doi :10.3969/j.issn.1671-1122.2019.11.002

一种面向 S7 协议的工控系统入侵检测模型

田峥，李树，孙毅臻，黎曦
（国网湖南省电力有限公司信息通信分公司，湖南长沙 410000）

摘　要：随着“中国制造 2025”战略的提出，工业控制网络和互联网技术的融合程度也越来越高，同时工业控制网络的封闭性在一定程度上被打破，使得工业控制网络安全问题日益严重。S7 协议是德国西门子公司的私有协议，广泛应用于工控网络的通信过程中。文章提出一种基于深度解析和白名单自学习的工控复合入侵检测模型，该模型利用深度解析算法实现对 S7 协议包的解析，通过白名单自学习算法动态构建白名单，采用白名单检测和异常行为检测相结合的复合入侵检测方法来检测异常。实验证明，该方法能有效检测出工业控制网络中异常的 S7 协议包，在 5000 个 /s 的发包速率下检测精度可达到 98.3%。

关键词：协议解析；入侵检测；白名单自学习；S7 协议

中图分类号：TP309　**文献标识码：**A　**文章编号：**1671-1122（2019）11-0008-06

中文引用格式：田峥，李树，孙毅臻，等 . 一种面向 S7 协议的工控系统入侵检测模型 [J]. 信息网络安全，2019，19（11）：8–13.

英文引用格式：TIAN Zheng, LI Shu, SUN Yizhen, et al. Industrial Control System Intrusion Detection Model Based on S7 Protocol[J]. Netinfo Security, 2019, 19(11): 8–13.

Industrial Control System Intrusion Detection Model Based on S7 Protocol

TIAN Zheng, LI Shu, SUN Yizhen, LI Xi
(*State Grid Hunan Electric Power Company Limited Information and Communication Branch*, *Changsha Hunan* 410000, *China*)

Abstract: With the proposal of “made in China 2025” strategy, the integration of industrial control network and Internet technology is getting higher and higher. At the same time, the closeness of industrial control network has been broken to a certain extent, making the problem of industrial control network security increasingly serious. S7 protocol is a private protocol of Siemens company in Germany, which is widely used in the communication process of industrial control network. This paper proposes an industrial control composite intrusion detection model based on deep analysis and white list self-learning. The model uses deep analysis algorithm to realize the analysis of S7 data packets, dynamically builds a white list through white list self-learning algorithm, and uses the composite intrusion detection method of white list detection and abnormal behavior detection to detect anomalies. The experiments show that the method can effectively detect the abnormal S7 protocol packets in the industrial control network, and the detection accuracy can reach 98.3% at 5000/s packet rate.

Key words: protocol analysis; intrusion detection; white list self-learning; S7 protocol

收稿日期：2019-9-16
作者简介：田峥（1983—），男，湖南，高级工程师，博士，主要研究方向为网络与信息安全；李树（1991—），男，湖南，工程师，博士，主要研究方向为网络信息安全、无线信道建模；孙毅臻（1990—），男，湖南，工程师，硕士，主要研究方向为网络安全、关键信息基础设施安全；黎曦（1982—），女，湖南，高级工程师，硕士，主要研究方向为网络安全。
通信作者：李树 lis_sgcc@163.com

0 引言

工业控制系统（Industrial Control System，ICS）是不同类型控制系统的统称，一般包括数据采集与监控系统（Supervisory Control and Data Acquisition，SCADA），过程控制系统（Process Control System，PCS），分布式控制系统（Distributed Control System，DCS）和可编程逻辑控制器（Programmable Logic Controller，PLC）等。工控系统广泛应用于电力系统、石油化工、铁路系统等国家支柱领域，是国家关键信息基础设施中的重要组成部分[1]。近年来，随着“中国制造2025”战略的实施，工控系统的信息化程度越来越高，不可避免地削弱了工控系统的封闭性，使得工控网络安全问题日益严重[2]。近年来世界各地工控网络安全事故频发，这些安全事故给当地带来了巨大的经济和财产损失。因此，对工控网络安全问题的研究是十分必要的[3]。

