From NoC Security Analysis To Design Solutions

Samuel Evain, Jean-Philippe Diguet

From NoC Security Analysis To Design Solutions

Samuel Evain
Université de Rennes 1,
IETR-INSA, UMR 6164 CNRS,
20, avenue des Buttes de Coësmes,
35043 Rennes Cedex - France
samuel.evain@univ-ubs.fr

Jean-Philippe Diguet
Université de Bretagne Sud
LESTER, FRE 2734 CNRS,
Rue de Saint-Maudé,
56325 Lorient Cedex - France
jean-philippe.diguet@univ-ubs.fr

Abstract—**This paper addresses a new kind of security vulnerable spots introduced by Network-on-chip (NoC) use in System-on-Chip (SoC) design. This study is based on the experience of a CAD framework for NoC design and proposes a classification of weaknesses with regard to usual routing and interface techniques. Finally design strategies are proposed and a new path routing technique (SCP) is introduced with the aim to enforce security.**

I. Introduction

Network on Chip (NoC) provides designers with a systematic and flexible framework to manage communications between a large set of IP blocs [1], as well as their reconfiguration [2]. However, this flexibility introduces new weaknesses in the system and offers opportunities to potential attackers. Moreover the complexity of applications, the heterogeneity of architectures and the reconfiguration requirements that can justify the use of a NoC within a SoC increases the gravity of potential attacks. Therefore, it is necessary to take the NoC security into account in a critical system and to our best knowledge, no specific study has been yet devoted to that upcoming hot topic. The rest of the paper is organised as follows, in the next section we present what are the potential attack types in a NoC. In section 3 we detail the different guard strategies and the way they can be used. In section 4 we present the NoC possible counter attacks. In section V we summary our design strategy and finally we conclude.

II. Noc Attack Analysis and Current Weaknesses

A. *NoC Definition*

A NoC is based on two basic elements: the routers and the network interfaces (NI). In a wormhole packet switching network, messages are divided into packets. Routers switch channels to carry packets from their source to their destination in the network. NIs connect IP block ports to router ports.

In our context, router ports are composed of unidirectional opposite channels. The routing technique is a deterministic source routing. A central configuration module (CCM) is added. The CCM is a unique IP block in the NoC that is in charge of the initialisation, configuration, and reconfiguration of the NoC. The Philips NoC, AEthereal uses a similar module [3]. Supervising and defending reactions can be added in our CCM, for security reason. They will be discussed latter in section IV.

B. *Security*

It may be needed to combine secured data with unsecured components or interfaces. For example read transactions to a memory can be authorised to any user (IP) but write operations can be restricted to only one given IP.

A system can be divided in two areas, secure and unsecure ones. The secured area stores, processes and carries critical information. The unsecured area is relatively opened and vulnerable. Typically, the unsecure area can be a FPGA that is easily re-programmable whereas the secure area can be an ASIC (Fig.1). In practice ASIC based solutions cannot be always selected. Actually for flexibility, power and performance reasons, reconfiguration becomes a key capability [2] for future SoC applications for instance in the domain of Software Defined Radio [4]. In such a domain, secure and unsecure areas can be associated to black and red areas respectively.

Finally, three kinds of network implementations can be:

- Full ASIC implementation: the NoC benefits from the chip intrinsic protection. The potential weaknesses to protect are the system interfaces, namely read and write accesses through chip I/Os. The NoC is a way to control I/O but also to extend the SoC vulnerable area.
- Full FPGA implementation. In addition to the previous aspects, the reconfiguration capability opens a new weakness opportunity. However, two subclasses can be distinguished since bitstream encryption can be partially or fully used.
- Partial FPGA/ASIC implementation (see Fig.1) introduces two challenges, first maintain the NoC functionality after FPGA reconfiguration and secondly control accesses between ASIC and FPGA.

