物联网安全：漏洞、攻击和防御措施（1-2）

汇报人：郭涵迪

物联网：定义、趋势与影响

物联网（IoT）定义

物联网”一词由宝洁公司的Kevin Ashton在1999年提出，并在后来麻省理工大学（MIT）的Auto-ID中心进一步发展。从那时起，物联网迅速发展成为一个涉及智能对象 互连和交互的领域，这些对象或设备具有嵌入式传感器、板载数据处理能力和通信手段，以提供自动化的服务和应用。IoT涉及WSNs、实时计算、嵌入式系统和执行技术的融合。如今，我们认为的大多数IoT是各种主要独立的设备和孤立的系统，如可穿戴健身监测器、智能手表、智能手机、以及远程视频流。新兴的IoT实现将使用更小、更节能的嵌入式传感器技术、增强的通信、先进的数据分析和更复杂的执行器来收集和聚合信息，实现智能系统，这些系统能够理解上下文、跟踪和管理复杂的交互，并预测需求。

物联网：定义、趋势与影响

智能家居中用于管理能源使用、控制电器、监测食品和其他消费品

汽车/交通：用于优化驾驶条件、评估驾驶员警觉性、碰撞/事故避免和管理车辆健康

电网和其他关键基础设施：用于电网优化、自动化故障诊断、自动化网络安全监控和响应

消费者应用：如健康和健身监测、状况诊断

制造和工业环境：用于供应链管理、机器人制造、质量控制、健康和安全合规

物联网：定义、趋势与影响

异构性：物联网由各种设备组成，如网关、交换机、传感器、执行器、智能家电、移动系统等。这些设备运行在不同的电路、使用不同的通信协议，并采用不同的数据处理算法。

• 可扩展性：管理、命名、服务数百万个设备是一个独特的挑战。

• 通信：物联网设备使用各种技术，如有线或无线通信，如蓝牙、ZigBee、LPWAN。

• 能耗：这是物联网的主要挑战之一。在物联网设备上运行的任何算法都需要设计为轻量级处理要求。

物联网：定义、趋势与影响

• 数据隐私：用户数据在物联网中的隐私是一个问题。例如，在常规（公共）操作模式下，物联网中的事物可以向网络管理员或其他邻近设备提供其位置信息。

• 自感知：物联网中的智能对象应自主组织自己，以响应真实世界的环境情况，而不需要太多的人工干预，以完成某些预定的特定任务。

• 互操作性：为了使异构的物联网设备能够相互通信、协作和共享数据，应预先确定和标准化数据交换格式。

物联网：定义、趋势与影响

未来预测

ioT市场预计将从2015年的超过150亿台设备增长到2025年的超过750亿台。这一预测意味着，平均每个人在地球上至少将拥有25个个人IoT设备。因此，IoT预计将对我们未来的生活产生巨大影响。在这一时期，WSNs将被整合到IoT中，无数的传感器节点将加入互联网，旨在与其他节点合作感知和监测它们的环境。IoT将通过使用WSNs越来越多地实现人与环境之间的互动。

针对WSNs和IoT的攻击

- 被动攻击
  - 被动攻击的定义
  - 被动攻击是在无法察觉的情况下进行的，因为攻击者不会产生任何无线电辐射。由于无线链路更容易被窃听，无线网络更容易受到被动攻击，例如窃听，攻击者可以在不捕获任何传感器节点的情况下轻松监听WSN中的无线通信。被动攻击主要是针对数据机密性。
  - 在被动攻击中，攻击者通常是隐藏的，即伪装起来，并窃听通信线路以收集数据。被动攻击可以分为窃听、节点故障、节点篡改/破坏、节点故障和流量分析类型。

