Securing InfiniBand Networks with the Bluefield-2 Data Processing Unit

Noah Diamond[1], Scott Graham[1] and Gilbert Clark[2]
[1]Air Force Institute of Technology, Wright-Patterson AFB, USA
[2]Sensors Directorate, Air Force Research Laboratory, Wright-Patterson AFB, USA
Noah.Diamond@afit.edu
Scott.Graham@afit.edu
Gilbert.Clark.2@us.af.mil

Abstract: Interest in securing InfiniBand networks with encryption is growing. However, the performance benefit realized by InfiniBand's use of Direct Memory Access (DMA) to bypass the kernel and avoid intervention from host Central Processing Units (CPUs) is at odds with IP datagram encryption techniques. Encryption forces data through the CPU before transmission and decryption, incurring multiple clock cycles. The Bluefield-2 Data Processing Unit (DPU) is Nvidia-Mellanox's latest system on chip that combines a high-performance, programmable processor, network interface card (NIC), and flexible hardware accelerators. This research characterizes the Bluefield-2's capability to accelerate IPsec encryption in hardware. Results show that the Bluefield-2's hardware accelerators are capable of supporting a secure IPsec tunnel with a throughput of nearly 16 Gb/s. Offloading IPsec encryption operations to the hardware accelerators on the Bluefield-2 is a promising method for adding confidentiality, integrity, and authentication to InfiniBand networks.

Keywords: Cybersecurity, InfiniBand, Bluefield-2 DPU, Hardware Acceleration, IPsec

1. Introduction

InfiniBand is an industry leading high-bandwidth, low-latency interconnect for hyperscale datacenters and high-performance computing (HPC) clusters. Previous research identified that native InfiniBand clear text key exchange makes the IBA vulnerable to man-in-the-middle (MiTM), denial of service (DoS), and replay attacks (Lee and Kim, 2007). These vulnerabilities have mostly been ignored during InfiniBand's development because datacenters and HPCs are assumed to be physically secure. However, interest in securing InfiniBand with encryption is growing. While methods of encryption like IP security protocol (IPsec) can increase data confidentiality, integrity, and authentication, encryption is inherently computationally demanding and increases the compute load placed on central processing units (CPUs). Data processing units (DPUs) are a new class of programmable processor designed to assist CPUs and meet the tremendous computational demand found in hyperscale datacenters and HPCs. DPUs are a system on chip (SoC) that combines a high-performance, programmable processor, network interface card (NIC), and flexible hardware accelerators. This additional hardware is capable of supporting network management and security applications while requiring little interaction from host CPUs. They are specifically designed for processing datacenter software for virtualization, networking, storage, and security. Although previous research suggested that DPU processors are capable of line-rate encryption, Nvidia Mellanox's Inova Flex SmartNIC and Bluefield-1 DPU were not inherently able to accelerate offloaded IPsec encryption operations in hardware. This research seeks to characterize the capability of Nvidia Mellanox's Bluefield-2 DPU's hardware accelerators to encrypt Ethernet traffic.

2. Background

2.1 InfiniBand Architecture

The InfiniBand Architecture (IBA) is a low-latency, high-bandwidth fabric architecture for server input/output (I/O) and inter-server communication. It was developed by the InfiniBand Trade Association (IBTA) to meet the growing demand for a high-performance interconnect capable of providing low-latency and high-bandwidth in hyperscale data centers and HPCs. InfiniBand provides a standard of reliability, availability, performance, and scalability that far surpasses that of bus-oriented I/O architectures (Pfister, 2001). InfiniBand leads the industry in both chassis backplane applications as well as in external copper and fiber optic connections (*InfiniBand Trade Association*, 2021). Six out of the top ten supercomputers in the world use IBA as their core interconnect and it is currently in use in thousands of datacenters, HPC clusters, and embedded applications. (Strohmaier *et al.*, 2021).

Widespread demand for high-performance, scalable, and reliable networks in a diverse set of applications has promoted interest in InfiniBand networks. Amidst the rapid development of the IBA, developers have paid more

attention to performance and cost efficiency than to security. Lee and Kim (2007) and Rothenberger et al. (2021) state that there are numerous security loopholes within the IBA that have been revealed and, consequently, the design of secure clusters has recently surfaced as a critical issue.

