طراحی و پیاده سازی سخت افزاری دیواره آتش منطبق با کاربرد عملی در ماهواره های مخابراتی

امیر چگینی[۱]
کیان کیقباد[۲]، جعفر فهیم[۳]

چکیده

شبکه های ماهواره ای حوزه ای در حال گسترش است،که از زمان ساخت اولین ماهواره مخابراتی رشد قابل توجهی داشته است . با افزایش پهنای باند و تقاضاهای مخابراتی متحرک درآینده ، ماهواره ، انتخابی مناسب و منطقی برای ایجاد پهنای باند وسیعتر و پوشش جهانی ورای توانمندی های شبکه های زمینی به شمار می رود .این زمینه از فناوری افق روشنی در آینده خواهد داشت. بنابراین ارتباط شبکه آنها با شبکه زمینی و پروتکل ها بخش عمده ای از شبکه ای کردن ماهواره ها را تشکیل می دهد . هدف نهایی از شبکه سازی ماهواره ایجاد خدمات و کاربردهاست . در این میان برقراری امنیت اطلاعات ارسالی بین ماهواره و ایستگاه های زمینی دارای اهمیت فراوان است.یکی از عناصری که امنیت را در شبکه برقرار می سازد دیواره آتش است . ما دراین مقاله به ارائه یک دیواره آتش سخت افزاری و پیاده سازی آن با زبان VHDL برروی FPGA می پردازیم . سامانه طراحی شده در این مقاله دارای سرعت و کارآیی بالا ، مصرف توان کم و فضای اشغال شده اندکی می باشد . برای افزایش سرعت پردازش و کاهش حجم سیگنالینگ در ارتباط با حافظه های خارجی متصل شده به FPGA که چندین برابر کندتر از سرعت پردازش FPGA ها می باشند ، در این طراحی از حافظه های توکار (EMBEDDED) خود FPGA استفاده شده است و با تکنیک پایپلاینی نیز در هم آمیخته است و کارآیی و سرعت بالا در عین مصرف توان کم حاصل گردیده است . مزایای این معماری پیشنهادی ، گلوگاه های پردازشی مانند سرعت را برطرف می نماید و استفاده آن را در ماهواره های مخابراتی امکان پذیر می سازد .

کلید واژه

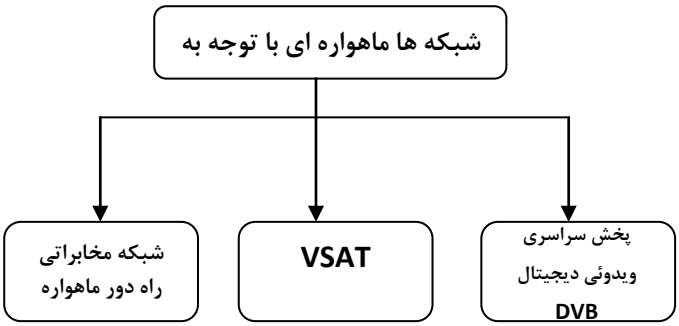
ماهواره های مخابراتی، دیواره آتش، پایپلاین، پیاده سازی سخت افزاری، VHDL ، FPGA.

۱.کارشناس ارشد الکترونیک، دانشگاه شهید بهشتی chegini@irsig.ir
۲. دانشگاه صنعتی مالک اشتر
۳. دانشکده مهندسی برق، دانشگاه علم وصنعت ایران
تاریخ دریافت:۸۹/۵/۲ تاریخ پذیرش: ۸۹/۶/۷

