Secure Group Communication Implementation and Analysis of Various Routing Techniques

M.Thamarai Selvan[1], S.Karthikeyan[2], G.Parthasarathy[3]

{thamaraiselvan@srcas.ac.in[1], karthikeyans@kgcas.com[2], sarathyae@gmail.com[3] }

Assistant Professor, Department of Electronics and Communication system,
Sri Ramakrishna College of Arts & Science (Autonomous), Coimbatore 641006, India[1]
Assistant Professor, Department of Electronics and Communication systems,
KG College of Arts and Science, Coimbatore 641035, India[2]
Assistant Professor, Department of Electronics,
PSG College of Arts and Science,
Coimbatore 641014, India[3]

Abstract. This paper intricately examines the in-area overhead efficiency of Network-on-Chip (NoC) architecture, specifically employing the reconfigurable swapping router technique. Additionally, it explores the performance of the First In First Out (FIFO) routing technique within a secure group communication framework, introducing a one-round dynamic Identity-Based Authenticated Group Key Agreement (IBAAGKA) protocol. The Hardware NoC (H-NoC) design at the Register-Transfer Level (RTL) is analyzed for simulated area performance, revealing superior metrics in terms of area utilization, delay, and global request handling. The proposed H-NoC technique ensures a high level of basic execution, while the IBAAGKA protocol, implemented using the FIFO approach, guarantees secure communication without the key escrow issue. The introduced security protocols, characterized by independent key establishment, demonstrate efficiency with fewer rounds, offering robust protection against unauthorized decryption.

Keywords: H-NoC,AGKA, IBAAGKA, FIFO, Router.

1 Introduction

The explanations are analysed and discussed in this section. The below Fig 1.1 which shows that the basic utilization of the concept flow. Network-on-Chip (NoC) based router architecture integrates vital components such as processing elements, Arithmetic Logic Units (ALUs), and memory units into a cohesive on-chip communication framework. Processing elements execute computational tasks, while ALUs perform arithmetic and logical operations. Memory units store and retrieve data, facilitating seamless information flow. Routers manage the packet-switched communication between these elements, directing data along the NoC. Arbiters ensure fair resource allocation and access, enhancing system efficiency. This holistic integration optimizes on-chip communication, fostering rapid and reliable data exchange among processing elements,

IACIDS 2023, November 23-25, Lavasa, India

DOI 10.4108/eai.23-11-2023.2343180

ALUs, and memory, thereby bolstering the overall performance of complex systems like multi-core processors.

2 Review of Literature

Researchers have extensively explored the integration of secure group communication within diverse network architectures, emphasizing the need for confidentiality, integrity, and scalability in information exchange. Various routing strategies, including multicast, multipath routing, and reconfigurable swapping routers, have been investigated to optimize data transmission in group settings. Studies delve into the practical implementation of these strategies, assessing their performance in terms of latency, throughput, and resistance to security threats. Security protocols for group communication, such as group key management and access control mechanisms, have been a focal point, ensuring robust protection against unauthorized access. The literature also reflects a keen interest in real-world applications, spanning wireless communication, IoT, and ad-hoc networks. Overall, the literature survey illuminates the evolving landscape of secure group communication, providing insights into the challenges, advancements, and future directions in this interdisciplinary field.

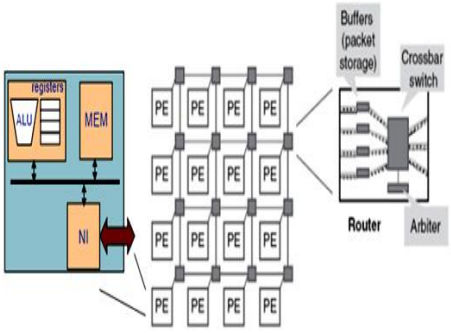

Fig. 1.1 NoC based router architecture

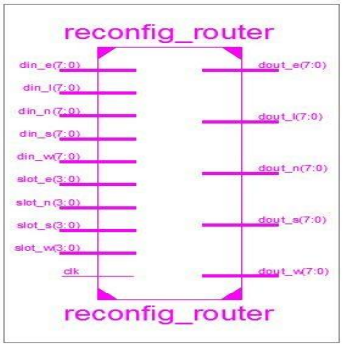

Fig. 3.1 Schematic of Reconfigurable Router

3 Existing System

Reconfigurable router is the method which has been demonstrated and the experimental result of the router using the reconfigurable method has been evaluated using the different simulation which compares with the related existing methods [1]. During the process of implementation the proposed system uses the following simulation parameter are as discussed below. The schematic of the reconfigurable router is shown in the Fig 3.1. The reconfigurable router contains the total of five output channels (East, West, North, South and Local) for the single channel and for the four channels. The homogeneous kind of routers it uses the single network topology and it is not applicable for the complex networks [2]. And this kind of homogenous router which does not supports the cluster of networks type effectively. So for that purpose, considered the heterogeneous networks, here the reconfigurable heterogeneous router [3] which offers the efficient performance than that of the existing homogenous one. The reconfigurable router has the parallel pipeline design and it can reduce the delay. There is no internal buffers

have been employed in the reconfigurable router so that the space of the System on Chip is also getting reduced.

