{\frac{c-b}{a}\tau} - C_2 e^{\frac{-c-b}{a}\tau} + bp_2 + b\boldsymbol{T_{amb}}g_2 - cp_1 \end{cases} \tag{6}$$

where C_1 and C_2 are coefficients.

When there are m cores running in the system, within the time of one period, *i.e.*, (0, T_b), the temperature signals of both the transmitter and receiver in the thermal covert channel can be expressed as.

$$s(t) = \alpha_1 e^{\beta_1 t} + \alpha_2 e^{\beta_2 t} + \alpha_3 p + \alpha_4 \tag{7}$$

where α_1, α_2, α_3, α_4, β_1, and β_2 are coefficients, α_4 is the temperature contribution of the receiver core (or the transmitter core) and other cores, and p is the power consumption of the transmitter core (or the receiver core). The coefficients are determined by regression [18] with data collected from simulation or experiment performed on a real machine. Note that only a single set on simulation or experiment is actually needed to fit the model for a given configuration.

4.2 Computation of Bandwidth

Bandwidth B can be expressed as

$$B = \frac{1}{T_b} \tag{8}$$

where T_b is the symbol width of one bit. The bandwidth can be computed by solving the following problem.

$$\text{maximize} \quad B \tag{9}$$

$$\text{subject to} \quad s(\frac{T_b}{2}) - s(0) \geq r \tag{10}$$

where r is the resolution of the thermal sensor. Eqn. 10 ensures that temperature varies due to TCC can be detected by the thermal sensor. Solving the above problem yields the maximum bandwidth for a given sensor resolution.

4.3 Modeling Channel Capacity

According to Eqn. 7, the power spectral density can be expressed as

$$P_s(f) = \lim_{T_b \to \infty} \frac{E\left|S_{T_b}(f)\right|^2}{T_b} \tag{11}$$

$$S_{T_b}(f) = -\frac{2\alpha_1\beta_1}{\beta_1^2 + 4\pi^2 f^2} - \frac{2\alpha_2\beta_2}{\beta_2^2 + 4\pi^2 f^2} + (\alpha_3 p + \alpha_4)\phi(f) \tag{12}$$

where $S_{T_b}(f)$ is the spectral function derived from $s(t)$, $\phi(\cdot)$ is the Dirac delta function. The power spectral density of the band-limited Gaussian noise (*i.e.*, the temperature variations of other cores except the TCC's transmitter) can be expressed as follows and the coefficients can be determined by curve fitting [19].

$$P_n(f) = \lambda_1 e^{\epsilon_1 f} + \lambda_2 e^{\epsilon_2 f} + \lambda_3 \quad (0 < f < +\infty) \tag{13}$$

where λ_1, λ_2, λ_3, ϵ_1, and ϵ_2 (ϵ_1, $\epsilon_2 < 0$) are coefficients. One can see from Eqn. 13, when the transmission frequency

increases, the power spectral density of the noise decreases as well.

Capacity C is defined in terms of number of bits transmitted per second. Following the Shannon formula [19], we can estimate the channel capacity as

$$C = \int_B \log_2(1 + \frac{P_s(f)}{P_n(f)})df \tag{14}$$

where B is the bandwidth of the thermal covert channel, $P_n(f)$ is the power spectral density of the Gaussian noise, $P_s(f)$ is the power spectral density of the signal transmitted in the channel.

One can see from Eqn. 14, the channel capacity can be improved by reducing the power density of noise. As indicated in [15], noise power density decreases at high frequencies, as their temperatures do not vary abruptly when the applications are running on the cores.

4.4 The BER Model

In the thermal covert channel, the signal is attenuated and distorted when transmitting through the channel that is exposed to white Gaussian noise. According to Eqn. 7, in each period of $(0, T_b)$, the received signal of the receiver can be expressed as follows.

$$r(t) = \alpha_1 e^{\beta_1 t} + \alpha_2 e^{\beta_2 t} + \alpha_3 p + \alpha_4 + n_i(t) \tag{15}$$

where $n_i(t)$ is additive white Gaussian noise of zero mean.