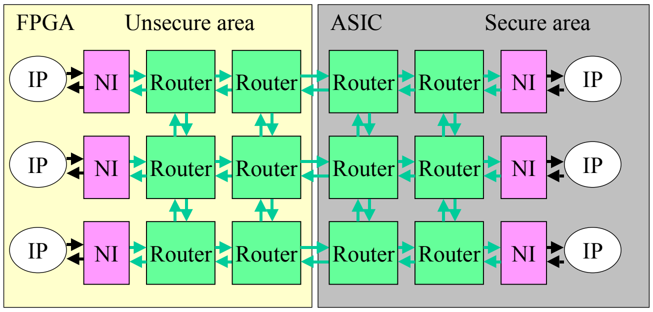


Figure 1. NoC distributed over FPGA and ASIC

C. *Attack Scenarios*

Attacker may have different goals and so different attack scenarios. Different kinds of attacks can be identified, and are shown in Table I. These attack types are explained as follows.

TABLE I. ATTACK TYPE AND SCENARIOS

	Attack types	**Attack scenarios**
Remote attack	Denial of service	Bandwidth denial
		Incorrect path
		Deadlock
		Livelock
	Extraction of secret information	Unauthorised read
	Hijacking (behaviour alteration)	Unauthorised write or reconfiguration
Proximity attack	Reverse engineering	Design data extraction
	Extraction of secret information	Run time observation

a) Denial of service.

This kind of attacks aims to bring down the system performances. The Network over utilisation downgrades the operability of the system. Frequently requests waste bandwidth and cause higher latency transfers in the system resulting in deadline misses for instance.

The three following attacks scenario are more damaging because they aim to obstruct channels in the NoC.

- **Incorrect path**. It consists of introducing in the network a packet with erroneous paths with the aim to trap it into a dead end. The body of the trapped packet takes some channels and makes them unavailable for the others valid packets.

- **Deadlock**. It means the use of packets with paths that intentionally disrespect deadlock-free rules of the routing technique with the intent to create deadlocks in the network. This leads to the contention of the channel and consequently of a part or the entire NoC.

- **Livelock**. This is the introduction of a packet that can't reach its target and stay turning infinitely in the network, causing a waste of bandwidth, latency and power.

b) Extraction of secret information

The aim is to read data in an unauthorised secure target. The stolen information can be sensible data, instructions from critical programs, IP configuration registers and so on

c) Hijacking (spyware)

This is a write access in the secure area in order to modify the behaviour or the configuration of the system.

d) Reverse engineering and Extraction of Secret Information by proximity access

With a physical access to the chip, the attacker can intend to theft intellectual property information through unauthorised reads in memories to obtain pieces of firmware. This may also be achieved through a differential power analysis (DPA) to proceed cipher keys extraction. [5].

III. PROTECTION STRATEGIES

Standard network cipher and authentication techniques are oversized (time, area and power). So they can't be easily and reasonably implemented in a NoC. Some original and NoC-oriented techniques must be implemented.

A. *Traffic Guaranty Consideration for Bandwidth Denial*

A first simple solution we propose against bandwidth denial attacks, consists of using classical separate virtual channels [6] for secured and unsecured communications. Virtual channels (VC) have the ability to control communication throughputs by assigning to some packets a priority greater than other ones in order to interrupt and overtake them. Virtual channels are multiplexed on a single physical communication. In literature such channels are already used to build guarantied traffic (GT) [3][6].

We use two VCs, a low security virtual channel and a high security virtual channel to secure internal exchanges in the secure area. The secure area manages both types of VCs giving always priority to packets carrying on the high security virtual channel.

If no TDMA (time division multiplexing access) technique is available for time slot allocation to unsecure traffics, then a simple implementation consist of assigning to the unsecure area only low security virtual channel capabilities. The communications between unsecure area and secure area use only low security virtual channels (see Fig. 2). This prevents packet coming from the unsecure area from obstructing secured packet paths in the secure area. Thus, secured communications in the secure area are isolated from the potential denial of service attacks.

If guaranteed throughput (GT) [3] reservation is possible then traffic access from outside can use reserved slots to get GT priority. This needs the use of an interface between the both domains. This point is presented in section B.

Note also that a second utilisation of VCs can be made. Indeed, a nice implementation of CCM control communications consists of using guarantied traffic channels, contrary to [2], a solution with a single NoC is required for control, configuration and data transfers.

