



# 毕业论文中期答辩

汇报人：殷悦 学号：150120526

# 目录



```
graph LR; A((目录)) -.-> B(Part1 : 完成内容); A -.-> C(Part2 : 程序展示); A -.-> D(Part3 : 后期内容); A -.-> E(Part4 : 进度安排);
```

Part1 : 完成内容

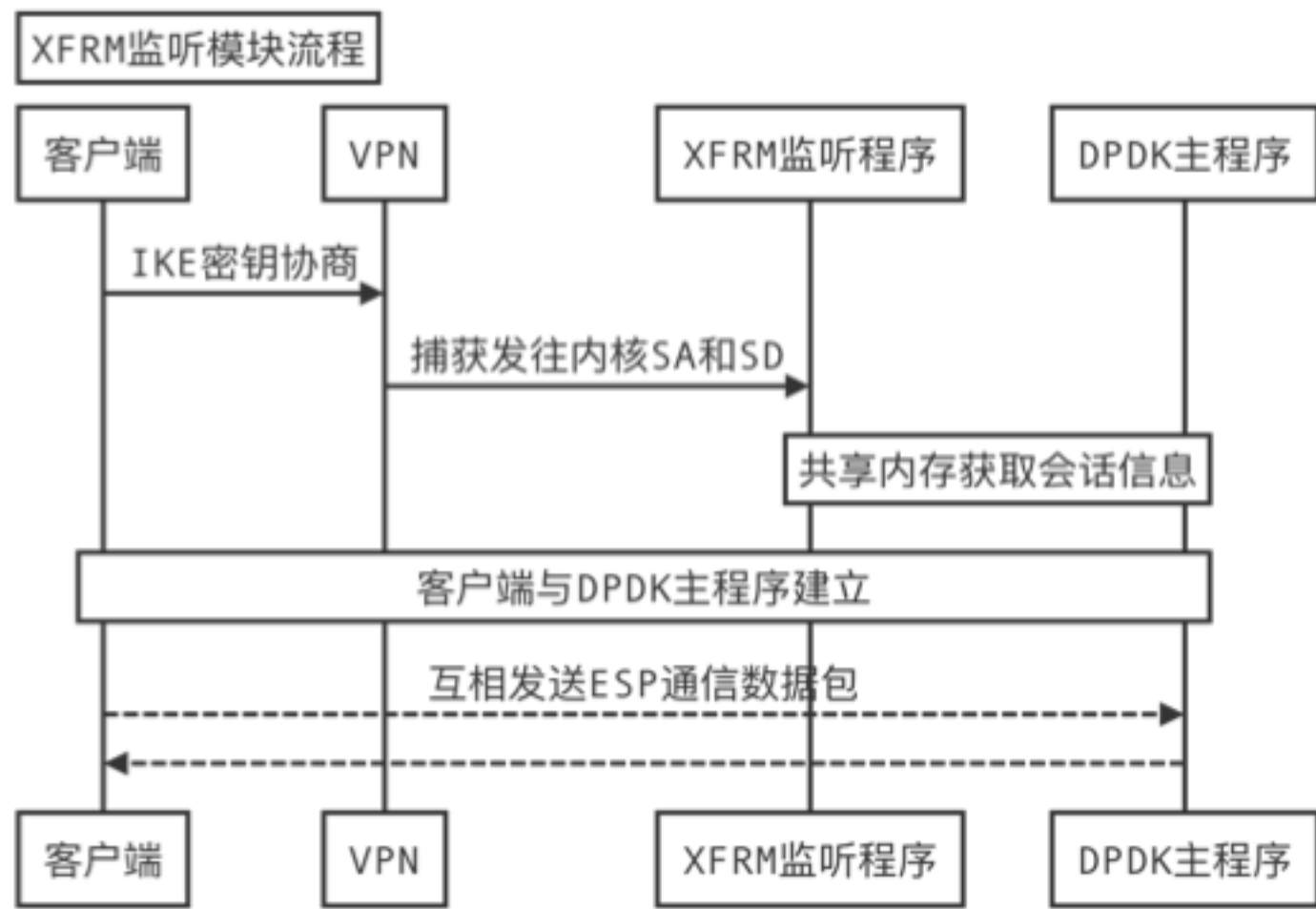