2.2 Bluefield-2 DPU

The Nvidia-Mellanox's Bluefield-2 DPU combines a ConnectX-6 DX network adapter with an array of Advanced RISC Machine (ARM) cores and hardware accelerators. The Bluefield-2 operates as an independent system that communicates with its host over 16 lanes of fourth generation Peripheral Component Interconnect express (PCIe), offering a theoretical transfer rate of 256 Gbps. Alternatively, the card may be used in systems with third generation PCIe, but the maximum theoretical transfer rate is substantially lower at only 128 Gbps. The card itself includes two multi-function 100 Gbps ports, 16 GB of local Double Data Rate 4 Random-Access Memory (DDR4 RAM), 8 ARM Cortex A72 processors, and local persistent storage. The transfer rate of the Bluefield-2's DDR4 RAM is 3200 T/s. The card runs a tailored version of Linux provided by NVIDIA Mellanox allowing developers to both develop new applications and deploy existing applications directly onto the card itself. These applications can process and modify traffic before it is ever seen on the host. The Bluefield-2s, therefore, can host a wide variety of applications and services for networking, storage, and security ('NVIDIA BLUEFIELD-2 DPU DATA CENTER INFRASTRUCTURE ON A CHIP', 2021).

Even though these desirable properties have been established, the high data throughput supported by the card can quickly overwhelm its available processors and memory should all traffic be directed through Linux itself. To address this, the card offers several different hardware offload and acceleration features that can operate directly on network traffic without routine involvement from the ARM CPU. This allows the ARM multi-core CPU to orchestrate the hardware to perform operations on traffic at high rate instead of rather than trying to process all the traffic directly.

2.3 IPsec

This paper focuses on a unique IPsec hardware acceleration feature on the Bluefield-2. IPsec is a protocol that is commonly used to provide security at the network layer. This research uses Encapsulation Security Payload (ESP) protocol to provide confidentiality, integrity, and authentication at the network layer (Kurose and Ross, 2017).

2.3.1 IPsec Datagram

Figure 1. shows the format of an IPsec datagram using ESP and tunnel mode. The IPsec datagram still meets the requirements of an IPv4 datagram. The IPsec datagram's payload consists of an ESP header, the original IP datagram, an ESP trailer, and an authentication field.

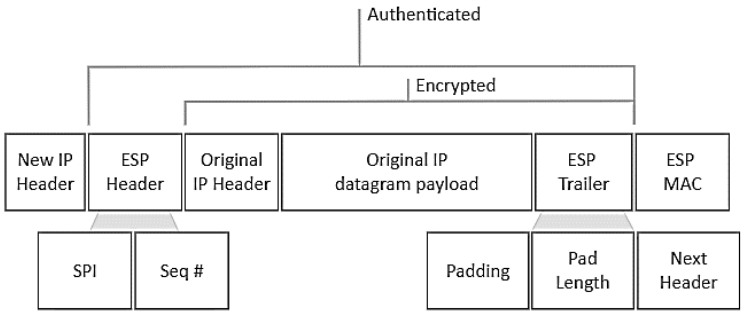

Figure 1: IPsec datagram format (Kurose and Ross, 2017)

These headers and trailers create additional overhead and must be accounted for when configuring the Maximum Transmission Unit (MTU) of network interfaces. In total, the protocol suite can add over 100 bytes of overhead to IP datagrams. As a result, care must be taken to ensure that the payload, when combined with the IPsec headers, does not exceed the MTU of the network link. If it does, the resulting packets could be fragmented or dropped. Further, to optimize operation, the maximum segment size (MSS) of any TCP streams traveling over an IPSec tunnel should also account for the reduced MTU.

2.4 Tools

2.4.1 iPerf3

iPerf3 actively measures the maximum achievable bandwidth of IP datagram networks. iPerf3 provides various tuning options and allows parameters like transport protocol, MSS, and multi-threading to be selected during bandwidth tests. An iPerf3 server and client are run on the workstations during this research to record real throughput measurements.

2.4.2 Libreswan

Libreswan is a free software implementation of IPsec that supports customed configurations. This research uses symmetric key encryption. Keys are defined by the user and located in Libreswan IPsec tunnel configuration files.

2.4.3 Top

Top is a Linux command line tool used to show real-time summary of the system which includes CPU utilization and Luniux processes. The real-time statistics provided by top are useful for verifying that the Bluefield-2s are the bottleneck in the network rather than the host CPUs generating traffic.

2.4.4 tcpdump

Tcpdump is a free command-line packet analyzer. Tcpdump is useful for monitoring network traffic, and is used in this research to verify the network is properly configured. For example, this research studies the effect encryption has on network performance. Tcpdump displays the type of packet an interface is receiving and an ESP header indicates that the traffic is encrypted.