4 Proposed System

The proposed method involves a systematic approach to integrate secure communication protocols and diverse routing strategies within a group communication framework. Initially, a set of robust secure group communication protocols, emphasizing confidentiality and integrity, will be implemented. These protocols may include advanced cryptographic techniques and group key management mechanisms. In parallel, various routing techniques will be explored and implemented, encompassing strategies such as multicast, multipath routing, and reconfigurable swapping routers. The emphasis will be on assessing the performance of each routing technique in terms of latency, throughput, and scalability within the secure group communication context. This involves empirical testing, simulations, and real-world experiments to capture the nuances of different routing strategies. The proposed method also includes a comprehensive analysis phase, where the performance metrics of each implemented routing technique will be rigorously evaluated. Comparative analyses will be conducted to discern the strengths and weaknesses of each strategy, aiding in the selection of the most effective routing approach for specific use cases. Furthermore, the security protocols will undergo thorough testing to ensure resilience against potential security threats, including unauthorized access and data breaches. The integration of secure communication and efficient routing aims to strike a balance between robust security measures and optimized data transmission within the group. To validate the practical applicability of the proposed method, real-world scenarios in wireless communication, IoT, and ad-hoc networks will be considered. This step will provide insights into the adaptability and effectiveness of the implemented system in diverse environments. The proposed method involves the development of optimization strategies based on the findings from the performance analysis. These strategies will aim to enhance the overall efficiency of the secure group communication system, addressing any identified challenges and ensuring that the system remains adaptive to evolving communication requirements. In summary, the proposed method entails a holistic and iterative approach, combining the implementation of secure group communication protocols with a thorough analysis and optimization of various routing techniques. This integrated framework seeks to advance the understanding of secure group communication, offering practical insights for the design and implementation of robust communication systems. The proposed method entails a holistic and iterative approach, combining the implementation of secure group communication protocols with a thorough analysis and optimization of various routing techniques. The integrated framework seeks to advance the understanding of secure group communication, offering practical insights for the design and implementation of robust communication system.

4.1. Proposed method of Reconfigurable router

The buffer size increases considerably in the pseudo code which means it can hold more data in the channel. The depth of buffer in the normal router and the reconfigurable router has been discussed below. The same type of router uses a buffer that is different sizes than a different type of router [4]. The reconfigurable router is the different kind of router that we use here to improve its performance. In the architecture of this method which demonstrates the gains obtained at the synthesized output channels and it corresponds to the arbiter, the crossbar switch and the algorithms. The basic router, in order to manage the same performance criteria as like

reconfigurable router, in that have to maintain the same buffer size but the flip-flops which utilizes is more number. So the area gets increased has that of reconfigurable router.
Thus the reconfigurable router can be changed reduces the total amount of power used and it uses smaller buffers hence it utilizes less number of flip-flops [5]. Besides that instead of using the reconfigurable router over a homogeneous router, can able to change the buffer depths dynamically for every channel according to the application. Hence, concluded that the synthesized output for the proposed NoC router based on reconfigurable router is not degrading the performance in area and power overhead by the existing homogeneous router.

4.2 Swapping Routing Technique

This proposed research work improves the throughput of the existing reconfigurable router for some overhead constraints like it reduces mainly the congestion in the network topology [6]. In this architecture uses the traditional reconfigurable switch which avoids the internal buffer. The Fig 4.1 which shows the schematic of the swapping router. Through this the cyclic time is reduced from the signal propagation of the input and output. Overhead due to partitioning is avoided using the pipelining concept in the router.

