Optimization of Latency of Temporal Key Integrity Protocol (TKIP) Using Graph Theory and Hardware Software Co-Design

Vilas V Deotare[1], Dinesh V Padole[2], Swati Shelke [3]

GHRCE, Nagpur, India
vilasdeotare@gmail.com[1],dvpadole@gmail.com[2],swati.wani@gmail.com[3]

Abstract:

Temporal Key Integrity Protocol (TKIP) [1] encapsulation consists of multiple-hardware and software block which can be implemented either software or hardware block or combination of both. This papers aims to design the TKIP technique using graph theory and hardware software co-design for minimizing the latency. Simulation results show the effectiveness of the presented technique over Hardware software co-design.

Keywords:

ROBUST SECURITY NETWORK ASSOCIATION, WIRED EQUIVALENT PRIVACY, TKIP,HARDWARE SOFTWARE CO-DESIGN.

1. INTRODUCTION

Cryptography is a part of communication used for higher security and it is done through different algorithm in network communications. The importance of cryptography is in the field of ecommerce and other network field. User can use same algorithm with a key of long sequence and at the receiving end with the same key it is decrypted and the message of encrypted is received. Key is always changes for higher security.

1.1 TKIP OVERVIEW

The TKIP is a cipher suite enhancing the WEP [1] protocol on pre-RSNA hardware. TKIP modifies WEP as follows:

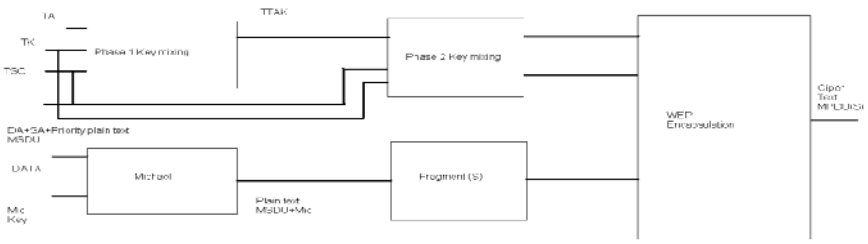


Figure 2 TKIP Block diagram

DOI : 10.5121/ijcseit.2013.3304

TKIP uses a cryptographic mixing function to combine a temporal key, the TA, and the TSC into the WEP seed.

1.2 TKIP MIC[2]

Flaws in the IEEE 802.11 WEP [2] design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer.

1.3 HARDWARE/SOFTWARE DESIGN ALTERNATIVES

The SoPC-based approach [3] offers new design space alternatives to explore. It is possible to consider design options that use software, dedicated custom hardware, or a mixture of both. Software implementations require less development time, but in many cases, a general-purpose processor will be too slow to perform all of the calculations using only software. To speed up the system, some frequently executed functions can be implemented in hardware in an SoPC design using the FPGA's logic.

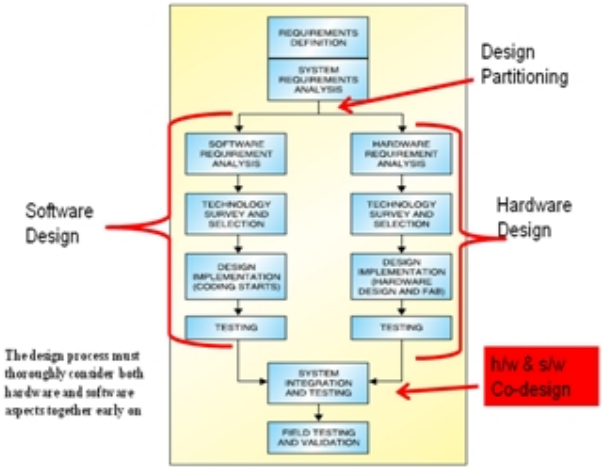


Figure 3 Flow of Hardware Software Codesign

SOPC hardware/software [3] design space tradeoffs as seen in Figure 4, for simple algorithms a hardware solution offers faster computation times, but it offers less flexibility since the hardware remains dedicated for that calculation and it may require a larger FPGA that consumes more power and increases system cost. Potential SOPC applications to implement in hardware in this region include pre-processing of real-time data with high sample rates, multimedia encoding and decoding, low-level communication protocols, and digital signal processing algorithms such as filters and FFTs. Hardware IP cores designed for FPGAs are available for many of these more common functions such as encoders/decoders, communication protocols, filters, and FFTs. The new hardware can also be designed using the traditional VHDL or Verilog FPGA synthesis tools. As the size of the hardware needed for implementation of more complex algorithms increases, the hardware starts to slow down, achieves diminishing performance levels, and becomes increasingly more difficult for designers to implement. This occurs due to increasing numbers of