2.4.5 R

R is a free statistical computing and graphics software. The figures and statistical analysis in this research were generated using R.

2.5 Related work

2.5.1 A Comprehensive Framework for Enhancing Security in InfiniBand Architecture

Prior research investigated security vulnerabilities within the IBA and proposed a comprehensive security framework for securing the IBA. Lee and Kim identified that most of the vulnerabilities found in InfiniBand networks stem from InfiniBand's plain text key management scheme. In response, they proposed light weight encrypted key management schemes that add confidentiality, authentication, and availability to InfiniBand networks. For confidentiality and authentication, Lee and Kim created a partition-level and queue-pair (QP) level secret key management scheme. Further, they demonstrated how IBA accommodates GCM with minor modifications to the IBA specification. GCM combines encryption and authentication by using Galois Field (GF) multiplication and counter (CTR) mode encryption. For availability, Lee and Kim proposed a stateful ingress filtering (SIF) system which is enabled only when there is a DoS attack using invalid IBA keys.

Lee and Kim ran a variety of simulations to test their hardware-based encryption approach against a variety of attacks. The results showed marginal performance degradation due to the adoption of encryption and authentication algorithms. Future research could use the Bluefield-2 to implement Lee and Kim's secure key management scheme.

2.5.2 AFIT: Securing InfiniBand

Schmitt was the first master's student at the Air Force Institute of Technology (AFIT) to study InfiniBand. His cyber vulnerability assessment of InfiniBand Networks paved the way for subsequent research investigating the capabilities of several Nvidia-Mellanox channel adapters. The following year, Mireles researched the possibility of encrypting at line rate (e.g., >100Gb/s) using hardware acceleration technology using the Nvidia-Mellanox Innova IPsec Adapter and the Innova 2 Flex Adapter. He concluded that both adapters were unable to hardware accelerate IPsec encryption given the most recent firmware and FPGA images. Lastly, Hintze investigated the capability of the Bluefield-1 DPU to hardware accelerate IPsec encryption. He found that the Bluefield-1 was unable to hardware accelerate IPsec encryption. This research builds off previous research at AFIT by investigating the Bluefield-2 capability to hardware accelerate IPsec.

2.5.3 Performance characteristics of the Bluefield-2 DPU

Liu et al. focused on characterizing the networking and computing aspects of the Bluefield-2 in a 100 Gb/s Ethernet Environment. They ran a wide variety of benchmarks on the Bluefield-2 and compared the results to the performance of several, commercially available host CPUs. Their research complements this research by concluding that the offloading encryption/decryption is a promising feature of the Bluefield-2. They identified that offloading encryption/decryption to the Bluefield-2 could significantly save CPU cycles for applications running on the host and reduce function latency. This research further investigates the benefit of offloading encryption/decryption to the Bluefield-2.

3. Experimental Setup

3.1 Network Topology

The network topology used for this research is shown in Figure 2. The Bluefield-2s on each workstation ride on sixteen lanes of PCIe gen 3 and are connected in tandem by a 100 Gb/s fiber optic cable. Figure 2. also illustrates how traffic moves through each Bluefield-2 while operating in SmartNIC mode (also known as Embedded Mode). While in SmartNIC mode, the Arm subsystem takes control of the Bluefield-2, and a virtual bridge, Open v Switch (OVS), forwards traffic to the appropriate interface on the SmartNIC. The Bluefield-2s use OVS in conjunction with OpenFlow (OF) rules to configure hardware offload and other filtering functions.