Part2 : 程序展示

Part3 : 后期内容

Part4 : 进度安排

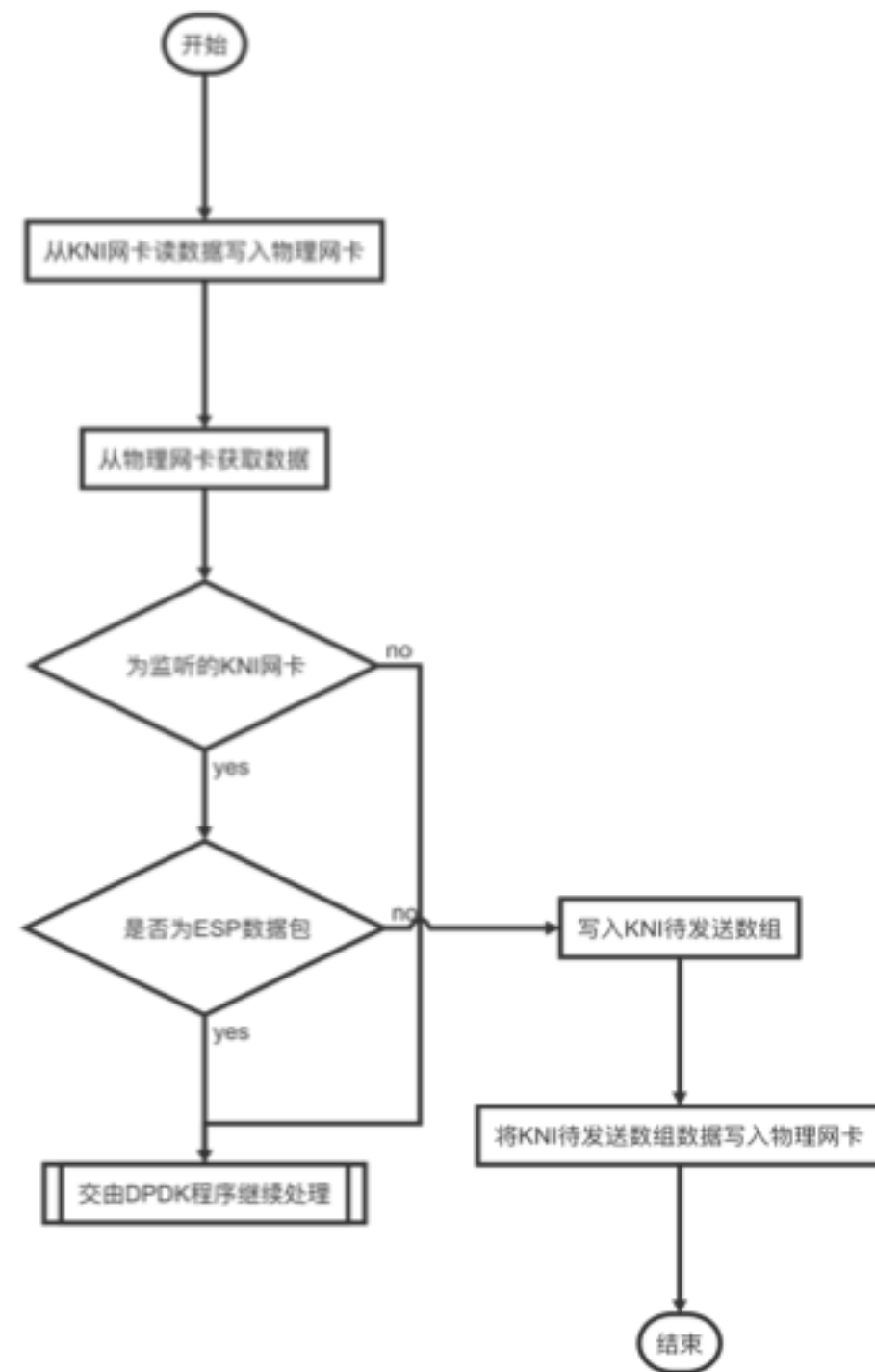
# IKE部分数据处理流程

由于IKE阶段数据包较少，实现非常复杂，因此可以使用其他IPSec VPN实现IKE过程，ESP阶段数据量巨大，实现相对容易，需要使用DPDK进行加速。ESP部分通信数据加解密使用对称加密算法，若使用软加密，则加密速度成为瓶颈，可使用硬加密来提升加密速度。