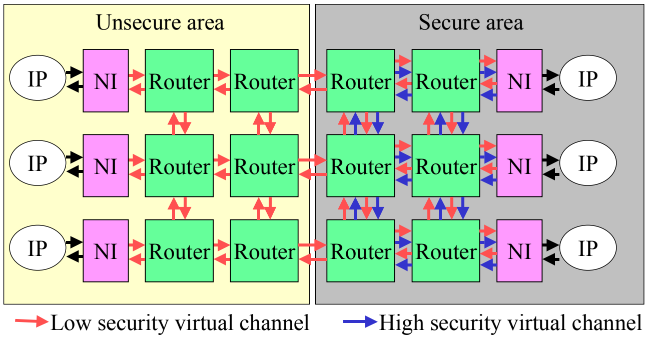


Figure 2. Virtual channels to prevent denial of service

However this solution prevents only from bandwidth denied and doesn't manage right access.

B. *Multi-Boundary Filtering for Security Purpose*

Three boundaries between secure and unsecure areas can be considered. Each one can be equipped with a specific shield. The first shield (1 in Fig.3) is an authorisation checking at NoC I/O access. The second is a path filter in the body of the network. The third is an authentication of the sender at secured NIs.

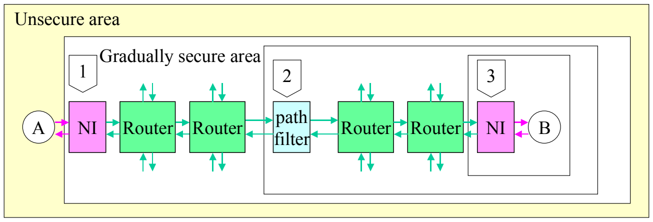


Figure 3. Multi-boundary area

These three levels of security are explained in the next subsections.

1) *Boundary 1 : NIs Inside the Secure Area*

The entire NoC is in the secure area. Some IPs are also in the secure area because they are critical, but some other IPs are in the unsecure area and can access only to some information within controlled time windows in the secure area. An example is shown Fig. 4.

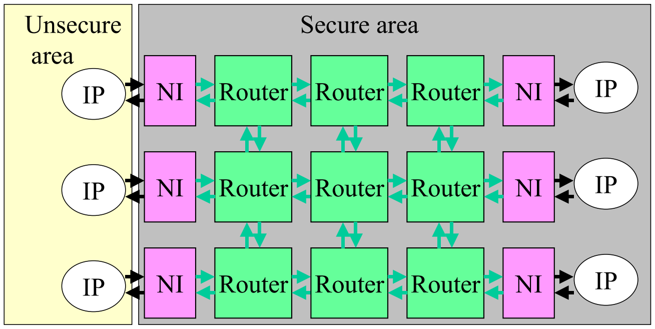


Figure 4. Example of an entire NoC in secure area

Details of our NI are shown in Fig. 5. NI contains various configurable parameters. These parameters are configurable via the NoC itself.

We distinguishes the following elements in a NI:

- A protocol wrapper to communicate properly with the connected IP port protocol.
- A memory-mapping table first converts the logical global address into the target IP location and check if this IP access is allowed, secondly the right access to the local address within the target IP memory space is checked.
- A path table provides the corresponding path instructions for each authorised target IP.
- A slot table for GT reservation [3].
- A best effort bandwidth instruction for non-GT transactions.

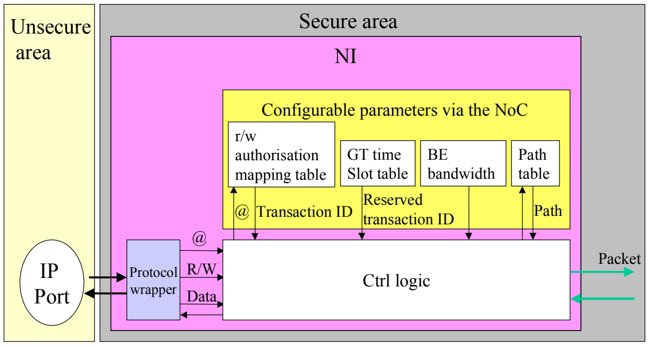


Figure 5. NI inside the secure area

The CCM delivers memory-mapping authorisation to NIs. NIs filter the memory-mapping addresses. By this way irregular transactions are forbidden. A NI must solicit the CCM to obtain a new authorisation. The CCM can take off an authorisation.