مقدمه

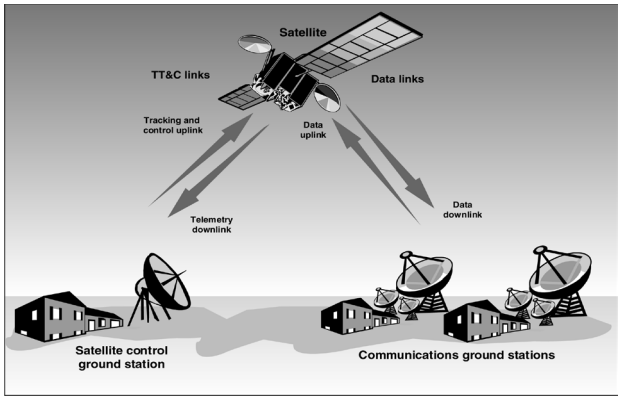
ماهواره های مخابراتی نقش مهمی در ارتباطات تلفنی و خدمات پخش سراسری TV و انتقال اطلاعات دارند . از این که ماهواره در خدمات پهن باند و اینترنت نقش مهمی دارد ، اطلاعات کمی در دسترس است .اما ماهواره ها در شبکه های ارتباطی نسل آینده نقش با اهمیتی خواهند داشت .[14] در سال های اخیر شبکه سازی ماهواره ها در مقایسه با دیگر فنّاوری های شبکه سازی ، پیشرفت چشم گیری داشته است. به طوری که امروزه کاربردهای فراوان استفاده از این ماهواره ها را در ارتباطات جهانی شاهد هستیم . نمونه آشکار این کاربرد ماهواره های ایریدیوم هستند .[15] شبکه های مخابراتی راه دور در ابتدا برای افزایش کیفیت انتقال صوت خدمات تلفنی ۳.۱ KHz طراحی ، توسعه و بهینه شدند. در نسل های اولیه شبکه های داده سرعت انتقال ترمینال های داده ، نسبتا پایین بود . علاوه بر خدمات تلفن ، شبکه ها می توانستند سیگنال های غیر صوتی مانند نامبر را پشتیبانی نمایند . در آن زمان شبکه های مخابراتی راه دور تا حدی می توانستند تقاضاهای مخابره داده را برآورده نمایند . به دلیل گسترش و پیشرفت شبکه ها به صورت ترمینال های شبکه ای ، شبکه های داده پرسرعت باید طراحی می شد تا تقاضای مخابرات داده را برآورده نماید . این مسئله منتهی به ساخت انواع شبکه ها با خدمات متفاوت گردید .[16] طبیعی است که با استفاده از این شبکه ها ، به مرور زمان تعداد خدمات ، تعداد کاربران و در نهایت ترافیک در شبکه های داده رفته رفته بزرگتر می شود. ترمینال های کاربر ظرفیت بالا و فنّاوری شبکه اجازه دادند تا خدمات مختلف مانند تلفن، داده، پخش سراسری و ارتباطات به هم نزدیک شوند . امروزه با ظهور ارتباطات ماهواره ای و مزایای این نوع ارتباط تقریبا برقراری تمامی خدمات داده توسط بستر ماهواره امکان پذیراست . اما برای یک شبکه ماهواره ای اتصال به همه شبکه های مختلف، خود یک چالش بسیار بزرگ است .[17] در اوایل دهه ۱۹۹۰ ، تحقیق و توسعه در مخابرات پهن باند مبتنی بر ATM و انتقال کابل فیبر نوری ، تقاضای زیادی را برای ارتباطات ارزان قیمت بین شبکه های ATM LAN خصوصی و عمومی (به این نوع شبکه ها جزایرATM نیز می گویند)، از طریق ماهواره به دنبال داشت . با این وجود ، در نواحی وسیعی به خصوص در نواحی دور افتاده و روستایی که خطوط زمینی گران و نصب و اداره آن ها پرهزینه است ، ماهواره به دلیل انعطاف و پوشش وسیع جهانی بهترین بستر ارتباط امن می باشد . [16] شبکه های ماهواره ای نیز مانند شبکه های زمینی ، رفته رفته ترافیک داده و به خصوص ترافیک اینترنت زیادی را تحمل می نمایند. اخیرا ترافیک اینترنت عمدتا به دلیل خدمات اینترنت و کاربردهایی مانند FTP،WEB و پست الکترونیکی است .

همگرایی اینترنت و مخابرات راه دور منجربه ایجاد صوت روی IP(Voice Over IP) ، ویدئو کنفرانس روی IP و خدمات پخش سراسری روی IP شده است . بنابراین انتظار می رود بسته های IP کلاس های بیشتری از خدمات و کاربردها را روی شبکه های ماهواره حمل کنند .IP به این دلیل طراحی شد تا مستقل از هر فنّاوری شبکه بتواند با همه فنّاوری های شبکه موجود قابل انطباق باشد. در شکل ۱ سه نوع فنّاوری شبکه سازی ماهواره ای با توجه به IP نشان داده شده است . امروزه چالش امنیت در محیط های ماهواره ای یکی از موانع اصلی در استفاده گسترده از کاربردهای ماهواره ای چندبخشی IP است . مشکل اصلی این است که استراق سمع و مزاحمت فعال خیلی ساده تر از شبکه های زمینی ثابت و متحرک است و این به دلیل پخش سراسری ماهواره است . [13] چون ماهواره با کاربران مختلف زمینی در تماس است ، ممکن است کاربران مزاحمی برای ایجاد ناامنی در شبکه مخابراتی مبتنی بر ماهواره سعی در تداخل امنیتی این سامانه ارتباطی نمایند. (شکل ۲) با توجه به افزایش روز افزون خدمات ماهواره ای تجاری نظیر شبکه های اینترنت خصوصی[15] نیاز به امن بودن بستر های ارتباطی بیش از پیش احساس می شود . از طرفی شبکه های مدرن سعی در جدایی وظایف هر قسمت از شبکه از قسمت دیگردارند.[۱۷] با توجه به مدل ۷ لایه ای OSI ، یک سیگنال صوت دیجیتالی به قطعات کوچکی برای پروتکل حمل بلادرنگ (RTP) در لایه کاربرد ، پروتکل داده گرام (UDP) در لایه حمل و سپس پروتکل اینترنت (IP) درلایه شبکه تقسیم می شود. در تمامی این لایه ها با توجه به پیشرفت نرم افزاری و سخت افزاری ، امکان نفوذ و تغییر وجود دارد ، اما در لایه فیزیکی کمترین احتمال برای تغییر اطلاعات توسط نفوذگران وجود دارد . بنابراین نیاز به ابزاری برای برقراری امنیت فضای تبادل اطلاعات(افتا) در ارتباطات ماهواره ای احساس می شود .