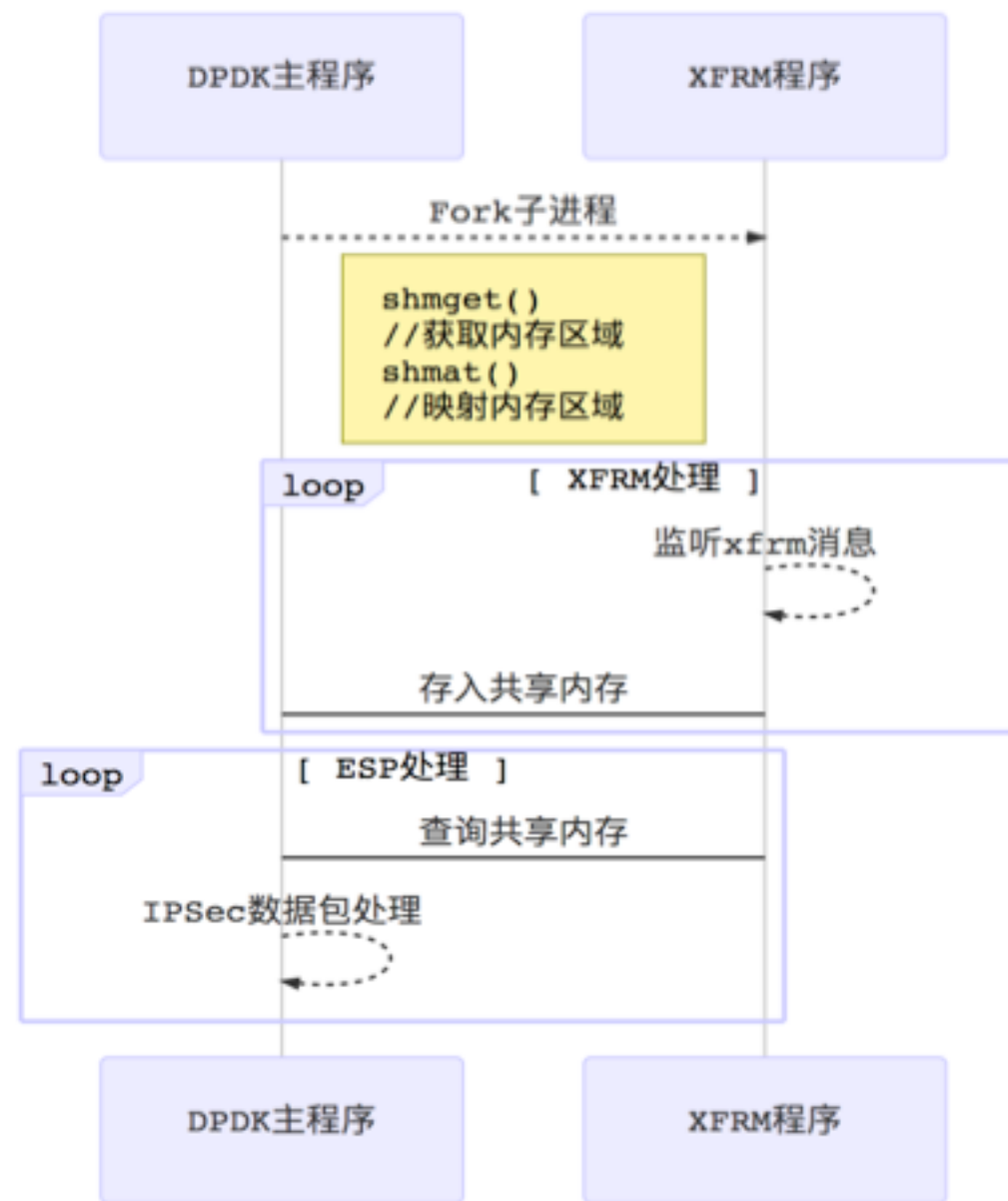
# 分流ESP和IKE及其他数据

由于ESP部分需要加密，而IKE部分不需要加密，当数据到达网卡后，需要对数据进行分流，ESP部分交由DPDK进行处理，而IKE和其他数据需要传入Linux内核协议栈。DPDK和Linux内核态协议栈交换报文有两种模式：KNI或TUN/TAP。KNI比Linux现有的TUN/TAP接口速度更快，因为和TUN/TAP相比，KNI消除了系统调用和其数据拷贝。本程序采用KNI来实现DPDK和Linux内核态协议栈通信。当数据到达网卡后，DPDK取到数据，获取数据包IP头的协议类型，若是IPv4或IPv6的ESP协议，则交由DPDK继续处理，否则交由Linux内核进行处理。这样就完成了分流功能。



# 多进程及共享内存

共享内存是通过将同一块内存区映射到不同进程地址空间中，不经过内核，因此共享内存是IPC中速度最快的，但共享内存需要用户来操作并且同步也需要用户来完成。因此本程序采用最复杂的mmap共享内存完成，并使用CAS无锁技术来避免加锁，提高性能。



# IP&MAC映射表

Mac地址获取如图，当数据不为ESP数据包时，其他数据(如ARP,ICMP,TCP,UDP)走KNI网卡，若数据为UDP协议，目标地址为KNI网卡IP，端口为500时，此数据包为IKE通信数据包，可将该数据包的IP和端口作为一组IP和MAC映射表存入数组以备查询使用

## UDP数据封装

以太网头:目的地址(6)|源地址(6)|帧类型(2)

