Fan Speed Control Based Defence for Thermal Covert Channel Attacks in Multi-Core Systems*

Parisa Rahimi[1], Amit Kumar Singh[1], Xiaohang Wang[2]
[1] University of Essex, [2] South China University of Technology
[1] {pr19863, a.k.singh }@essex.ac.uk, [2]xiaohangwang@scut.edu.cn

***Abstract*—Multicore systems are vulnerable to thermal covert channel attacks as the increased power consumption may remain undetected, while occurring alongside normal, CPU-intensive applications. The purpose of this work is to study thermal effects on modern multi-core systems and decrease the possible risk of attacks. In this research, by controlling the fan speed, we have tried to decrease the temperature of the system to an appropriate level to fight these kinds of attacks. The results indicate that when the temperature decreases at a considerable level, lower power consumption is achieved.**

***Index Terms*—Multi-core systems, Thermal covert channel, temperature, power consumption, cooling, security**

I. Introduction

Multi-core systems are increasingly used for general purposes as well as embedded applications. Powerful CPUs and GPUs are used in multi-core/many-core systems to execute compute-intensive processes [1]. One of the by-products of these processed data is heating, which not only damages a physical system but also affects the system's performance. In general, active cooling system (using heat sinks only) and passive cooling systems (the fan's speed is either dynamically or statically controlled and paired with a heat sink) are used to prevent the systems and devices from overheating [2]. However, if the temperature threshold is exceeded, the processor's maximum frequency will be throttled to reduce the amount of heat generated, significantly lowering the processor's performance, and reducing the system's memory bandwidth [3]. Previous research has shown that uncontrolled heat management can affect power consumption as well as system performance and usability [4]. In multi-core systems where low power consumption and high performance are prime factors; excessive temperatures can dramatically undermine their availability [5]. Furthermore, existence of covert channels in multi-core systems can result in catastrophic data or information breach. In many communication systems, a thermal covert channel can be available to construct the covert channels. Thermal covert channels are remained the most widely used, and harmful [6]. In this work, we considered the potential security threat that can increase in multi-core systems, by using temperature measurements. In our experiment, we monitored the temperatures of the system, then by controlling the speed of the fans, tried to keep the temperature at an appropriate level to fight thermal covert channel of attacks. We found that thermal effects are more pronounced when operational power is higher and maximum CPU frequency is higher. Various cooling strategies have significant impacts on application performance and energy consumption. Excessively high temperatures and long-term changes will greatly affect the quality of service and the life of hardware.

II. Related Work

Several works addressed the topic of thermal and temperature side channels. For instance, Masti et al. [7] indicated that processors inside a multi-core system can exchange leaks or information through the temperature side channel. In this, they focused mostly on a methodology to calibrate and perform inter-processor communication using temperature as a covert channel. They even showed that isolated cores are vulnerable to such a covert channel. Bartolini et al. [8] used specific programs to heat the processor and encode information through the cooling fan behaviour; no fan activity represents a binary zero, while the opposite is a binary 1. They successfully demonstrate that the heat can be manipulated by an attacker and exploited externally by simply observing the system's behaviour, i.e., the cooling system, and achieved an even lower BER of 0.1% at 8 b/s. Long et al. [9] considered the influence of the noise generated by the other applications running on the system. They used a high signal frequency thermal covert channel to avoid noise. Hengli et al. [10] confirmed that by using Dynamic Voltage Frequency Scaling (DVFS) technique, the bit error rate of a TCC attack can soar to 92%. In our previous work, we showed that changing the pattern of the thermal signal can achieve high BER. In our proposed work, called Selective Noise Based Power-Efficient and Effective Countermeasure against Thermal Covert Channel Attacks in Multi-Core Systems, we tried to add extra selective noise (thread), to generate extra heat which results in, changing the pattern of the thermal signal. That experiment confirmed that the BER increased to 94% and the power consumption is 22.81277 (w) [11]. Despite all benefits, the previous approach has drawbacks. If the pattern of the main thermal signal is, e.g., 1 1 0 0 1 1 1 1 instead of 1 0 1 0 1 0 1, as Figure 1 shows, this strategy cannot work very well. Because, the proposed approach, which was mentioned, is based on both recording and monitoring the temperatures and then applying countermeasures. Thus, when the temperature of the current bit (e.g., 1 1 1) is higher than the previous bit (e.g., 1 1), the system cannot decide to apply the selective-noise countermeasure. Hence, the multi-core system will be at risk.

