2022 第十三届信息与通信技术融合国际会议(ICTC) | 978-1-6654-9939-2/22/$31.00 ©2022 IEEE | DOI:

5G 工业物联网环境下基于 ai 的网络安全增强

李钟勋、金贤珍、朴哲熙、金永洙、朴钟根
电子与电信研究所网络安全研究部
韩国大田市
{我的,。继任者，chpark0528，闪电战，queue}@etri.re.kr

***摘要*:5G 网络旨在提供更高的速度、更低的延迟和更大的容量;因此，与以往的移动网络相比，5G 网络需要更先进、更智能的网络安全。为了检测未知的和不断发展的 5G 网络入侵，本文提出了一种基于人工智能(AI)的网络威胁检测系统，对 5G 网络流和安全事件数据进行数据标记、数据过滤、数据预处理和数据学习。首先在 nsl - kdd 和 CICIDS 2017 两个知名数据集上进行绩效评估;然后，在 5G 工业物联网环境中对所提出的系统进行了实际测试。为了演示在真实 5G 环境中对网络威胁的检测，本研究利用了 5G 模型工厂，该模型工厂被缩小为一个真实的智能工厂，其中包括许多基于 5G 工业物联网的设备。**

关键词:5G 网络安全，5G 边缘安全，智能网络入侵检测，基于 ai 的入侵检测，5G 模型工厂

I. 介绍

第五代(5G)网络提供先进的网络基础设施，使许多领域的新应用成为可能。5G 网络不仅是对之前 4G 蜂窝网络的演进，而且是一种具有许多新业务能力的网络架构[1]。大多数 5G 研究都是为了支持各种先进特性，如移动宽带用户的容量和密度高于之前的 4G 网络，以及大规模的设备对设备通信[2]。特别是，用于企业对企业(B2B)应用的 5G 专用网络从根本上基于面向 5G 网络的海量设备、可靠的低延迟通信和使用 5G 新无线电技术的增强型移动宽带的特点[3,4]。

因此，在 5G 组网环境下，针对海量物联网(IoT)设备、用户设备(UE)和各种边缘业务不断演变的攻击，智能网络安全变得越来越重要。即时识别靠近可疑网络活动或行为的网络入侵是维护 5G 设备安全性和可靠性的最关键挑战之一。因此，基于人工智能(AI)的网络入侵和网络威胁检测系统在 5G 安全领域得到了进一步完善。

本文的其余部分组织如下。第二节介绍了 5G 网络安全体系的相关安全问题，第三节介绍了 5G 网络安全体系，第四节给出了 5G 真实环境的测试与演示。最后，第五部分给出了结论。

II. 拟议 5G 网络的安全问题本节介绍与 5G 网络相关的安全问题

提出 5G 网络安全体系。在[2,3,4,5]中，提出了 5G 网络安全的各种问题和挑战。在[1,5,6]中，介绍了基于所提供的安全服务(如身份验证、可用性、数据机密性、密钥管理和隐私性)的安全解决方案。除了以往研究中的各种安全挑战外，本文还进一步讨论了与本研究相关的问题。

首先，尽管假警报率很高，但使用基于异常的网络入侵检测方法可以帮助识别以前未知的网络攻击[7]。在 5G 网络环境中，收集大量虚假警报的成本非常高，安全分析师需要付出大量努力来调查此类警报。

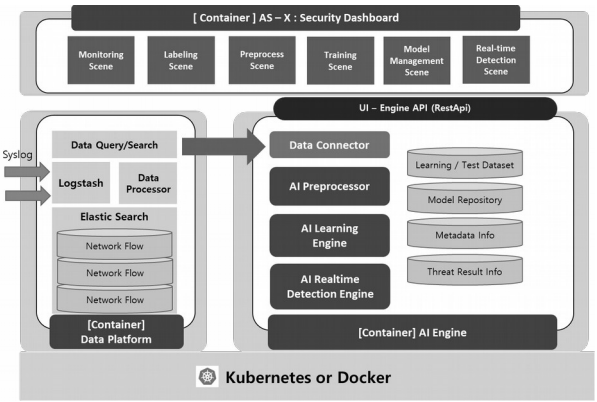

图 1 所示。提出基于人工智能的 5G-NTD 系统

其次，网络入侵已经演变成更加智能和多样化的方式。一些黑客可以通过不断发展他们的可疑行为和活动模式来完美地掩盖他们的恶意攻击。尽管可以使用适当的人工智能模型来检测这些恶意活动，但不断变化的攻击模式可能会使它们无法被检测到。此外，几乎所有的网络入侵检测方案都侧重于分析短期网络安全事件日志和警报。为了防御黑客不断演变的恶意活动，安全系统必须分析与较长时间相关的相关安全事件。此外，检测恶意行为和操作的最明显方法是基于与长期数据的比较，立即应用类似的模式[8]。