针对WSNs和IoT的攻击

- 被动攻击
  - 被动攻击的种类
  - 1) 被动信息收集（窃听）：窃听也被称为“被动信息收集”。机密数据可以通过窃听通信线路被窃听。因此，无线网络更容易受到被动攻击。由于WSN使用短距离通信，攻击者必须接近才能通过窃听收集有用的信息，因此与长距离无线技术相比，WSN受到窃听的暴露程度较低。拦截通过WSN传输的消息可能会揭示以下有用的信息：特定节点的物理位置，如簇头、网关、密钥分发中心等；消息标识符（ID）、时间戳、其他字段等，几乎所有未加密的内容。
  - 2) 节点破坏：通过任何手段（如电涌、物理力或弹药）破坏节点，使其无法正常工作。
  - 3) 节点故障：由于传感器故障或能量耗尽等原因，可能会发生节点故障。
  - 4) 节点故障：当节点无法正常工作时，会发生节点故障。例如，如果异构网络的簇头在正常操作中失败，则WSN协议必须足够强大，以减轻这种节点故障的负面影响，通过选举新的簇头和/或提供网络路径的备用路由。
  - 5) 流量分析：通过分析流量模式，可以推导出有关网络拓扑的重要信息。

针对WSNs和IoT的攻击

- 被动攻击
  - 被动攻击的种类
  - 4) 节点故障：当节点无法正常工作时，会发生节点故障。例如，如果异构网络的簇头在正常操作中失败，则WSN协议必须足够强大，以减轻这种节点故障的负面影响，通过选举新的簇头和/或提供网络路径的备用路由。
  - 5) 流量分析：网络的流量模式可能与数据包的内容一样有价值。通过分析流量模式，可以推导出有关网络拓扑的重要信息。在WSN中，靠近基站的节点，即汇点，比其他节点进行更多的传输，因为它们比远离基站的节点转发更多的数据包。同样，分组是WSN可扩展性的重要工具，簇头比网络中的其他节点更忙。检测基站、靠近基站的节点或簇头可能对攻击者非常有用，因为拒绝服务攻击针对这些节点或窃听发往这些节点的数据包可能产生更大的影响。通过分析流量，可以推导出这种有价值的信息。此外，流量模式可能涉及其他机密信息，如行动和意图。在战术通信中，沉默可能表明准备攻击、战术行动或渗透。同样，流量速率的突然增加可能表明故意攻击或突袭的开始。

针对WSNs和IoT的攻击

01

在主动攻击中，恶意行为不仅针对数据保密性，还针对数据完整性。主动攻击还可以针对未经授权访问和使用资源，或者干扰对手的通信。主动攻击者会发出无线电辐射或动作，可以被感知到。在主动攻击中，攻击者实际上影响了被攻击网络的运行。这种影响可能是攻击的目标，并且可以被检测到。例如，网络服务可能会因这些攻击而降级或终止。

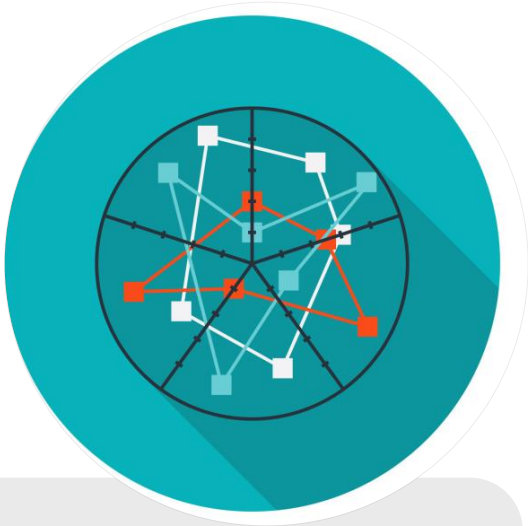
02

涵盖物理层到应用层的DoS、数据篡改等，影响网络服务和数据完整性，攻击者主动干扰网络运行。

针对物理层的攻击：

阻塞式DoS攻击

在这种物理层DoS攻击中，恶意设备可以通过在相同频率上发送信号来干扰信号。干扰信号会增加载波噪声，其强度足以将信噪比降低到节点需要正确接收数据的水平以下。干扰可以持续进行，从而阻止该区域的所有节点进行通信。或者，干扰可以在随机的时间间隔内暂时进行，仍然可以非常有效地阻碍传输。



