物联网电子医疗的DoS / DDoS检测

Iftikhar ul萨
米人
巴基斯坦卡拉奇经济与技术研究院理学与工程研究生院
卡拉奇

Maaz斌艾哈迈德
巴基斯坦卡拉奇经济与技术研究院理学与工程研究生院
卡拉奇

穆罕默德阿西夫
拉合尔大学拉合尔大学

拉菲乌拉
巴基斯坦卡拉奇经济与技术研究院理学与工程研究生院
卡拉奇

摘要 **– 物联网（IoT）已经成为通信时代的一个新的视野。物联网为各种新兴技术和应用增长提供了平台。 电子医疗服务也已经整合，并从物联网中受益匪浅。 由于计算机技术的日益普及，计算机网络面临严峻的安全挑战，物联网也面临着同样的安全威胁。 由于物联网已经为电子健康等其他领域提供了平台，这些服务也容易出现这种威胁。 对物联网中的电子健康服务器的拒绝服务（DoS）和分布式拒绝服务（DDoS）攻击会危及病人的实时监控以及电子健康服务的整体可靠性。 在本文中，已经对物联网中的DoS / DDoS攻击的现有解决方案进行了审查，并提出了一种可靠的解决方案来保护服务器免受这些攻击。**

关键词：E-保健； DDoS攻击；物联网

I. 介绍

物联网（IoT）融合了环境监测，基础设施监测，能源管理，交通管理和医疗保健管理等各个领域的生活。 今天，这些领域正在取得新的进展。 这些进步背后的基本动机是创造简单的基础设施，并为消费者提供可靠的解决方案。 图1显示了物联网的概况。 由于这些技术的异构性，交通系统监控和医疗监控等关键应用需要特别注意及时安全地传输数据。 世界各大城市都在从物联网中受益，进行实时交通监控，并将各医院整合到物联网中，扩大患者的健康监测。 患者也从这些技术中受益，因为他们正在不断地进行监测，而无需定期到医院就诊。

目前，不少医院正在为病人提供电子医疗设施，而医生也不断地对这些病人进行监测。 这些医院正在与这些患者正式达成协议，以扩大所需的服务。 由于这些医院地理位置在

一个国家的特定地点，他们的病人也离这些医院更近或中等距离。 如果这些患者需要体检，那么他们可以轻松访问这些医院。

图1. 物联网。

电子医疗是医疗服务的现代化，主要是为了使电子健康消费者和健康专业人员受益。 图2显示了电子医疗场景。在身体上使用传感器监测健康状况的患者是电子医疗系统的消费者，负责扩展医疗服务的医生，护士和相关人员是健康专业人员。 患者数据的保密性非常关键，必须保证证明系统的可靠性。 电子卫生系统中的服务器非常关键，因为在这些服务器的帮助下对病人进行实时监控。 如果这些服务器暂时无法使用，病人的健康监控可能会受到影响。 网络的扩张增加了网络漏洞，同时也引发了专业黑客对关键资源的复杂攻击。 电子健康是关键和最具挑战性的领域，其中网络的可用性是最重要的，如果网络变得