第三，在 5G 网络中，终端和基站以及服务提供商的双向认证可以保护

978-1-6654-9939-2/22/$31.00 ©2022 ieee

防止中间人(MITM)攻击。然而，这并不能阻止一个假基站嗅探直接连接到它的终端的流量[6]。然而，在[6]中描述的 5G 标准中的一个缺陷允许攻击者重用前一个会话的认证密钥来创建一个虚假的基站。这可能会给监控设备带来问题，比如以前 4G 网络中使用的 ISMI 捕获器。特别是在安全威胁分析方面，针对各种攻击类型进行了大量研究，针对恶意基站和恶意终端试图异常连接 5G 核心网进行漏洞分析。在[6]中，作者提出除了认证问题外，对 DNS 流量的拦截保护不足也会产生一系列问题。将合法 DNS 请求更改为返回恶意 IP 地址将允许攻击者执行 MITM 攻击、窃取凭据和部署远程恶意软件。

III. 5g 网络智能安全

本节介绍了基于人工智能的威胁检测系统，并简要描述了该系统的性能评估。

A. 基于 5G 人工智能的网络威胁检测系统

为了应对上述挑战，一个基于人工智能的网络

本研究提出了安全增强模型。的
模型基于基于相关性的安全事件分析和使用全连接神经网络(FCNN)、卷积神经网络(CNN)和长短期记忆(LSTM)对安全事件进行相互关联分析的组合，如图 1 所示。因此，我们分四个阶段开发并实现了基于 5G 人工智能的网络威胁检测系统，称为 5G- ntd。

首先，根据检测到的入侵结果报告中包含的相关信息(如威胁开始时间、威胁结束时间、受害者 IP 地址、攻击者 IP 地址信息)，对需要标记的数据集进行有监督学习。其次，在预处理阶段，将事件集转换为事件向量，并将事件向量嵌入到相关事件的最终事件轮廓中。随后，将包含模式配置文件的结果集合馈送到已实现的深度学习引擎中，例如在 5G-NTD 系统中执行的 FCNN、CNN 和 LSTM。最后，将学习生成的模型存储在模型库中，从模型库中加载模型后，即可进行实时网络入侵检测。

B. 5G-NTD 系统的贡献

5G- ntd 系统采用各种深度学习技术和数据预处理机制，能够处理大规模 5G 网络数据。具体而言，5G-NTD 系统的主要目标是通过执行多个分析引擎，自动分析与真实安全警报相关的网络安全事件和网络流，从而检测网络入侵。它还利用多个图形处理单元(GPU)内核的处理能力来进行更快的并行分析。

0.029，如表 1 所示。同样，对于 CICIDS 2017 数据集，所提出系统的准确性从
0.98 ~ 0.99, TPR 也接近 0.97,F-指标均在 0.96 以上。更详细的结果见[8]。

为此，系统旨在通过嵌入程序将收集到的大量 IPS 安全事件和原始网络数据分别转换为并发事件和网络流的统计模式概要文件。接下来，系统的目标是使用基于关联的事件分析和机器学习模型将原始事件分类为正常或威胁类。

该系统基于特定时间窗口内的数据特征，通过学习网络入侵模式和网络流，研究了一种泛化的安全事件分析方法。5G-NTD 系统包括一种事件模式提取方法，称为基于关联的安全事件分析，通过聚合事件同时发生的频率并将收集到的数据中的一组事件关联起来。

表 1 . nsl-kdd 数据集的评估

	NSL-KDD 数据集			
fpr 精度 f -measure 方法				
FCNN	0.941	0.029	0.958	0.952
美国有线电视新闻网	0.926	0.028	0.952	0.945
LSTM	0.919	0.025	0.950	0.943

表二。 cicids 2017 数据集的评估

	CICIDS 2017 数据集			
fpr 精度 f -measure 方法				
FCNN	0.982	0.002	0.995	0.987
美国有线电视新闻网	0.985	0.011	0.988	0.971
LSTM	0.978	0.011	0.986	0.967

