LUND UNIVERSITY

A generic hardware MAC for wireless personal area network platforms

Dasalukunte, Deepak; Öwall, Viktor

2008

Link to publication

Citation for published version (APA):
Dasalukunte, D., & Öwall, V. (2008). *A generic hardware MAC for wireless personal area network platforms*. Paper presented at International Symposium on Wireless Personal Multimedia Communications (WPMC), 2008, Saariselkä, Finland.

Total number of authors:
2

General rights
Unless other specific re-use rights are stated the following general rights apply:
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.
• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Read more about Creative commons licenses: https://creativecommons.org/licenses/

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

LUND UNIVERSITY

PO Box 117
221 00 Lund
+46 46-222 00 00

A GENERIC HARDWARE MAC FOR WIRELESS PERSONAL AREA NETWORK PLATFORMS

Deepak Dasalukunte and Viktor Owall
Department of Electrical and Information Technology
Lund University, Sweden.

ABSTRACT

This paper presents a generic hardware-MAC for systems designed based on high rate (IEEE 802.15.3) and low rate (IEEE 802.15.4) Wireless Personal Area Networks. Functionality that are better run in hardware are moved over from the software part of the MAC layer. An easy to access memory like interface has been defined for data and control transfer between the software and hardware parts of the MAC layer. A key challenge in designing such a system was to arrive at a generic architecture without compromising with either of the standards on the lines of which the two systems are implemented. Emphasis on reuse of the modules has been done in order to avoid repetition of design and implementation effort and in turn reducing the time required for testing. The design has been successfully tested on different FPGA platforms.

I. INTRODUCTION

This paper deals with Wireless Medium Access Control (MAC) implementation for high and low rate Personal Area Networks (PAN) defined as the IEEE 802.15.3 [6] and IEEE 802.15.4 [7] standards respectively. The MAGNET Beyond project [3] works along the lines of these standards to realize Personal Networks (PN). In MAGNET Beyond, the IEEE 802.15.3 standard compliant system is called the High Data Rate (HDR) system while the one compliant with IEEE 802.15.4 is termed Low Data Rate (LDR) system. Most part of the MAC layer is implemented in software (an ARM processor in case of the HDR system), while the PHY layer is custom hardware.

A key feature in the implementation is that some of the functions of the MAC layer is moved to hardware and an interface similar to a memory is designed for transfer of data and control information. With this, the MAC functions in software (SWMAC) can treat those in hardware (HWMAC), and in turn the PHY layer, as any other peripheral and attend to it as the need arises. With the terminal functions of the MAC moved over to hardware the primary MAC functions running in software will be more efficient. The HWMAC also takes care of some book keeping functions that are important for the MAC layer to function as a whole . The block diagram in Fig. 1 gives a general overview of the presence of HWMAC with different layers marked. It also provides a view of how the different blocks are implemented and in what form. It can be seen that a functional part of the MAC layer is in hardware implemented on an FPGA along with the PHY layer. The hardware is prototyped in a FPGA because of the ease with reconfigurability and testing.

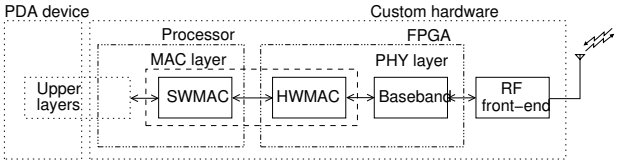

Figure 1: General block diagram of the HWMAC in HDR/LDR system

II. HARDWARE MAC

The HWMAC consists of operations carried out in the final stages before the data is passed onto the PHY layer. A generic block diagram for both HDR and LDR architectures is shown in Fig. 2. The interface towards the SWMAC is a set of configuration and status registers, along with FIFOs that hold the packets to be transmitted or those received. Both the registers and the FIFOs are mapped on to an address space to which the SWMAC can write into and read from. The encryption unit is a 128-bit Advanced Encryption Standard (AES) [4] encryption engine. A global controller takes appropriate action on requests through control signals from the PHY layer and through configuration registers from the software and directs the flow of data within the module. The Cyclic Redundancy Check (CRC) modules for the HDR system, is a 32-bit CRC [6], while an ITU-T 16-bit CRC [7] is used for the LDR system.

The HWMAC from the two systems, in spite of being strikingly similar, have several differences starting from the specifications in the standards from which they are implemented. One such being the way the information fields are contained in the header. Further, the size of the header for the HDR system is constant while that of the LDR can vary. This creates the need for processing the packets differently in the two systems. In the HDR system, the CRC is calculated over the payload, while it is over the entire packet (header+payload) in case of the LDR system. The CRC modules themselves follow different standards as mentioned previously. However, a common data flow architecture (Fig. 2) has been designed after several iterations of comparison between the requirements for the two systems. Such an approach was carried out in an attempt to reuse the modules being designed among which, the interface module, AES unit and global controller are notable.

