工业互联网下基于 SDN 架构的 ARP 攻击防御系统设计

卢煜茜　郑　灿　唐　成
武汉工程大学电气信息学院　湖北武汉　430205

摘　要：近年来，随着工业互联网的体系化发展，软件定义网络（SDN）作为一种创新的网络架构被引入以应对其庞大的数据体系和提升网络攻击防御能力。尽管如此，在工业物联网（IIoT）环境下，SDN 仍面临 ARP 攻击的安全威胁。为应对此问题，本研究提出了一种基于地址位置信息绑定的 ARP 攻击防御机制。该机制通过构建并维护一个准确的 IP 与 MAC 地址对应表，对 ARP 数据包进行验证，以鉴别并拦截伪造的 ARP 请求，确保网络的正常运行。实验结果显示，该系统有效防止了 ARP 泛洪和欺骗攻击，同时降低了网络中的 ARP 广播流量，并缩短了 ARP 处理时间，从而提升了网络的通信效率。

关键词：软件定义网络；IP-MAC 绑定；DHCP 动态分配；ARP 攻击防御

引言

工业物联网（Industrial Internet of Things, IIoT）通过整合先进的物联网技术，改革传统工业系统，实现机器间通信与自动化，以提高生产效率、可靠性和性能。然而，随着设备数量的增加和设备安全性的限制，IIoT 面临诸多安全挑战，其中 ARP（Address Resolution Protocol）攻击是一大安全威胁。在软件定义网络（Software-Defined Networking, SDN）环境中，ARP 攻击不仅针对终端设备，还可能影响网络控制器，这对 IIoT 系统构成了更为严峻的安全风险。鉴于此，对 SDN 环境下 ARP 攻击的检测、缓解和防御研究具有重要意义，旨在保障工业物联网的安全稳定运行。

1. 系统模型设计

1.1 系统框架

基于 SDN 这个背景下，本系统选取了 ARP 泛洪攻击和 ARP 欺骗这两种工业互联网中最常见的 ARP 攻击形式，设计了针对这两种攻击方式的一种基于 SDN 架构的 ARP 攻击防御系统，并将其应用于工业互联网，实现对网络性能的保护。

本系统分为三个阶段：攻击阶段、检测阶段、防御阶段。

在攻击阶段中，攻击者以广播的形式不断向网络中发送虚假的 ARP 数据包，并使用虚假的 MAC 地址作为其映射，导致受害主机错误地更新自己的缓存表，无法正常通信，从

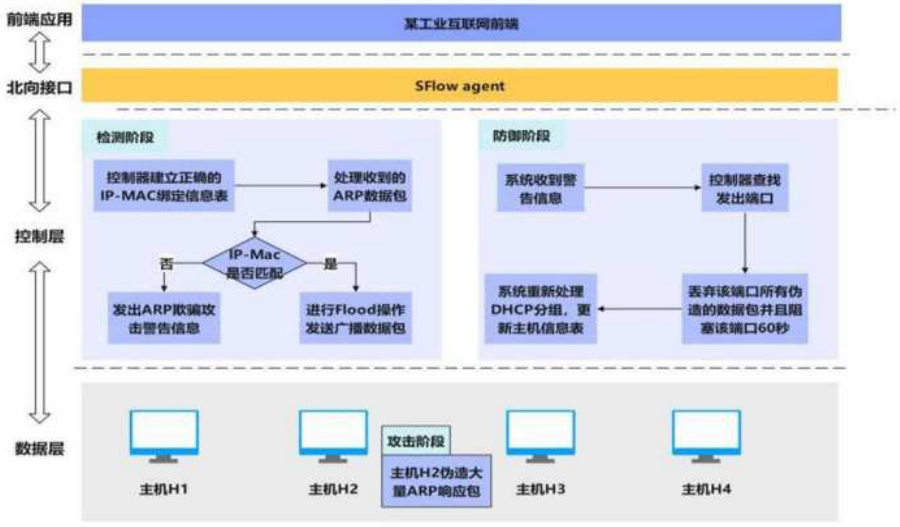

图 1 ARP 攻击防御模块整体架构

而泄漏信息。

在检测阶段中，利用搭建 DHCP 服务器，监听 Port-status 和 Packet_in 消息，获取动态包含 IP 和 MAC 的对应表，并对收到的 ARP 请求包进行判定，若信息不匹配，则检测到 ARP 欺骗攻击，输出警告信息；如果 ARP 包的数量超过阈值显示异常，则检测到 ARP 泛洪攻击。

在防御阶段中，根据检测阶段中 IP-MAC 信息不匹配，输出警告信息并通过 SDN 中的 Ryu 控制器对网络进行防护，进行 ARP 代理并且丢弃该数据包，有效提高工业控制系统的网络安全性能。