gate delays in logic circuits and increases in the distance and communication time needed to transfer data values between hardware units. Pipelining and parallel processing techniques can be used to extend the useable range of hardware solutions, especially for non-recursive algorithms with a high degree of parallelism.[10] The system specification is divided Hardware/Software Co-design into a set of smaller pieces, so-called granules (e.g. basic blocks).

The remaining part of the work is elaborated in different sections as; Section II presents a review of related works. Section III describes the proposed mathematical model used for partitioning algorithms. Section IV describes the details about SOPC of Altera. Section V describes the parameters used in simulation and discusses the results. Finally, paper is concluded in section VII with future work.

2. RELATED WORK

Hardware software partitioning technique is commonly used for system integration [4].The different algorithms are commonly used to improve the performance. The validation is checked on system on programmable chip and the results are verified [5]. But the mathematical treatment on modular architecture is not defined. Based on mathematical modeling the advanced optimization algorithm is applied to improve the performance.

3. PROPOSED MATHEMATICAL MODEL

The modular block of TKIP are considered and is differed from hardware and software latency is considered as the unit value and based on each module is shown in the undirected graph. Initially consider one subset as a hardware block based on that calculation of HO, SP & HP is made through the algorithm. Using algorithm if it is proved that the selected subset HP is less than the SP, the subset is used to implement in hardware or else the subset is implement in software or using NIOS processor. An undirected simple graph G = (V,E), V = {q,. . . , un},

P1: HO, SO € R+ are given. Is there a P HW- SW partition so that HP <=HO and SP <=SO. [3]

P2: HO € R+ is given. Find a P HW-SW partition so that HP<= HO and SP is minimal. (Cost-constrained systems)

P3: SO € R+ is given. Find a P HW-SW partition so that SP<= SO and HP is minimal. (Systems with hard real-time constraints) [3]

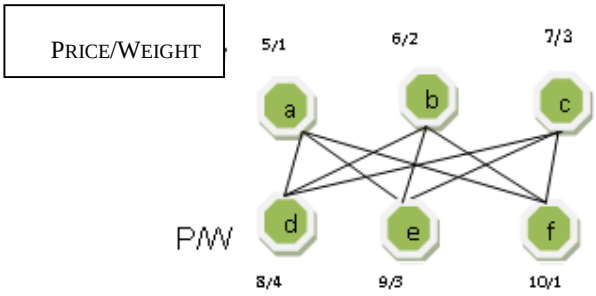


Figure 4 Complete Graph for a model

3.1 THEOREM 1. [3]

G = (V,E) , V = {v1,. . . ,Vn},

P is called a hardware-software (HW-SW) partition it is a bipartition of V: P = (VB, VS)

Vs = V ,VH U VS =V and VH ∩ VS=Φ The crossing edges are: Ep

Hardware cost HP=$\sum_{Vi\in VH}$ hi and software cost SP=$\sum_{Vi\in Vs}$ Si+$\sum_{(Vi,Vj)\in Ep}$ c(Vi, Vj) i.e. the software cost and the communication cost.

3.2 PARTITIONING ALGORITHM BASED ON VERTICES OR NODES OF THE BLOCK NOT EDGES

```
Procedure partition 1(n:integer
Price,weight[1..n]of integer
 X[1..n]: of integer
Var best[1..n] of  integer );
     Var:SP,HP,W,P, V.price, v.weight, v.node,
u.node, total u.price;
      Q :queue of node;
            begin
                  Initialize(Q);
                  V.price=0;
v.weight=0;
v.node=0;
A=0;
total u.price=0;
HP=0;
Asssume P=10,K=W=10;
Accept the value from user Total u.node;
Select subset from a graph;
enqueue(Q,V); //subset is stored in a queue
while notempty queue do
   dequeue(Q,v)
u.node=v.node+1;
u.weight=v.weight+w[u.node];//calculate price of selected subset
u.price=v.price+w[u.node]//calculate weight of selected subset
if u.weight<=w and u.profit>=k
 SO=W
end;
for i 0 to totalu.node
A=A+total u.price[i];
HO=A-K;
for j=0 to node.selected subset
HP=HP+ total u.price[j];
If k<=(A-u.price) and (H0>=(HP <=SP))
best=X //subset is selected;
end;
```