شکل ۱- سه نوع فنّاوری شبکه سازی ماهواره ای با توجه به IP

دیواره آتش یکی از وسایلی است که برای برقراری امنیت در شبکه استفاده می شود. اگر چه فنّاوری دیواره‌های آتش[1] جوان است و تازه شکل گرفته اما بسیار سریع رشد کرده و در کمتر از بیست سال تحولات زیادی را پشت سر گذاشته است . از فایروال برای جداسازی و امنیت شبکه های داخلی در مقابل شبکه های خارجی و نا امن استفاده می شود. با پیاده سازی فنون های پالایش بسته ، بخشی از وظایف یک دیواره آتش را می توان به روترها یا مسیریاب های لب مرز واگذار کرد. ولی روترها به تنهایی قادر به انجام کل وظایف یک دیواره آتش نیستند و امروزه استفاده از دیواره آتش ها آنها در شبکه های کامپیوتری امری اجتناب ناپذیر است. دلیل ناکافی بودن پالایش بسته در روترهای لب مرز دو چیز است: یکی اینکه اصولا تمامی فنون هایی که در دیواره آتش ها پیاده سازی می شوند، در روترها قابل اجرا نیست و گذشته از آن، رعایت اصل دفاع لایه به لایه (یا دفاع در عمق) که انجام محافظت در بیش از یک لایه را بیان می کند. شکل ۳ نشان دهنده این موضوع است.



شکل ۲- ارتباط ماهواره مخابراتی با کاربران زمینی

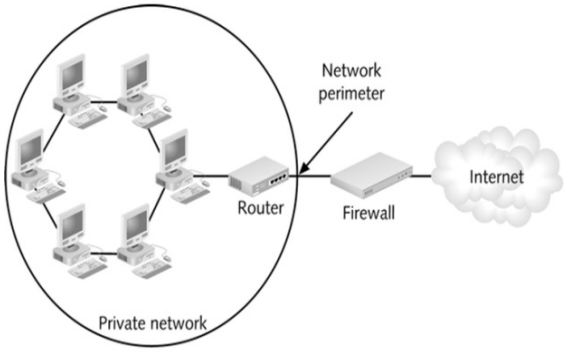
انجمن NCSA (Network Computer Security Association) تعریف زیر را از دیواره‌های آتش ارائه داده است.“دیواره آتش یک سامانه یا ترکیبی از چندین سامانه است که یک سری محدودیت را بین دو یا چند شبکه اعمال می‌کند. ” دیواره آتش ها عملا یک سری پالایشگر بسته هستند، که با تعریف یک سری قوانین ، مشخص می کند کجا و چه موقعی بسته ها باید عبور کنند و یا BLOCK شود.[۵] اما خود طبقه بندی بسته نیز دارای مشکلاتی هستند که در [7-9] بررسی شده اند. هم اکنون روترها و فایروال های شبکه به طور افزاینده ای از مدارهای طراحی شده خاص برای طبقه بندی بسته (شکل ۴) استفاده می نمایند تا علاوه بر رسیدن به سرعت و کارآیی بالایی

1.Firewall

برای پردازش بسته ها در سخت افزار ، به طور همزمان ، به استقلال از نرم افزار و پردازنده مرکزی دست یابند .[1] اگر P مجموعه ای از بسته های ورودی به سامانه دیواره آتش در نظر گرفته شود و S مجموعه ای متناهی از قواعد امنیتی باشد داریم:

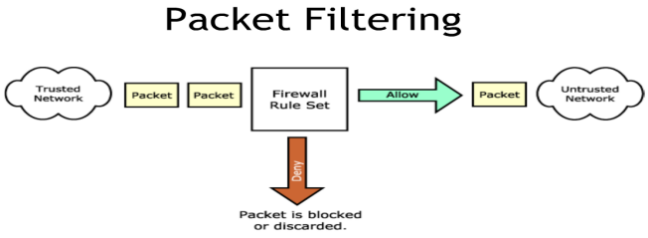
$$X= F (P, S)$$

F تابع عملکرد دیواره آتش و X نتیجه تحلیل بسته (شامل سه حالت فوق) خواهد بود.