C. 系统性能

本研究比较了网络入侵检测领域常用的两个知名数据集(NSL-KDD 和 CICIDS 2017)。 NSL-KDD[9]数据集包括四个可用分区:两个用于训练文件，两个用于测试文件。每个文件由 42 个特征组成，包括标签信息。CICIDS 2017[10]数据集的收集时间为 5 天，数据实例数量约为 280 万，包含 85 个包含标签信息的网络特征。虽然第一天的日志只包含正常捕获的活动，但其他几天的日志包含各种恶意攻击活动的数据点，包括 DoS、web 攻击和端口扫描。

为了评估系统的性能，使用了四个重要的指标:真阳性率(TPR)、假阳性率(FPR)、准确性和 F-measure，这是机器学习方法中常用的指标。此外，仅考虑一个度量作为系统性能评价的标准是不够的。各指标的评估结果表明，采用三种学习模型的基于 5G 人工智能的网络威胁检测系统在实验过程中取得了足够的数据分类性能。

两个数据集的每个指标的值如下:在 NSL-KDD 数据集上，系统的精度从 0.95 提高到 0.96,TPR 从 0.91 提高到 0.95,FPR 从 0.025 提高

IV. 在真实 5g 环境中进行测试

A. 5G 模型工厂

为了进行测试，我们使用了一个专用的测试平台来演示对类似于真实 5G 工业物联网环境的网络威胁的检测，该

环境包括几个基于 5G 网络的可编程逻辑控制器(PLC)设备、控制机器人和控制服务器。

5G 模型工厂是一个小型测试工厂，它将被缩小为一个真正的智能工厂，其中包括许多基于工业 5G 物联网的设备。 在模型工厂内部，有几个 PLC 设备、一个移动机器人和几个使用 5G UE 进行 URLLC 服务的传感器。此外，模型工厂还配备了机器人控制服务器、MEC 平台和 SCADA 服务器对其进行控制和管理。特别是，为了通过无线电资源互联，高效地支持数据传输，在模型工厂中提供了[11]开发的 5G 无线网络，并在 UE 与 gNB 之间进行了配置。

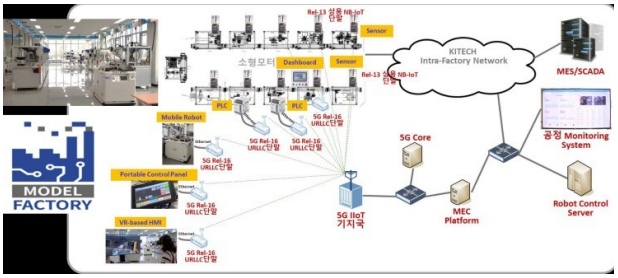

图 2 所示。小型 5G 测试环境的模型工厂

B. 测试环境

对于真实环境，当检测到网络攻击时，我们通过 5G 终端与 5G 核心网之间的网络镜像，收集 5G IPS 系统产生的安全事件和网络转储数据。为此，在 gNB 和终端之间部署网络采集器和一台 IPS 系统，由 IPS 系统通过 syslog 协议向 5G-NTD 系统发送安全事件。对于 5G-NTD 系统的监督学习和模型创建，通过利用攻击开始和结束的时间信息进行数据标记。

通过两种类型的数据采集，并相应地请求 5G 核心块进行 UE 分离

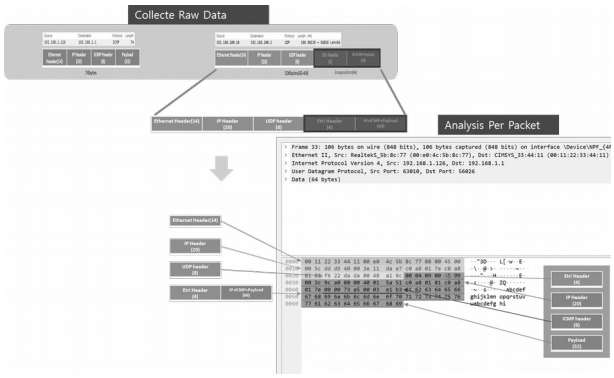

图 3 所示。调查网络 PCAP 文件的网络攻击证明

C. 针对攻击的系统演示

在本研究中，我们不仅将网络采集器和一个 IPS 系统应用于模型工厂，还将 5G-NTD 系统应用于模型工厂。还测量了系统在假攻击者执行网络攻击(如 slowloris 攻击)时的检测性能。slowloris 攻击是一种拒绝服务攻击，它允许一台机器以最小的带宽和对不相关服务和端口的副作用拿下另一台机器的 web 服务器[12]。此外，在进行真正的攻击之前，对收集到的数据进行综合调查，提取网络攻击的证据。查看网络 pcap 数据，如图 3 所示，可以确定响应时间增加了，这与正常状态不同，如图 4 所示。