3.3 SOFTWARE SPECIFICATIONS

Once bit file is downloaded into FPGA, there will be interface to the computer through RS232. We will give the input data to the TKIP. Hardware will encrypt that data. Encrypted data will be given to the decryption block. Decrypted data will be same as the input data which will be stored in another file.
This way we will confirm the input data and decrypted data is same.

4. ALTERA'S SOPC BUILDER

The SOPC builder is used for developing the central processing unit or rather the architectural block for the system. The NIOS II of Quartus is used to implement Michel of TKIP.

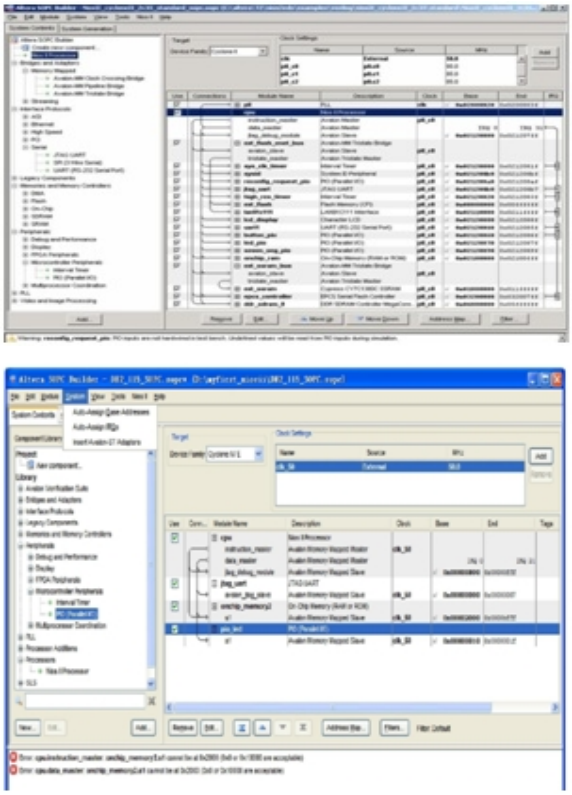


Figure 5 Snapshots of architecture using System on programmable chip

5 SIMULATION PARAMETERS FOR TKIP (MICHEL BLOCK)

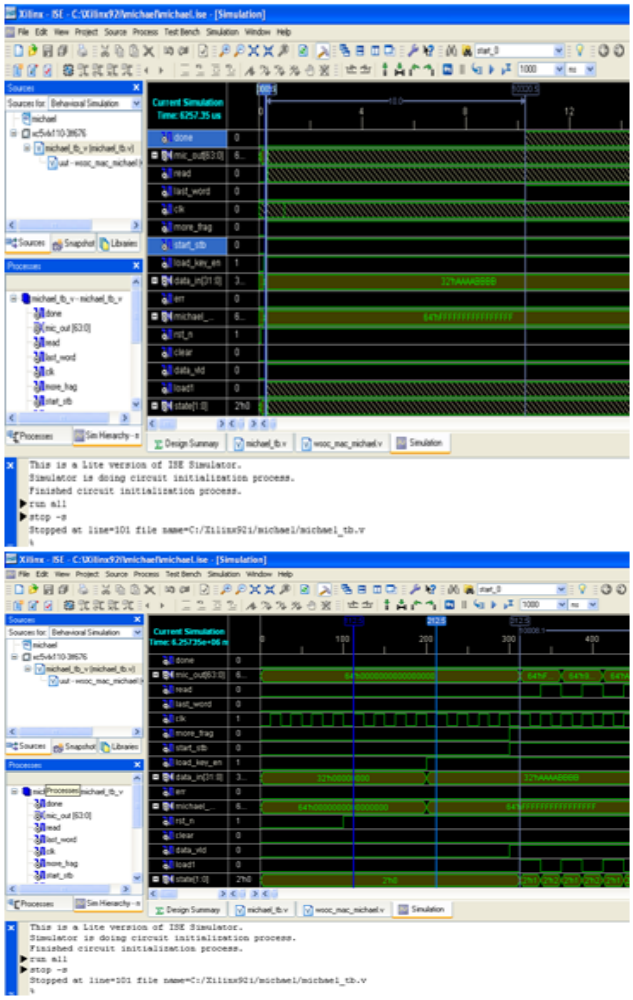
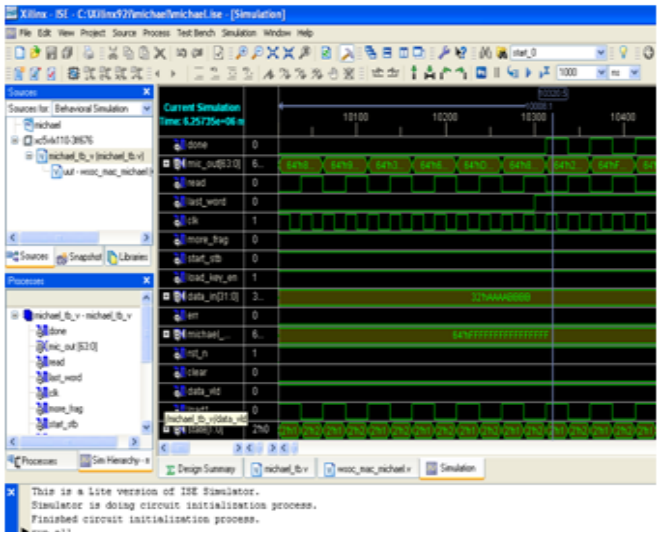