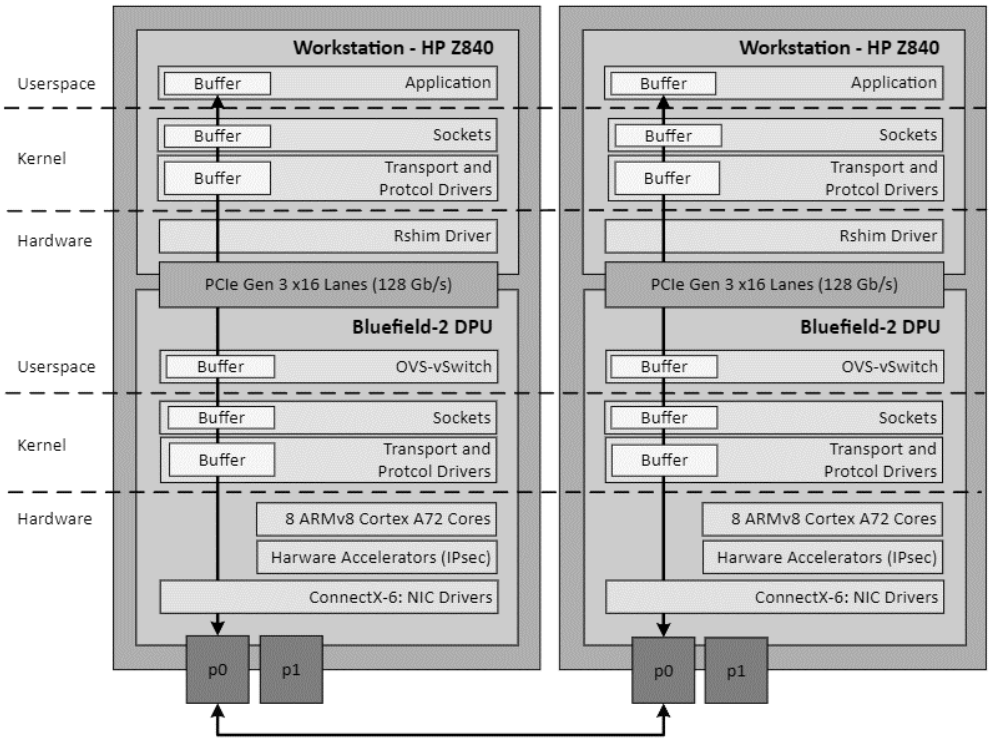

Figure 2: Network Topology: No hardware acceleration

3.1.1 Workstations

Bluefield-2s are installed on two identical HP Z840 workstations. The HP Z840s have up to PCIe gen 3 which are capable of 128 GT/s using sixteen lanes. The PCIe gen 3 should be able provide sufficient throughput for this research even though the Bluefield-2s are compatible with PCIe gen 4. Additionally, the HP Z840s have 20 Intel Xeon Cores, 256 GB of RAM, and a 1 TB hard drive.

4. Methodology

This research focuses on characterizing the end-end throughput achievable using two the Bluefield-2 DPU's hardware accelerators while using Ethernet and TCP at the link and transport layers respectively. Four application scenarios are required to fully characterize the Bluefield-2 hardware accelerators because encryption and hardware acceleration are two level factors (2^2). In combination, the four application scenarios

form a full factorial design. Full factorial experimental designs minimize aliasing and aid in reducing noise from the experimental results. Each experiment in this research was randomized in an attempt to further reduce noise incurred by run order.

4.1 Variables

The control variables are those held constant over the execution of the various scenarios and experiments of this research. These are listed in Table 1.

Table 1: Control Variables

Variable	Value	Description
Test Duration	10 seconds	iPerf3 takes active bandwidth measurements for each second for the duration of the test

Independent variables are specific to the scenarios aimed at evaluating and optimizing the performance of the network. These are listed in Table 2.

Table 2: Independent Variables

Variable	Low Level	High Level	Units	Description
MSS	890	8900	Bytes	Maximum Segment Size
Thread	1	8	N/A	iPerf3 test threads
Performance Setting	ONDEMAND	PERFORMANCE	N/A	Performance setting of host CPU
Direction	WS3 $\rightarrow$ WS4	WS3 $\rightarrow$ WS4	N/A	Direction of iPerf3 Test

Response variables are correlated to the performance of the network given a specific scenario. These are listed in Table 3.

Table 3: Response Variables

Variable	Units	Description
Throughput	Gb/s	Maximum rate of data transfer across a given path

4.2 Application Scenarios

This research tests the effect two factors have on throughput in the network described in Section 3.1. First, this research captures the performance degradation IPsec has on network performance under normal conditions. Second, this research measures the performance benefit hardware offloading provides because processing network traffic in software is often slower than hardware implementations.

4.2.1 Sending plain text without hardware acceleration

The first application scenario of this research establishes the baseline performance of the Bluefield-2s using Transmission Control Protocol (TCP) and Ethernet at the transport and link layers respectively. Traffic at each Bluefield-2 is inspected by a virtual bridge.

4.2.2 Sending plain text with hardware acceleration

This scenario offloads *all* traffic through the hardware accelerators onboard the Bluefield-2 using OpenFlow rules. Sending all traffic to the hardware maximizes the network performance because network traffic has little to no interaction with software at the Bluefield-2.

4.2.3 Sending encrypted (IPsec) without hardware acceleration

This scenario implements IPsec using the open source LibreSwan library configured in tunnel mode. IP datagrams are encrypted by the workstation CPUs in this scenario, and the virtual switch on each Bluefield-2 forwards encrypted datagrams from the host across the network.