Avoided attacks are denial of service (by bandwidth monitoring in the NIs) and unauthorised read or write transaction (by filter verification in NIs).

2) *Boundary 2 : NIs Outside of the Secure area.*

In this case, only a part of the NoC is in the secure area. In this case we can't have confidence in the NIs into the unsecure area. Not any memory mapping information is available. So, in this case the checked information is the path instructions.

Path filters must be added in the secure area at the interfaces with the unsecure area (see Fig.6). In this case the CCM delivers path authorisation (and no memory mapping like in the previous case) to the path filter.

The path filter receives packets from unsecure area and allows only some path accesses to the secure area and forbid all others. This solution prevents an unauthorised sender to communicate with a secured target and offer deadlock-free and livelock-free guarantees.

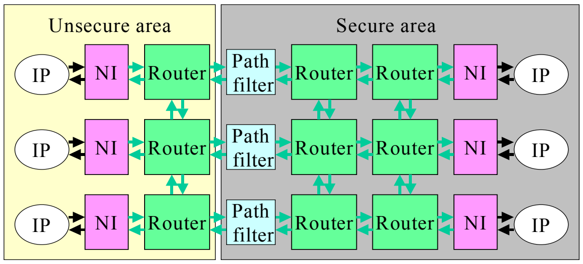


Figure 6. NoC in secure area and unsecure area

Path filter looks like NI, except that it is not connected to an IP and so doesn't have protocol wrapper, and has a path table in place of the memory-mapping table (see Fig.7). In practice, to avoid wasting time, this path filters are integrated in the port of the router on the secured area. It allows to proceed simultaneously to the path checking and the routing decoding step.

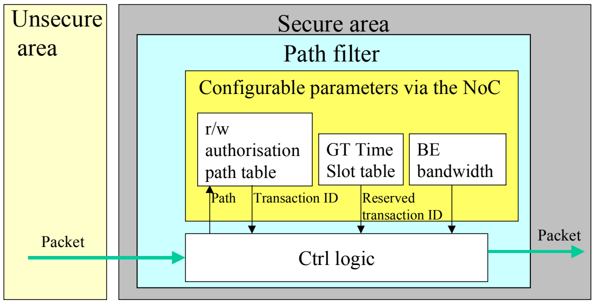


Figure 7. Path filter

3) Boundary 3 : Self Complemented Path coding

A receiver needs to be confident in sender identity for secure reasons. An ID number is not sufficient because a malicious sender can use the ID of another one. To solve this problem, we introduce the new concept of Self Complemented Path coding (SCP). The principle is the following. The only information that can't be corrupted to intend to usurp an identity is the path information to reach a destination. To do this the path instructions must be preserved during the travel of the packet from the sender to the receiver in such a way that this instruction set is a unique identity of the communication from a sender to this receiver. However usual source routing techniques (for instance XY or classical street sign) consume the path information.

To cope with this issue, our routing technique is a relative street-sign with or without "forward by default". Thus the choice of the direction in a router is given by the turn number in counter-clockwise from the considered input port (Fig. 8). This feature induces some key improvements detailed hereafter.

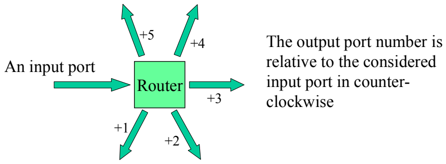

An input port
Router
+5
+4
+3
+2
+1
The output port number is relative to the considered input port in counter-clockwise

Figure 8. Routing instruction in our relative street-sign routing technique

SCP property 1 : *The used path is not removed. In this way, the path is a kind of identity certificate.*

Our path technique allows backward path computing. The backward path can be deducted from the forward path instructions and the arity of each crossed routers (Fig. 9).

