深入探索基于可扩展网络安全的分布式 SDN 架构设计

陈翰杰

（泰国格乐大学，泰国 510310）

摘要：尽管互联网相对成熟，但今天的计算机网络仍然容易受到攻击。为了实现广域连接，网络必须具有分布式特性，这在传统上导致了安全网络设计和实现的高成本和复杂性。随着软件定义网络（SDN）和网络功能虚拟化（NFV）的引入，有机会进行有效的网络威胁检测和保护。SDN 的全局视图提供了一种跨越整个网络的监视和防御手段。然而，当前基于 SDN 的安全系统受到集中式框架的限制，该框架引入了大量控制平面开销，导致重要控制链路饱和。在本文中，我们介绍了 TENNISON，一种新型的分布式 SDN 安全框架，它将 SDN 控制和监控的效率与分布式系统的弹性和可扩展性相结合。TENNISON 提供有效和适当的监控和修复，与广泛可用的网络硬件兼容，支持遗留网络，以及模块化和可扩展的分布式设计。我们通过使用四种攻击场景来演示 TENNISON 框架的有效性和能力。这些突出了多个级别的监控，快速检测和修复，并提供了对多个控制器对大规模网络攻击检测的影响的独特见解。

关键词：定义网络；网络安全；互联网；虚拟化

在一个日益网络化的世界里，我们依靠可靠的通信技术进行日常业务和社会互动。与此同时，网络攻击导致网络中断的频率也在增加。例如，2015 年至 2016 年间，分布式拒绝服务（DDoS）攻击增加了 71%，同期大于 100 Gbps 的攻击增加了 138%。2016 年 10 月，多起针对域名服务器（DNS）提供商 Dyn 运营的系统的 DDoS 攻击。这次攻击被认为是由感染了 Mirai 恶意软件的物联网设备僵尸网络精心策划的，超过 60 个服务受到影响。这些例子突出了当今网络攻击的几个特点；它们是分布式的，可能涉及高流量，并通过网络入侵远程执行。这些特性说明了监控网络事件（包括网络流量、流量和设备状态）对于有效检测和保护攻击的重要性。

一、网络概念含义

传统网络中的网络威胁检测和保护通常是通过专用硬件实现的安全设备（中间设备），成本很高，需要仔细放置在网络中，以确保适当的流量捕获。这种固定的位置限制了对特定网段上流量的可见性，从而限制了对捕获数据进行上下文分析的可能性，从而限制了网络安全功能的能力。

软件定义网络（SDN）作为一种动态控制计算机网络配置的概念而出现。从根本上说，SDN 将网络设备中的控制平面和数据平面分开。然后将这种控制交给基于软件的控制器，该控制器定义网络的行为和操作。

二、软件网络的特征

SDN 的特点包括全局网络视图和数据平面的可编程性。此外，OpenFlow （OF） Switch 规范描述了 SDN 数据和控制平面之间的通信协议，它为交换机流表中的每个流项 / 规则定义了计数器。流规则定义还支持大量的报头字段（> 40 个字段）。这些在数据平面捕获的网络统计数据的粒度支持安全功能的流量监控。

这些特征使一个强大的反馈循环如下：网络攻击可以通过捕获流量信息和分析流量统计与已知的签名 / 模式（或通过机器学习技术的应用）。通过流量、类型或模式检测到攻击后，即可部署入侵防护系统。SDN 的好处是，它可以用于对流规则进行编程，以阻止或过滤流量，或者应用另一种补救机制。然而，在大规模部署流量监控服务时，会出现性能 / 准确性的权衡。要收集的信息量可能导致整体性能下降，而引入较长的收集间隔可能导致不准确或延迟修复。在集中式 SDN 安防系统中，监控数据量的影响尤其显著，有可能压倒控制器的处理功能。对 DoS 攻击的监控有可能产生足够的针对控制器的监控流量，从而使控制器本身受到 DoS 攻击。因此，需要一种解决方案来提供灵活和适当的监视功能，并使用分布式功能来分散控制和监视负载，以实现可伸缩性和弹性。为了应对这一挑战，我们提出了 TENNISON，一个建立在多层次补救机制之上的分布式 SDN 安全框架。许多安全框架和应用程序之前已经提出，每一个都建立在这些 SDN 特性的选择之上。然而，TENNISON 的新颖之处在于它支持多级监控功能。它提供了在大量流中执行轻量级监控的能力，同时提供了对选定流执行深度数据包检测（DPI）的能力。TENNISON 是一个分布式 SDN 安全框架，支持多级监控。在本节中，我们回顾了与基于 SDN 的监控，基于 SDN 的安全系统和分布式 SDN 控制器性能相关的先前工作。还有许多与此工作相关的 IETF 文档。如 I2NSF （Interface to Network Security Functions）、DDoS Open Threat Signaling（DOTS）、Network Security Header （NSH）等。