4.2.4 Sending encrypted (IPsec) with hardware acceleration

Lastly, this scenario implements IPsec using the Bluefield-2 hardware accelerators. Each Bluefield-2 is configured in legacy single root I/O virtualization (SR-IOV) mode and has full hardware offload enabled. Further, IPsec full offload rules specific to the network topology shown in Section 3.1 are loaded on the Bluefield-2. Each Bluefield has a matching set of offload rules and keys so that an IPsec tunnel is properly configured between the two Bluefield-2s. IPsec keys are manually distributed in this research.

4.3 Assumptions

Nvidia-Mellanox provides a tuning tool for the Bluefield-2 optimizes network performance. This research does not use the tuning tool because reverting the system to the original state would require that the operating systems and other software to be reinstalled on each workstation and Bluefield. This research assumes that the tuning tool would improve system performance, but the results presented by this research are still representative of the impact encryption and hardware offload have on system performance.

4.4 Data Collection and Verification

4.4.1 Full Factorial Design

Confounding variables and uncontrolled factors can introduce noise into experiment results. This research applies the Kruskal-Wallis analysis of variance test on a full factorial design to identify factors that have a significant effect on the response variable, throughput. Table 4 illustrates how factor levels are set during each trial of the full factorial design. The full factorial design applies to all four of the application scenarios described in Section 4.2.

Table 4: Full Factorial Design

Treatment	MSS	Thread	Performance	Direction
1	-	-	-	-
2	+	-	-	-
3	-	+	-	-
	⋮	⋮	⋮	
15	-	+	+	+
16	+	+	+	+

4.4.2 Performance Characterization

Factors introducing noise into the full factorial design are controlled in this experiment. This is accomplished by holding them constant at the level that produces the greatest average throughput in the full factorial design. Noise is further reduced by randomization of trials. The Kruskal-Wallis Test assumes that experimental results are independent of run order and randomizing can help disperse noise caused by the run order of an experiment. This experiment characterizes the performance of the Bluefiled-s2 DPU according to the four application scenarios described in Section 4.2.

4.4.3 Verification

Hosts on either end of the network topology described in Section 3.1, see network traffic in plain text regardless of whether it's being encrypted across the network. This is a common problem for verifying encryption. This research verifies encrypted IP datagrams by configuring a single Bluefield-2 to send encrypted traffic across the network. If the other Bluefield-2 is able to see the ESP headers on the IP datagrams sent from the other side the network, it is reasonable to assume that the IP traffic is properly encrypted. This verification method is assumed to be sufficient for the purposes of this research, but other verification methods should be used in switched networks.

In switched networks, a third workstation set-up with port mirroring would be required to verify data is properly encrypted. The third workstation would be capable of monitoring network traffic and verifying encrypted IP datagrams. Alternatively, a software bridge on a third Bluefield-2 could be used to capture traffic between two other Bluefield-2s.

5. Results and analysis

5.1 Factor screening

The full factorial design described in Section 4.4.1 was performed on each of the application scenarios with three replicated of each trial. In total, 190 (16 treatments x 4 scenarios x 3 replicants) iPerf3 throughput tests were performed. The residuals of the collected dataset were *nonnormal*. Therefore, ANOVA is *not* an adequate model for the data set.

5.1.1 Kruskal-Wallis Test

The Kruskal-Wallis test is a nonparametric alternative to ANOVA for situations where the normality assumption is unjustified (Montgomery, 2019). Kruskal-Wallis uses an F-test analysis of variance that does not require normal residuals. This test is a good fit for the data collected for the full factorial experiment in this research.

Table 2: Full factorial design: Kruskal-Wallis test results

Treatment / Factor	Plain Text	Plain Text Offload	IPsec	IPsec Offload
Thread	90.0%	N.S.	90.0%	90.0%
MSS	99.9%	99.9%	99.9%	99.9%

Table 2. lists the results of the Kruskal-Wallis test performed on the full factorial design dataset. In all the application scenarios, the response variable is dependent on MSS according to a 99.9% confidence interval. The results of the Kruskal-Wallis test also indicate the three of the four application scenarios are dependent on the number of iPerf3 threads used in the throughput test according to a 90% confidence interval.

5.2 Hardware accelerator characterization

This section seeks to characterize the performance of the Bluefield-2's hardware accelerators. This is accomplished by running additional throughput tests with varying MSS and thread factor levels. The direction of throughput tests and the performance setting of workstation CPUs are held constant for the remaining experiments because the Kruskal-Wallis test in Section 5.1 determined that they do not significantly affect the response variable. Workstation 3 and workstation 4 act as the client and server for the following throughput tests. The workstation CPUs are configured in *performance* mode.