SCP Property 2 : *At every router, the sum of the current instruction in forward direction and the corresponding instruction in backward direction is equal to the router arity.*

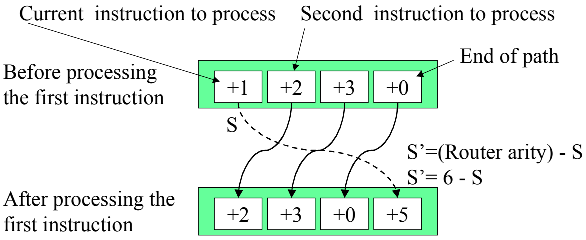

Current instruction to process
Second instruction to process
End of path
Before processing the first instruction
+1
+2
+3
+0
S
S'=(Router arity) - S
S'= 6 - S
After processing the first instruction
+2
+3
+0
+5

Figure 9. Path instruction complementing in a router

When the CCM creates a connection between two NIs, NIa and NIb, it gives them forward paths. Each router executes the current path instruction, and then complements it with respect to its own arity through a round shift technique explained in Fig.10. The router arity is the number of bi-directional ports of this router (the arity of the router R1 in Fig. 9 and in Fig.10 equals six).

SCP Property 3 : *A complemented and reversed path in one way is equal to the path in the other way. This is noted as follows for a connection between two IPs A and B:* $R(\overline{AtoB})=BtoA$

Each receiving NI checks SCP Property 3 to authenticate sender identity.

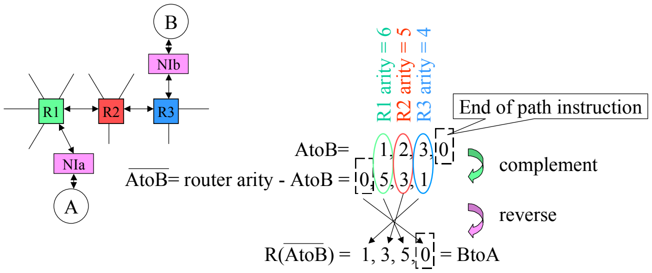


Figure 10. Forward and backward paths with SCP properties

However an additional "End of path" instruction is necessary (equal to 0 in Fig. 10) to avoid an infinite loop of the path and a livelock possibility.

SCP Property 4 : *A "End of Path" instruction is present in each path and becomes the current instruction only when arriving at target NI.*

In a correct transfer, the "End of path" becomes the current instruction when arriving in the target NI. The destination NI checks the current instruction to ensure this is an "End of path" instruction. Otherwise the packet is considered incorrect and removed.

Each crossed router checks two times the current instruction and processes it. First, if the instruction "End of path" appears, the router removes this incorrect packet. Secondly, if not any “End of path” instruction appears in the path, the router removes the packet to avoid livelock attack.

Fig. 11 shows an example. B authorises write data only from A. C intends to write in B. When receiving the packet, B checks the used path and detects the malicious sender. Moreover the reversed received path is the backward path to answer to the sender.

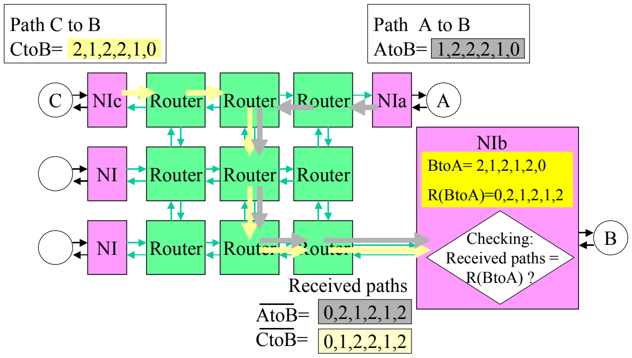


Figure 11. Source Path Authentication

The minor overhead du to complement operations is balanced with memory and communication savings since CCM provides only forward paths. Note also that in the context of security the complement operation is not compulsory. However, it remains relevant since it makes the authentication dependent on the path and the router arities.

This technique is efficient in terms of delay and implementation, since the complemented instruction is computed in parallel with the routing decoding step and this subtraction can be optimised for the router arity.