## IP头:

版本(4)|首部长度(4)|服务类型(8)|总长度(16)|

标识(16)|标志(3)|片偏移(13)|

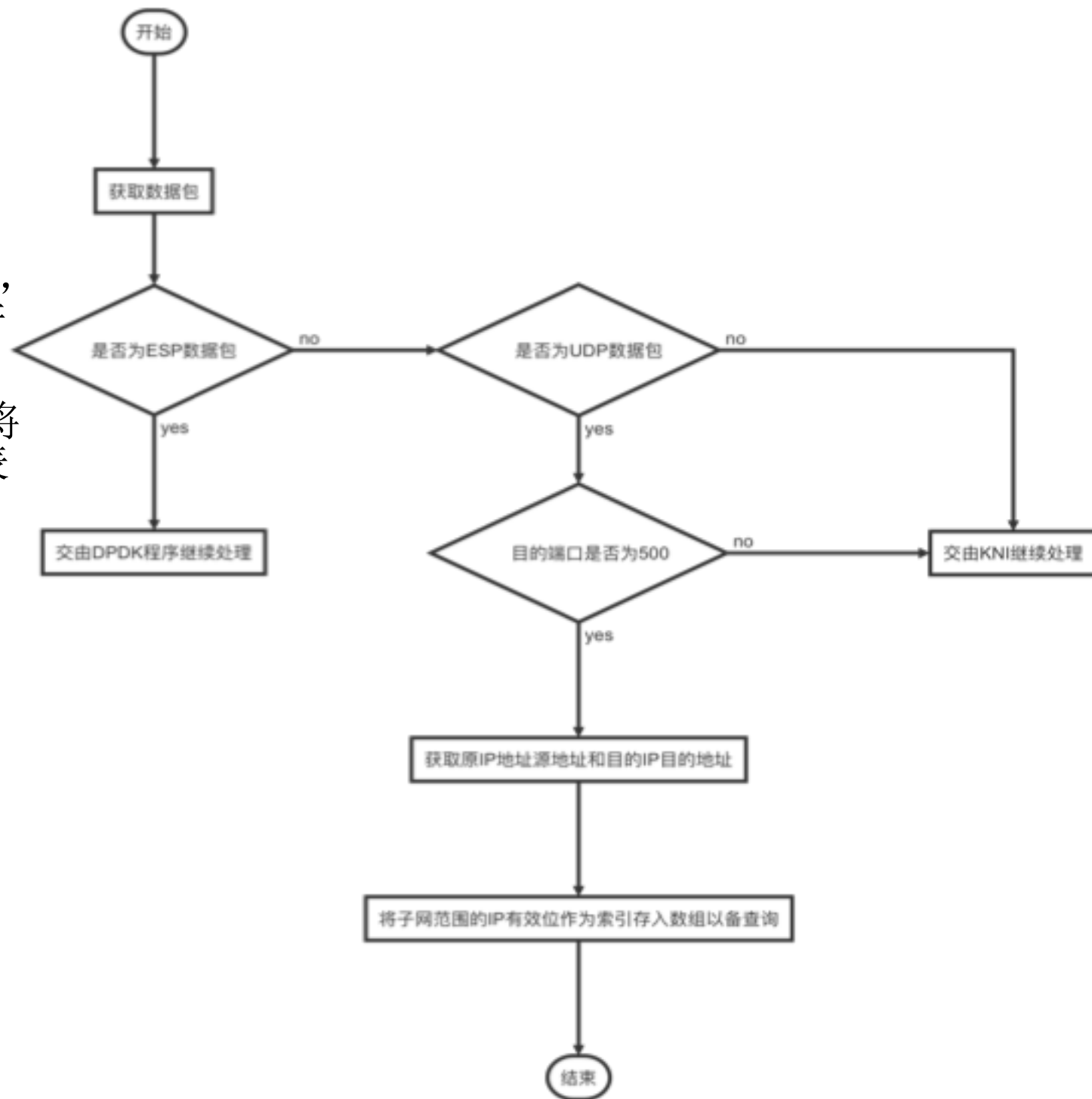
TTL(8)|协议(8)|首部校验和(16)|

源IP地址(32)|

目的IP地址(32)|

## UDP头:

源端口(8)|目的端口(8)|包长度(8)|校验和(8)



# ESP数据包格式

ESP头部:

安全参数索引SPI(32位):用来确定唯一的安全联盟

序列号SeqNum(32位): 用于保护接收端免受重复操作攻击

ESP尾部:

