Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

Enhancing Security in On-Chip Communication: A Survey of Threats and Solutions

Thinzar Aung Win

Information Technology Dept., Stamford International University, Thailand

E-mail: thinzaraung.win@stamford.edu

Abstract

As the complexity of integrated circuits (ICs) continues to increase, ensuring the security of on-chip communication becomes paramount. With the rise of interconnected devices and the Internet of Things (IoT), vulnerabilities in on-chip communication pose significant risks to data integrity, privacy, and system reliability. This article presents a comprehensive survey of the threats and solutions associated with enhancing security in on-chip communication. The survey begins with an overview of on-chip communication and its critical role in modern ICs. It then explores the diverse range of security threats faced by on-chip communication systems, including side-channel attacks, information leakage, unauthorized access, and the insertion of hardware Trojans. Each threat is examined in detail, highlighting its characteristics and potential impact on system security.

In response to these threats, the survey examines various solutions and countermeasures aimed at enhancing on-chip communication security. These include encryption and authentication techniques, secure routing protocols, hardware-based security mechanisms, and software-based security solutions. Examples of real-world security breaches and successful implementations of security solutions are also presented to provide practical insights.

Keywords: Security Threats, Security Solutions, Side-Channel Attacks, Information Leakage, Unauthorized Access, Hardware Trojans.

DOI: https://doi.org/10.36548/jismac.2024.3.004
Received: 05.06.2024, received in revised form: 01.07.2024, accepted: 13.07.2024, published: 22.07.2024

1. Introduction

Within the domain of integrated circuits (ICs), on-chip communication serves as a vital route for the seamless exchange of data among various components residing on a single silicon die. From microprocessors and memory units to input-output devices and specialized accelerators, on-chip communication plays a crucial role in facilitating efficient and reliable operation of complex electronic systems. Fundamentally, on-chip communication involves the transmission of digital signals and information between different functional blocks or modules within an IC. These functional blocks may include processing cores, memory banks, interconnect fabrics, and peripheral interfaces, each fulfilling specific computational or data storage tasks. The efficiency and effectiveness of on-chip communication directly impact the overall performance, power consumption, and scalability of IC designs, making it a focal point of research and development in the semiconductor industry [1-3].

The evolution of on-chip communication has closely mirrored the progression of Moore's Law, which has witnessed transistor densities doubling approximately every two years, leading to increasingly intricate and interconnected IC designs. As the number of transistors per chip continues to rise, the demand for robust and scalable communication infrastructures becomes ever more critical. Furthermore, emerging applications such as artificial intelligence, autonomous vehicles, and Internet of Things (IoT) devices impose additional demands on on-chip communication, necessitating low-latency, high-bandwidth, and energy-efficient solutions to accommodate diverse workloads and data traffic patterns. In this context, the design and optimization of on-chip communication architectures pose formidable challenges and opportunities for researchers and engineers. Factors such as signal integrity, timing constraints, power consumption, and reliability considerations must be carefully balanced to achieve optimal performance and meet stringent design specifications. Additionally, the proliferation of security threats, ranging from side-channel attacks and information leakage to hardware Trojans and unauthorized access, adds an extra layer of complexity to the design and implementation of secure on-chip communication systems[4,5].

Despite these challenges, recent advancements in on-chip communication technologies have propelled innovations in interconnect topologies, routing algorithms, error correction mechanisms, and security protocols. By leveraging advances in semiconductor manufacturing processes, heterogeneous integration, and system-level co-design methodologies, researchers

continue to push the boundaries of on-chip communication, unlocking new possibilities for future generations of computing systems [6-8].

In this article, we undertake a comprehensive exploration of on-chip communication, examining its fundamental principles, emerging trends, and key challenges. Through a multidisciplinary lens encompassing electrical engineering, computer architecture, and cybersecurity, we aim to provide readers with a thorough understanding of the critical role that on-chip communication plays in shaping the future of computing. By analyzing the latest research findings, industry developments, and real-world applications, we seek to illuminate the path forward for advancing the state-of-the-art in on-chip communication and addressing the pressing challenges that lie ahead[9-12].