节点捕获攻击

攻击者通过物理攻击接管传感器节点的控制，例如将电缆连接到其电路板上并读取存储的数据以及WSN中的传输。此外，通过篡改，攻击者可以更改电子板更改节点的内存内容，并使用捕获的从属节点进行任何操作。捕获节点可能会暴露其关键数据，尤其是揭示与密码学相关的密钥，从而可能导致整个WSN的妥协。捕获的节点可以代表攻击者进行任意查询（针对可用性的DoS攻击）。

捕获的节点可以向合法用户提供虚假数据（针对完整性的攻击）。

针对数据链路层的攻击：

- 数据链路层，尤其是MAC方案中的算法，提供了许多利用机会。例如，通过DoS攻击持续干扰信道，或者基于MAC层寻址方案设计更复杂的攻击。数据链路层攻击可以分为以下几类：碰撞攻击、睡眠拒绝攻击、去同步攻击、耗尽攻击、链路层泛洪、链路层干扰、ARP欺骗和不公平性攻击。

针对数据链路层的攻击：

01

碰撞攻击

攻击者会在网络中的合法节点开始传输时立即在同一信道上进行传输。结果，两个传输发生碰撞，接收器将无法解释接收到的数据。最终，接收器会请求重新传输同一数据包。消息的一个字节的碰撞就足以导致循环冗余校验（CRC）错误，从而使整个消息变得无用。对于攻击者来说，这种攻击比干扰更有优势，因为消耗的传输能量较低，检测到的概率较小。

02

睡眠拒绝攻击

针对电池设备，通过执行碰撞攻击或重复握手来实现，即通过持续操纵请求发送（RTS）和清除发送（CTS）流量控制信号，最终阻止节点进入睡眠阶段。耗尽设备能量。

03

去同步攻击

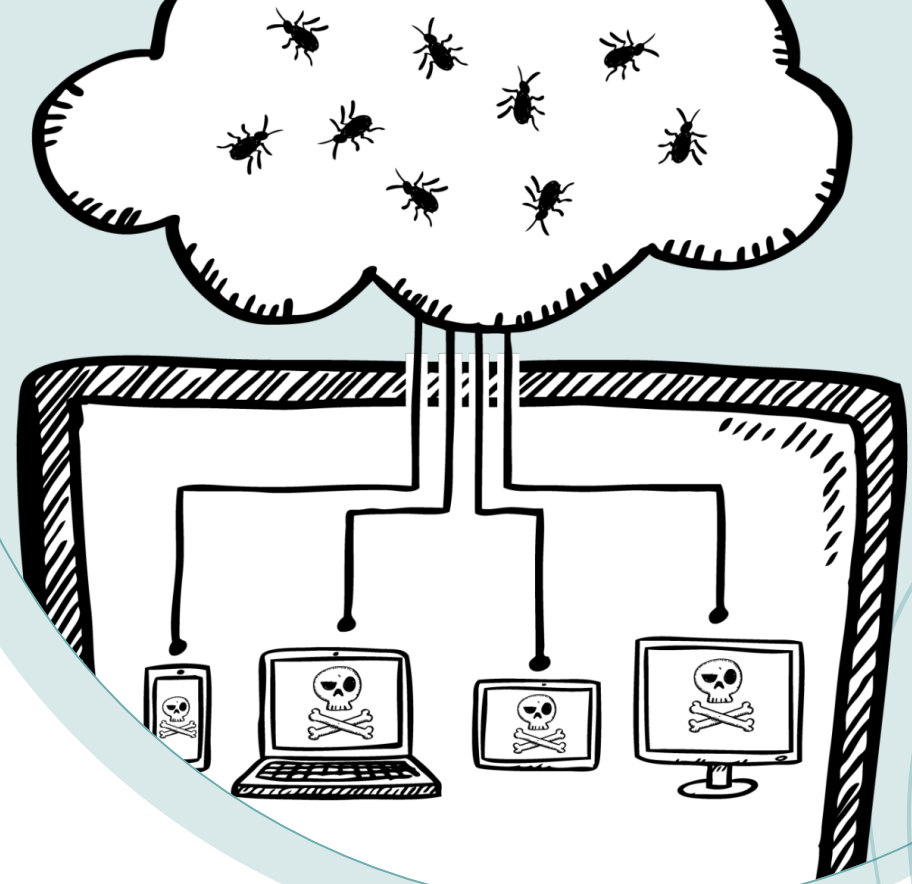
干扰TSCH时间同步协议，导致节点错位，影响一致性这种攻击可以被视为碰撞攻击的升级版。

