**IPSec协议在5G网络中能力扩展的需求**

**1、背景**

IPSec是3GPP推荐的网络层安全协议，已经成功在3G&4G网络中商用部署了，5G的IPSec功能也是一个传输安全必备的核心功能，IPSec是一个庞大协议族，协议也在不停更新，最新的协议版本是RFC7296。

随着5G的来临，IPSec协议已经逐渐不能满足业务的需求了。5G基站网络架构和4G差别不大，采用扁平化的基站和核心网，用户面数据承载在基站到核心网GTPU隧道中。但是5G单个基站的流量远远超过了4G，下行流量可达40Gbps，上行流量20Gbps，现有协议的不能满足5G大流量的场景。

**2、现有解决方案**

目前IPSec的解决方案都是基于标准的RFC7296：

1）基于五元组做IPSec Tunnel的协商。

2）基于RFC7296的IPSec自建立碰撞算法。

上述标准定义，在实际应用中的效果并不好，无法满足实际应用的要求。

**3、问题**

请大家结合自身知识，以及RFC7296标准协议，调研业内当前关于5G网络大容量大流量IPSec的解决方案。解决如下5G网络遗留的IPSec疑难问题：

1. 因为运营商IP地址有限，大部分情况下基站只会配置一个用户面IP，与之对接的核心网用户面网关也只有一个IP，基站和核心网之间的用户面数据（GTPU）只能有一个五元组，即相同的源IP，目的IP，协议号，源端口、目的端口。即如果遵循现有的IPSec协议，基站到核心网的用户面数据大部分情况下将承载在同一个安全隧道中。而当前硬件的处理能力，单核IPSec加解密性能，处理不了5G大流量（下行40Gbps，上行20Gbps），请设计一种方法解决目前IPSec性能难题。
2. 由于IPSec序列号和滑窗机制的限制（参考RFC2406：3.4.3 Sequence Number Verification），大流量的数据报文同时到达基站，由于链路不同，低QoS的报文可能先到达，导致后到达的高QoS的报文丢失，这违背了高优先级数据优先处理的。请设计一种方法解决目前大流量情形下保障高QoS数据在IPSec隧道内不丢包的方案。
3. 商用网络要求两个基站间建立X2的IPSec隧道，当时间或者网络周期到期rekey时，会存在双方同时发起IPSec协商的情况（尤其在网络规模较大，比如上万站点网络规模，概率较高），两个站点同时协商IPSec，会导致双方IPSec同时切换到自协商的IPSec隧道上，但是双方使用的IPSec隧道的SA并不相同，导致链路不通。请设计一种方法解决这种自协商时IPSec隧道碰撞的问题。

要求：请您以Word输出整体运作方案，并将其中要点以PPT形式进行输出，在极致挑战环节进行宣讲。