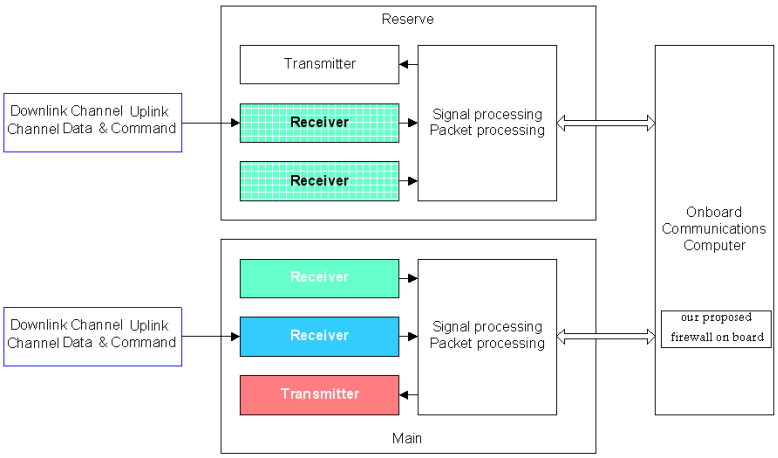
شکل۳–حفاظت شبکه داخلی از شبکه های نا امن توسط فایروال

هنگامی که می خواهیم به سرعتهای بالا در پردازش بسته ها دست یابیم، پیاده سازی الگوریتم های طبقه بندی اطلاعات در نرم افزار امکان پذیر نیستند .[10]



شکل۴- عملکرد دیواره آتش با پردازش بسته

نوعی از دیواره آتش ها هستند که به طور مجزا از سامانه اصلی فعالیت نموده و منابع سامانه اصلی را اشغال نمی نمایند . با وجود المان هایی نظیر FPGA و پیشرفت روزافزون آن ها ، امروزه طراحی و پیاده سازی این نوع سامانه های توکار به بحث مهمی در دنیای طراحی دیجیتال تبدیل شده است. روترها و دیواره آتش های سخت افزاری که دارای سخت افزارهای خاص منظوره برای مکان ها و شرایط مختلفی هستند برای انجام عمل پردازش بسته ها خیلی سریع تر از سایر روش های نرم افزاری می باشند [۲] ، بنابراین امروزه پیاده سازی عناصر والمان های شبکه بر روی سخت افزار و بخصوص سخت افزارهایی مانند FPGA که دارای قابلیت پیکربندی مجدد هستند برای رسیدن به کارآیی و سرعت بالا و مصرف توان کم دارای اهمیت می باشند . در سال های اخیر نیاز به سامانه های امنیتی که پرسرعت و در عین حال قابل گسترش(Extensible) ، قابل نگهداری (Maintainable) و انعطاف پذیر (Flexible) باشند، باعث شده است شرکت های فعال در زمینه امنیت در تکاپوی یافتن راه حل هایی مناسب و کاربردی برای پاسخگویی به این نیازها باشند. اما دیواره آتش های کنونی دارای مصرف توان بالا و ابعاد بزرگ هستند و برای کاربرد در مخابرات ماهواره ای و بر روی ماهواره مقرون به صرفه نیستند . در این مقاله روشی برای طراحی و پیاده سازی دیواره آتش سخت افزاری بر روی FPGA ارائه شده است که دارای قابلیت اطمینان بالا ، مصرف توان کم ، وزن پایین و ابعاد کوچک است . در ادامه مقاله درقسمت ۲ ، به بیان روش پیاده سازی این دیواره آتش و بیان معماری آن پرداخته و فرض های خود را درطراحی ارائه می نماییم سپس در قسمت ۳ الگوریتم بیان شده را به زبان VHDL می نویسیم و آن را با ابزار سنتز و شبیه ساز های رایج برای زبان های توصیف سخت افزار شبیه سازی نموده و به صورت عملی آن را روی سخت افزار پیاده سازی می نماییم و نتایج حاصل را بیان می کنیم . برای مشاهده کارآیی این معماری نرم افزار (Quartus II) شبیه ساز و سنتزکننده کدهای VHDL ، از شرکت Altera را استفاده می نمائیم . دیواره آتش پیشنهادی را می توان بر روی برد پردازشی و مخابراتی ماهواره قرار داد . محل قرار گیری این دیواره آتش بر روی برد پردازشی ماهواره در شکل ۵ نشان داده شده است .