三、新时代网络监控面临的挑战及解决方法

A.SDN 监控全球网络视图和数据平面上捕获的网络统计粒度的结合使人们对 SDN 网络监控的进展产生了极大的兴趣。传统的监控协议如 NetFlow/IPFIX 和 sFlow 与 SDN 协议 OpenFlow 的结合已经被探索过。先前的工作旨在解决大规模监测的挑战。例如，FlowSense 使用基于推送的方法从交换机接收流量统计信息。自适应速率监测也被引入；OpenNetMon 和 OpenTM 以自适应速率轮询选择交换机，以减少网络和交换机的 CPU 开销。PayLess 使用自适应采样算法根据测量的吞吐量改变轮询频率。同样，FlowCover 通过优化轮询功能来降低监控通信成本。OpenMeasure 使用在线学习来适应流量测量。这支持可扩展的测量，包括对大多数信息流的监控，以及跨多个交换机的监控规则的最佳放置。基于代理的监控在代理中引入监控表来指定流量监控的测量间隔，并将相关的流规则推送到 OpenFlow 交换机。然后，流统计 – 请求 / 应答只交换那些指定的被监视流，而不是所有流。

这减少了与 OpenTAM 类似的统计通信量，OpenTAM 是一种特定于 onos 的自适应监控工具。然而，这项工作有几个明确的限制；

抓包性能是有限的到 60Mbps 时，系统被限制为 600 个条件条目（即：规则捕获 / 监控），它是基于 OpenFlow 1.0。在 FlowRadar 中，作者解决了在数据中心监控的挑战，其中现有 NetFlow 实现选项不适合，要么是由于高端路由器（基于硬件）的过高成本，要么是交换机 CPU 资源需求过高（基于软件）。FlowRadar 解决方案是通过编码每流计数器来平衡工作负载，这些计数器具有低内存需求和恒定的交换机插入时间。然后在有可用计算资源的远程收集器上执行流计数器的解码和分析。FlowRadar 为跨数据中心的全网监控提供了一个可扩展的解决方案，独立于 SDN 或 OpenFlow。SDN mon 试图通过将监控逻辑与转发逻辑分离的 SDN 监控框架来改进监控应用程序的粒度。SDNMon 实现监控的方式与 TENNISON 类似，它使用多个表来分离监控和转发。

最近，Tsai 等人概述了 SDN 监控解决方案，确定了挑战和开放问题。研究进展根据监测阶段进行分类，即收集、预处理、传输、分析和呈现，大多数研究集中在预处理阶段，例如 OpenTM。利用 sFlow 的好处是将混合环境中的监控与传统网络设备集成在一起，这是 TENNISON 采用的方法。同样，我们解决了中确定的开放性问题；利用监控和数据收集来检测安全威胁，以及多域协作网络监控。TENNISON 扩展了现有的监控解决方案，提供了在大量流中执行轻量级监控的独特能力，同时提供了在选定流上执行 DPI 的能力。TENNISON 多级监控设计为所需的检测选择合适的监控工具，如采样监测足够时选择 sFlow，详细监测时选择 IPFIX，有效载荷检查时选择镜像 / 重定向到 DPI。这样可以减少监控流量，支持大规模网络部署。TENNISON 的设计通过跨多个控制器实例的监视分布（和协调）进一步支持可扩展的监视。

CIPA 在 of – sdn 交换机上应用人工神经网络（ANN）来检测扫描、蠕虫爆发和 DDoS 等分布式、协同入侵攻击。假阳性 / 检测率和通信开销都显示为比 Gamer 有所改进。Ha 等人考虑了 sdn 中的入侵检测。在中，提出了一种流分组方案来确定哪些流转发给哪些 ids，以获得最佳的入侵检测性能。使用主成分分析（PCA）对可疑流量进行分组，并使用基于重力的聚类将这些分组分配给 ids。在示例结果中，每个 tap 都进入一个聚合交换机，从该交换机分配到 ids。从延迟的角度来看，这将抵消分布式实现的好处。