填充Padding: 字段长范围为0-255, 用于将明文扩充到需要加密的长度, 同时隐藏载荷数据的真实长度。

填充长度PadLength(8位): 表示填充的字节数

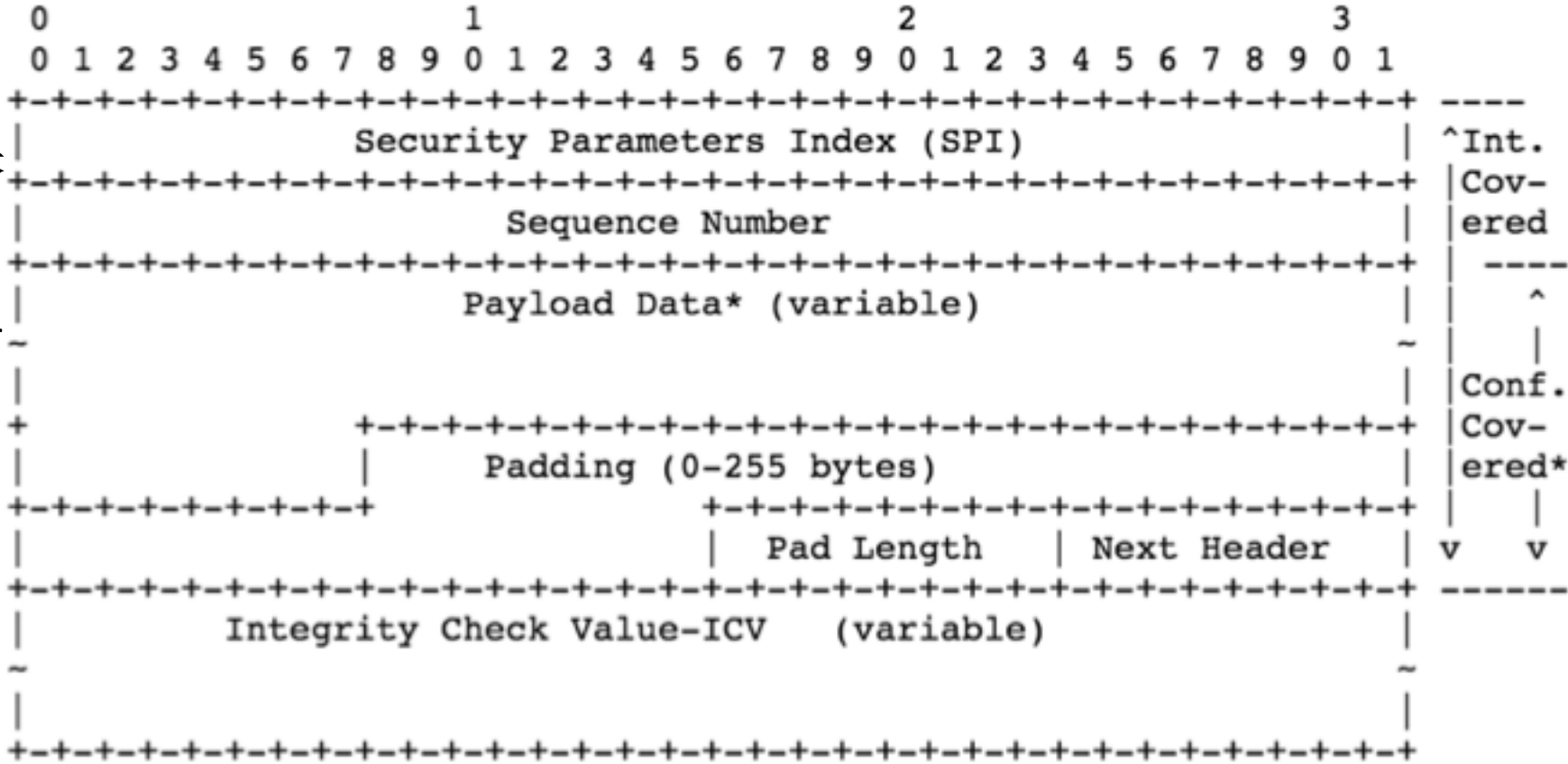
