万物互联，该怎么联?

(2021 年 3 月 3 日)

万物互联，相信大家看到这个名字就很兴奋和有很多畅想。简单的讲，万物互联就是把人和物通过各种联网技术有机地连接起来，实现人和人、人和物、物和物的互联互动、信息交互和资源共享，从而推动人类文明向更高层次发展，并进一步造福人类。

据有关报道，目前全球物联网连接设备已经超过 500 亿个，而随着 5G 的快速发展而使得更多的物体实现互联，可以说一个万物互联的时代已经到来。本文题目有点大，“该怎么联”已经有了许多方案，并且这些方案正在实践和完善中，作者结合自己的工作经验和实践也提出自己的一些想法，就当抛砖引玉吧。

互联网从发明到现在已经有 52 年了，各种联网技术和应用技术都已经非常成熟，我认为物联网或者万物互联的联网方式还是互联网协议，只不过是现在互联网的人与人，人与物之间的连接拓展到物与物，并让更多的物实现与人的连接。实际上，目前各种智能家电已经就是这样连接起来了。

但是，目前的物联网的连接或者说物联网之间的通信存在巨大的安全隐患，必须在起步时得以解决，否则将来普及时将一定是一个巨大的灾难！目前，物联网通信主要存在两个方面的问题：一是中心化的通信方式不适合于物联网，庞大的物联网的物与物，人与物之间的通信如果必须通过中心化的云端服务器才能获得通信，那一旦这个中心服务系统出故障或被攻击，则整个万物互联就瘫痪了，这是一个不可接受的结果。二是硬把互联网安全防护的那一套搬到物联网安全防护体系中，也是行不通的，不仅仅是成本高的问题而且可以说是行不通的，因为物联网的物不是人，物也不具备人使用的电脑和手机的数据处理能力。这一点值得相关安全厂商高度重视。

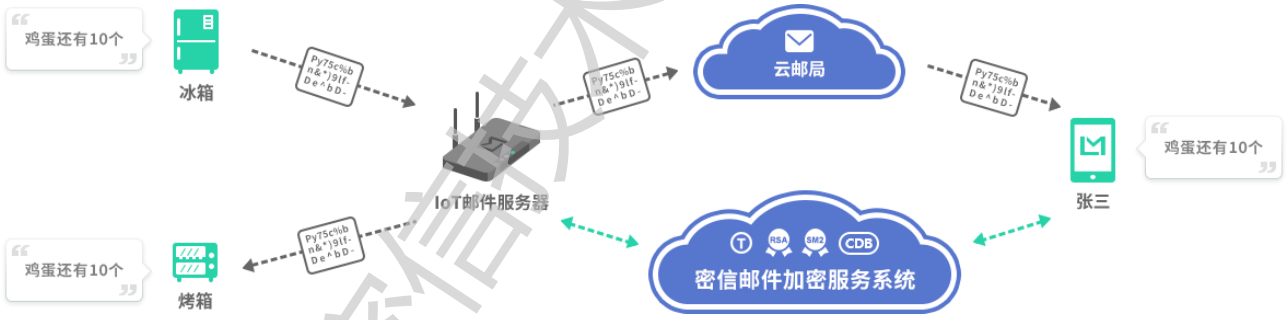
对于第一个问题，我提出了一个去中心化的基于电子邮件通信协议的物联网通信解决方案。大家都知道，电子邮件就是一个去中心化的通信系统，全球任何人都可以通过电子邮件实现可靠通信，所有邮件服务器就是分布于全球的不同的通信节点，邮件通信没有中心节点，邮件并不像高度中心化的社交网络一样人们必须依赖某个服务提供商实现通信，人们如果不使用同一个社交服务系统是无法实现通信的。显然，电子邮件通信系统不是这样的，你只要有一个邮箱，就可以给其他任何邮箱用户发邮件而不用关心对方使用哪一家的邮件服务。

对于物联网，也可以像人一样拥有一个电子邮件地址，由物联网服务节点为本节点的物提

供电子邮件通信服务，如家里路由器可以作为一个服务节点，为家里的所有电器和物提供电子邮件服务，就可以实现全球范围的物与物，人与物的邮件通信，而不管人和物属于那个邮件服务器。这是一个去中心化的可靠的实现人与物和物与物的通信方案，彻底解决中心化的通信方式的不可靠问题。

而对于第二个问题，则可以通过数字签名和加密技术来实现物联网的加密电子邮件通信服务，每个物都有数字身份，用邮件数字签名来证明自己的身份，而用加密证书来加密所有通信，确保通信内容不会非法窃取和非法篡改，从而保护物联网通信安全。这样的话，物联网的安全防护就非常简单，通信接收方必须验证数字签名而根据安全规则决定是接收还是拒绝这次通信。也就是说物只接收可信的通信，从而有效地抵御了各种攻击，而无需额外的复杂的安全防护模块。

当然，不仅是物与物通信，人与物通信也是需要人用其签名证书数字签名邮件，才能让物能自动识别是否应该同这个人通信，从而真正能保护物不会遭遇来自人的攻击。这就是一个非常高效的、低廉的并且可靠的万物互联通信安全保障措施，彻底解决目前的物联网安全防护同样陷入的互联网安全防护一样的“道高一尺魔高一丈”的恶性循环怪圈。



万物互联时代已经到来，但是该如何联，笔者认为：应该充分借鉴已经非常成熟的互联网发展思路，把已经成熟的技术复制到物联网中，但又要考虑到物联网的特殊性，认识到物与人的不同而采用不同的方案。而采用加密电子邮件方式实现安全的可靠的人与物和物与物的通信则是成本最低、也是最容易实施的方案。当然，对于实时性要求很高的物与物或人与物通信也可以采用更高效的 https 加密通信方式，但仍然需要人和物使用其数字证书来证明其身份才能实现通信，以确保物与物和人与物的通信安全。

----------END----------

想联系我讨论此话题？请使用 密信 App（ - ）扫码发加密邮件给我，我一定会回复您的加密邮件。