四、优化网络研究试验分析

作者提出了优化每个交换机的采样率以提高大型网络中恶意流量检测性能的结果。优化是交换机的数据速率、流量的恶意流量速率和交换机的采样率的函数。但是，首先需要估计恶意流量的速率，然后根据调整后的采样率收敛到实际值。该速率的选择对收敛时间有很大影响。为了展示 TENNISON 将在各种网络大小和拓扑结构中运行，通过分析了系统的多个组件，并将结果与真实网络轨迹的统计数据进行了比较得出以下结论。

（一）多级监控：基于响应式 SDN 应用在极端流量下的局限性

沉重的控制器通信 / 处理工作量得到了突出体现。为了解决这个问题，TENNISON 实施了多级监控，如 IV–D 所述。还应用了特定的优化来保护网络控制器免受流量泛滥场景的影响，例如由 DDoS 攻击引起的影响。这是为了响应 ONOS 发现的一个问题而引入的，在这个问题中，控制器会经历高 CPU 和内存使用，失去与交换机的通信，最终导致网络崩溃。该解决方案利用了 TENNISON 资源监视器，并在适当的时候引入了阈值机制来缩减监控流量的数量，以防止控制器和控制平面被流量淹没。尽管 ONOS 被设计为在故障情况下将控制转移到备用控制器，但实际上这种转移发生得太晚了。我们的 TENNISON 解决方案先发制人地维护网络控制。

（二）轮询速率根据三个阈值进行调整

阈值 A：当网络流量达到阈值 A 时，TENNISON 资源监视器触发 TENNISON 将 IPFIX 轮询间隔从 1 秒增加到 5 秒。这减少了控制器上的处理，从而提高了性能。阈值 B：当超过第二个阈值时，将轮询时间间隔增加到 10 秒。阈值 C：一旦超过第三个阈值，TENNISON 禁用 IPFIX 轮询并增加 sFlow 采样率。在这种情况下，TENNISON 完全依赖 sFlow 进行网络监控。

对于每一个阈值，默认的超时是 20 多岁即在 20 年代，TENNISON 重置 IPFIX 轮询间隔回到默认（A 和 B）的阈值或重新启用 IPFIX 轮询（在阈值的情况下 C）。增加轮询间隔的影响在 DDoS 攻击检测 / 保护延迟时间见表四。结果平均在一系列 5 测试阈值，B 和 C 设置为 1 Kpps，5 Kpps，分别和 20 Kpps。在深入研究面向可扩展网络安全的分布式 SDN 框架时，我们特别关注其检测和保护能力以及在大型网络中实现可扩展监控的潜力。它支持基于合理的控制器与交换机分配以及最佳监控规则放置，优化了网络监控与保护流程。这一创新不仅提升了网络的安全性能，也提高了网络管理的效率。

五、总结与展望

随着网络规模的扩大和复杂性的增加，我们需要进一步探索如何自动化这一扩展过程。这包括配置额外的控制器以应对不断增长的网络负载，确保网络始终保持高效、稳定的运行状态。此外，我们还将研究在 TENNISON 架构内的不同层进行扩展的可能性，以进一步提升网络的安全性和性能。特别是在协调层引入分布式策略时，我们必须认识到这会产生一致性方面的额外需求。为了保持网络的持续覆盖和可见性，我们需要采取适当的措施来处理这些需求，确保网络的安全和稳定。

综上所述，面向可扩展网络安全的分布式 SDN 框架研究是一个充满挑战与机遇的领域。通过深入研究和实践，我们有望为网络安全领域的发展贡献更多的力量。

参考文献：

[1] 林川，韩光洁，毕远国，等 . 一种基于 SDN 的车联网分布式雾计算体系结构设计方法 .CN201910693875.7[2024-05-07].

[2] 王浩 . 信息动员潜力资源分布式管理系统的设计与实现 [D]. 电子科技大学 [2024-05-07].

[3] 詹志宏 . 基于 SDN 的数据中心路由策略与安全认证研究 [D]. 安徽大学 [2024-05-07].DOI：10.7666/d.Y3018723.

[4] 高小涵，李皓，刘丽哲，等 . 一种分层型分布式 sdn 网络安全防护方法及系统：202311705713[P][2024-05-07].