1 研究现状

近年来，为了解决工控网络中的安全问题，研究人员提出了各种网络安全防护策略。常见的有工业防火墙和入侵检测方法。前者注重被动防御，后者注重主动检测。入侵检测方法是对工控网络中的流量进行检测和分析，如果发现异常，则发出入侵警报信息[4,5]。相比于工业防火墙，入侵检测方法可用性更好，不仅所需的资源较少，基本不影响工控系统的运行性能，且能动态地进行调整。

一般来说，入侵检测方法从类型上可分为误用检测方法和异常检测方法[6]。误用检测方法采用的是黑名单方式。该方式采集已知的攻击方式形成黑名单，在检测时分析系统通信行为的特征，并将特征与黑名单中的攻击方式进行比对。如果特征与黑名单中的攻击方式相符，则判定为入侵攻击行为；否则为正常通信行为。误用检测方法通常对于已知的攻击具有较高的检测率，但是不能很好地检测未知攻击行为。VASILOMANOLAKIS[7]等人通过蜜罐技术来采集针对集成电路网络的攻击，收集攻击的签名用于误用入侵检测系统。

与误用检测方法不同，异常检测方法首先对工控系统中的正常通信数据构建白名单，然后监测系统中的通信行为。如果通信行为不符合正常行为，则发出异常警报信息。PONOMAREV[8]等人通过获取网络会话的特征来鉴别攻击者的会话与正常机器的TCP会话，该模型在同一网络中可以有效区分正常业务人员和攻击者，精度可以达到99.98%。DUNLAP[9]等人通过基于时序的边信道分析来建立唯一的设备指纹，通过指纹来检测未经授权的修改行为。MUTHA[10]等人基于白名单构建了入侵检测系统，对SCADA网络中的通信行为进行异常检测。

现有的入侵检测方法有基于协议解析的检测方法、基于模型的检测方法和基于机器学习的检测方法。本文主要讨论基于协议解析的入侵检测方法。该方法首先捕获工控系统中的通信数据包，然后根据通信协议的具体格式解析通信数据包的各个字段，如IP地址、协议类型、地址字段和功能字段等，通过对字段信息进行分析判断是否是正常通信行为。

协议解析技术一般应用于传统IT网络的入侵检测方法。在5G网络中，基于状态的协议分析检测（Stateful Protocol Analysis Detection，SPAD）是一种有效的入侵检测方法，它通过解析TCP和UDP协议对网络进行攻击检测[11]。在传统网络中，作用于网络层、应用层和传输层的状态全协议分析方法通过使用预定义供应商的规范设置来检测异常[12]。但是由于工控系统较为复杂，在应用层不采用公有协议，而是私有协议，如Modbus、S7和DNP3等，这对使用传统协议解析技术解析通信数据包造成了一定的困难。本文采用深度解析算法来弥补传统协议解析的不足，针对工控网络中应用较为广泛的S7协议，在传统协议解析的基础上，根据S7协议的格式对工控系统中的数据包进行深度解析。

现有的入侵检测方法往往采用静态方法来构建白名单。CASELLI[13]等人利用配置文件中所允许的操作构建静态白名单进行入侵检测。KWON[14]等人通过分析IEC 61850协议的特征来构建检测规则，对SCADA

网络进行入侵检测。静态白名单配置起来往往比较麻烦，而且不具备动态性，移植性较差，在更换工业控制系统后需要重新构建白名单。因此，本文采用白名单自学习的方式来构建动态白名单。通过系统自学习的方式，自动采集工控网络中正常通信数据来动态构建白名单。该方法相较于静态白名单具有更好的智能性和通用性。

入侵检测方法有基于白名单的异常检测方法和基于黑名单的误用检测方法，但是这两种方法都有一定的不足。因此，本文结合白名单和黑名单的优势，采用复合入侵检测方法对工控网络中的通信行为进行检测，如果有异常通信行为，则发出异常警报信息。

2 基于深度解析和白名单自学习的工控入侵检测模型

本文提出一种面向S7协议的工控系统入侵检测模型，该模型的总体架构如图1所示。该模型首先使用基于S7协议的深度解析算法来解析数据包；然后使用白名单自学习算法来学习工业控制网络中的正常通信行为，并动态构建白名单；最后使用复合入侵检测方法对工控网络中的各种通信行为进行检测，复合入侵检测方法包括白名单检测和基于黑名单的异常行为检测。