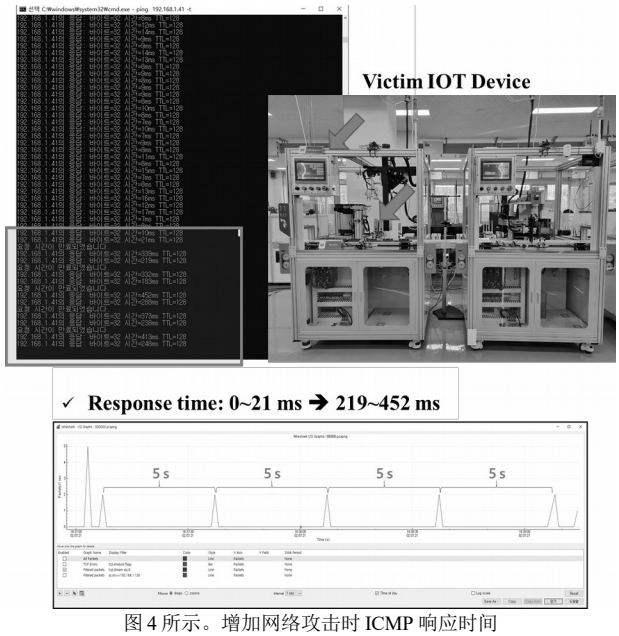

图 4 所示。增加网络攻击时 ICMP 响应时间

D. 论证结果

图 5 显示了测试和演示的主要配置。放置网络采集器用于采集网络流量信息，IPS 系统根据安全策略生成安全事件。此外，5G-NTD 系统检测并识别网络入侵

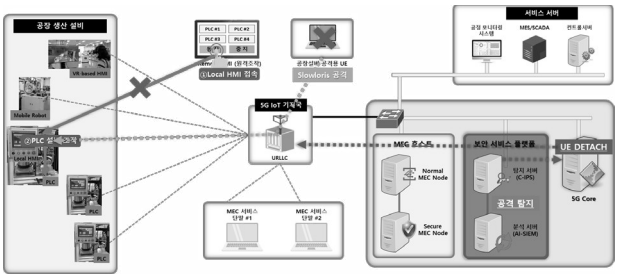

图 5 所示。测试和演示环境

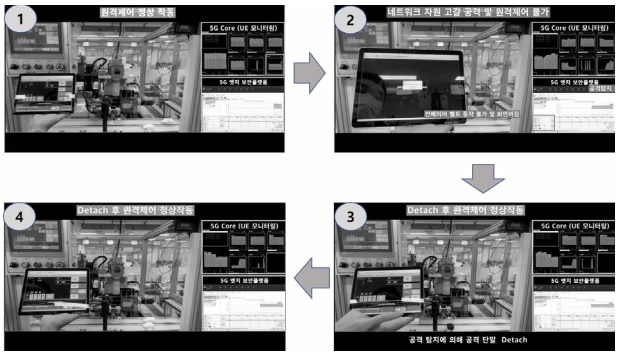

图 6 所示。测试过程中的四个主要程序

如图 6 所示，测试过程分四个阶段执行。首先，在稳定和正常阶段，我们仔细检查 PLC 设备是否被控制和正常运行。其次，利用一个攻击者终端进行模拟慢速攻击，模拟时间约为半小时，通过终端监控系统检测网络资源是否耗尽;观察到 PLC 仪表盘系统堵塞，PLC 设备运行缓慢。第三，5G- ntd 系统通过激活的 AI 模型即时识别网络入侵，请求 5G 核心网功能脱离恶意终端;结果表明，5G 核心成功完成了剥离过程。在最后阶段，证明了受害 PLC 设备恢复到正常稳定状态。