III. IMPLEMENTATION

A common hardware MAC architecture for both platforms with re-use of different possible blocks resulted in portability to both systems and reduced design effort. This was a key issue as the two systems targeted different FPGA vendors, namely the

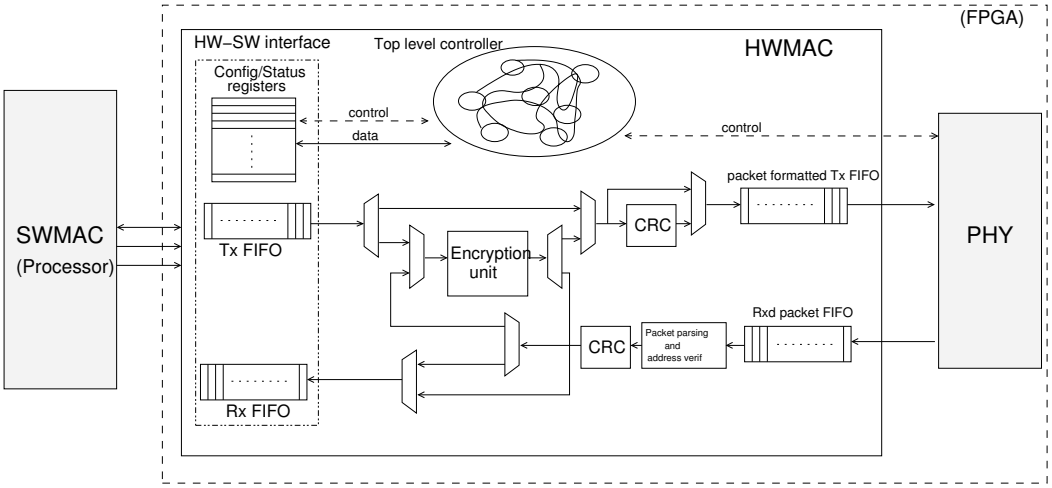

Figure 2: A generic HWMAC architecture for HDR and LDR system

Xilinx Virtex^{TM} 4 for the HDR and Altera Cyclone^{TM} for the LDR system. VHDL based design further eased integration with the PHY layer and porting towards different FPGAs. The design was simulated and tested in ModelSim^{TM} and Xilinx ISE^{TM} was used for post-synthesis and post-place-and-route simulations of the netlists. For the LDR system, because of the re-use of the modules a test at the behavioral level resulted in the design working on the FPGA with minimal effort.

A. *Hardware-Software interface*

The interface module provides a common area for the MAC functions, split between hardware and software, to share the data and configuration information. The SWMAC can program through a set of configuration registers and the HWMAC can take decisions based on this information. The advantage of having this type of interface is that, the MAC functions implemented in hardware can perform several actions simultaneously based on several fields in the register bank. For example, to start timers, provide precise timeouts, process the payload and header data and pass it to the PHY layer, interrupt the processor for packets received while retransmitting the acknowledgment to PHY layer and so on. The SWMAC makes use of this interface to write/read entire data packets consisting of several hundreds of bytes of data (header and payload) onto a single address, which internally is mapped onto a FIFO. Thus, eliminating the need for pointer management on the FIFOs by the software. Further, the software performing the core MAC operations need to respond only at the occurrence of an interrupt and the type of attention required is reflected through the status registers in the interface module.

B. *CRC for HDR and LDR systems*

The CRC needs to be calculated over several hundreds of bytes, which form the packet, and calculating it through a bit-serial approach consumes considerable amount of time (section 7.2.1.8 in [7]). Fig. 3 shows the block digram of the CRC module using a byte wise approach used in the LDR system [12] [13]. The calculation starts with an initial value in the CRC register. The incoming data byte is XORed the higher byte from CRC register and the result is used to look-up a value from a table. The so obtained look-up table value is then XORed with the contents of the CRC register and stored back. The final CRC value is obtained after performing these set of operations on all the data. A byte wise approach is more suited in this application because, the encrypted/unencrypted data to be transmitted can be simultaneously used to calculate CRC and also passed on to the PHY layer for transmission. Though this is also possible in a bit-serial approach, the latency of the system becomes large. The PHY baseband can start transmitting the packet much earlier when compared to a bit-serial implementation.