1.2 ARP 攻击防御模块整体架构

本文设计一种 ARP 泛洪攻击和欺骗攻击防御的系统，可主要分为两个模块：异常检测模块、攻击防御模块。

（1）异常检测模块

本模块采用端口计数器监控 ARP 流量，通过设定阈值识别 ARP 泛洪与欺骗攻击。结合 DHCP 与 ARP 机制，控制器基于 OpenFlow 协议 v1.3 实现对交换机的监控。模块分析 DHCP 分组，提取 IP-MAC 对应关系，并更新主机信息表以便检测 ARP 欺骗。

ARP 泛洪检测：通过量化 ARP 请求并在异常时调用 handle_spoof 方法，限制攻击者网络接入，从而检测出 ARP 泛洪攻击。

ARP 欺骗检测：当网络中出现源 IP 和源 MAC 不匹配的情况时，控制器判断该情况是否为 ARP 欺骗攻击。如果控制器在信息表中找不到该 IP 地址对应的 MAC 地址，或者该 IP 地址对应的 MAC 地址与请求包中的源 MAC 不匹配，则可以判断出现了 ARP 欺骗攻击。

（2）攻击防御模块

攻击防御模块处理 Packet_in 与 Port_status 消息，优先处理封装 ARP 的 Packet_in 消息。Ryu 控制器更新主机位置

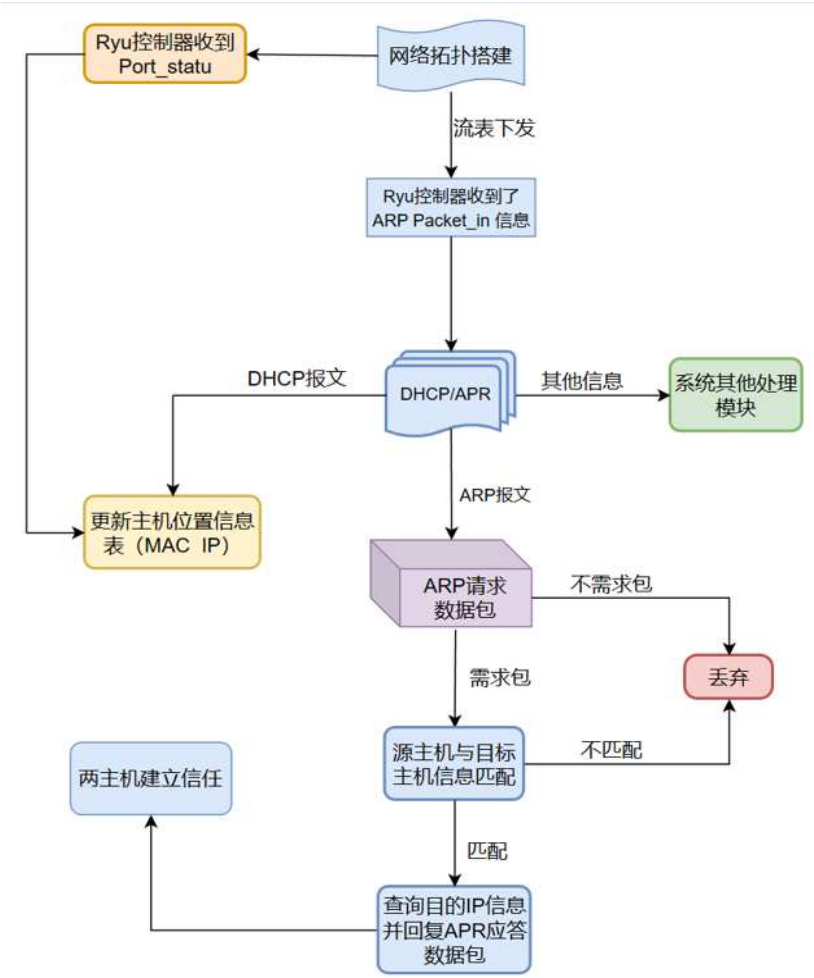

图 2 攻击防御模块流程架构

信息表以响应 DHCP 封装的 Packet_in 和 Port_status 消息。针对 ARP 封装的 Packet_in，控制器执行合法性验证及 ARP 代理。其他 Packet_in 类型由相应模块处理。攻击防御模块流程架构如图 2 所示。

基于主机信息表，验证 ARP 数据包中的信息，对比是否匹配，若不匹配则视为发生了 ARP 欺骗攻击，控制器将丢弃此 ARP 请求数据包。检测通过的 ARP 请求数据包，基于主机信息表中的地址信息，控制器将代替目标主机给请求主机回复 ARP 响应数据包，控制器并且不再将其封装于 Packet_out 消息中下发给交换机进行洪泛，大量减少了网络中 ARP 数据包流量。