The performance characterization experiment described in Section 4.4.2 was performed on each of the application scenarios with three replicates of each trial. In total, 960 (10 MSS levels x 8 thread levels x 4 scenarios x 3 replicants) iPerf3 throughput tests were performed.

5.2.1 Sending plain text without hardware acceleration

The baseline performance of the Bluefield-2 peaks just above 15 Gb/s as shown by the results in Figure 3-A. Increasing the MSS during the iPerf3 throughput tests increases the average throughput of the system, whereas increasing the thread count decreases the average throughput. It is possible that the virtual bridge on the Bluefield-2 is saturated. Additional threads slow system performance due to additional context switching.

5.2.2 Sending plain text with hardware acceleration

Hardware acceleration on the Bluefield-2 increases the throughput to over 30 Gb/s as seen in Figure 3-B. The overall throughput increases by over 100% from the baseline throughput, and the maximum performance recorded during these experiments used 7 iPerf3 threads and had an MSS of 8900. The perfromance improvement seen in this experiment demonstrates one of the benefits of hardware offloading network traffic.

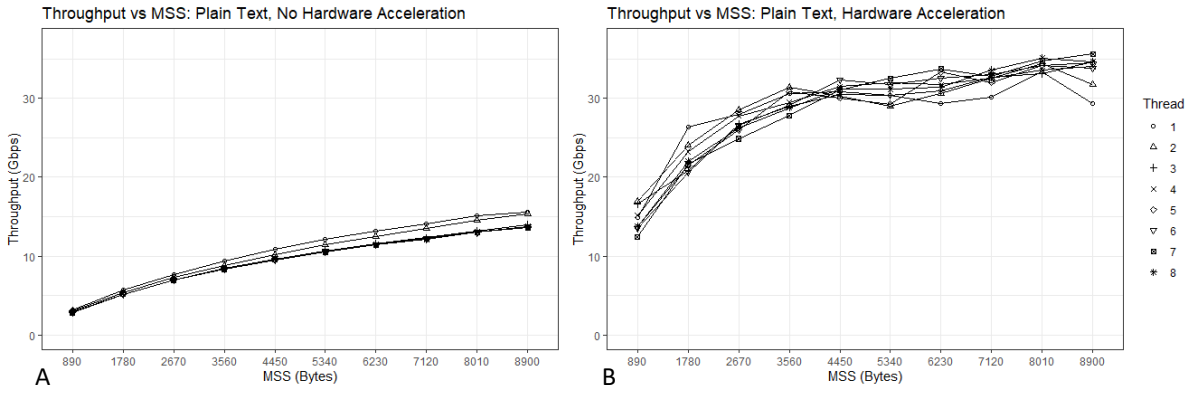

Figure 3: Sending plain text (A) No hardware acceleration (B) Hardware acceleration

5.2.3 Sending encrypted text (IPsec) without hardware acceleration

IPsec encryption significantly reduces network performance when Libreswan is run on the host CPUs. Figure 4-A. lists the performance results when IPsec is implemented without hardware acceleration. The throughput

increases as MSS and thread count increase. The average throughput peaks just above 6.5 Gb/s which is a 130% loss in performance from the baseline performance.

5.2.4 Sending encrypted text (IPsec) with hardware acceleration

Lastly, Figure 4-B. illustrates network performance when IPsec operations are offloaded to the hardware accelerators on the Bluefield-2s. When the MSS is 8900 Bytes, the average throughput of the network peaks at nearly 16 Gb/s. The hardware accelerator of the Bluefield-2 increases the average network throughput by over 140% from performance of implementing IPsec without hardware offload, and is similar to the baseline performance of the Bluefield-2.