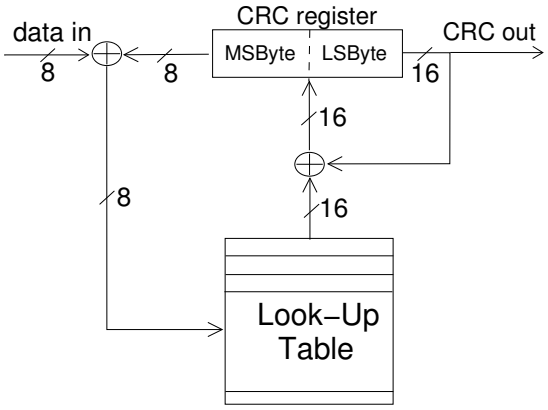

Figure 3: CRC module implemented in LDR system calculating a 16-bit CRC using byte-wise data

C. *AES encryption unit*

The encryption unit within the HDR and LDR systems incorporates a two-pass encryption scheme. In the first pass the data is encrypted in counter mode [5], while the entire packet to be transmitted is authenticated in the second pass using Cipher Block Chaining (CBC) type of message authentication. The message authentication code is appended at the end of the

packet being transmitted so that when the encrypted data is received it can be verified if it has been tampered with or not. Because of the two pass scheme involving Counter mode encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) it is called as CCM mode [8] of encryption.

The specifications for encryption in [6] and [7] uses a cipher key of 128 bits to encrypt data in blocks of 128 bits. A block diagram of the AES unit involving the functional blocks shown in Fig. 4 [10] primarily consist of *Key generator*, *Shift-rows*, *S-box* and *Mix-columns*. The block of data to be encrypted goes through this cycle of operations for 10 iterations [4] and use the round-key generated every iteration through the *Key generator* module that begins the encryption with the given 128bit cipher key. The shift rows module is implemented in hardware by just routing the data depending on the amount of shift and does not consume logic resources. The S-box and the mix-columns architectures suggested in [14] and [9] perform both the forward and inverse operations which is not required if CCM mode is being used. Thus they have been optimized within the encryption unit. This means that the inverse of the Mix-columns and S-box operations need not be implemented. Similarly, the inv-mix columns block in the key generator is also eliminated.

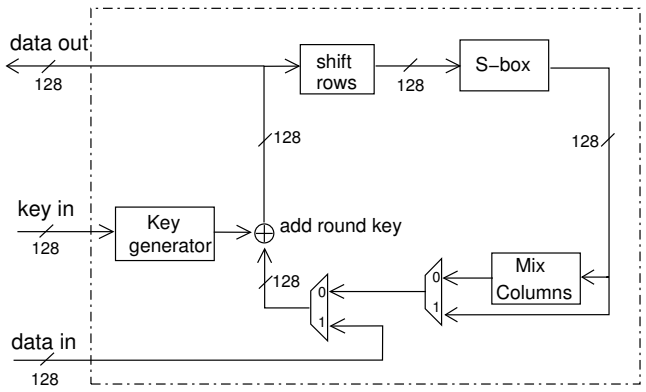

Figure 4: Block diagram of 128-bit AES architecture

D. Top level controller

Since the HWMAC has to perform several control and data handling functions depending on the situation a master controller is needed to prioritize the work and function accordingly. The function of this top level controller is to direct data through different modules within the HWMAC according to a predefined configuration from the SWMAC. For example, a raw packet to be transmitted, is formatted as required by the PHY layer besides appending CRC, encrypting the data and so on. Also, a packet received from the PHY layer is first parsed through and the controller takes decisions depending on to whom the packet is intended. This kind of pre-processing by the controller on the received packets will ensure that only those packets intended to the device is passed on and avoids the SWMAC to process each and every packet that is received. The packets presented to the processor are in their raw form and some vital information is stored in the register bank at the interface so that it is available for immediate reference and the SWMAC can work readily on the received data. The controller can initiate the operations like CRC verification and decryption to happen simultaneously as and when the data is available.

The global controller is designed to work for both systems, but there are some minor details and some modifications are required. For example, in the HDR system, the header information is of fixed length and a 32 bit CRC is calculated over the variable length payload information. In the case of LDR system, CRC is calculated over both the header and payload and both of them have variable lengths depending on the type of packet being transmitted.

E. Other features

The HWMAC also incorporates dedicated timers that interrupt SWMAC at regular intervals. These timers help normal devices to periodically synchronize with co-ordinator device within the Personal Network and exchange control and other crucial information such as, an encryption key.

IV. RESULTS

The prototype board developed and being used for the integration and testing of the HDR system [11] is shown in Fig. 5. A PDA hosting higher layers such as the application layer and other software along with the custom hardware hosting MAC and physical layers allows the user to network with several devices. Though the target application is intended for low-power, a prototype board with an FPGA is chosen initially because of its ease of reconfigurability thus simplifying the testing of modules in stand alone mode as well as a complete system. The HWMAC is completely integrated into the protocol stack(as in Fig. 1) with the MAC layer until the RF front-end on the custom hardware device (Fig. 5). Information is successfully transmitted through the entire chain and over the air. The so transmitted data packets are received by second device (Fig. 5) and decoded through the receiver chain. A series of tests like associating a device into a network, which is assumed to already exist, through a set of MAC protocols defined in the standards [6], [7] were performed. A device can also initiate to form its own network based on the commands issued by the user. Once the devices were associated with a particular network other key tests like data transfer, command issuance by a network co-ordinator to other devices were done. Several such prototypes thus connect with each other to form a Personal Network that can be used for various applications defined in MAGNET project and beyond.