2. 实验分析

2.1 实验环境

实验的仿真模拟环境中，具体配置如下：

(1) 操作系统为 Linux–Ubuntu18. 04 LTS 或者更高版本；

(2)CPU:AMD Ryzen 7 5700U with Radeon，主频 1.8GHz;

(3) 内存 2GB 或者更高配置；

(4) 运行 SDN 控制器的网络模拟平台。

其中，SDN 控制器选用 RYU 开源控制器，使用 Open vSwitch 交换机，虚拟网络运用 Mininet 网络仿真平台构建，南向接口协议使用 OpenFlow v1.3 协议，使用 Wireshark 作为流量分析工具，其次使用 Scapy 作为 ARP 攻击的手段，编程语言为 Python3.10

2.2 实验结果

本实验搭建一个包含 4 台主机和 4 台交换机的简单网络，通过观测 ARP 表项、端口流量和 ARP 交互时间，来验证本防御系统的可行性。

(1) ARP 表项对比

模拟 ARP 欺骗攻击，主机 H1 攻击 H3，使得网络中主机 H3 对 H2 的 MAC 地址缓存被篡改。通过观察部署防御模块前后的主机 H3 的 ARP 表项，发现部署防御模块后 ryu 控制器检测到异常攻击并且将 ARP 表项恢复正常，如下图 3、

图 3 防御前后 ARP 表项对比

图 4 系统检测到异常 ARP 数据包

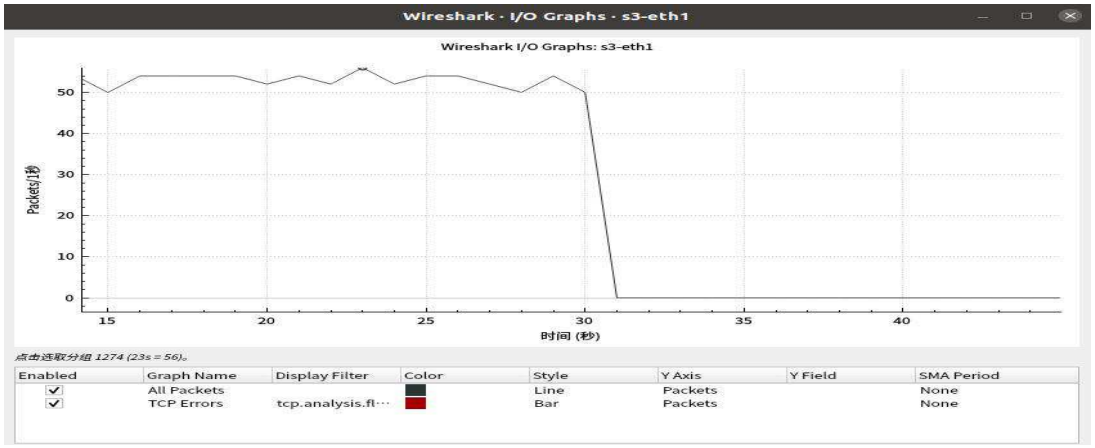

图 5 主机 H3 端口流量图

4 所示。

(2) 端口流量变化

利用 wireshark 抓包软件对各个主机和交换机的端口进行流量监控。如图 5 为部署前后的主机 H3 的端口流量，通过观察部署防御模块前后的主机 H3 端口流量变化情况，可以看出部署模块后，流量相较于部署前得到较大缓解，此时攻击主机 H1 的端口被阻塞，有效地阻断了泛洪攻击。

(3) ARP 交互时间

由于上述方案以模块化运行在控制器代码中，对控制器增加了一定工作量，且工业互联网规模较大，4 台主机说服力较小，为了验证方案的实际可行性，因此需要部署规模更大的 20 台主机检验模块，来验证该方案是否会影响主机间的正常通信，增加主机间通信时延。

实验重新搭建包含 20 台主机的复杂网络拓扑，选取其中同一对通信主机（以主机 H1 和 H16 为例），测量部署防御模块前后 H1 ping H16 共 30 次的 ARP 交互时间，并计算 30 组时间的期望值和方差做对比，分析本方案是否会影响主机间的正常通信。

其中 ARP 交互时间的期望定义为

$$M = \frac{\sum_{i=1}^{n} \chi_i}{n}$$

式中 M 为期望（平均值），Xi 是第 i 次 ARP 交互时间，n 是 30 次实验次数。

ARP 交互时间的方差定义为

$$S^2 = \frac{\sum_{i=1}^{n} (\chi_i - \overline{\chi})^2}{n}$$

式中 S2 为方差，Xi 是第 i 次 ARP 交互时间，是 ARP 交互时间平均值，n 是 30 次实验次数。

将本次实验所测得的 ARP 交互时间做对比，部署防御 ARP 交互时间（图 6）相较于部署防御前（图 7）有明显下降，期望值（Mean）从 0.14ms 下降到了 0.11ms，方差（Variance）波动幅度也同样由 0.03 下降到 0.02，ARP 交互时间波动减小，更趋于稳定。