2. Related Study

The discovery and characterization of risks to the security of on-chip communication have been the subject of numerous recent studies. Guo et al.'s work [1] identified and addressed two main security threats in NoC-based systems: Denial-of-Service (DoS) attacks and unauthorized secret information extraction. They implemented an anomalous high-packet injection rate detector and a node-blocking mechanism to detect and recover from DoS attacks. Additionally, they introduced the Secure Packet ExchAngeR (SPEAR) system to enable secure communication between NoC nodes and prevent unauthorized access to in-flight data.

Sudeep Pasricha et al. [2] provided a comprehensive overview of on-chip communication architectures and highlighted the importance of addressing security issues in NoC design. They discussed verification and security challenges in on-chip communication architecture design.

Lukovic et al. [3] proposed a solution to secure attached processing units from buffer overflow attacks by enhancing NoC components. They implemented a hardware-assisted security module to protect against such attacks.

Ahmed Saeed et al. [4] presented a secure communication architecture for reconfigurable multi-core systems using NoCs. They designed an Identity and Address Verification (IAV) security module embedded in each NoC router to verify the identity and address range of incoming and outgoing packets. The IAV module was evaluated in terms of

area, power consumption, and performance overhead on FPGA-based systems. The field of on-chip communication security is significantly shaped by legislative and compliance frameworks as well as technological developments. The effects of legislative requirements like GDPR and HIPAA on security specifications for on-chip communication networks have been the subject of recent research. In order to ensure the comprehensive security of embedded systems and reduce the legal risks connected with data breaches and privacy violations, it is imperative that these compliance considerations are understood and addressed.

There are still a number of unanswered questions and untapped research opportunities in the subject of on-chip communication security, despite notable advancements. The creation of reliable intrusion detection systems suited for on-chip communication networks, the incorporation of machine learning methods for anomaly detection and threat mitigation, and the investigation of lightweight cryptographic primitives ideal for embedded systems with limited resources are important areas that require additional research.

3. Threats to On-Chip Communication Security

Threats to on-chip communication security refer to various vulnerabilities and attacks targeting the data exchange pathways within integrated circuits (ICs). As ICs become more complex and interconnected, ensuring the security of on-chip communication becomes critical.

a. Eavesdropping

Eavesdropping, as shown in Figure 1, is a passive attack where adversaries monitor communication channels within the chip to intercept sensitive data being transmitted between components. This can include snooping on bus lines, memory accesses, or interconnects to capture data packets or messages. The unauthorized disclosure of confidential information can lead to privacy breaches, intellectual property theft, or the compromise of cryptographic keys and credentials. To mitigate this threat, encryption techniques such as symmetric or asymmetric cryptography can be employed to protect data confidentiality. Additionally, secure communication protocols like Secure Socket Layer (SSL) or Transport Layer Security (TLS) can safeguard data in transit.

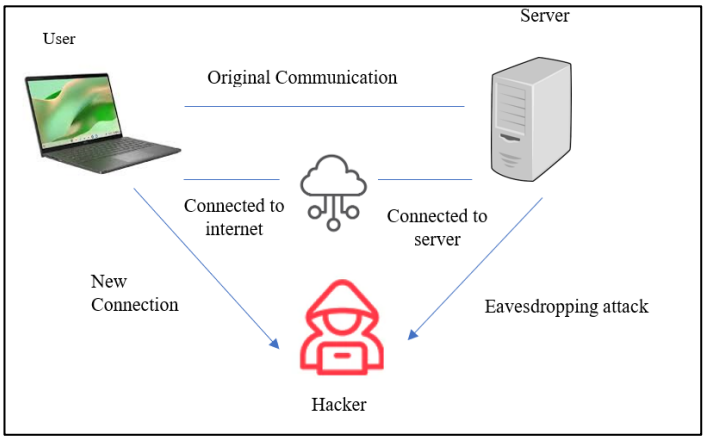

Figure 1. Eavesdropping Attack

b. Data Manipulation

Data manipulation attacks involve adversaries tampering with data being transmitted on the on-chip communication network, altering its content to compromise integrity or validity. This can include modifying control signals, data payloads, or memory contents. Data manipulation can result in data corruption, unauthorized access, or the execution of malicious commands, leading to system malfunction, unauthorized privilege escalation, or the injection of malware. Message authentication codes (MACs), digital signatures, and hash functions can be used to ensure data integrity and detect unauthorized modifications. Secure boot mechanisms and code signing can also prevent the execution of tampered firmware or software components.