Figure 6 Simulation Waveform of Hardware and software of TKIP Michel block



DE2 Board Clock Frequency	Latency	
	TKIP Hardware	Proposed approach HW/SW Codesign
40 MHz (25 ns)	10us (400 cycles)	8us (320 cycles)

The above results show how the performance is improved using co-design and graph theory.

6. ACKNOWLEDGEMENT

This work is supported by GHRCE and University of Pune.

7. CONCLUSION

In this paper we have introduced mathematical treatment and the algorithm to decide the block usage in terms of hardware and software to get optimized latency.

REFERENCES

[1] IEEE Computer Society, Std 802.11i™-2004 pp43-56

[2] Yu-Tsang Chang1 "A Modularized FPGA-Based Embedded System Development Platform, (2010) A Hardware/Software Co-specification Methodology Based Upon OpenMP ". Pp 1697-1702,International Conference on Electronic Computer Technology The Application of Genetic Algorithm in Embedded System Hardware-software Partitioning Shijue Zheng,Yan Zhang

[3] Peter Arato, Sandor Juhasz, 201th Adam Mann, Andras Orban, David Papp "Hardware-software partitioning in embedded system design" pp 197-202,WISP 2003, Budapest, Hungnry 4-6 September, 2003.

[4] Yi Zou Zhenquan Zhuang Huanhuan Chen "HW-SW Partitioning Based on Genetic Algorithm" pp 627-633,0-7803-55 15-2/04, 02004 IEEE

[5] Andreas Gerstlauer, Member, IEEE, Christian Haubelt, Member, IEEE, Andy D. Pimentel, Senior Member, IEEE "Electronic System-Level Synthesis Methodologies "IEEE Transactions On Computer-Aided Design Of Integrated Circuits And Systems, Vol. 28, No. 10, October 2009

AUTHORS

Mr. Vilas V. Deotare completed Engineering from University of Pune. Post Graduation from BAMU Aurangabad. He is pursuing Doctorate from Nagpur University (India). He is a member of Professional bodies like ISTE, His Research of Interest in VLSI and D evelopment of algorithms in VLSI.

Mr. Dinesh Padole completed Engineering from RTM Nagpur, Post Graduation from CEDTI Aurangabad & awarded as Doctorate from RTM Nagpur University. He is associated with Various professional societies like Member IEEE, life member ISTE and CSI. His re search interest includes Multiprocessor /Multi-core systems, Embedded System Design. He worked as reviewer & Chaired technical sessions for several International conferences at India and abroad.

Miss Swati Shelke completed Engineering from University of Pune. She is pursuing Post Graduation from BAMU University of Pune. Her research I nterest in VLSI.