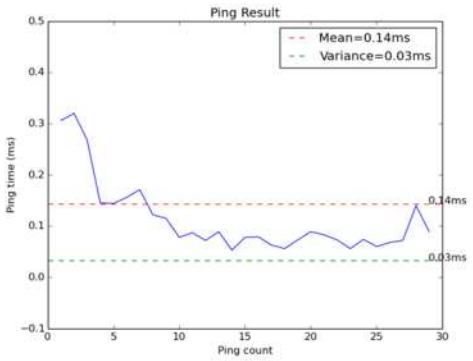

图 6 部署防御前 ARP 交互时间

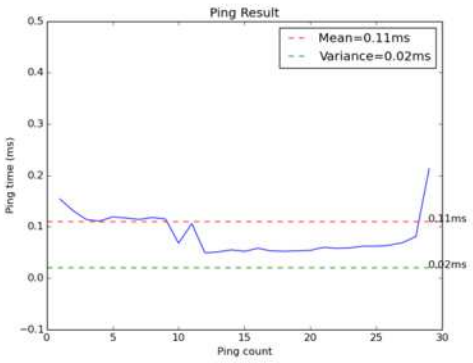

图 7 部署防御后 ARP 交互时间

对同样的网络拓扑进行 15 次试验，将每次实验的期望值统计，绘制条形图如图 8 所示。

图 8 进行 15 次实验统计

在部署防御后，同一对源目主机 H1 和 H16 之间的 ARP 数据包平均交互时间比未部署防御模块前至少减少了 15%。

实验结果表明，部署本方案能够有效防御 ARP 泛洪和 ARP 欺骗攻击，不会影响到主机间的正常通信，并且在一定程度上减少了网络中 ARP 广播数据流量，缩短了 ARP 交

互时间，使得网络的通信效率更高。

3. 结语

在工业互联网环境下，ARP 攻击是一种严重的安全威胁。为了有效防御 ARP 泛洪和欺骗攻击，本研究设计了一个基于 SDN 的 ARP 攻击防御系统。该系统通过集成检测和防御模块，广泛监控并应对这两种常见的攻击模式。与传统方法相比，本系统展现了以下优势：

（1）广泛的检测与防御能力：模拟并针对工业互联网中频繁出现的 ARP 泛洪和欺骗攻击进行设计，有效再现实际环境中的安全风险。

（2）高度可扩展性：通过与 SDN 控制器和 DHCP 服务器的集成，系统可动态适应工业互联网设备的增减，提供灵活的安全防护机制。

（3）快速 ARP 交互处理：利用 SDN 控制器集中处理 ARP 请求，当 IP 与 MAC 地址验证无误时，直接回复 ARP 响应，降低广播流量并加快响应速度。

本系统不仅提升了网络性能，同时确保了工业互联网的稳定运行和信息安全，防止潜在的信息泄露风险。

参考文献

[1] 庄慧敏 . 软件定义工业物联网下基于半监督学习的 ARP 攻击检测方法研究 [D]. 东华大学 ,2022.DOI:10.27012/d.cnki.gdhuu.2022.001992.

[2] 周琨 . 基于 SDN 的工业互联网中间人攻击检测与防护 [D]. 北京交通大学 ,2022.DOI:10.26944/d.cnki.gbfju.2022.001622.

[3] 工业互联网产业联盟 . 工业互联网体系架构（版本 2.0）.[EB/OL].（2020–04–23）[2021–05–20].

[4] D. Kreutz, F. M. V. Ramos, P. E. Ver í ssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, “Software–Defined Networking: A Comprehensive Survey,” in Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.

[5] Boyes H, Hallaq B, Cunningham J, et al. The industrial internet of things (IIoT): An analysis framework[J]. Computers in industry, 2018, 101: 1–12.

[6] 王维 . 面向工业物联网的雾网络优化策略研究 [D]. 上海交通大学 , 2019.

[7] 姚博文 . 面向工业物联网数据安全保障的低时延数据存储分配方案研究 [D]. 西安电子科技大学 , 2019.

项目基金：

武汉工程大学校长基金项目“工业互联网安全保障：基于 SDN 架构的 ARP 攻击防御系统设计”（编号：XZJJ2023015）

作者简介：

1. 卢煜茜（2003.11–），女，汉族，湖北十堰人，本科在读，武汉工程大学，在读学生，专业：通信工程；

2. 郑灿（2003.09–），男，汉族，湖北黄冈人，本科在读，武汉工程大学，在读学生，专业：通信工程；

3. 唐成（2003.07–），男，汉族，湖北孝感人，本科在读，武汉工程大学，在读学生，专业：通信工程。