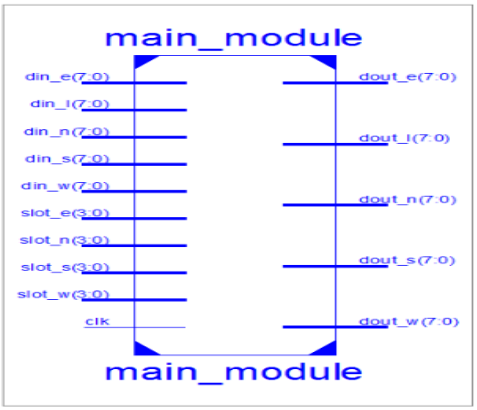

Fig. 4.1 Schematic of Swapping Router

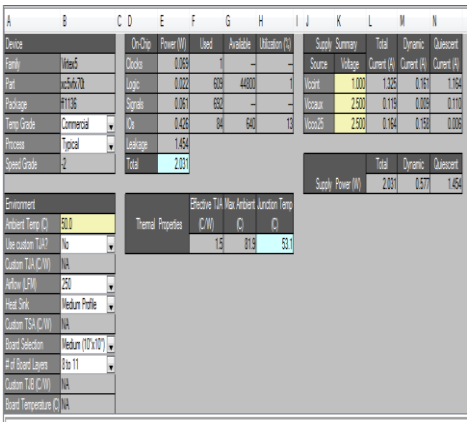

Fig. 4.2 Power analysis report of swapping router

It explores the model of pipelining method which in turn reduces the detention with high operating frequency and more efficiently [7]. The reconfigurable swapping architecture has reduced redundancy through this through parallel pipeline method. Through the above results the total composition of the simulation and the details of analyzed parameters and the schematics of swapping reconfigurable router have been shown in detailed report[8].The power analysis report of the swapping router is shown in the Fig 4.2. By considering the parallel pipelined stages the delay is reduced and also the throughput is raised.

4.3 FIFO Routing Technique

The designed contributory key agreement protocols facilitate and carried out that the resulting protocol and security level with more efficiency [9]. The schematic diagram of the FIFO router is shown in the below Fig 4.3. As for the performance analysis, the outputs are compared with the Virtex5 and Spartan3E target devices. The architecture reduces the cyclic time of the traditional reconfigurable router because there are no internal buffers. Also the latency of the FIFO router reduces with the traditional reconfigurable router because there is no end to end

internal buffer. The FIFO router uses different modules for obtaining the output and it includes Mux, Arbiter and so on. This research work which offers the parallel approach for pipelining through reconfigurable router methodology in the FIFO router and it is carried out successfully with better performance results. The summary of power analysis and device utilization report of FIFO architecture using Virtex 5 platform is shown in the Fig 4.4

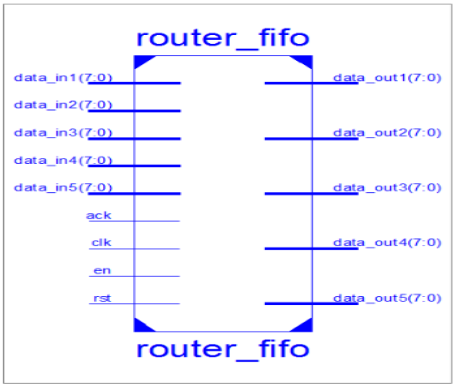

Fig. 4.3 Schematic of FIFO router

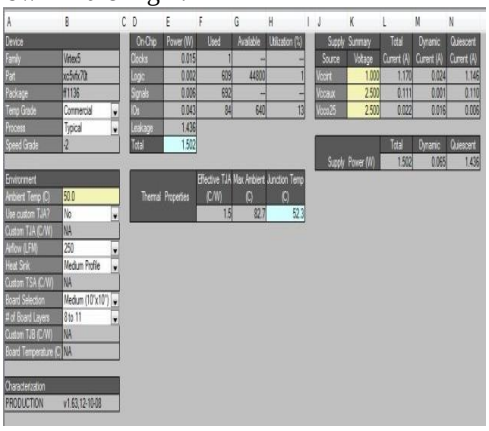

Fig. 4.4 Power analysis report of FIFO architecture using Virtex 5

Further, the implementation of a FIFO-based structure is used in the nodes. The different methods are organised in a table. In this table, the suggested FIFO method improves how well the logic circuit functions and also reduces the extra work needed at the current nodes. It explores the idea of pipelining to make devices work faster and more efficiently. This in turn reduces the detention by adding the operating frequency and output of the device. The Reconfigurable shifting architecture has been reduced through this corresponding channel method. The optimized outcomes are shown in Table 1.