在像DDoS这样的大规模攻击下，患者的救命行动可能非常困难。 所以，必须有一个机制来确保可靠性并防止/检测这种类型的攻击。

本文的内容安排如下：第二部分是关于文献综述。 在第三部分，提出了解决方案。 第四节是关于结论和未来的工作。

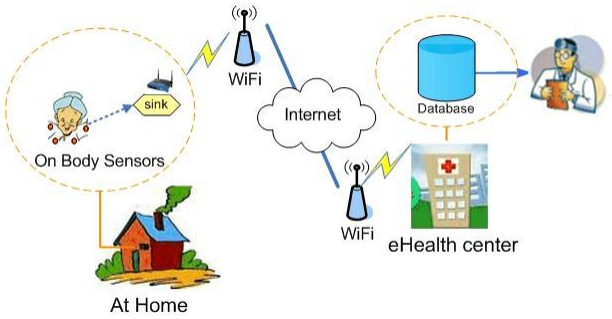

图2. 电子医疗系统。

II. 文献评论

[1]的作者已经将DDoS攻击分为洪泛和逻辑（软件）攻击两类。 在泛洪攻击中，他们强调了SYN泛洪，ICMP攻击，UDP洪泛和逻辑攻击，他们发现了死亡，泪滴攻击和地面攻击。 他们建议通过安装最新的补丁和在这些边缘路由器上应用过滤来防止边缘路由器的DDoS攻击。 通过拒绝协议，IP地址和端口来防御DDoS攻击，可以有效地利用防火墙。 他们还强调了DDoS检测技术，例如基于签名的检测和基于异常的检测。 本文提出了利用负载均衡，容错和服务质量等技术来应对威胁的对策。 [2]的作者提出了一项调查，他们已经在网络上突出显示了各种类型的DoS / DDoS攻击，其中包括UDP Flood，ICMP / PING flood /，SYN flood，死亡ping。 他们还确定了可以发起DoS攻击的场景，如干扰，杀死命令攻击和去同步攻击。在本文中，他们没有提出任何防止网络上的Dos / DDoS攻击的方法。 [3]的作者已经讨论了干扰等各种攻击，可以通过使用密码技术（基于属性和基于模糊属性）来避免。他们提出了扩频，优先消息和循环任务来对付干扰和窃听攻击。 通过应用纠错码可以避免网络冲突攻击。 洪泛攻击是用来造成网络混乱的。 [4]的作者已经确定了针对DDoS的各种防御方法，如过滤攻击数据包，单/多源攻击以及IDS系统的应用。 他们提出了适应性防御机制，可以根据攻击的严重程度自适应调整自己。 在自适应的方法中，他们把重点放在特定时间的流量值上，这在当时显然是非常高的攻击。 文献[5]的作者利用支持向量机分类器分析了基于源IP地址HTTP GET请求熵的应用层攻击模式。 [6]的作者提出了一个基于信息论的检测方案，他们使用了用户浏览行为。 在熵的基础上，确定可疑的请求。 他们建议限速器将服务降级为恶意用户。 [7]的作者在各种情况下探讨了DDoS洪水攻击的范围，并根据拥塞程度，根据其中一种对策是丢包的情况探讨了各种对策。

文献[8]的作者分析了安全措施的协同环境，并确定了各种工具，并对现有的追溯机制进行了调查，以确定真实的攻击者。 文献[9]的作者提出了应对物联网服务器上的DDoS攻击的网络架构和思想。 他们提出了一个路由器节流技术，通过在压力较大的服务器上提供漏斗率。 在他们提出的解决方案中，他们使用k级最小公平技术来分配路由器中的服务器容量。

在上面的参考文献中，研究人员尝试了不同的技术来应对这种攻击，因为对于不同的网络情况没有具体的解决方案 随着时间的推移，攻击的性质和严重程度也在发生变化，这也需要最先进的技术来应对这个问题。 一些研究人员也尝试使用机器学习的方法来学习不同的攻击检测模型，这反映出仅仅使用传统的网络分析技术是不够的，需要各种其他的综合措施来保护网络资源免受这些攻击。DDoS攻击的基本场景如图3所示。

III. 建议的方法

在我们提出的解决方案中，我们采取了一些假设，使服务器在正常运行情况下具有一些正常的缓冲区利用率，即70%或75%。 但是当其利用率从正常范围增加到最大时，怀疑服务器正在遭受DoS攻击。 在这种情况下，服务器要采取有选择性的丢包方法等自适应措施逃避这种攻击。

在提出的解决方案中，我们使用了服务器的数据包缓冲区利用率和到达数据包的TTL值，并将这两个值与预定义的值匹配，以便分析攻击模式。

我们知道，当数据包在路径中时，其可变字段在各个路由器处发生变化，其TTL值也在每个路由器处递减。 因此，启发式方法是在网络中距离较远的数据包有较少的生存时间，这表明这些数据包来自地理距离较远的地方。这些数据包可能由机器人或使用各种DoS攻击技术的某些子网生成。 以下算法已被建议检查DoS攻击

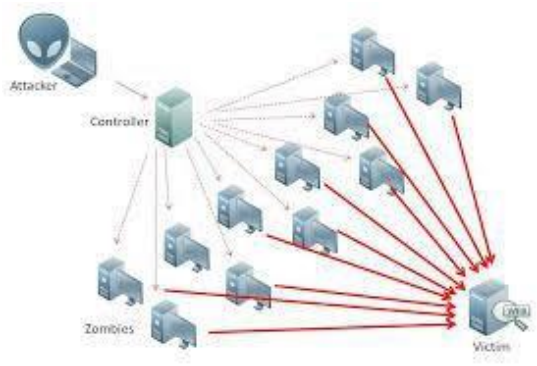

图3. DDoS攻击

算法：

1. 读取服务器缓冲区使用
2. 如果缓冲区利用率>阈值
   //服务器被怀疑受到DoS攻击
3. 如果（数据包TTLvalue <最小\
   值）丢弃这些数据包
4. 其他