04

耗尽攻击

如果上述描述的碰撞攻击持续进行，直到目标节点耗尽能量，这被称为耗尽攻击。这种攻击可以通过使用普通节点或笔记本电脑来执行，这些设备具有在传感器使用的同一频段内传输无线电信号的能力。

针对数据链路层的攻击：



01 链路层泛洪

恶意节点滥用介质访问的公平性，向其相邻节点发送过量的MAC数据包或MAC控制包。最终，受害节点遭受DoS攻击或电池电量耗尽。此外，这种攻击还可能耗尽信道带宽资源。

02 链路层干扰

数据包到达时间的概率分布被获取并用于针对特定数据包传输进行干扰，影响协议如B-MAC、L-MAC和S-MAC的效率。

03 欺骗/ARP欺骗

恶意节点欺骗受害节点的MAC地址，然后从受害节点创建各种合法身份，并在网络的其他地方使用这些身份。在ARP欺骗攻击中，攻击者向网络发送伪造的ARP（地址解析协议）消息。通常，目标是将自己的MAC地址与更高级别的节点的IP地址关联起来，例如默认网关，导致原本发往该IP地址的流量被发送到攻击者那里。

04 不公平性攻击

间歇性的耗尽攻击或协作MAC协议的误用可能导致网络不公平。这种攻击不会使用户或节点完全断开网络，但会导致间歇性的黑屏，用户发送/接收延迟消息。这种攻击降低了网络的服务质量，因此为最少数量的传感器节点提供了优势，而对网络的其他部分造成了不利影响，因为其他节点在实时MAC协议配置中错过了传输截止日期。

05 针对6LoWPAN攻击

利用了接收者无法在6LoWPAN层验证碎片是否来自同一IPv6数据包的先前接收到的碎片的事实。因此，接收者在接收时没有用于检查接收到的碎片是原始碎片还是伪造的重复碎片的身份验证机制，这种攻击可以轻松欺骗接收者。为DoS攻击创造条件。

针对网络层的攻击：

01

HELLO泛洪

攻击者广播广告消息，使其成为邻居，导致网络拥塞。

02

黑洞攻击

恶意节点可能会丢弃它接收到的所有用于转发的数据包。这种攻击组合可能会停止黑洞周围的所有数据流量。

03

选择性转发攻击

特殊的黑洞攻击，，选择性地丢弃一些数据包。通过这种方式，攻击者期望保持未被IDS检测到。

04

Wormhole攻击

攻击者通过非带内通道建立快速传输路径，吸引流量。难以检测，影响许多网络服务的性能，如时间同步、定位和数据融合。

05

Node-Replication（克隆）攻击

攻击者复制被攻击节点的多个副本，引起不一致性。它使攻击者能够通过使用几个被攻击的节点的副本来改变网络的行为。

针对传输层的攻击：

攻击者通过在它们之间去同步传输来破坏两个节点之间的实际链接。这种攻击的一个例子是连续向通信双方发送伪造的消息，例如发送带有伪造序列号或控制标志的伪造数据包，这些标志会去同步端点，使它们重新传输数据，从而迫使它们失去同步。