شکل ۵- محل قرارگیری دیواره آتش سخت افزاری پیشنهادی

طراحی سخت افزاری دیواره آتش

یک استاندارد مناسب را برای انجام این پیاده سازی در نظر می گیریم. برای این کار طرح و برنامه را به طورکلی ماژولار می نویسیم این مسئله دارای مزایایی می باشد .

فرضیات

فایروال ارائه شده در این مقاله دارای قابلیت های زیر می باشد :

۱- بسته ها به صورت سریال و با چارچوب مشخصی به یکی از پایه های ورودی سخت افزار وارد می شوند. بسته های IP ورودی دارای چارچوب نشان داده شده در جدول شماره ۱ هستند :

Preamble	State of frame Delimiter	MAC destination	MAC Source	Source Address	Destination Address	Source Port	Destination Port	DATA	Interframe Gap
7 bytes	1 byte	6 bytes	6 bytes	4 bytes	4 bytes	16 Bits	16 Bits	256 Bits	X bytes (1)

جدول ۱- بسته IP ورودی به سامانه

۲- سخت افزارطراحی شده باید با شناسایی هر قسمت از این بسته IP ، درصورت تعریف در جداول آن را BLOCK نماید و هرگاه بسته هیچ مشکلی نداشت آن را به صورت سریال به پورت خروجی راهنمایی کند . [۳,۴] سامانه ارائه شده در این طراحی اگر تطابقی با اطلاعات جدول ها وجود داشته باشد، فرمان BLOCK را صادر می نماید . جدول مورد استفاده در این طراحی که در داخل

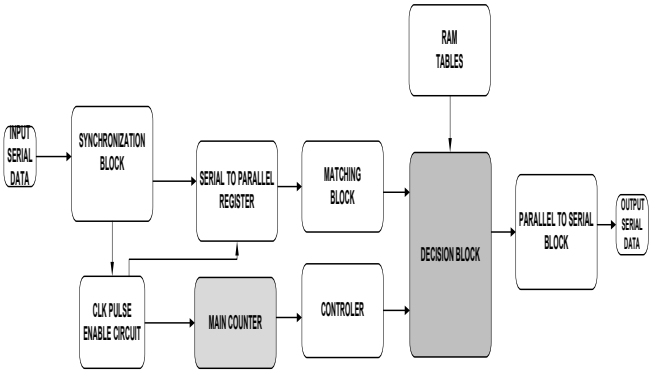
خود FPGA قرار می گیرند، در جدول ۲ نشان داده شده است. به دلیل این که ما ۵ قسمت از این بسته IP را در این سخت افزار بررسی می کنیم به ۵ جدول نیاز داریم .

جدول۲ - جدول قوانین مربوط به آدرس های مبدا و مقصد

ROW	Address NUMBERs (32 BITs)
1	10001010010011001111000101001001
2	10110000111100001010001010110011
3	11110001011010011010100010110011
....	.....
N	10101010100100111010100010001010

روند طراحی

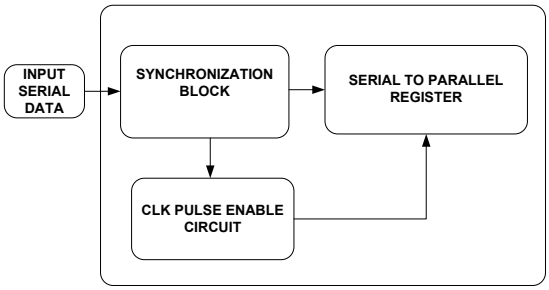
بلوک ها و ماژول هایی که برای این طرح در نظر گرفته شده، بصورتی است که فرضیات این پروژه را برآورده می نمایند . این بلوک ها به صورت کلی در شکل شماره ۶ نشان داده شده اند :