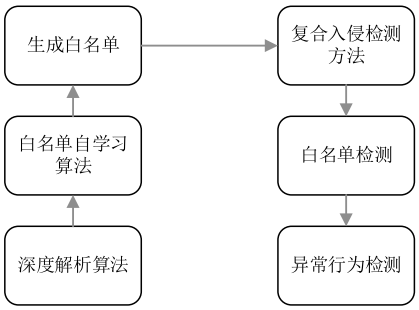

图 1 本文模型架构

2.1 面向 S7 协议的深度解析算法

一般的协议解析技术是针对常用的公有协议进行解析，如解析链路层源MAC地址和目标MAC地址、解析网络层IP协议中的源IP地址和目标IP地址、解析运输层TCP协议中的源端口号和目标端口号以及解析应用层HTTP协议。但是对于工业控制系统网络来说，一般采用自家厂商的私有协议。例如，德国西门子公司采用S7协议，有效数据被封装在应用层协议中传输。所以要采用深度解析方法对应用层数据进行分析。

深度解析算法通过解析S7协议数据包可以得到包含解析结果的元组。首先对元组进行初始化。深度解析算法首先遍历S7协议数据包，获取数据包的长度，并将结果写入目标元组；然后解析网络层、运输层和应用层数据，得到IP地址、端口号和应用层协议类型，并将上述结果写入目标元组。S7 Comm协议和一般应用层协议不同，数据包首先被封装在COTP协议中，然后被封装在TPKT协议中进行传输。COTP协议包根据Type字段的不同可分为COTP功能包和COTP连接包。查找COTP协议包中的Type字段，如果COTP协议包中的Type字段不是0xf0，说明是COTP连接包，解析得到COTP Type字段并写入目标元组中的功能码字段；否则说明是COTP功能包，进一步查找S7 Comm协议中的PDU Type字段。如果是0x07,说明是S7协议扩展，继续解析S7 Comm 协议的功能组和子功能码并写入目标元组的功能码字段；否则首先解析得到功能码字段，然后根据功能码字段的不同做出不同的处理。如果是读命令，遍历解析所有item中的地址信息并写入元组；如果是写命令，遍历解析所有item中的地址和数据信息并写入元组；如果是上传和下载命令，需要解析文件名字段并写入元组；如果是其他命令，则仅需要将功能字段写入元组。此外为了更好地区分不同S7协议包的功能字段，在COTP功能包的功能字段前加1，在S7协议扩展包的功能字段前加2。

2.2 白名单自学习算法

白名单指允许通行的名单，对于工业控制系统网络来说，就是在工控网络中通信行为正常的数据包的集合。在工控网络中可以将正常行为数据包的特征记录下来，形成白名单，然后将网络上的数据包与白名单进行比对，若不符，则发出警告，这样就可以有效检测出行为异常的恶意数据包。

白名单分为静态白名单和动态白名单。静态白名单需要管理员手动输入，不仅繁琐，正确性也不能得到很好的保证，且一旦更换环境后，就需要重新配置。动态白名单则很好地解决了静态白名单所存在的问题。动态白名单采取自学习模块，即在给定的自学习周期时间 T 内，对工控系统中正常通信的数据包进行学习，建立合法通信行为的动态白名单。

白名单自学习算法还需输出最大数据包长度 max 和最小数据包长度 min，以便后续对异常数据包进行检测。首先对S7协议数据包进行深度解析得到解析元组，查看长度信息并更新 max 和 min，然后查看白名单是否有约束数据包长度范围的规则。如果没有，则在白名单中插入对应规则；如果存在，则需要根据功能码对相应的字段进行合并处理。

2.3 复合入侵检测方法

常见异常类型可以分为两种：格式异常和行为异常。前者指传输一些非法格式的S7数据包，常见的格式异常类型有非法长度、非法IP地址、非法协议类型、非法功能字段、非法地址字段、非法数据字段和非法文件名字段等。后者指攻击者做出一些非法的工控行为。

复合入侵检测方法设置变量 *isAlarm* 来表明是否发出异常警告信息，默认值为true，表示发出异常警告信息。该方法首先对数据包进行深度解析，得到解析信息，如数据包长度、网络层IP地址、运输层端口号、应用层协议类型和S7协议的功能字段、地址字段、数据字段和文件名字段；然后检测数据包长度是否合法，防止攻击者发布过长的恶意数据包堵塞信道。如果数据包长度合法，接着进行白名单检测。如果通过白名单检测，说明数据包的格式正确，继续进行异常行为检测。如果通过异常行为检测，则将 *isAlarm* 设置为false，即不发出异常警告信息。