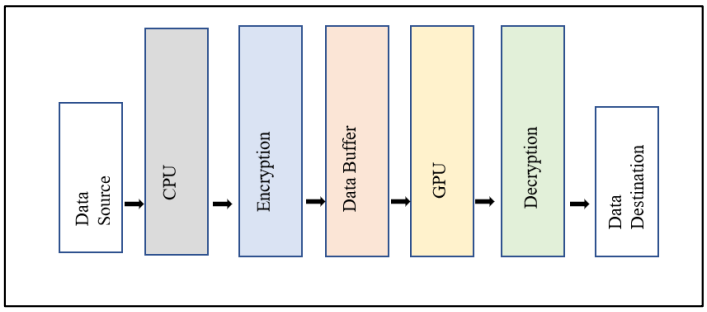

Figure 2. Data Manipulation

Figure 2. shows the conceptual model of a data flow diagram showing data being manipulated and secured as it travels across different components on a chip.

c. Denial of Service (DoS)

DoS attacks aim to disrupt the normal operation of the on-chip communication network by flooding it with excessive traffic, malicious requests, or resource-intensive operations. This can overwhelm the network infrastructure, causing service degradation or system downtime. DoS attacks can impair the availability and reliability of the chip, leading to performance degradation, loss of functionality, or the exhaustion of critical resources such as bandwidth, buffers, or processing capacity. Mitigation strategies include rate limiting, traffic shaping, and congestion control mechanisms to regulate the flow of data and prioritize critical traffic. Additionally, intrusion detection systems (IDS) and firewalls can identify and block malicious traffic to prevent DoS attacks. Figure 3 visualizes the overload caused in network traffic.

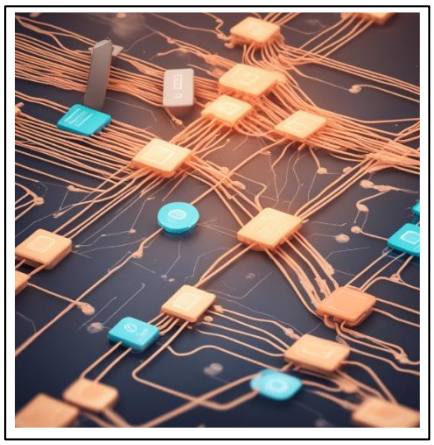

Figure 3. Network Traffic Overload

d. Injection Attacks

Injection attacks involve adversaries injecting malicious payloads or commands into the on-chip communication network to exploit vulnerabilities in the system. This can include injecting malware, command injection, or buffer overflow attacks. Injection attacks can compromise the security or functionality of the chip, leading to unauthorized access, privilege escalation, or the execution of arbitrary code. Input validation, parameterized queries, and code signing can prevent injection attacks by validating user inputs and data, and ensuring the integrity of executable code. Secure coding practices and runtime defenses such as Address Space Layout Randomization (ASLR) can mitigate the impact of injection attacks.

e. Man-in-the-Middle (MitM) Attacks

MitM attacks occur when an attacker intercepts and alters communication between two parties without their knowledge. This can involve passive interception, active manipulation, or relay attacks to compromise the confidentiality and integrity of data. MitM attacks can lead to data interception, modification, or impersonation, allowing attackers to eavesdrop on sensitive information, tamper with communication, or masquerade as legitimate entities. Encryption, mutual authentication, and digital certificates can mitigate the risk of MitM attacks by ensuring the confidentiality, integrity, and authenticity of communication channels. Secure key exchange protocols such as Diffie-Hellman key exchange can also prevent eavesdropping and tampering.