In this will discuss in this work and tried to address them.

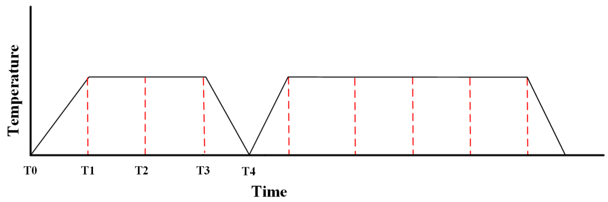

Fig. 1. Thermal signal with new pattern

III. METHODOLOGY

In this study, we have tried to propose a new methodology to address previous issues. In this technique, we have controlled the fan's speed by monitoring the behaviour of the system's temperature. As Figure 3. illustrates, the approach has different steps:

1) Step 1 (Set up the Fan speed): In this step, the fan's speed is set up at the appropriate level (1,200 RPM) when the bit is "1".

2) Step 2 (Record temperature): This step is monitoring and recording temperature after setting up the fan's speed. Then the current temperature is recorded and used for the next step.

3) Step 3 (Temperature monitoring of processors and adopting an appropriate level for fan speed): In this step, the next bit's temperature is compared with the recorded temperature (TR) from the previous step. If the temperature of the current (Tc) bit is greater than TR, the speed of the fan begins to increase to 2,000 RPM. For considering this speed, first we monitored the behaviour of the fan by *S-tui* which is a free and open-source terminal UI for monitoring a system. *S-tui* allows monitoring processors temperature, frequency, power, and utilization in a graphical way from the terminal. It is written in Python and need root permission to use the *S-tui* (Figure 2.). Furthermore, when we should consider the power consumption of fan, which may affect the total energy consumption. Therefore, in this rang of fan speed the power of the fan is 3.6 (w) [1].

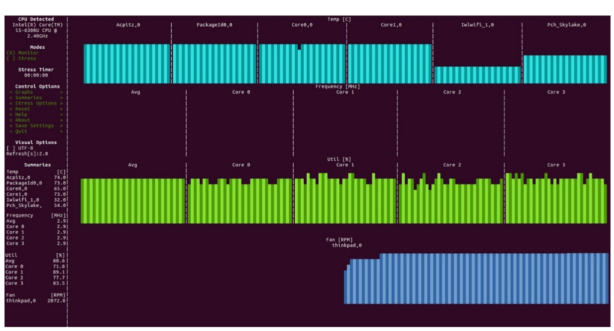

Fig. 2. Monitoring system behaviour

Otherwise, if the Tc is less than TR the speed of the fan decreases to 1,000 RPM. If the Tc is equal to TR the process will come back to the recording temperature step. This progress continues until the end of the transmission process.

Here, we adopt different countermeasure strategies along with different temperature rang that take into account both security requirements and power consumption. In this approach, to avoid rising power consumption due to the speed

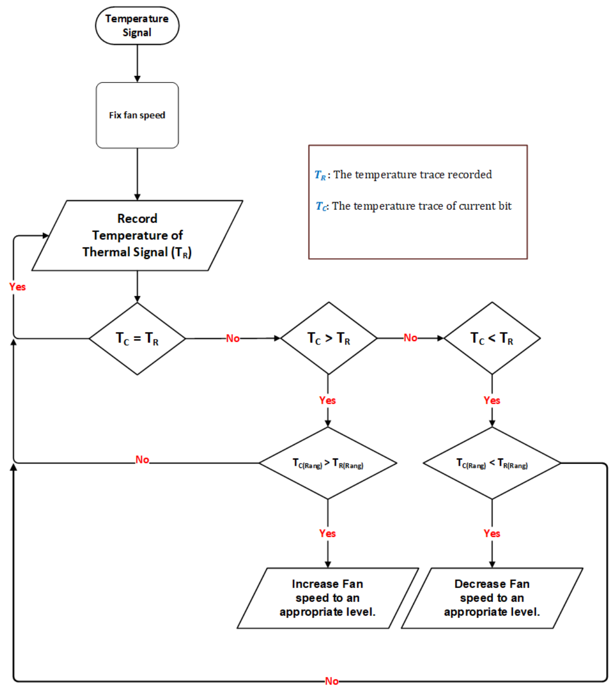

Fig. 3. The process of proposed work

TABLE I
DIFFERENT STATUES OF FAN SPEED (5°C)