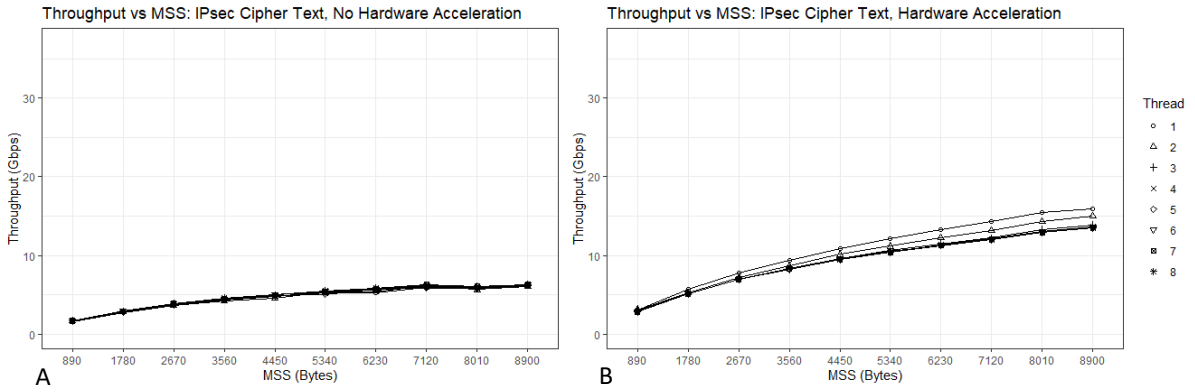

Figure 4: Sending encrypted text (IPsec) (A) No hardware acceleration (B) Hardware acceleration

5.2.5 Combined Results

Figure 5. illustrates the difference in throughput achieved by each treatment. The baseline plain text throughput is nearly identical to that of the hardware accelerated IPsec encryption. Further, hardware acceleration of plain text traffic more than doubles the throughput in the network.

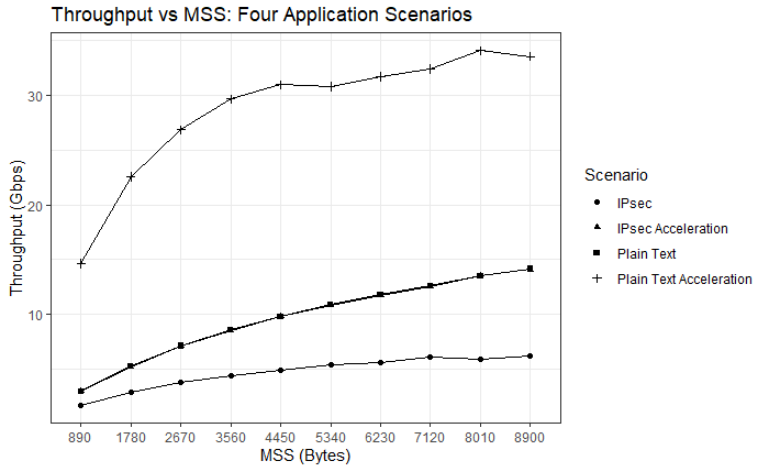

Figure 5: Comparison of average throughput

Figure 6. compares the average throughput measured during of the four application scenarios of this research and illustrates the increase in performance as a result of offloading traffic through the Bluefield-2's hardware accelerators. Hardware acceleration significantly improved the throughput for both plain text and IPsec encrypted traffic based on a 99.9% confidence interval.

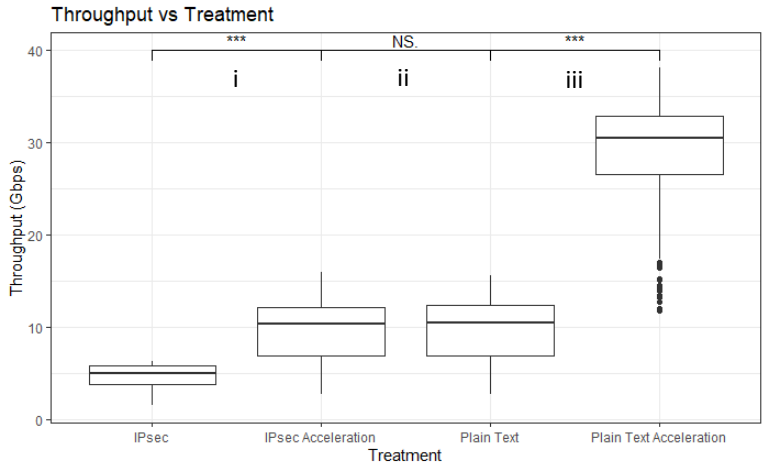

Figure 6: Combined Results (i and iii) Hardware acceleration significantly improves throughput for Plain Text and IPsec (ii) Baseline and hardware accelerated IPsec throughput are statistically the same