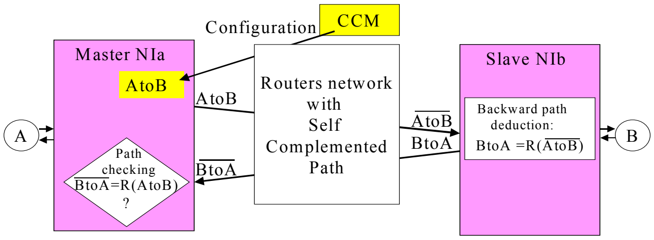
The path used to answer the CCM is stored in all master and slave NIs, to allow NIs to check this path and to prevent another NI or IP blocs to usurp the CCM identity.

Note that the SCP property 2 has another great interest. If security is not the main concern, the backward path property is useful to allow a slave IP block to answer to a read request from any master IP block. By this way, not any additional path table configuration is needed in the slave NIs. The received packet path provides directly the reversed backward path to answer to the initiator master. So, a great advantage our routing technique is that slaves can ignore master locations, thus it enables the mobility of IPs in a re-configurable system [2].

In summary, a NI may use the SPC technique according to two distinct objectives :

- **Security purpose**: Source Path Authentication (SPA). The CCM provides only allowed forward paths to NIs and NIs check whether an incoming packet path (complemented by crossed routers) is well equal to one of the reversed forward paths.
- **Mobility purpose**: Trusted Boomerang Path (TBP). For easy mobility and configuration in the NoC, the reversed path is directly used to answer to the communication master that can move from a location to another depending on FPGA reconfigurations.

A transaction between a Master and a Slave is described Fig. 12. NIa uses Source Path Authentication while Nib uses Trusted Boomerang Path to answer. The SCP routing technique performs the complementation of paths.



Configuration
CCM
Master NIa
AtoB
AtoB
Path checking $\overline{BtoA}$=R(AtoB) ?
$\overline{BtoA}$
A
Routers network with Self Complemented Path
$\overline{AtoB}$
BtoA
Slave NIb
Backward path deduction:
BtoA =R($\overline{AtoB}$)
B

Figure 12. Source Path Authentication and Trusted Boomerang Path

C. *Encrypted Bitstream*

The configuration of the CCM must be safe as traditional high security chip, since it’s the key point to secure NoC. To prevent any malicious accesses to the CCM, a standard encryption technique can be used. This reconfiguration is usually not frequent, so encryption and decryption don’t waste significant time.

When an unsecure area is implemented in a FPGA, a classic authentication may be used to check the identity of the IP and avoid the replacement of the authorised IP by a usurper. The IP authentication key can be protected with techniques used for bitstream encryption, this is not the focus of this paper see [8] for details.

D. *Design Strategy Epilogue*

The real challenge happens when the network is distributed over secure and unsecure areas and when flexibility imposes hardware reconfiguration capabilities. In that case the designer must pay attention to a couple of critical points.

- CCM is weak point, so it must be in the secure area. SPA enables to authenticate CCM access during NIs configurations. The CCM configuration must be secure with an encryption technique.
- Mobility and FPGA reconfiguration is easy thanks to the TBP. None any configuration is needed to inform the secured area about the required path to use to answer to a Master NI in the unsecure area.

Ideally, the following rules should be respected:

- NI must be inside the secure area, which is implemented in an ASIC or encrypted FPGA.
- The write access to the CCM program memory must be protected with a strong encryption technique used

by the designer. (Note that encryption key can be simply based on SPA property. It means that the CCM can be configured through a NI using a complex path within the NoC).

IV. Counter Attack

A. *Wrong path reaction*

When a NI in the secure area receives a packet from an unauthorised sender, it advises the CCM. Multiple reasons can produce such a result so the CCM can react by different ways:

- First this problem may be caused by a transmission error between a sender and a receiver. The CCM asks the sender to re-send the lost data.
- It may be issued from a configuration error. The CCM proceed to reconfiguration actions on both sender and receiver.
- If the error persists and error counter in the CCM reaches a specified threshold, the CCM identifies an attack and throttles the NI bandwidth of the faulty sender IP.

B. *Reverse Engineering and Extraction of Secret Information by Differential Power Analysis*

The NoC can also be used with the intention to increase the security in the system. By changing alternately the used paths, transaction observation becomes more difficult. This can be completed by moving master locations with the TBP technique. This may preserve the system against a key extraction by Differential Power Analysis. [5].