4. Techniques for Enhancing On-Chip Communication Security

Table 1. Techniques for Enhancing On-Chip Communication Security

Technique	Description	Specific Methods
Encryption	Protects data during transmission from unauthorized access	Symmetric Encryption (e.g., AES) Asymmetric Encryption (e.g., RSA)
Authentication and Authorization	Ensures legitimate components can communicate and perform actions	Message Authentication Codes (MACs) Public Key Infrastructure (PKI)
Secure Protocols	Implements secure communication channels	Transport Layer Security (TLS) Secure Packet Management (SPM)
Physical Security	Protects the chip from physical tampering and side-channel attacks	Shielding Sensor Integration
Fault Tolerance and Error Correction	Detects and corrects errors in data transmission	Error-Correcting Code (ECC)

		Redundancy
Access Control	Limits access to sensitive areas and data paths	Firewalls Secure Boot
Intrusion Detection Systems (IDS)	Monitors communication channels for malicious activity	Anomaly Detection Signature-Based Detection
Design for Security	Incorporates security into the chip design process	Secure Architecture Formal Verification
Randomization	Obscures communication patterns to prevent prediction and exploitation	Randomized Memory Access Dynamic Key Generation
Side-Channel Attack Countermeasures	Reduces the risk of information leakage through side-channels	Noise Injection Constant-Time Algorithms

Table 1. provides a concise overview of the various techniques and methods used to enhance on-chip communication security.

5. Real-world Examples

5.1 Security Breaches in on-chip Communication

Table 2. Comparing Different Examples of Security Breaches

Security Breach	Description	Mechanism	Impact	Solutions
Meltdown and Spectre (2018)	Vulnerabilities in speculative	Side-channel attacks exploiting	Leaked sensitive	Patches and updates,

	execution affecting CPUs	speculative execution	information like passwords and keys	performance penalties
Rowhammer (2014)	Vulnerability in DRAM causing bit flips in adjacent rows	Electromagnetic interference from rapidly accessing memory	Privilege escalation, arbitrary code execution	Error correcting code (ECC) memory, increased refresh rates
Heartbleed (2014)	Flaw in OpenSSL's Heartbeat extension	Exploiting Heartbeat extension to read server memory	Compromised private keys and sensitive user data	Updates to OpenSSL, widespread patching of affected systems
Intel Management Engine (2017)	Vulnerabilities in Intel ME allowing remote code execution	Exploiting firmware flaws in the Intel ME	Full system control, bypassing OS-level security	Firmware updates, security advisories
Bluetooth Vulnerabilities (2018)	Flaws in Bluetooth firmware and stack implementations	Exploiting vulnerabilities for code execution or DoS attacks	Compromised millions of Bluetooth-enabled devices	Firmware updates, patches from manufacturers
Glitching Attacks on HSMs (2010)	Fault injection attacks on hardware security modules	Inducing faults via power glitches or electromagnetic interference	Extracted cryptographic keys, compromised data integrity	Enhanced hardware design, better fault detection and mitigation

Table 2. provides a concise comparison of various security breaches, their mechanisms, impacts, and the solutions implemented to address them.

5.2 Successful Implementation of Security Solutions in Industry or Research Projects

Table 3. Security Solutions in Industry

Project/Technology	Description	Implementation	Impact
Intel CET (Control-flow Enforcement Technology)	Mitigates control-flow attacks like ROP and JOP	Includes Shadow Stack and Indirect Branch Tracking	Enhanced security of Intel processors against sophisticated exploits
Google Titan Security Key	Hardware-based two-factor authentication device	Uses secure elements and cryptographic algorithms	Significantly reduced account takeover incidents
ARM TrustZone	Security extension for ARM processors creating secure execution environments	Divides system into secure and non-secure worlds, isolating sensitive operations	Enhanced security for a wide range of devices, protecting critical assets
Apple Secure Enclave	Dedicated security coprocessor for sensitive data	Isolates cryptographic keys and operations from the main processor	Improved protection of user data on iOS devices, ensuring privacy and security
Microsoft Pluton Security Processor	Security processor integrated into CPUs for secure boot and identity protection	Provides hardware root of trust, secures firmware and cryptographic keys	Strengthened device security, protecting against firmware attacks and unauthorized access
DARPA SSITH (System Security Integration Through Hardware and Firmware)	Research project to develop secure hardware architectures	Focuses on eliminating classes of hardware vulnerabilities	Advancements in hardware security, influencing future secure chip designs