The waveform after passing through an FIR filter with a center frequency of f and impulse response of $h(t) = s(T_b - t)$ can be expressed as follows [19].

$$x(t) = \begin{cases} n & \text{when sending bit '0'} \\ s_c + n & \text{when sending bit '1'} \end{cases} \tag{16}$$

where s_c is the temperature signal component, which is the output of $r(t)$ through the FIR filter by convoluting $r(t)$ and $h(t)$, n is the output noise of $n_i(t)$ through the filter, which is a narrowband Gaussian noise with zero mean and variance of σ_n^2. Thus, $x(t)$ is also a stochastic process with variance of σ_n^2, and its mean values are s_c (when transmitting bit '1') and 0 (when transmitting bit '0'), respectively.

Suppose the sampling time of the i-th symbol is iT_b. Then x is the discrete sample of $x(t)$, which is a Gaussian random variable at time iT_b. Thus, when sending bit '1', the probability density function of x can be expressed as follows.

$$f_1(x) = \frac{1}{\sqrt{2\pi}\sigma_n} \exp\left\{-\frac{(x-s_c)^2}{2\sigma_n^2}\right\} \tag{17}$$

When sending bit '0', the probability density function of x is given as

$$f_0(x) = \frac{1}{\sqrt{2\pi}\sigma_n} \exp\left\{-\frac{x^2}{2\sigma_n^2}\right\} \tag{18}$$

Fig. 3 shows the curves of $f_1(x)$ and $f_0(x)$, where γ is the decision thresholds and the decision rule can be expressed as follows.

$$\text{decision} \quad \text{result} = \begin{cases} 1 & \text{when} \quad x > \gamma \\ 0 & \text{when} \quad x \le \gamma \end{cases} \tag{19}$$

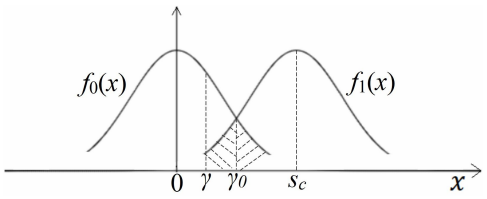

Fig. 3. The curves of $f_1(x)$ and $f_0(x)$.

When sending bit '1', the bit error rate (the probability of sending bit '1', but bit '0' received) can be expressed as follows.

$$P(0|1) = P(x \le \gamma) = \int_{-\infty}^{\gamma} f_1(x)dx = 1 - \frac{1}{2}\text{erfc}(\frac{\gamma - s_c}{\sqrt{2}\sigma_n}) \tag{20}$$

where $\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-u^2} du$. When sending bit '0', the bit error rate (the probability of sending bit '0', but bit '1' received) can be expressed as follows.

$$P(1|0) = P(x > \gamma) = \int_{\gamma}^{\infty} f_0(x)dx = \frac{1}{2}\text{erfc}(\frac{\gamma}{\sqrt{2}\sigma_n}) \tag{21}$$

The total bit error rate of the thermal covert channel E_1 then is given as

$$\begin{aligned} E_1 = P(1)P(0|1) + P(0)P(1|0) = P(1)\int_{-\infty}^{\gamma} f_1(x)dx \\ + P(0)\int_{\gamma}^{\infty} f_0(x)dx \end{aligned} \tag{22}$$

where $P(1)$ and $P(0)$ represent the probabilities of sending bit '1' and bit '0', respectively.

One can see from Eqn. 22, where $P(1)$, $P(0)$, $f_1(x)$ and $f_0(x)$ are constants, the bit error rate E_1 is solely dependent on the value of the decision threshold γ. From Fig. 3, one can see that the bit error rate E_1 is equal to the area of the shaded area in Fig. 3. Moreover, the bit error rate E_1 is the smallest when the decision threshold is γ_0, which can be computed using the maximum likelihood method [18].

$$\gamma_0 = \frac{s_c}{2} + \frac{\sigma_n^2}{s_c} \ln \frac{P(0)}{P(1)} \tag{23}$$

We assume that the probability of sending bit '1' in the thermal covert channel is equal to the probability of sending bit '0', that is, $P(1) = P(0)$. In this case, γ_0 is equal to $s_c/2$. The total bit error rate of the thermal covert channel E_1 can be expressed as follows.