Range of Temperature (°C)	*Fan's Speed (RPM)*
$Tc < 65$	1000
$65 < Tc < 70$	1500
$70 < Tc < 75$	2000
$75 < Tc < 80$	2500
$Tc > 80$	Max

of the fan, we consider different levels for different ranges of temperatures (Table1).

We have also considered more range temperature (e.g. table 2) for controlling fan speed to check the behaviour of the system, however, as table 3 indicates, it results in decreasing the temperature, but average power consumption will increase because the fan needs to work more which affects energy consumption.

TABLE II
DIFFERENT STATUES OF FAN SPEED (5°C)

Range of Temperature (°C)	*Fan's Speed (RPM)*
$Tc < 65$	1000
$65 < Tc < 67$	1300
$67 < Tc < 69$	1500
$69 < Tc < 71$	1700
$71 < Tc < 73$	1900
$73 < Tc < 75$	2100
$75 < Tc < 77$	2300
$77 < Tc < 79$	2500
$79 < Tc < 81$	2700
$Tc > 81$	Max

IV. EXPERIMENTAL RESULT

All experiments are performed using a multi-core simulator, Sniper-v7.2 [12] as a multi-core simulator that is quick and dependable. As the power model, McPAT-v1.0 is included. McPAT is a multithreaded and many-core/multi-core architecture power, area, and timing modelling framework [13]. This analysis was performed in order to prevent a covert thermal channel attack on our targeted device. Thermal covert channel programmes require generating and measuring temperature signals using the HotSpot simulator in order to covertly transmit sensitive information from a secured zone to a non-secured one. To generate temperatures dynamically for all the cores, we used the Hotspot-v6.0 thermal model. We use a few PARSEC and SPLASH-2 benchmarks, and their temperature signals are treated as thermal noise to a thermal covert channel. Sniper and Hotspot are used in the experimental setup. There are different works have been done to fight TCC attacks. Figure 4 shows different outcomes of different experiments. As Figure 4(e) indicates, when the controlling fan speed is implemented into the system, the temperature of the thermal signal decrease significantly which results in avoiding low power consumption. Furthermore, the bit error rate increases as well, which means that the potential attacks can happen to the system hardly.