C. *Bandwidth and Power Supervisor*

A power control may be realised by the CCM to supervise the system in regard of the expected system life. If the power consumption grow up over a threshold, the BE traffic is reduce to prevent the risk of an attack (draining of battery) [9]. The CCM is in charge of configuring and supervising the NIs behaviours. This assumes for the CCM a previous knowledge of the expected behaviour of the application. So a profiling (e.g. allowed data rate upper bound) must be done and some threshold must be identified to allow the CCM to detect an irregular behaviour in the NoC and consequently to launch a reaction by means of parameter adjustments in NIs in order to recover a regular behaviour of the system. This aspect is another research topic that can’t be treated here.

V. Conclusion

Intentional fault introduction and increasing error rate expected in future technologies may lead designers to pay attention to security aspects in SoC communications. It is important to be aware of the potential attacks relative to NoC specific features. We have described how NoC can be protected with path filters or secure NIs. A new SCP routing technique allowing to destination to authenticate the sender identification has been presented. Moreover, we have exposed how this technique can improve the reconfiguration capabilities for performance and security purposes. Our propositions in terms of defence techniques to attack are summarised in Table II. A cross indicates a protection capability. We have design our NoC CAD tool µSpider in a flexible way [7] that provides the designers with capabilities, to obtain the needed level of security depending on the application and implementation constraints.

TABLE II. Defence techniques to attacks

Attack scenarios	**protection strategies**						
	NIs in secure area	**Path filter**	**SPA**	**VCs**	**Encrypted Bitstream**	**Bandwidth monitoring**	**IP mobility with TBP**
Bandwidth denial				X		X	
Incorrect path	X	X	X				
Deadlock	X	X	X				
Livelock	X	X	X				
Unauthorised read	X	X	X		X		
Unauthorised write or reconfiguration	X	X	X		X		
Design data extraction					X		X
Run time observation							X

References

[1] W.J.Dally and B. Towles, “Route Packets, Not Wires: On-Chip Interconnection Networks”, DAC'01, pp. 684-689.

[2] T. Marescaux, A. Bartic, D. Verkest, S. Vernalde, and R. Lauwereins “Interconnection Networks Enable Fine-Grain Dynamic Multi-Tasking on FPGAs”, Proceedings of the 12th International Conference on Field-Programmable Logic and Applications, Montpellier, September 2002, pp. 795-805.

[3] K. Goossens, J. van Meerbergen, A. Peeters, and P. Wielage “Networks on Silicon: Combining Best Effort and Guaranteed Services”, Proc. DATE, March 2002.

[4] J. Mitola, “The software radio architecture”, IEEE Communications Magazine, May 1995, pp. 26-38.

[5] F.X. Standaert, L. van Oldeneel tot Oldenzeel, D. Samyde, J.J. Quisquater, “Power Analysis of FPGAs: How Practical Is the Attack”. In proceeding of 13th International Conference on Field-Programmable Logic and Applications, FPL’2003, September 2003, Lisbon, Portugal, pp. 707-711.

[6] W. J. Dally, “Virtual-Channel Flow Control”, IEEE Trans. on Parallel & Distributed Syst., Vol. 3, no. 2, March 1992.

[7] S. Evain, J. P. Diguet, and D. Houzet, “A Generic CAD Tool for Efficient NoC Design”, IEEE ISPACS 2004, International Symposium on Intelligent Signal Processing and Communication Systems, Seoul, Korea, November 18-19, 2004.

[8] L. Bossuet, G. Gogniat, W. Burleson, “Dynamically Configurable Security for SRAM FPGA Bitstreams”. In 11th IEEE Reconfigurable Architectures Workshop, RAW 2004, Workshop of IEEE IPDPS 04, Santa Fé, New Mexico, USA, April 26-27, 2004.

[9] T. Martin , M. Hsiao, D. Ha and J. Krishnaswami, “Denial-of-Service Attacks on Battery-powered Mobile Computers”, Proceedings of the 2nd IEEE Pervasive Computing and Communications Conference, Orlando, Florida, March 2004, pp.309-318.