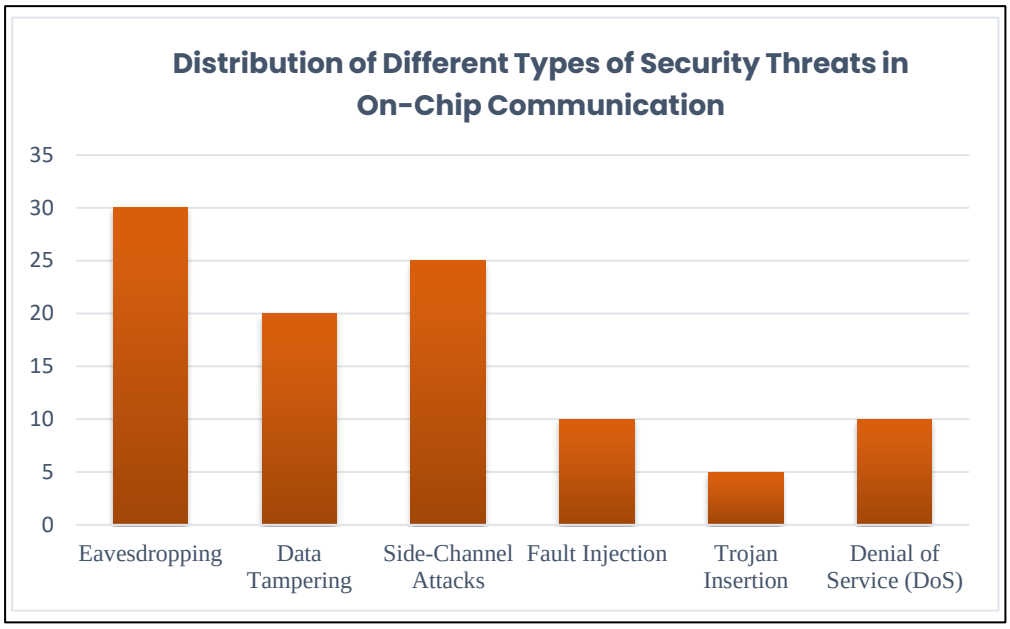

Figure 4. Different Types of Security Threats in On-Chip Communication

Figure 4. shows the frequency or distribution of different types of security threats in on-chip communication and Table 3 illustrates the security solutions that used in industry

6. Solutions and Countermeasures

Enhancing security in on-chip communication requires a comprehensive set of solutions and countermeasures addressing various threats. Key strategies include detecting and preventing hardware Trojans through design-time verification and runtime monitoring, and mitigating side-channel attacks with noise injection, constant-time operations, and physical shielding. Denial-of-service (DoS) attacks can be countered using traffic regulation, quality of service (QoS) protocols, and adaptive routing. Information leakage is prevented through strong encryption, secure communication protocols, and data obfuscation. Additional measures such as anomaly detection, hardware-based security modules, error correction codes (ECC), and redundant communication paths ensure continuous monitoring and fault tolerance. Implementing strict access control policies, multi-factor authentication (MFA), secure boot mechanisms, and security-aware design tools further fortify the overall security framework, providing a robust defense against emerging threats in on-chip communication.

7. Conclusion

The increasing complexity and integration of modern system-on-chip (SoC) architectures necessitate robust security measures to safeguard on-chip communication. This survey has highlighted the diverse range of threats, including hardware Trojans, side-channel attacks, denial-of-service (DoS) attacks, and information leakage, each posing significant risks to the integrity, confidentiality, and availability of data within SoCs. To counter these threats, a multifaceted approach encompassing both hardware and software solutions is essential. Techniques such as design-time verification, runtime monitoring, and split manufacturing are critical in detecting and preventing hardware Trojans. Mitigating side-channel attacks requires a combination of noise injection, constant-time operations, and physical shielding. Preventing DoS attacks involves traffic regulation, quality of service (QoS) protocols, and adaptive routing algorithms to ensure network resilience.

