Comparative Performance Evaluation of Thermal Covert Channel Attacks on Multi-Core Systems

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

***Abstract*—Thermal covert channel (TCC) attacks have been a serious security concern to the use of many-core chips. Severity of these attacks is directly linked to the TCC's transmission rate and its BER (bit error rate) performance, both of which are impacted by the transmission characteristics of thermal signals and adopted encoding, modulation, and multiplexing schemes. This paper examines, compares, and analyzes various TCCs built upon different combinations of encoding, modulation, and multiplexing. In particular, our study shows that TCC using non-return-to-zero (NRZ) line coding and frequency shift keying (FSK) modulation achieves the highest throughput of 120 bps and BER of below 10%.**

I. Introduction

A TCC [1]–[4] can be built by combining various modulation, encoding, and signal multiplexing methods. Until now, there is no study to evaluate as all the different TCC designs under a unified framework. Note that the power budget and signal bandwidth of a real machine's TCC can be limited. These physical constraints have implications on the TCC modulation and encoding, and subsequently, on the TCC's BER, transmission rate, anti-jamming ability, and bandwidth. Thermal signal in TCC is drastically different from wireless signals as follows, (1) the signal amplitude and transmission frequency are coupled, (2) the thermal signal bandwidth is very limited, and it varies at relatively low speed, (3) the initial temperature of signal impacts on the symbol length, (4) thermal noise concentrates on low- frequency domain. Therefore, the line coding and modulation methods must be carefully redesigned to fit for thermal signals. This study is placed on addressing the following relevant aspects:

(1) We redesign the encodings and modulations and attempt to examine various TCC designs involving different design combinations of modulation and encoding schemes.

(2) Through extensive computer simulations and evaluations on a real machine, we determine the design combination of encoding, modulation, and signal multiplexing that achieves the low BER and the high transmission throughput. Having the knowledge of TCC's maximum transmission throughput is critical to the TCC detection and development of adequate countermeasures against TCC attacks.

The rest of this paper is organized as follows. The impacts of the components on TCC performance are studied in Section IV. The conclusions are finally drawn in Section V.

II. Line Coding Methods

In order to transmit data through the thermal covert channel, data must be encoded first. The purpose of line coding is to increase the reliability of data transmission in TCC. The encoded signal is a base-band signal with its energy concentrating in the spectrum typically below a few hundred Hz.

The non-return-to-zero (NRZ) code uses a continuous high temperature to represent the bit '1' and a continuous low temperature to represent the bit '0'.

For return-to-zero (RZ) code, to encode a bit '1' that has a duration of T_B (symbol length), the CPU is heated up for a duration of γ, followed by a cooling down phase lasting $T_B - \gamma$. CPU is cooled down for a duration of T_B to encode bit '0'. The heating time γ is calculated by equations.

In Manchester coding, thermal transitions, instead of thermal levels, are used to represent ones and zeros. Specially, the CPU is heated up for a duration of $T_B/2$, followed by a cooling down phase lasting $T_B/2$ to encode a bit '0'. CPU is cooled down for $T_B/2$, followed by a heating up phase for $T_B/2$ to encode bit '1'.

III. Modulation Methods

Modulation loads the information of the source signal to the carrier, which changes the frequency spectrum of the signal to a range suitable for channel transmission. This section introduces the modulation methods for band-pass transmission in TCC.

This work was supported in part by the National Natural Science Foundation of China under Grant 61971200, in part by Zhejiang Lab under Grants 2021LE0AB01 and 2021PC0AC01, in part by Major Scientific Research Project of Zhejiang Lab under Grant 2021LE0AC01, in part by the Open Research Grant of State Key Laboratory of Computer Architecture Institute of Computing Technology, Chinese Academy of Sciences under Grant CARCH201916, in part by the Key Technologies R&D Program of Jiangsu (Prospective and Key Technologies for Industry) under Grant BE2021003, in part by the Key Laboratory of Big Data and Intelligent Robot (South China University of Technology), Ministry of Education, and in part by the National Key Research and Development Program of China under Grant 2019QY0705.

J. Wang is with the School of Software Engineering, South China University of Technology, Guangzhou, Guangdong, 510006, China. E-mail: jiachenwang3@gmail.com.

X. Wang is with the School of Software Engineering, South China University of Technology, and also with Zhejiang Lab and State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences. Xiaohang 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, NV89557. E-mail: ying tao.jiang@unlv.edu, mei.yang@unlv.edu.