$$E_1 = \frac{1}{2}\text{erfc}(\frac{s_c}{2\sqrt{2}\sigma_n}) = \frac{1}{2}\text{erfc}(\sqrt{\frac{SNR}{4}}) \tag{24}$$

where the signal-to-noise ratio $SNR = \frac{s_c^2}{2\sigma_n^2}$, $\frac{s_c^2}{2}$ is the power of the signal, and σ_n^2 is the power of noise. According to Eqn. 13, the total bit error rate of the thermal covert channel E_1 can be expressed as follows.

$$E_1 = \frac{1}{2}\text{erfc}(\sqrt{\frac{2s_c^2}{\lambda_1 e^{\epsilon_1 f} + \lambda_2 e^{\epsilon_2 f} + \lambda_3}}) \tag{25}$$

Eqn. 25 confirms that the total bit error rate of the thermal covert channel can be reduced by increasing the frequency of temperature signal.

TABLE 1
Configurations used in the simulation

Many core system configuration	
Number of Cores (2D)	3×3 / 4×4
Number of Cores (3D)	3×3×3 / 4×4×3
Fetch/Decode/Commit size	4/4/4
L1 D cache	16KB, 2-way, 32 B line, 2 cycles, 2 ports, dual tags
L1 I cache	32KB, 2-way, 64 B line, 2 cycles
L2 cache	64KB, 64 B line, 6 cycles, 2 ports
Main memory size	2 GB
Benchmarks	
PARSEC	Blackscholes, Canneal, Fluidanimate, Streamcluster, Swaptions, X-264, Dedup, Freqmine
SPLASH-2	Barnes, Raytrace
Hotspot configuration	
Chip thickness	$0.00015m$
Specific heat capacity	$1.75 \times 10^6 J/(m^3 \cdot K)$
Silicon thermal conductivity	$100W/(m \cdot K)$
Temperature threshold for DTM	$373.15K$
Heat sink side	$0.06m$
Heat sink thickness	$0.0069m$
Heat sink thermal conductivity	$400W/(m \cdot K)$
Specific heat capacity of heat sink	$3.55 \times 10^6 J/(m^3 \cdot K)$
Thermal sensor resolution	0.1^oC

TABLE 2
Configurations of bit streams

ID of bit streams	Percentage of bits '1'(%)
1/2/3/4/5	20/40/60/80/100

5 Experimental Results

5.1 Experimental Setup

Experiments were performed on a real machine and a many-core simulator, Sniper, with McPAT integrated as the power model, and Hotspot version 6.0 as the temperature simulator. In the simulation, multiple applications are running in the system. Table 1 lists the simulator configuration. We used two kinds of benchmarks in the experiment, which are also listed in Table 1. The benchmarks are selected from PARSEC and SPLASH-2. During the experiments, cores other than transmitters and receivers are running the threads of these benchmarks. Each of the benchmarks are parallelized into 4, or 8, or 16 threads. The floorplan of the processor cores is adopted from the one adopted in [20].

In what follows, Section 5.2 analyzes noise, Section 5.3 validates the thermal covert channel model of Section 4, and Section 5.4 analyzes two countermeasures.

5.2 Noise analysis

To analyze the feature of noise (*i.e.*, to decide whether it is Gaussian or not), an experiment recorded the temperature traces by running applications on a real computer. The CPU is AMD A10-7300 @1.9GHz with the operating system of Ubuntu 16.04.5 LTS. We run the **modprobe msr** instruction to load the model specific register (msr) module for the temperature reading, and the temperature traces are recorded every 10 ms under ten different system loads (treated as noises) as shown in TABLE 1.

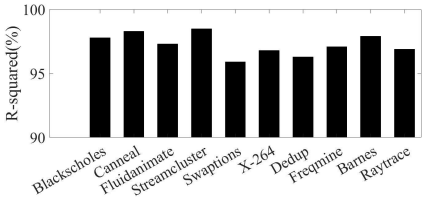

Fig. 4. The Gaussian fitting results of noise from different benchmarks.