Information leakage can be effectively combated with strong encryption, secure communication protocols, and data obfuscation. Intrusion detection systems, anomaly detection, and hardware-based security modules provide continuous monitoring and quick response to potential intrusions. Additionally, redundancy and fault tolerance mechanisms, such as error correction codes (ECC) and redundant communication paths, enhance the reliability and integrity of on-chip data transmission. Access control policies and multi-factor authentication (MFA) fortify access control, while secure boot mechanisms and security-aware design tools embed security considerations throughout the design process. In conclusion, enhancing security in on-chip communication requires a comprehensive and integrated approach that addresses multiple attack vectors and leverages advanced technologies and methodologies. As SoCs continue to evolve, ongoing research and development in security solutions will be paramount to staying ahead of emerging threats, ensuring the continued protection of sensitive information and the reliable operation of critical systems. By adopting the solutions and countermeasures discussed in this survey, the security of on-chip communication can be significantly fortified, paving the way for more secure and resilient SoC architectures in the future.

References

[1] Guo, Xiaoming, Sijia He, Amlan Nayak, and Jay Zhang. "SecureNoC: Enhancing On-Chip Network Security for Many Integrated Core Systems.", https://www.eecs.umich.edu/courses/eecs578/eecs578.f15/projects/Colonel_Panic_report.pdf

[2] Pasricha, Sudeep, and Nikil Dutt. On-chip communication architectures: system on chip interconnect. Morgan Kaufmann, 2010.

[3] Lukovic, Slobodan, and Nikolaos Christianos. "Enhancing network-on-chip components to support security of processing elements." In Proceedings of the 5th Workshop on Embedded Systems Security, Arizona United States 2010. pp. 1-9.

[4] Saeed, Ahmed, Ali Ahmadinia, and Mike Just. "Hardware-assisted secure communication in embedded and multi-core computing systems." Computers 7, no. 2 (2018): 31.

[5] Charles, Subodha, and Prabhat Mishra. "A survey of network-on-chip security attacks and countermeasures." ACM Computing Surveys (CSUR) 54, no. 5 (2021): 1-36.

[6] Indrusiak, Leandro Soares, James Harbin, Cezar Reinbrecht, and Johanna Sepúlveda. "Side-channel protected MPSoC through secure real-time networks-on-chip." Microprocessors and Microsystems 68 (2019): 34-46.

[7] Jiang, Nan, Daniel U. Becker, George Michelogiannakis, James Balfour, Brian Towles, David E. Shaw, John Kim, and William J. Dally. "A detailed and flexible cycle-accurate network-on-chip simulator." In 2013 IEEE international symposium on performance analysis of systems and software (ISPASS), Austin, TX, USA, IEEE, 2013. pp. 86-96.

[8] Becker, Daniel U. Efficient microarchitecture for network-on-chip routers. Stanford University, 2012.

[9] Daoud, Luka. "Secure network-on-chip architectures for MPSoC: overview and challenges." In 2018 IEEE 61st international midwest symposium on circuits and systems (MWSCAS), Windsor, ON, Canada. IEEE, 2018.pp. 542-543.

[10] Bertozzi, Davide, and Luca Benini. "Xpipes: A network-on-chip architecture for gigascale systems-on-chip." IEEE circuits and systems magazine 4, no. 2 (2004): 18-31.

[11] Bjerregaard, Tobias, and Shankar Mahadevan. "A survey of research and practices of network-on-chip." ACM Computing Surveys (CSUR) 38, no. 1 (2006): 1-es.

[12] Ogras, Umit Y., Jingcao Hu, and Radu Marculescu. "Key research problems in NoC design: a holistic perspective." In Proceedings of the 3rd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis, Jersey City, NJ, USA 2005. pp. 69-74.