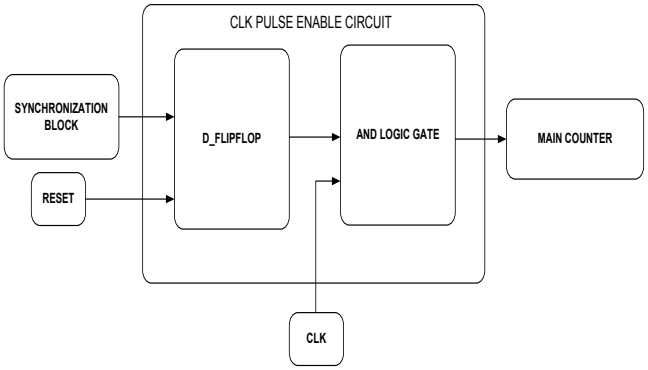
شکل ۶- نمایش بلوک های داخلی معماری دیواره آتش ارائه شده

لزوم داشتن ماژول همزمانی نشان داده شده در شکل شماره ۷ به خاطر این است که اگر سخت افزار شروع به کار کرد و بسته ای دریافت نشد، مدار هیچ عملی را انجام نمی دهد. اما اگر بسته ای روی پایه ورودی دریافت شد، آن را شناسایی و سپس کل سامانه را راه اندازی می نماید . پس تا هنگامی که هیچ بسته ای دریافت نشود، مدار سخت افزاری کار نخواهد کرد . بلوک دیاگرام مدار فعال ساز

پالس ساعت ورودی به سامانه در شکل شماره ۸ نشان داده شده است . این قسمت از این سامانه نقش مهمی در پایین بودن مصرف توان این معماری ایفا می نماید . هنگامی که هیچ بسته ای روی خط ورودی سامانه نیست و هنوز همزمانی اتفاق نیافتاده است این ماژول مانع عبور پالس ساعت به سایر بلوک های سامانه شده و عملا اتلاف توان دینامیک(DYNAMIC POWER LOSS) را کاهش می دهد .



شکل ۷- ارتباط ماژول همزمانی با سایر بلوک ها و نقش آن



شکل ۸- اجزای ماژول فعال ساز پالس ساعت ورودی به سامانه

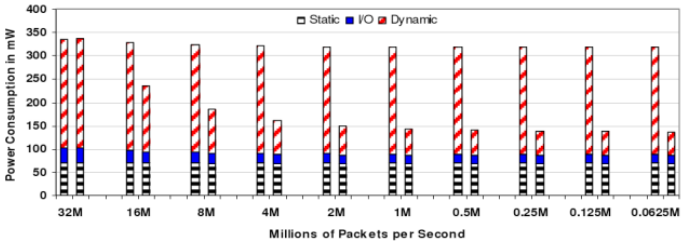
پیاده سازی سخت افزاری و مقایسه نتایج

در این قسمت از مقاله برای درک بهتر و عملی تر طرح بیان شده در قسمت ۲ را با زبان استاندارد VHDL می نویسیم و در ادامه نتایج حاصل از شبیه سازی و سنتز آن را ارائه می نماییم .

نتایج شبیه سازی و بررسی توان مصرفی

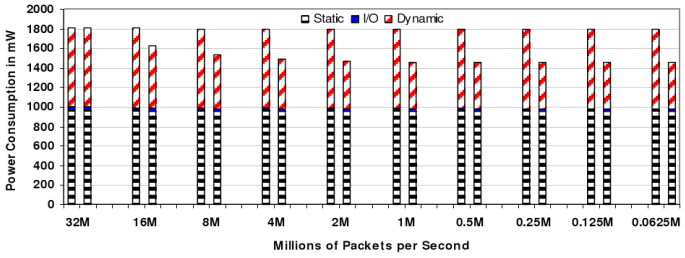
در [۶] سامانه ی معرفی شده است که با معماری موازی خود می تواند توان کمتری را نسبت به

مشابه خودکه دارای معماری غیر موازی است ، مصرف نماید و این مصرف توان بر روی سه خانواده CYCLONE III و STRATIX III و CYCLONE II از شرکت ALTERA پیاده سازی شده اند . دراین قسمت از مقاله با ارائه و مشاهده نتایج حاصل از سنتز ادعا می کنیم که با همان نرم افزار استفاده شده در [6] ، (QUARTUS II) ، به یک سامانه توکار ولی با مصرف توان کمتر و با فرکانس کاری بیشتر رسیده ایم . نمودارهای شکل ۹ این مسئله را نشان می دهند : نمودار الف و ب از مرجع [6] می باشند . همانطوری که ملاحظه می شود توان استاتیک برای خانواده CYCLONE III حدودmW 70و برای خانواده STRATIX III حدود 980mW می باشد . نتایج حاصل از سنتز و مصرف توان در طراحی ارائه شده در قسمت ۲ در جدول شماره ۳ نشان داده شده اند .