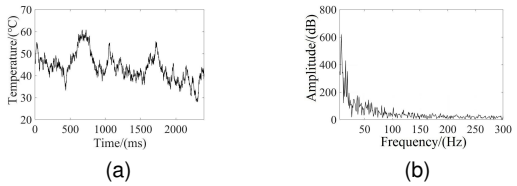

Fig. 5. (a) The channel noise in temporal domain, and (b) the corresponding power spectrum of the noise.

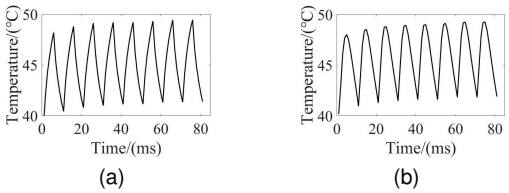

Fig. 6. The temperature signal in the time domain obtained from (a) simulation and from (b) the model.

Gaussian fitting is performed to check whether traces follow a Gaussian distribution. Fig. 4 shows the fitting results for the different benchmarks. It can be seen that the average R-squared of the thermal noise for each benchmark is 97.3%, which justifies the assumption of noise being Gaussian.

Fig. 5(a) shows a channel noise in the time domain, and its frequency spectrum is shown in Fig. 5(b). From Fig. 5(b), one can see that majority components of the signals concentrate in the low frequency band.

5.3 Evaluating the Thermal Covert Channel Models

Fig. 6 shows the comparison of temperature signal in the time domain obtained from simulation and from the model. From Fig. 6, one can see that the temperature signal in the time domain obtained from the simulation agrees reasonably well with that obtained from the model. In addition, we compare the R-squared of the thermal signal model in Eqn. 7 when transmitting the bit streams in Table 2, and the results are shown in Fig. 7. The average R-squared is about 98.4%. One can see that the simulation results of the thermal covert channel are in good agreement with those predicted by the thermal signal model by Eqn. 7.

From Fig. 8, one can see that the power spectral density of the temperature signal computed from the simulation agrees reasonably well with that obtained that predicted by Eqn. 11.

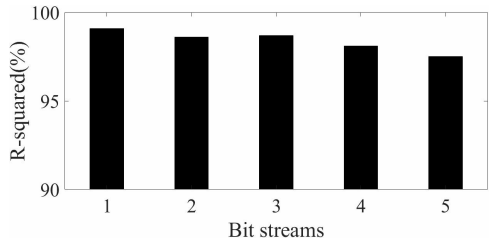

Fig. 7. R-squared of the thermal signal model in Eqn. 7.

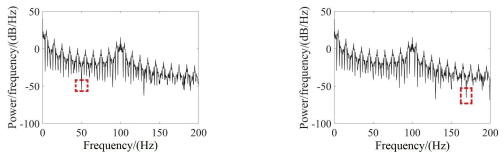

Fig. 8. (a) Power spectral density of temperature signal obtained from simulation. (b) Power spectral density of temperature signal derived from the model given in Eqn. 11.

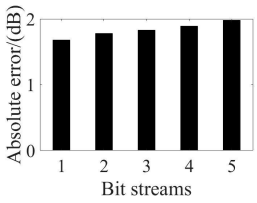

Fig. 9. Absolute error of the proposed power spectral density model.

Fig. 9 shows the error of the power spectral density model in Eqn. 11 when transmitting different bit streams. Error is defined as below:

$$error = \frac{1}{N}\sum_{i=1}^{N}\left|P_i' - P_i\right| \tag{26}$$

where P_i' is the power from the power spectral density model in Eqn. 11, P_i is the power computed from simulations. It can be seen that the average error of the power spectral density predicted by Eqn. 11 is within 1.83dB of the simulation results.

Fig. 10 compares the BER from simulation with the proposed BER model in Eqn. 25 under different transmission frequencies. The system is set to have a total of 4×4 cores, and the distance between the transmitter and receiver is 1 hop. As can be seen from Fig. 10, both the simulation results and the predication by the proposed models indicate that the BER decreases with the increase of the transmission frequency. The BER of the TCC reported in [7] is higher than that of the TCC reported in [15] since the channel noise concentrates at low frequency, as shown in Fig. 5(b), and it impacts the former more seriously. It can also be seen from Fig. 10 that the prediction by the proposed BER model is very close to the result obtained from simulation; the average error of the proposed BER model is 6.2%.