在一些特定的时间之后去

我们也可以考虑节点的地理位置。 我们知道协调员（控制器体域网络）必须在某些地理位置预定义。 通过使用这些信息，我们可以计算可能进入数据包路径的路由器（估计）的数量，以检测DoS攻击。 由于合法的节点有一些预定义的时间向服务器发送数据，攻击者节点可能花费比正常的计算时间更长的时间。

MTU = 1500字节（1460字节有效载荷+ 40字节标题）

链路数据速率= d_rate

在协调方"A是协调员"

按节点获取数据的时间"A"= TGA数据包大小\

（以位为单位）= Psize

数据速率以位为单位= Dr

TGA = Psize / DrTGA = Psize / Dr (1)

数据发送到服务器的速度或速率= V数据包到

达服务器所用的时间= T_travel

T_travel = total_dist / VT_travel = total_dist / V

从服务器获取链接的时间（Receiver）= TGs注意

TGs = TGA

总时间=总时间

(2)

使用这个Total_time我们可以检测到DoS攻击。 通过使用启发式，我们的实际节点必须有一定的时间才能到达服务器。 我们将丢弃Total_time大于某个阈值的所有其他数据包。

算法：

1. 计算传入数据包的总时间
2. 如果Total_time> =阈值
   //怀疑受到攻击的服务器丢弃这些
   数据包
3. 其他
   接受数据包

我们提出的解决方案是基于这样的假设：所有通信节点都存在于特定的地理位置（由于某些原因暂时离开实际区域的几个节点除外），并且最有可能的路线是在调试前的试验中计算的。 一天中不同时间的分组的总分组行程时间也被采用，并且基于这些分组行程时间来计算阈值速率。 服务器的缓冲区利用率也是基于预先计算的

系统的调试试验。

IV. 结论

在我们提出的解决方案中，我们侧重于提高服务器能力以观察攻击模式，并采取适应性措施来处理DoS / DDoS攻击。 我们也试图避免过度加重边缘/路径路由器来梳理这些攻击。 在我们提出的解决方案中，也可以通过预先计算的TTL值来识别合法的数据包，并且在攻击达到其峰值点之前，可以容易地识别和丢弃攻击数据包。 通过这种方式，合法用户的正常流量也可以实现，并且实时地对包进行过滤。

V. 未来的工作

在今后的工作中，我们将采用机器学习的方法来提高系统处理DDoS攻击的能力。 我们系统的日志将被用来训练我们的模型，基于训练样例，可以及时的观察到攻击行为，并且可以有效地利用自适应的防御机制。

我们提出的解决方案存在一个问题。 如果攻击者与我们的合法用户距离相同，那么我们的算法将在这里检测到攻击。 对于这种情况我们提出了多层检查。 我们设定了一些范围，我们提出的解决方案将使用一些现有的方法。

参考

[1] A. Srivastava, BB Gupta, A. Tyagi, Anupama Sharma和Anupama Mishra, "最近对DDoS攻击和防御机制的调查", "并行分布式计算的进展", 第570-580页, 2001年。

[2] Krushang Sonar和Hardik Upadhyay, "调查：DDOS对物联网的攻击", 国际工程研究与发展杂志, pp. 58-63。 2014年

[3] Masdari, Tahmineh Haddadi Bonab和Mohammad, "无线人体局域网中的安全攻击：挑战和问题", 2015年10月10日, 西班牙科学与技术学院。

[4] 李慕海, 李明, "防御DDoS攻击的自适应方法", 工程数学问题, 2010。

[5] 倪同光, 顾小青, 王洪源, 李煜, "应用层DDoS攻击的时间序列分析实时检测", 控制科学与工程, 2013。

[6] S. Renuka Devi和P. Yogesh, "Detection of Application Layer DDoS Attacks using Information Theory based matrics", 计算机科学与信息技术（CS&IT）, 第217-223页, 2012。

[7] M. Young，“防御分布式拒绝服务（DDoS）洪水攻击的防御机制综述”，IEEE通信调查与教程，第2046-2069页，2013年

[8] Arun，Raj Kumar P.和S. Selvakumar。 “协作环境中的分布式拒绝服务（ddos）威胁 - 对ddos攻击工具的调查和回溯机制。“在先进的计算会议，2009年IACC 2009. IEEE国际，页1275-1280,2009。

[9] 丘，大卫，吕，冯良，杨萌。 “用最大最小公平的服务器中心路由器节流阀来防御分布式拒绝服务攻击”。 IEEE / ACM网络交易（TON）13，no。 1（2005），第29-42页。