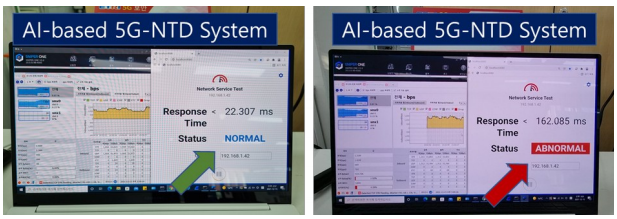

图 7 所示。测试的系统屏幕

图 7 显示了用于测试的系统屏幕。当当前状态正常时，显示为“normal”。然而，一旦 5G-NTD 系统识别到网络入侵，其状态将被标记为“异常”。一个更

5G-NTD 仪表板可以显示详细的网络流状态和检测到的安全事件，如图 8 所示。

图 8 所示。仪表盘监控系统的屏幕截图

V. 结论

检测智能网络入侵的主要挑战之一是提供基于人工智能的检测技术;这也是 5G 网络的一个重要挑战。因此，为了检测 5G 网络入侵并应对恶意 UE，我们在本研究中开发了基于人工智能的网络威胁检测系统。我们在 5G 模型工厂中展示了系统的性能，该模型工厂是现有的智能工厂缩小为模型工厂。通过模拟网络攻击，我们展示了使用 AI 模型进行真实攻击检测的有希望的结果。未来，为了解决 5G 网络中不断发展的网络攻击问题，将使用无监督人工智能模型增强网络入侵检测能力。此外，我们将在 5G 模型工厂中执行更多数量的各种网络攻击，以提高系统性能。

鸣谢

这项工作得到了信息研究所的支持;通信技术规划&;韩国政府(MSIT)资助的评估(IITP)资助项目(No.2020-0-00952，确保 5G+服务稳定性和可用性的 5G 边缘安全技术开发)。

参考文献

[1] 方丹，钱勇，胡仁强，“5G 移动无线网络的安全性”;IEEE Access, vol. 6, pp. 4850-4874, 2018, doi: 10.1109 / ACCESS.2017.2779146。

[2] J. Park 等，“3GPP 5G 安全架构特征与改进”，韩国信息安全与密码研究所，Vol.29, No.5, pp.21-30, 2019。

[3] 金旸，朴家国，j -H。Lee，《5G 边缘计算环境中的安全威胁》;2020 年信息通信技术融合国际会议(ICTC)， 2020, pp. 905-907, doi: 10.1109 / ICTC49870.2020.9289521。

[4] L. Fernández Maimó; ÁL. Perales Gómez, F. J. García Clemente, M. Gil Pérez 和 G. martínez Pérez，“5G 网络中基于自适应深度学习的异常检测系统”;IEEE Access, vol. 6, pp. 7700-7712, 2018, doi: 10.1109 / ACCESS.2018.2803446。

[5] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila 和 A. Gurtov，“5G 安全挑战与解决方案概述”;在 IEEE

通讯标准杂志，第 2 卷，第 2 期。1，第 36-43 页，2018 年 3 月。

[6] Shane Fonyi。2020.5G 安全与漏洞概述。网络防御，Rev. 5,1(2020)。

[7] N.Hubballiand V.Suryanarayanan，“基于签名的入侵检测系统中的误报最小化技术”；一项调查，“计算。Commun。， vol. 49, pp. 1-17, august 2014。

[8] J. Lee, J. Kim, I. Kim 和 K. Han，“基于事件概况的人工神经网络网络威胁检测”;IEEE Access, vol. 7, pp. 165607-165626。

[9] Mahbod Tavallaee, ibrahim Bagheri, Wei Lu and Ali A. Ghorbani，“kdd cup 99 数据集的详细分析”;《第二届 IEEE 会刊》。相依。广告样稿。Int。参议员和参议员。应用，第 53-58 页，2009。

[10] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Idris, A. M. Bamhdi 和 R. Budiarto，“基于信息增益的 CICIDS-2017 数据集特征分析”;IEEE Access, vol. 8, pp. 132911-132921, 2020。

[11] 黄毅，姜世祥，Shin J.，“基于 3GPP NB-IoT 系统的工业物联网小数据高效传输研究”;2020 年信息与通信技术融合国际会议(ICTC)， 2020, pp 1848-1850。

[12] “ Slowloris(计 算 机 安 全)” ， [在 线] 可 获 取:https://en.wikipedia.org/wiki/Slowloris_(computer_security)