Fig. 11 compares the BERs from simulation with the BERs from the proposed model in Eqn. 25 under different system sizes. The 3×3×3 and 4×4×3 cases follow the 3D mesh topologies. Specifically, the 3×3×3 NoC is organized

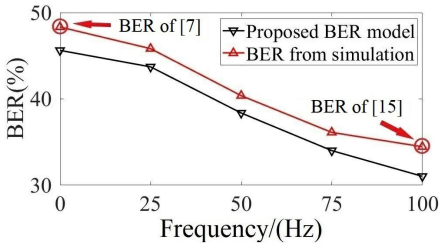

Fig. 10. Comparison of the proposed BER model and BER from simulations under different transmission frequencies.

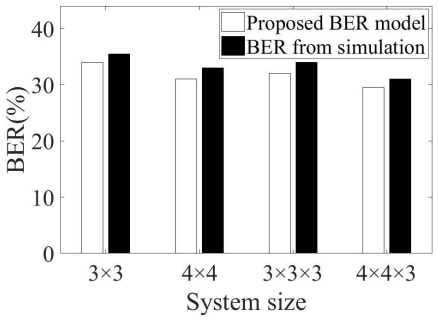

Fig. 11. The BERs predicted by the proposed model vs. the BERs from the simulation for different system sizes.

as three 3×3 2D meshes, and the 4×4×3 has three 4×4 2D meshes. The distance between the transmitter and receiver is 1 hop, and the transmission frequency is 100Hz. From Fig. 11, one can see that, the average error of the proposed BER model is 5.6%.

To explore the highest throughput in theory, we investigate the maximum transmission frequency at an acceptable bit error rate with the sensor resolution of 1 degree Celsius. The most ideal bandwidth B of the TCC is 80Hz, as the thermal noise concentrates between 0-20Hz and the highest transmission frequency is 100 Hz. The signal-to-noise ratio SNR is 0.49dB. According to the proposed capacity model in Eqn. 14, the ideal channel capacity C is 46.3 bps for one single channel. However, to achieve such a wide bandwidth and high data rate, more sophisticated modulation schemes, instead of OOK, should be used, which calls for future research.

5.4 Performance Analysis of Countermeasures against the Thermal Covert Channel

The proposed models can be used to allow quick estimate of many countermeasures against TCC attacks without going through time-consuming simulations.

5.4.1 Jamming based countermeasure

In [9], a countermeasure to combat the thermal covert channel was proposed, where a jamming noise whose transmission frequency matches any detected TCC is emitted to block the TCC from transmitting data. Emitting jamming noise reduces the signal-to-noise ratio by increasing the power of the noise, thereby increasing the BER. Since the jamming noise emitted is expected to behave in the way

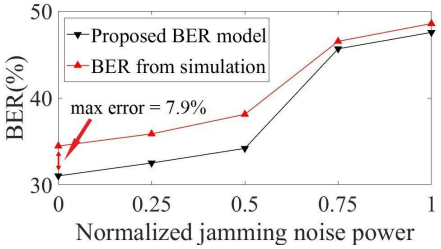

Fig. 12. The BERs vs. the jamming noise power.

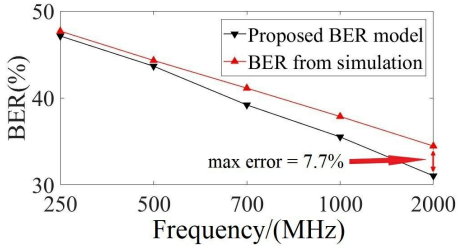

Fig. 13. The BERs vs. CPU frequencies.