Power figures for Cyclone 3 implementation

شکل۹- الف- مصرف توان برای معماری موازی برای خانواده CYCLONE در[۶]



Power figures for Stratix 3 implementation

شکل ۹- ب- مصرف توان برای معماری موازی برای خانواده STRATIX در [6]

جدول ۳ – نتایج میزان مصرف توان حاصل از سنتز

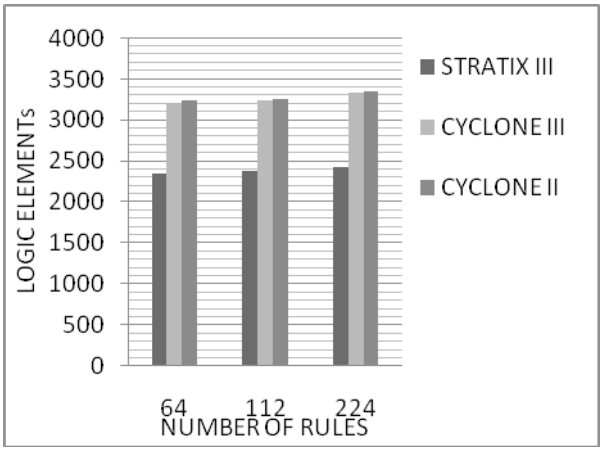
FAMILY	NUMBER OF RULES	POWER CONSUMPTIONS mW
STRATIX III	64	610.2
	112	623.19
	224	625.6
CYCLONE III	64	34.8
	112	35.31
	224	36.4
CYCLONE II	64	17.2
	112	18
	224	18.7

همانطور که ملاحظه می شود مصرف توان نسبت به مرجع [6] کاهش یافته است در صورتی که برای خانواده STRATIX III فرکانس کاری حدود150.7MHz می باشد ولی فرکانس کاری در [۶] 128 MHz است . بنابراین هم در فرکانس کاری و هم در مصرف توان ، این مدار نسبت به معماری موازی ارائه شده در [6] دارای مزیت می باشد . این مزیت یکی از عمده ترین مزایای استفاده از این دیواره آتش سخت افزاری در سامانه دریافت و ارسال اطلاعات بر روی ماهواره [1] می باشد . مکان قرارگیری دیواره آتش پیشنهادی در شکل ۵ نشان داده شده است .

نتایج شبیه سازی و سنتز روی مساحت اشغال شده

با سنتز و پیاده سازی سخت افزاری بر روی این سه خانواده از شرکت ALTERA نتایج قابل پیش بینی ملاحظه گردید. همانطوری که در شکل ۱۰ نشان داده شده است، با افزایش تعداد قوانین میزان حجم مصرفی تراشه ها نیز افزایش می یابد و این مسئله قابل پیش بینی است. با افزایش سطح اشغالی تراشه و استفاده از عناصر منطقی بیشتر ، طبیعی است که برای اجرای یک الگوریتم نیازمند مصرف توان بیشتری می باشیم .

1.Data-Transmission System



شکل ۱۰- مقایسه میزان مصرف منابع داخلی برای سه خانواده

نتایج سنتز و محیط اشغالی نشان می دهد که معماری پیشنهادی فضای کمی را از سخت افزار FPGA اشغال می نماید. و این مسئله برای داشتن یک دیواره آتش بر روی یک تراشه SOC[1] با توجه به محدودیت های وزنی و حجمی و توان مصرفی محموله های مخابراتی بسیار مناسب می باشد . در مراجع [18]و[19] ، قوانین امنیتی معمولا در خارج از سخت افزار مرکزی قرار می گیرند و باعث افزایش مدت زمان پردازش اطلاعات و دسترسی به حافظه می شوند . از طرفی با قرار گیری قوانین امنیتی بر روی حافظه های خارجی امنیت سامانه نیز به شدت کاهش می یابد . به خاطر این واقعیت که کارآیی حافظه ها خیلی کمتر از پردازنده ها است ، زمان بین درخواست داده ای توسط پردازنده و لحظه معتبر شدن داده ها در خروجی حافظه نسبتا زیاد و طولانی است . از این رو در این معماری ها مدت زمان زیادی از پردازنده صرف همزمانی و دریافت اطلاعات از حافظه می شود. در حالی که در معماری پیشنهادی به خاطر استفاده از حافظه های داخلی FPGA سرعت پردازش به مراتب بالاتر از این معماری ها است .