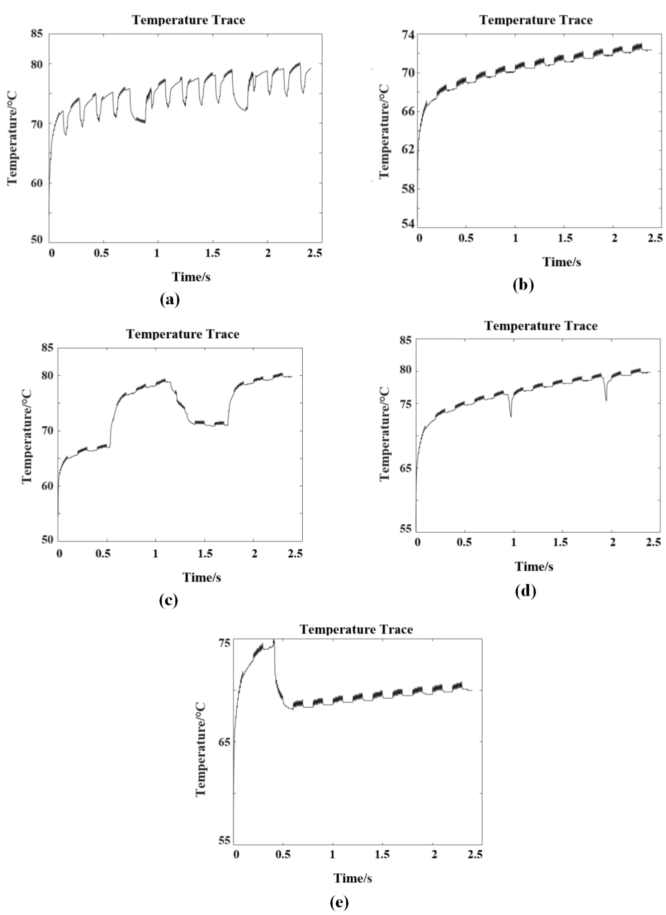

Fig. 4. Different research outcomes: (a) Thermal signal without countermeasure, (b) Thermal signal with DVFS countermeasure, (c) Thermal signal with One Extra Noise countermeasure, (d) Thermal signal with Selective Noise countermeasure, and (e) Thermal signal with controlling Fan Speed countermeasure

Figure 4 illustrates the temperature of the system with different methodologies. As this graph shows, by this new technique, we are able to decrease the temperature of the system as well as protect it from any potential attracts, which results in a decrease in the power consumption. Table 3 illustrates the experimental results of the different research. AS the table shows, the average BER of the thermal covert channel attacks across 8×8 systems can be higher than 95%.

A. Combination Methodologies

In this section we try to combine different mythologies in regard to TCC attack to achieve best result (Low temperature, low power consumption as well as high bit error rate).

1) TCC with DVFS and Fan speed controlling countermeasure: As figure 5 shows, when we add fan speed along with DVFS the temperature decreases which is result in decrease power consumption. Furthermore, as Table 3 indicates, a combination of two methodology (DVFS and Fan Speed) can improve BER.

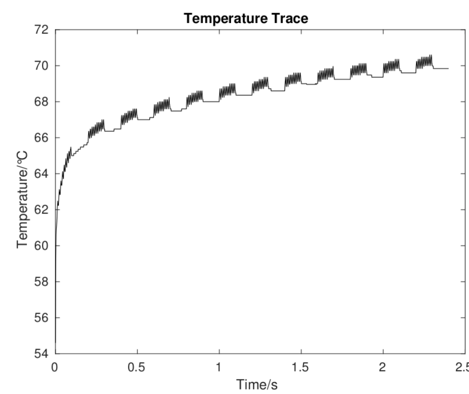

Fig. 5. DVFS countermeasure along with fan speed countermeasure

2) TCC with Selective Noise and Fan speed controlling countermeasure: Figure 6 illustrates that when the fan speed countermeasure is implemented with selective noise, the BER rise to 97%, and the average power consumption decrease which result from the reduction of average temperature

3) TCC with DVFS, Selective Noise and Fan speed controlling countermeasure: As Figure 7 and table 3 illustrate, when all countermeasures are applied to the system, we can achieve the best result by considering BER, average power consumption and temperature (Table 3).

As Table 3 shows, one can see that the average BER's of our new proposed countermeasure are higher than that of the other countermeasure. We also determined that the average power consumption decreased in this study. For this result, we consider very 5 °C, this is mainly because if we change the speed fan in a very short time (e.g. 1 °C) the BER does not show any changes, but the power consumption of the system increases, resulting from the power consumption of the fan. Furthermore, if we consider the large duration for controlling the fan, the system will be at risk.

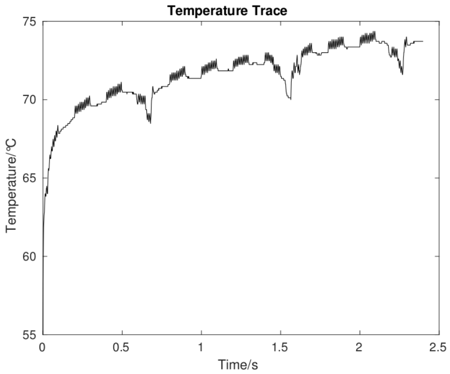

Fig. 6. TCC with Selective Noise and fan speed countermeasure.

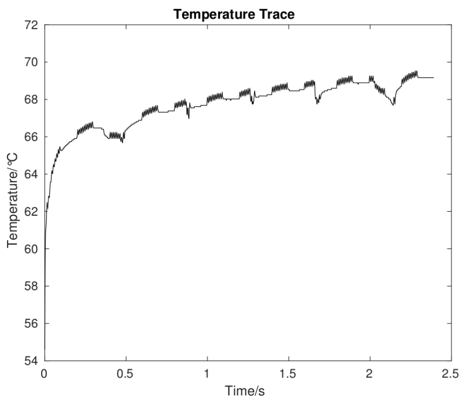

Fig. 7. TCC with Selective Noise and fan speed countermeasure.