Table 1: Complexity of different modules in HWMAC

Module	System	Slices	BlockRAMs
CRC-32	HDR	95	-
HW-SW interface	HDR	1228	5
HWMAC(total)[1]	HDR	2121	6
CRC-16	LDR	44	-
HW-SW interface	LDR	830	NA[2]
HWMAC(total)[1]	LDR	1650	NA[2]
AES 128bit	Both	2200	20[2]

Figure 5: View of the prototype board for HDR system. (Courtesy: CEA/LETI, Grenoble)

At the HWMAC level in the tranceiver chain, the complexity of a few key modules in terms of number of slices occupied on a Xilinx FPGA is shown in Table.1. For an LDR system, the complexity of the interface and HWMAC modules deviate slightly as shown in the table. This is because of the difference in number of registers in the interface modules and the way the global controller is performing the operations and the sizes of FIFO that hold the packets. Further, the LDR is implemented on an Altera device, the area reports are provided here only for comparison with the HDR system. It can be seen from Table. 1 that the complexity of the CRC modules are insignificant. The HWMAC indicated in the table represents the collective complexity of CRC generation and verification modules, the hardware-software interface, timers, and the Global controller. The complexity of the AES encryption unit is comparable to the entire HWMAC itself, consisting of all the other modules. This is due to the fact that 128 bits of data has to be processed simultaneously and LUTs in the form of memories and logic that generate the round-key for such data widths will use considerable FPGA real estate.

The fraction of the FPGA area occupied by the HWMAC is about 4400 slices (inclusive of AES) which accounts to about 17% of the total FPGA area (The Virtex-4 FPGA used in HDR has 24576 slices). This fraction of the hardware, that seem excess, is actually replacing the same functions that would have been carried out in software. It is also justified, as the SWMAC is benefited by complex and involved processing of the encryption, timers, ease of packet transmission, the way only relevant packets are provided, etc. carried out in hardware.

V. Conclusion

A generalized HWMAC has been implemented for the HDR and LDR systems under the MAGNET Beyond project. It forms an important link between the SWMAC and PHY layers and takes away the burden from the software on functions that can be terminated at the PHY layer. One such instance being pre-processing the received packets and pass only those necessary. The SWMAC can just program the way transmission needs to be carried out and it is reported back with information about a successful transmission or a failure. In the meantime, it can attend to the higher layers and other important MAC layer functions. The HWMAC can be seen as a co-processor and the SWMAC issuing instructions regarding the function that need to be carried out.

Acknowledgment

This work has been carried out within the Work Package-5 of the MAGNET Beyond [3] [2] project, supported by the Sixth Framework Programme (FP6) of the EU Commission [1].

References

[1] EU-Sixth Framework Programme.

[2] MAGNET Beyond - Link Level Prototypes(WP5).

[3] MAGNET Beyond - My Personal Adaptive Global NETwork.

[4] Advanced encryption standard (AES) (FIPS PUB 197), 2001.

[5] Recommendation for block cipher modes of operation - methods and techniques, 2001.

[6] Wireless medium access control (MAC) and physical layer (PHY) specifications for high rate wireless personal area networks (WPANs), 2003.

[7] Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (WPANs), 2003.

[8] Recommendation for block cipher modes of operation: The CCM mode for authentication and confidentiality, 2004.

[9] Hua Li and Zac Friggstad. An efficient architecture for AES mix columns operation. In *Proc. IEEE Intl. Symp. Circuits and Syst.*, volume 5, pages 4637– 4640, Kobe, Japan, May 2005.

[10] Hua Li and Jianzhou Li. A high performance sub-pipelined architecture for AES. In *Proc. IEEE Intl. Conf. Computer Design*, pages 491–496, October 2005.

[11] Dominique Noguet and et al. An MC-SS platform for short-range communications in the Personal Network context. *EURASIP Journal on Wireless Communications and Networking*, 2008, 2008.

[12] D. V. Sarwate. Computation of cyclic redundancy checks via table look-up. *Commun. ACM*, 31(8):1008–1013, 1988.

[13] Ross.N. Williams. A painless guide to CRC error detection algorithms, 1993.

[14] J. Wolkerstorfer, E. Oswald, and M. Lamberger. An ASIC implementation of AES S-boxes. In *Proc. of the The Cryptographer's Track at the RSA Conference on Topics in Cryptology*, volume 2271, pages 67–78, 2002.

[1] Without the AES module

[2] Not applicable to LDR because it is targeted to an ALTERA device