A. K. Singh is with the University of Essex, UK. E-mail: a.k.singh@essex.ac.uk

L. Huang is with the University of Electronic Science and Technology of China, China. E-mail: huanglt@uestc.edu.cn

TABLE I
Transmission schemes for evaluation

Scheme	Line coding	Modulation	Base-band/band-pass
1	NRZ code	/	base-band
2	Manchester code	/	base-band
3	NRZ code	ASK	band-pass
4	NRZ code	FSK	band-pass
5	NRZ code	FSK	band-pass
6	NRZ code	PWM	band-pass
7	Manchester code	ASK	band-pass
8	Manchester code	FSK	band-pass
9	RZ code	/	base-band
10	Differential code	/	base-band
11	NRZ code	ASK	band-pass
12	NRZ code	FSK	band-pass
13	NRZ code	PWM	band-pass

TABLE II
The configuration of the real machine

Processor	Intel i7-8700k @3.2GHz
Memory	8 Gbytes
DRAM frequency	2400MHz
Physical cores	6
Logical cores	12
Fan speed	2400rpm
Operate system	Ubuntu 16.04.5 LTS
High performance mode	ON
Dynamic fan speed	OFF

Amplitude shift keying (ASK) uses amplitude of the carrier to encode digital information. In 2ASK, the carrier amplitude variation has only two states to represent bits ‘0’ and ‘1’.

Frequency shift keying (FSK) is a frequency modulation method that uses discrete carrier frequency changes to transmit digital information.

As a digital representation of an analog signal that takes samples of the amplitude of the analog signal at regular intervals, pulse modulation has found its use in TCC. Essentially, the Pulse Width Modulation (PWM) modulates an intermediate ASK signal into a pulse wave.

IV. Performance Evaluation of TCCs with Different Configurations

TCCs can be built using different combinations of encoding and modulation schemes. In this section, we investigate different TCC designs in terms of BER and transmission rates. Table I lists all 13 transmission schemes in TCCs. The difference between scheme 4 and scheme 5 is that scheme 4 transmits consecutive bits of ‘0’ before transmitting the data packet to increase the CPU temperature. Schemes 11 and 12 use the heating times γ and ϑ calculated by equations. Schemes 3, 4 and 5 use half of the period of carrier as the heating time. Scheme 13 is an frequency division multiplexing (FDM) scheme implemented by PWM.

To demonstrate the applicability on a real machine, the experiments were performed on a desktop computer with an Intel i7-8700 CPU running at 3.2 GHz and the operating system is Ubuntu 16.04.5 LTS. The complete system configurations are summarized in Table II.

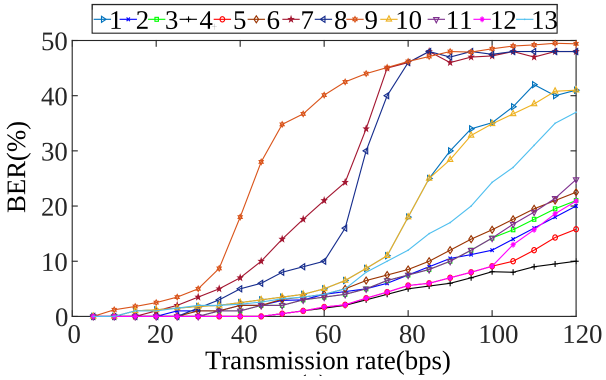

Fig. 1. The BER of different schemes (1-13) with respect to the transmission rate on the real machine.

A. BER and Transmission Rates of Different Transmission Schemes

Fig. 1 shows the BERs of different schemes with respect to the transmission rates. It can be seen from Fig. 1 that the BER of FSK is always lower than that of any other schemes. The reason is that the variation of the initial temperature of signal in FSK is lower, and thus the variation of the signal length is lower and there is a smaller amount of inter-symbol interference, which is translated to lower BER. For other schemes, the variation of the initial temperature of signal is high, and there is a higher amount of the inter-symbol interference, which gives high BER.

V. Conclusion

In this paper, we showed the versatility of TCCs employing different modulation methods, line coding methods, and multiplexing methods. We subsequently compared the performance of 13 different TCCs in terms of BER and transmission rate. The experimental results showed that the band-pass transmission system using the FSK modulation gives the best performance with a transmission rate of 120 bps at the BER level of lower than 10%. Understanding various TCC designs’ maximum transmission throughput can help assess potential damages quantitatively and guide the development of adequate countermeasures against the TCC attacks.

References

[1] R. J. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, and S. Capkun, “Thermal covert channels on multi-core platforms,” in *Proc. Usenix Conf. Security Symp.*, 2015, pp. 865–880.

[2] D. B. Bartolini, P. Miedl, and L. Thiele, “On the capacity of thermal covert channels in multicores,” in *Proc. Eur. Conf. Comput. Syst.*, 2016, p. 24.

[3] Z. Long, X. Wang, Y. Jiang, G. Cui, L. Zhang, and T. Mak, “Improving the efficiency of thermal covert channels in multi-/many-core systems,” in *Proc. Design Autom. Test Eur. Conf. Exhibit.*, 2018, pp. 1459–1464.

[4] 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,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 11, pp. 3276–3287, 2020.

[5] H. Huang, X. Wang, Y. Jiang, A. K. Singh, M. Yang, and L. Huang, “Detection of and countermeasure against thermal covert channel in many-core systems,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 2, pp. 252–265, 2022.