6. Conclusion

Previous research identified vulnerabilities in native InfiniBand's clear text key exchange and proposed changes to the IBA specification for a secure key exchange scheme using GCM encryption. The proposed key exchange scheme degraded InfiniBand network performance by up to 12%, and increased the computational load placed on in CPUs. This research demonstrates the performance benefit of offloading the encryption of Ethernet traffic to hardware accelerators like those found on the Bluefield-2 DPU. Bluefield-2 DPUs are capable of swapping Ethernet and InfiniBand at the link-layer. Open-source Ethernet tools like iPerf3 are well documented. As a result, this research uses Ethernet to demonstrate the Bluefield-2s capability to hardware accelerate IPsec encryption. Initial tests using iPerf3 showed that the Bluefield-2 DPUs were capable of offloading IPsec encryption to their hardware accelerators. Subsequent throughput tests determined that the Bluefield-2 DPU IPsec/TLS specific hardware accelerators are capable of encrypting IPsec datagrams at nearly 16 Gb/s while using TCP and Ethernet at the transport and data link layers respectively. Therefore, the hardware accelerators realize a significant performance improvement when compared to the throughput of encrypting Ethernet traffic using Libreswan on the workstation's CPUs. The Bluefield-2 DPU provides an effective means for improving network performance and providing confidentiality, integrity, and authentication to Ethernet traffic. Further research is required to characterize the capability of the Bluefield-2 DPU to accelerate DMA traffic in hardware, and measure the difference in CPU utilization as a result of kernel bypass.

6.1 Future work

SmartNICs like the Nvidia-Mellanox Connect-X 6 network adapter enable the execution of extended Berkely Packet Filters (eBPF) on the NIC itself using Express Data Path (XDP). Thus, eBPF provides a framework to enable offloading for a broad set of applications (Hohlfeld *et al.*, 2019). eBPF/XDP-based offloading from the user-space is an interesting research area. Future research should investigate the Bluefield-2s ability to offload encryption to the hardware of the Connect-X 6 NIC itself.

Additionally, DMA bypasses the OS kernel of the host and Bluefield-2s and prevents kernel space applications like TCP dump, Wireshark, and ntopng from capturing most network traffic. Therefore, monitoring InfiniBand traffic requires user space applications that use InfiniBand verbs to facilitate packet filtering. This research uses OpenFlow rules and Open vSwitch to offload encryption. These applications also do not work with InfiniBand Traffic. Therefore, future research should investigate user space applications that will enable packet filtering and encryption of RDMA InfiniBand traffic.

Acknowledgements

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, of the U.S. Government. This document has been approved for public release; distribution unlimited, case #88ABW-2021-0849.

References

Hintze, K. (AFIT/USAF) (2021) 'Infiniband Network Monitoring: Challenges and Possibilities', *M.S. thesis, Air Force Institute of Technology*.

Hohlfeld, O. *et al.* (2019) 'Demystifying the Performance of XDP BPF', *Proceedings of the 2019 IEEE Conference on Network Softwarization: Unleashing the Power of Network Softwarization, NetSoft 2019*, pp. 208–212. doi: 10.1109/NETSOFT.2019.8806651.

InfiniBand Trade Association. Available at: https://www.infinibandta.org/ (Accessed: 7 June 2021).

Kurose, J. and Ross, K. (2017) *Computer Networking A Top-Down Approach*. 7th edn. Pearson.

Lee, M. and Kim, E. J. (2007) 'A comprehensive framework for enhancing security in InfiniBand architecture', *IEEE Transactions on Parallel and Distributed Systems*, 18(10), pp. 1393–1406. doi: 10.1109/TPDS.2007.1079.

Liu, J. *et al.* (2021) 'Performance Characteristics of the BlueField-2 SmartNIC'. Available at: http://arxiv.org/abs/2105.06619.

Mireles, L. (AFIT/USAF) (2020) 'Implications and Limitations of Securing an InfiniBand Network', *M.S. thesis, Air Force Institute of Technology*.

Montgomery, D. (2019) *Design and Analysis of Experiments*. 10th edn. Wiley.

'NVIDIA BLUEFIELD-2 DPU DATA CENTER INFRASTRUCTURE ON A CHIP' (2021). Nvidia.

Pfister, G. F. (2001) 'An introduction to the InfiniBand™ architecture', *High Performance Mass Storage and Parallel I/O: Technologies and Applications*, pp. 617–632. doi: 10.1109/9780470544839.ch42.

Rothenberger, B. *et al.* (2021) 'ReDMArk : Bypassing RDMA Security Mechanisms', *Usenix Security'20*.

Schmitt, D. (AFIT/USAF) (2019) 'A Framework for Cyber Vulnerability Assessements of InfiniBand Networks', *M.S. thesis, Air Force Institute of Technology*.

Strohmaier, E. *et al.* (2021) *TOP 500 The List*. Available at: https://top500.org/statistics/list/ (Accessed: 7 June 2021).