similar to the thermal signal, following the same treatment as in Eqn. 7, the jamming noise can be expressed as

$$N(t) = \mu_1 e^{\nu_1 t} + \mu_2 e^{\nu_2 t} + \mu_3 q + \mu_4 \tag{27}$$

where μ_1, μ_2, μ_3, μ_4, ν_1, and ν_2 are coefficients, q is the power of the jamming core. Accordingly, the power spectral density of jamming noise is:

$$P_N(f) = \lim_{T\to\infty} \frac{E\left|N_T(f)\right|^2}{T_b'} \tag{28}$$

$$N_T(f) = -\frac{2\mu_1\nu_1}{\nu_1^2 + 4\pi^2 f^2} - \frac{2\mu_2\nu_2}{\nu_2^2 + 4\pi^2 f^2} + (\mu_3 q + \mu_4)\phi(f)) \tag{29}$$

where $N_T(f)$ is the spectral function from $N(t)$, and $\phi(\cdot)$ is the Dirac delta function, T_b' is the inverse of the detected TCC frequency. The BER of the thermal covert channel at the presence of jamming noise is:

$$E_2 = \frac{1}{2}\text{erfc}(\sqrt{\frac{P_s(f)}{4P_N(f)}}) \tag{30}$$

Fig. 12 shows the BERs from both simulation and the proposed BER model under different jamming noise power levels. One can see that the estimated BERs are very close to those from simulation experiments. The average and maximum errors of the proposed BER model are 6.1% and 7.9%, respectively. Both methods indicate that BER increases along with the escalation of jamming noise power.

5.4.2 DVFS based countermeasure

Another new countermeasure against the thermal covert channel attack is the use of DVFS [10]. Essentially, this technique tries to mitigate the impact of a TCC by dropping the V/F levels of cores involved in a TCC attack. In this experiment, we examine the relationship between V/F levels and BER.

The power consumption of the transmission p is a function of the V/F level and η [20]. The thermal signal model in Eqn. 7 can be used to compute TCC signal with different CPU frequencies.

$$p = \frac{1}{2} \cdot \zeta \cdot \xi \cdot V^2 \cdot \eta + p_l \tag{31}$$

where ζ is the switching activity, ξ is the effective capacitance, V is the supply voltage, η is the frequency, and p_l is the leakage power.

Fig. 13 compares the BER from simulation with the proposed BER model under different CPU frequency levels of the TCC transmitter core. The distance between the transmitter and receiver is 1 hop. Fig. 13 shows the estimated BER is very close to that from simulation. The average and maximum errors of the BER model are 4.1% and 7.7% respectively. The results in Fig. 13 confirm that BER increases with adoption of more aggressive DVFS to drop V/F even lower.

6 Conclusion

In this paper, the analytical models to determine the BER, SNR, and channel capacity of the TCC attacks were presented. These models reveal how the key parameters of TCC, including transmission frequency and transmission power are related to TCC performance in terms of BER. Effectiveness of two previously proposed countermeasures (*e.g.*, insertion of jamming noise and application of DVFS) was also analyzed using the proposed models. Experimental results show that these models are able to accurately predict the effectiveness of these countermeasures against TCC attacks with errors lower than 7%, without resolving to lengthy and expensive simulations and physical experiment. In a word, the proposed TCC models can be integrated into a design and test flow to assess the strength of new types of TCC attacks and/or design optimized countermeasures against TCC attacks.

Acknowledgments

This research program is supported by the National Natural Science Foundation of China No. 61971200, Zhejiang Lab No. 2021LE0AB01 and 2021PC0AC01, Open Research Grant of State Key Laboratory of Computer Architecture Institute of Computing Technology Chinese Academy of Sciences No. CARCH201916, Key Technologies R&D Program of Jiangsu (Prospective and Key Technologies for Industry) (Grant No. BE2021003), the Key Laboratory of Big Data and Intelligent Robot (South China University of Technology), Ministry of Education, and the National Key Research and Development Program of China No. 2019QY0705.

References

[1] Z. Wu, Z. Xu, and H. Wang, "Whispers in the hyper-space: high-speed covert channel attacks in the cloud," in Proc. Symp. Usenix Security, pp. 9-23, 2013.

[2] C. Marforio, H. Ritzdorf, A. Francillon, and S. Capkun, "Analysis of the communication between colluding applications on modern smartphones," in Proc. ACM Conf. Computer Security Applications, pp. 51–60, 2012.