去同步化

在计算机科学中，这种攻击被称为“利用”和“篡改”有效的通信会话（也称为会话密钥）以获得对系统信息或服务的未授权访问。作为IP网络的扩展，TCP消息的会话劫持也会影响和困扰物联网网络

会话劫持攻击

通过向节点发送大量虚假消息来耗尽节点的能量和/或内存。例如，通过发送多个连接请求但不完成连接，从而使缓冲区过载并最终导致节点死亡。更具体地说，在TCP SYN（同步）洪水攻击中，攻击者发送多个TCP连接请求但不完成连接，从而使目标的半开连接缓冲区过载。

SYN-flooding 攻击

针对应用层的攻击：

应用层协议也可以被利用进行DoS攻击。例如，节点定位、时间同步、数据聚合、关联和融合等协议可以被欺骗或阻碍。例如，一个恶意节点伪装成信标节点并提供虚假的位置信息或欺骗其传输功率，即传输的功率比其应该传输的功率多或少，可能会破坏节点定位方案。由于这种攻击会降低相关网络服务，因此也可以将其归类为DoS攻击。应用层DoS攻击的一个例子是路径型DoS攻击，将在下面描述。所有应用层攻击都被分类和描述如下。

01

错误信息注入

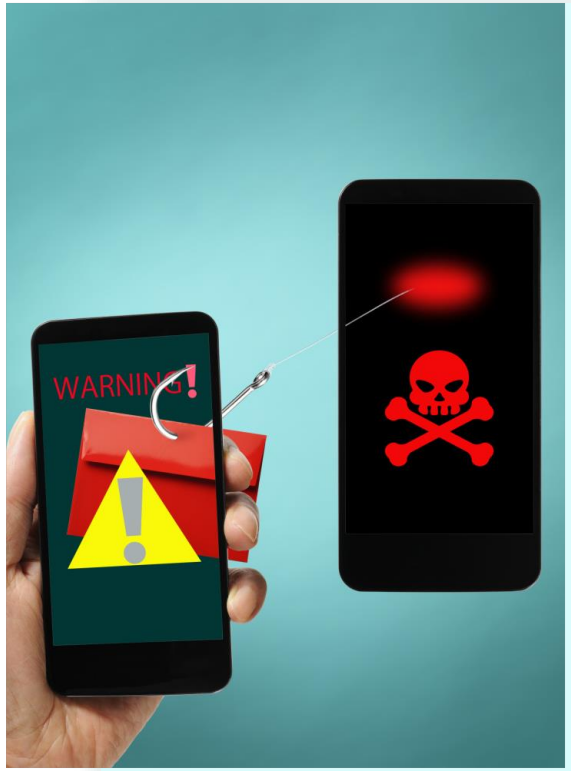
攻击者故意注入虚假数据，干扰测量结果，产生语义层面的攻击，影响逻辑但不破坏其他方面。

02

路径DoS攻击

攻击者通过向端到端的通信路径发送伪造包或重放包来淹没远距离的节点。从攻击者到目的地的路径上的所有节点都会受到影响

针对应用层的攻击：



重编程攻击

每个网络元素都需要定期打补丁或重新编程以进行版本控制、代码获取和编码解码，当切换到新版本时也是如此。对于WSN和IoT来说也是如此。如果这种重新编程（或补丁管理本身）的计划不是保密的，那么攻击者可以利用这个网络的脆弱时期，通过向节点发送虚假消息来利用这个机会。。

传感器压倒性攻击

通过向传感器发送大量虚假消息或干扰，攻击或改变其敏感性，淹没传感器功能，影响其正常操作。

谢谢