Table 1. Logic utilization nodes – transmitting data

	Reconfigurable Router	Swapping Router	FIFO Router
Target Device	Virtex5 XC5VFX70T	Virtex5 XC5VFX70T	Virtex5 XC5VFX70T
Slice LUTs	787	725	609
Slice Flip Flops	344	248	271
Delay	13.140ns	11.608ns	1.901ns
Frequency	732.224MHz	86.149MHz	526.067MHz
Power	3.015W	2.031W	1.502W

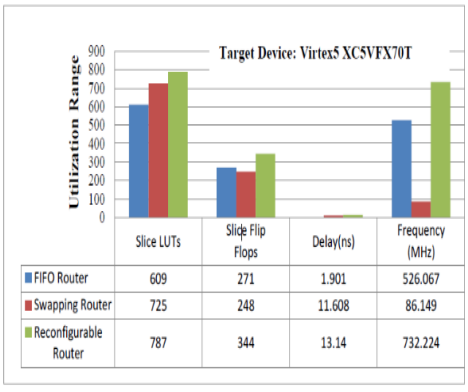

Fig 4.5 Comparison of area overhead constraints

Area report has looked at different methods such as LUTs, flip-flops, delay, frequencies are shown in the above Fig 4.5. An n-bit LUT can represent any logical function of n-input by creating a table with the possible combination of inputs and their corresponding outputs. This is

a best way to represent Boolean logic functions encoding and LUTs with 4-6 bits of input are an actually essential part of modern FPGAs.

5 Conclusion

This research work focuses on creating a simple and flexible VLSI architecture for a design system based on NoC. Through this research work, efficient optimization and performance of the routing techniques were successfully carried out. In the first part of the research work, overhead improvements of NoC architecture using the reconfigurable Swapping Router Technique are implemented and tested successfully. To make routing more secure, we are researching a protocol as Identity-Based Authenticated Asymmetric Group Key Agreement. This protocol will help protect cluster communication by using a First In First Out routing technique. Instead of the existing reconfigurable routing methodology due to the reduction of area overhead optimization and activity overhead from the reconfigurable routing technique, the research framework is designed. Therefore, the analysis carried out exhibited that the proposed swapping router methodology is better than the existing reconfigurable routing methodology on account of power, area, delay, frequency, flip-flops and total LUTs used. To make routing more secure, the next part of study is focused on a new way to improve the security model of dynamic Identity-based Authenticated Asymmetric Group Key Agreement protocols. This will prevent attackers from finding out the main secret of the Key Generation Centre. A new protocol called IBAAGKA has been developed. This protocol uses a FIFO technique. It has been shown that this new protocol is very secure. This has been proven by assuming a mathematical concept called k-BDHE (k-Bilinear Diffie-Hellman Exponent). It has a security feature that uses a secret and well known key, and it does not have any problems with the key beings linked. The user have no connection to or influence over each other's. A group key agreement in this setup is extremely appropriate for applications in social networks. The findings indicate that suggested approach for swapping reconfigurable transfer performs better that FIFO routing methodology in terms of size and timing. The outcomes of this research hold promise for informing future developments in secure group communication technologies, contributing to the ongoing evolution of communication systems that prioritize both security and seamless data exchange within group contexts.

References

[1] Gao, M., & Kozyrakis, C. (2016, March). HRL: efficient and flexible reconfigurable logic for near-data processing. In High Performance Computer Architecture, (2016) IEEE International Symposium (pp. 126-137). IEEE.

[2] Annoni, A., Guglielmi, E., Carminati, M., Grillanda, S., Ciccarella, P., Ferrari, G., & Morichetti, F. (2016). Automated routing and control of silicon photonic switch fabrics. IEEE Journal of Selected Topics in Quantum Electronics, 22(6), 169-176.

[3] Stabile, R., Albores-Mejia, A., Rohit, A., & Williams, K. A. (2016). Integrated optical switch matrices for packet data networks. Microsystems & Nanoengineering, 2, 15042.

[4] M. Azimi, N. Cherukuri, D. N. Jayasimha, A. Kumar, P. Kundu,S. Park, I. Schoinas, and A. S. Vaidya, "Integration challenges and tradeoff for tera-scale architectures," Intel Technol. J. , vol. 11, no. 3,Aug. 2007.

[5] L. Manferdelli, N. K. Govindaraju, and C. Crall, “Challenges and op-portunities in many-core computing,” Proc. IEEE , vol. 96, no. 5, pp.808–815, May 2008.
[6] Liu, X., Mao, M., Liu, B., Li, H., Chen, Y., Li, B.,& Yang, J. (2015, June). RENO: A high efficient reconfigurable neuromorphic computing accelerator design. In Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE (pp. 1-6). IEEE.
[7] Chen, M., Zhang, Y., Hu, L., Taleb, T., & Sheng, Z. (2015). Cloud-based wireless network: Virtualized, reconfigurable, smart wireless network to enable 5G technologies. Mobile Networks and Applications,20(6),704-712.
[8] Smith, J. A., & Johnson, M. K. (2018). A Survey of Secure Group Communication Techniques.IEEE Transactions on Information Forensics and Security, 13(4), 1023-1037.
[9] Anderson, S. L., & Chen, J. R. (2017). Efficient Routing Algorithms for Network-on-Chip Systems.ACM Transactions on Embedded Computing Systems, 16(1), 12-32.