下一头部NextHeader (8位): 标志下一头部的类型(被加密的数据类型)。

ESP验证尾部:

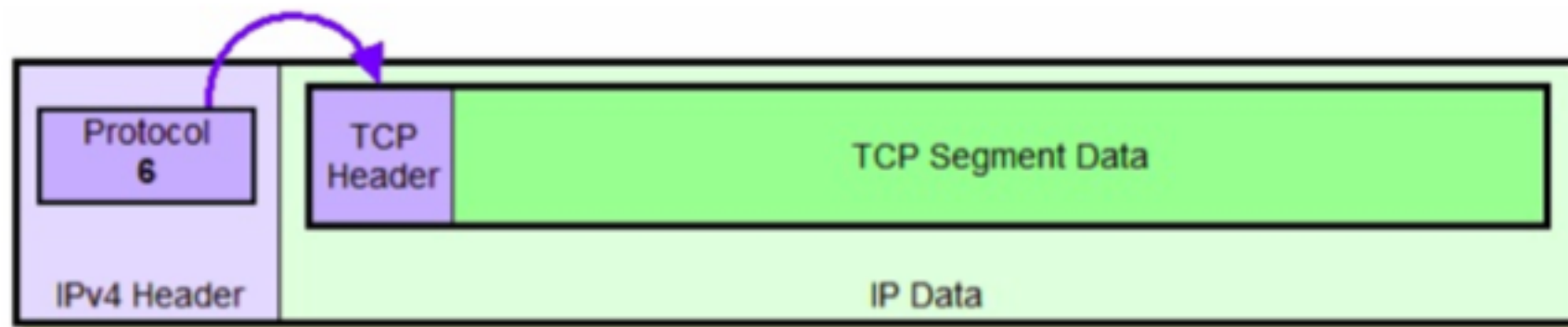
鉴别数据Integrity Check Value-ICV(变长): 在ESP数据包其他字段基础上计算出的完整性校验值。