[3] Y. Wang and G. E. Suh, "Efficient timing channel protection for on-chip networks," in Proc. IEEE/ACM Int'l Symp. Networks on Chip, pp. 142–151, 2012.
[4] G. Venkataramani, J. Chen, and M. Doroslovacki, "Detecting hardware covert timing channels," IEEE Micro, vol. 36, no. 5, pp. 17–27, 2016.
[5] S. K. Khatamifard, L. Wang, A. Das, S. Kose, and U. R. Karpuzcu, "POWERT channels: A novel class of covert communication exploiting power management vulnerabilities," in Proc. IEEE Int'l Symp. High Performance Computer Architecture, pp. 291-303, 2019.
[6] R. J. Masti, D. Rai, A. Ranganathan, C. Muller, L. Thiele, and S. Capkun, "Thermal covert channels on multi-core platforms," in Proc. USENIX Security Symp., pp. 865–880, 2015.
[7] D. B. Bartolini, P. Miedl, and L. Thiele, "On the capacity of thermal covert channels in multicores," in Proc. ACM Conf. Computer Systems, pp. 24–39, 2016.
[8] S. Chen, W. Xiong, Y. Xu, B. Li, and J. Szefer, "Thermal covert channels leveraging package-on-package DRAM," in Proc. IEEE Int'l Conf. Trust Security Privacy Comput. Commun., pp. 319–326, 2019.
[9] J. Wang, X. Wang, Y. Jiang, A. K. Singh, L. Huang and M. Yang, "Combating enhanced thermal covert channel in multi-/many-core systems with channel-aware jamming," in IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 11, pp. 3276-3287, 2020.
[10] H. Huang, X. Wang, Y. Jiang, A. K. Singh, M. Yang and L. Huang, "On countermeasures against the thermal covert channel attacks targeting many-core systems", accpted for publication in IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, 2021.
[11] S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou, "Designing and implementing malicious hardware," Proc. Usenix Workshop Large-Scale Exploits and Emergent Threats, pp. 1-8, 2008.
[12] Y. Xu, M. Bailey, F. Jahanian, K. Joshi, M. Hiltunen, and R. Schlichting, "An exploration of L2 cache covert channels in virtualized environments," in Proc. ACM Cloud Computing Security Workshop, pp. 29–40, 2011.
[13] S. Rusu, S. Tam, H. Muljono, J. Stinson, D. Ayers, J. Chang, R. Varada, M. Ratta, S. Kottapalli, and S. Vora, "A 45 nm 8-core enterprise Xeon processor," IEEE J. Solid-State Circuits, vol. 45, no. 1, pp. 7–14, 2010.
[14] X. Wang, B. Zhao, T. Mak, M. Yang, Y. Jiang, and M. Daneshtalab, "On fine-grained runtime power budgeting for networks-on-chip systems," IEEE Trans. Comput., vol. 65, no. 9, pp. 2780–2793, 2016.
[15] Z. Long, X. Wang, Y. Jiang, G. Cui, L. Zhang, T. Mak. "Improving the efficiency of thermal covert channels in multi-/many-core systems," in Proc. Design, Automation and Test in Europe Conf. and Exhibition, pp. 1459-1464, 2018.
[16] H. Lee and G. E. Sobelman, "FPGA-based FIR filters using digit-serial arithmetic," in Proc. IEEE Int'l Conf. ASIC Conf. and Exhibit, pp. 225–228, 1997.
[17] S. Pagani *et al.*, "TSP: thermal safe power: efficient power budgeting for many-core systems in dark silicon," in Proc. Int'l Conf. Hardware/Software Codesign and System Synthesis, pp. 10:1–10:10, 2014.
[18] J. Friedman, T. Hastie, and R. Tibshirani, The elements of statistical learning. Springer, 2001.
[19] R. E. Zeimer and W. H. Tranter, Principles of communications. Wiley, 1998.
[20] X. Wang, P. Liu, M. Yang, M. Palesi, Y.-T. Jiang, and M. C. Huang, "Energy efficient run-time incremental mapping for 3-D networks-onchip," J. Comput. Sci. Technol., vol. 28, no. 1, pp. 54–71, 2013.