نتیجه گیری

در این مقاله معماری و فنونی برای طبقه بندی اطلاعات و تصمیم گیری بر روی بسته های IP ارائه شد. معماری پیشنهادی بر روی FPGA های شرکت ALTERA سنتز و پیاده سازی شد. همانطوری که ملاحظه شد می توان با استفاده از ارسال کدهای جدیدی برای FPGA که حاوی

1.System on Chip

قوانین جدیدی هستند آن را بلادرنگ برنامه ریزی نمود . مشاهده شد که با افزایش تعداد این قوانین ، فرکانس کاری مدار کاهش و میزان استفاده از عناصر منطقی داخلی FPGA ها افزایش می یابد . ما با ارائه این معماری نوین نشان دادیم که معماری پیشنهادی دراین مقاله هم دارای سرعت بالا حدود 150 MHz و هم مصرف توان کم نسبت به معماری های ارائه شده در[6,11,5] می باشد. با استفاده از این معماری می توان سامانه ای واحد بر روی یک تراشه با مصرف توان کم ، ابعاد کوچک و وزن کم که قابل استفاده برای برقراری امنیت اطلاعات تبادلی در سامانه های مخابرات ماهواره ای و بر روی برد ماهواره است را در اختیار داشت .

مراجع

1.J. W. Lockwood, J. S. Turner, and D. E. Taylor, “Field programmable port extender (FPX) for distributed routing and queuing” , in FPGA, 2000, (Monterey, CA) - (144 – 137) , Feb. 2000.

2. J. W. Lockwood , “ Platform and methodology for teaching design of hardware modules in internet routers and firewalls” , 2001 , IEEE .

3. Marcus J. Ranum, “Thinking About Firewalls,” proceedings of the Second World Conference on Systems Management and Security (SANSII), 1993.

4. Gajanan S. Jedhe, Arun Ramamoorthy, and Kuruvilla Varghese “A Scalable High Throughput Firewall in FPGA” 978-0-7695-3307-0/08-2008 IEEE DOI 10.1109/FCCM.2008.31

5. Darrell Laturnas , Ron Bolton “Dynamic Silicon Firewall” 0-7803-8886-0/05©2005 IEEE CCECE/CCGEI, Saskatoon, May 2005 .

6. Alan Kennedy , Xiaojun Wang , Zhen Liu , Bin Liu “Low Power Architecture for High Speed” ANCS’08, November 6–7, 2008, San Jose, CA, USA Copyright 2008 ACM 978-1-60558-346-4/08/0011 .

7. P. Gupta and N. McKeown, “Packet classification using hierarchical intelligent cuttings,” IEEE Micro, vol.20, no. 1, pp. 34-41, 2000.

8. F. Baboescu and G. Varghese, “Scalable packet classification,” IEEE/ ACM Trans. Netw., vol. 13, no. 1 pp. 2-14, 2005.

9. F. Baboescu, S. Singh, and G. Varghese, “Packet classification for core routers: Is there an alternative to CAMs?” in IEEE INFOCOM, 2003, pp. 53-63.

10. A. Kennedy, D. Bermingham, X. Wang, B. Liu. “Power Analysis of Packet Classification on Programmable Network Processors”. 2007 IEEE Intl Conf on Signal Processing and Communications, Dubai, 24-27 Nov, pp.1231-1234.

11. A. Kinane, “Energy Efficient Hardware Acceleration of Multimedia Processing Tools” PhD thesis, Dublin City University, May 2006.

12. IEEE 802.11a ,1999 Edition (ISO/IEC 8802-11:1999)IEEE standards for information Technology telecommunication and information Exchange between Systems part 11: wireless LAN medium Access Control and Physical layer specification.

13. J. Qaddour and R.A.C Barbour,“Evolution to 4G wireless : problems, solutions, and challenges”, computer system and applications, 2005 .the 3rd ACS/IEEE International Conference,2005.

14. Brady, M. And M. Rogers, ”Digital Video Broadcasting Return Channel Via Satellite (DVB-RCS) Background Book“, Nera Broadband Satellite As (NBS), 2002.

15. www.iridium.com

16. Akyildiz, i.f. et al., satellite ATM networks: a survey, IEEE communication 35(7):30-43, 1997.

17.Yegenoglu, F., Alexander, R. and Gokhale, D., “An IP Transport And Routing Architecture For Next-Generation Satellite Networks”, IEEE network,14(5):32-8,2000 .

18. Ayman Kayssi, Louis Harik, Rony Ferzli, and Mohammad Fawaz , “Fpga-Based Internet Protocol Firewall Chip”, 0-7803-6542-9/00 2000 IEEE.

19.John W Lockwood, “Platform And Methodology For Teaching Design Of Hardware Modules In Internet Routers And Firewalls”, 0-7695-1156-2/01 2001 IEEE.