对数据的完整性验证需要计算SPI、序列号、载荷数据以及ESP尾部。

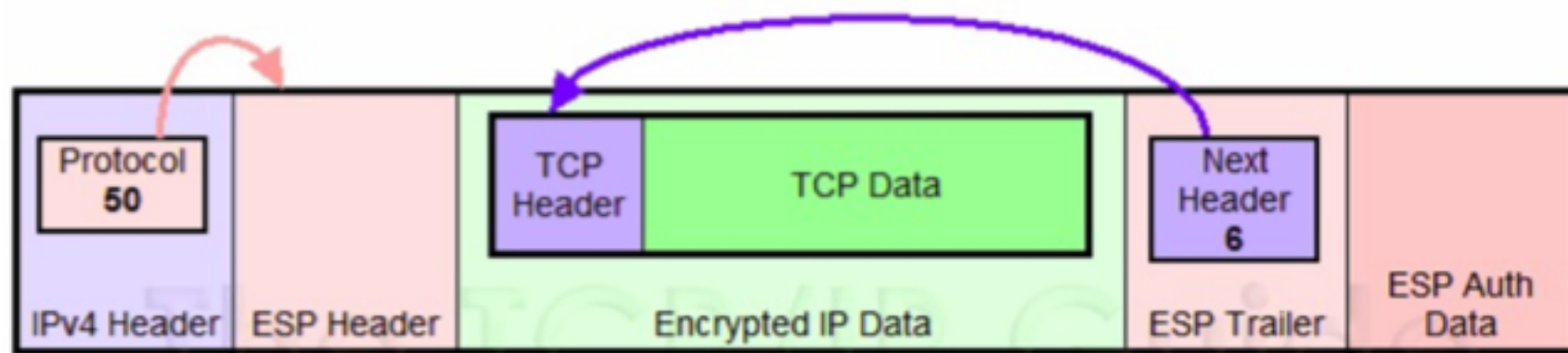
对数据的保密性验证需要计算载荷数据以及ESP尾部。



# ESP数据拆包与封包



Original IPv4 Datagram Format



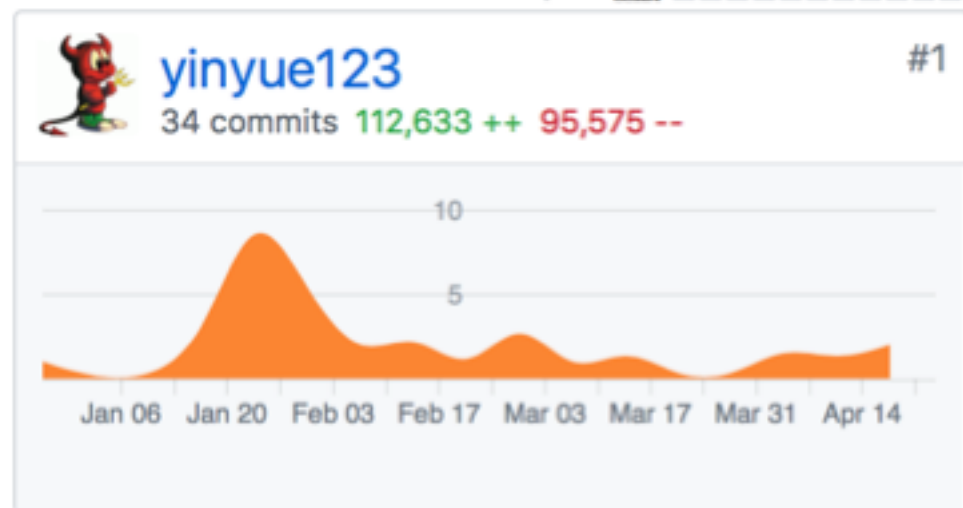
Authenticated Fields

IPv4 ESP Datagram Format - IPsec Transport Mode



# 程序展示

# 工作量



213 contributions in the last year

Contribution settings ▾

2019

2018

2017

2016

## PaperPass旗舰版检测报告 简明打印版

比对结果(相似度):