V. CONCLUSION

Our experimental results have confirmed that the new proposed countermeasure could be practically against TCC attacks with a high BER of 95% with its low temperature and low power consumption. The proposed countermeasure is a suitable scheme that can be used by multi-core systems to fight against these kinds of attacks. This study shows that thermal attacks are inevitable, however, an appropriate countermeasure should be designed to fight attacks by considering other aspects of the system such as power consumption as an essential metric in multi-core systems. Furthermore, by combining the proposed methodology with existing work (DVFS technique) and our previous experiment (selective noise countermeasure), we can achieve the best results (Low power, low temperature, and high BER).

TABLE III
EXPERIMENTAL RESULTS

Countermeasures	***BER***	***Avg Temperature (°C)***	***Avg Power Consumption(w)***
TCC with DVFS	92%	70.35	22.31
TCC with One Extra Noise	94%	75.875	23.74
TCC with Selective Noise	94%	74.66	22.81
TCC with Controlling Fan Speed (Range of temperature 5°C)	95%	68.50	20.09
TCC with Controlling Fan Speed (Range of temperature 4°C)	95%	68.39	20.29
TCC with Controlling Fan Speed (Range of temperature 3°C)	95%	68.30	20.51
TCC with Controlling Fan Speed (Range of temperature 2°C)	95%	68.25	20.79
TCC with Controlling Fan Speed (Range of temperature 1°C)	95%	67.98	21.159
TCC with DVFS and Fan Speed	95%	67.56	19.65
TCC with Selective Noise and Fan Speed	97%	70.11	21.43
TCC with DVFS, Selective Noise and Fan Speed	98%	65.95	18.82

REFERENCES

[1] Rahimi, P, et al. Trends and Challenges in Ensuring Security for Low-Power and High-Performance Embedded SoCs.*14th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC)* **2021**.

[2] Duchatellier, J., et al. An empirical study of thermal attacks on edge platforms. *ACM Southeast Conference.* **2021**

[3] Aljuffri, A., et al. Applying Thermal Side-Channel Attacks on Asymmetric Cryptography. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems.* **2021**

[4] Shao, Z., et al. 2021, Heat Behind the Meter: A Hidden Threat of Thermal Attacks in Edge Colocation Data Centers. *International Symposium on High-Performance Computer Architecture (HPCA).* **2021**

[5] Tian, S., and Szefer, J. Temporal thermal covert channels in cloud FPGAs. *ACM/SIGDA International Symposium on Field-Programmable Gate Arrays.* **2019**

[6] Wang, J., et al. 2Combating Enhanced Thermal Covert Channel in Multi-/Many-Core Systems With Channel-Aware Jamming. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.* **2020**

[7] Masti, R. et al. Thermal covert channels on multi-core platforms. *In 24th USENIX security symposium.* **2015**

[8] Bartolini, D. B., et al. On the capacity of thermal covert channels in multi-cores. *Eleventh European Conference on Computer Systems.* **2016**

[9] Long, Z, et al. March. Improving the efficiency of thermal covert channels in multi-/many-core systems. *Design, Automation Test in Europe Conference Exhibition.* **2018**

[10] Huang, H, et al. Detection of and Countermeasure against Thermal Covert Channel in Many-core Systems. em IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. **2021**

[11] Rahimi, P., et al. Selective Noise Based Power-Efficient and Effective Countermeasure against Thermal Covert Channel Attacks in Multi-Core Systems. *Journal of Low Power Electronics and Applications, MDPI.* bf 2022

[12] Chi¸s, R., et al. Multi-objective optimization for an enhanced multi-core SNIPER simulator. *Proc. Rom. Acad.-Ser.* **2018**

[13] Aljuffri, A., et al. Applying Thermal Side-Channel Attacks on Asymmetric Cryptography. IEEE Transactions on VLSI Systems. **2009**