总体: 13% (总体相似度是指本地库、互联网的综合对比结果)

本地库: 13% (本地库相似度是指论文与学术期刊、学位论文、会议论文、图书数据库的对比结果)

期刊库: 5% (期刊库相似度是指论文与学术期刊库的对比结果)

学位库: 10% (学位库相似度是指论文与学位论文库的对比结果)

会议库: 0% (会议库相似度是指论文与会议论文库的对比结果)

图书库: 4% (图书库相似度是指论文与图书库的对比结果)

互联网: 0% (互联网相似度是指论文与互联网资源的对比结果)

Repository page for **yinyue123 / bysj** (Private). The page shows 37 commits, 2 branches, 0 releases, 1 contributor, and 0 forks. The repository is titled "基于DPDK的IPSecVPN实现-殷悦的毕业设计".

Branch: middle ▾ New pull request

This branch is 3 commits ahead of master. Pull request Compare

File	Commit	Time
.idea	添加中期报告和参考文献	2 hours ago
bysjs	init	11 hours ago
dpdk_crypto_test	recv success	2 months ago
eth-tun	第二章加密和用户协议栈	7 days ago
ipsec-secgw	middle check	4 hours ago
ipsec-vpn	kni success	3 months ago
kni	add xfrm sp	2 months ago
mydpdkdns	add kni and xfrm	3 months ago
notes	添加中期报告和参考文献	2 hours ago
report	添加中期报告和参考文献	2 hours ago
xfrm-listen	add kni and xfrm	3 months ago

# 后期计划

- 1.完成DPDK数据转发到tun网卡
- 2.完成ipsec客户端，DPDK程序，Linux内核网卡的对接
- 3.搭建DPDK-pktgen发包工具环境并完成性能测试
- 4.如果有时间和设备，完成使用QAT加密卡、AES-NI CPU指令集加密加速及其性能提升
- 5.使用类似内核自旋锁模型的CAS操作来替换多进程共享内存数据同步安全问题

# 问题与困难

问题1: DPDK程序和pktgen性能测试工具同时启动，程序崩溃

解决方案：机器CPU性能和内存不足，发包机和测试机不能使用同一台机器

问题2: 内核无法收到来自KNI网卡的数据

解决方案：

rte\_kni的驱动不带入参数，直接insmod即可，例子中的insmod=lo\_mode的意思是仅仅把报文发给回环网卡而不处理，lo\_mode是disable状态时，数据才经过内核协议栈

使用kni设备的iptables关闭，在centos7.3中，需要将iptables先启动在停止才生效，iptables无法处理数据

问题3: 升级内核版本后DPDK无法启动

解决方案：DPDK程序依赖内核驱动，DPDK 17.02版本必须使用Linux 3.10.0-514版本的内核，不能随便使用yum update升级内核，可手动从官网下载对应版本内核的kernel、kernel-tools、kernel-tools-libs，然后先安装旧版本内核程序，再强制卸载新版本内核

问题4: 安装AES-NI CPU加速加密环境后，程序崩溃

解决方案：CPU j1900不支持AES加密加速AES-NI指令集，需更使用支持AES-NI指令集设备

问题5:数据必须攒满缓冲区才会发送到物理网卡

解决方案：程序默认缓冲区满时发送数据包。可设置定时器，定期发送缓冲区中数据到物理网卡

问题6:内核物理网卡无法接受DPDK物理网卡发出的数据

解决方案：将目的MAC地址设置为内核目的物理网卡MAC地址并添加ARP映射表，内核仍无法处理数据包，拟在后期使用将数据直接通过tun虚拟网卡使用异步非阻塞模型发送到内核。

# 进度安排

5月6日-5月10日 完成tun功能

5月10日-5月13日 完成对接工作

5月13日-5月20日 完成性能测试

5月20日-6月1日 完成毕业论文

6月1日-6月10日 修改论文



# THANK YOU

感谢聆听，批评指导