白名单检测算法设置变量 *isPass* 来表明是否通过检测，默认值为false，表示未通过白名单检测。算法首先检测IP地址和端口号是否在白名单中，如果通过检测，则筛选出所有包含该IP地址和端口号的白名单规则；然后检测协议类型和功能字段，如果符合白名单，则进一步缩小白名单；最后根据功能字段检测对应的地址、数据和文件名字段，如果合法，则说明该数据包格式正确，进一步进行异常行为检测。

通过白名单检测的S7数据包还要检测工控行为是否异常。异常行为检测算法首先查看当前执行的工控操作，然后查找记录非法工控行为的黑名单。如果该操作属于非法工控行为，发出异常警报信息；否则通过异常行为检测。例如，如果有同一IP反复进行当前操作，说明有异常主机在消耗系统资源，需要发出异常警报信息；也可以查看工控操作的时间是否在当前操作所允许的时间范围内，如果异常，则发出异常警报信息。

3 实验

为了验证本文模型能否有效检测出工控网络中异常S7数据包，搭建仿真环境来模拟真实工控网络进行实验。实验分为3部分，首先验证深度解析算法能否正常解析S7数据包，然后测试能否通过白名单自学习算法构建白名单，最后通过构造异常攻击事件检测复合入侵检测方法是否有效。

3.1 实验环境

仿真环境结构如图2所示，包括操作员站、工程师站、SCADA服务器、西门子S7-1200 PLC、西门子S7-300 PLC、施耐德PLC、HMI、交换机、现场控制层的工控设备和入侵检测系统。其中，交换机的镜像口连接入侵检测系统，以便检测工控系统中的网络流量。

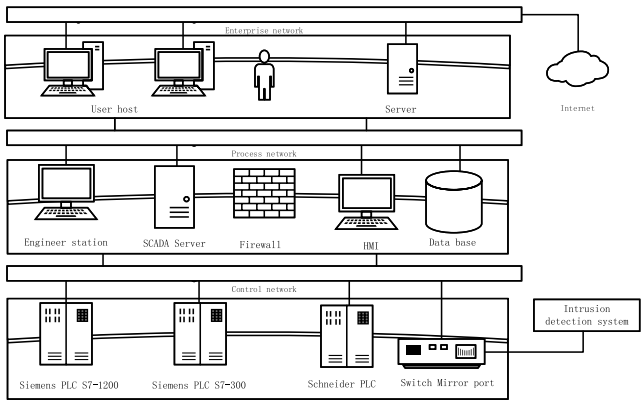

图 2 仿真环境结构

3.2 结果分析

1）深度解析算法测试

使用抓包软件对工控网络中的S7数据包进行抓取，利用深度解析算法进行解析，解析结果如图3所示。从图3可以看到，深度解析算法能够成功解析S7数据包的每个字段信息。

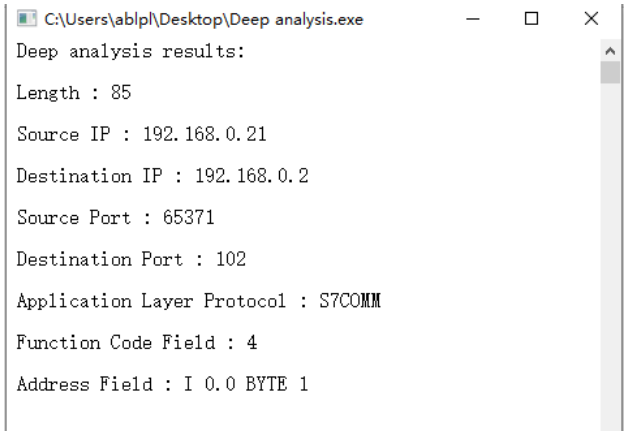

图 3 深度解析结果

2）白名单测试

白名单测试分为两个阶段，正确性测试和自学习时间测试。首先测试能否成功构建白名单，在工控系统中运行白名单自学习算法后，成功构建了工控网络通信白名单。由于白名单比较庞大，只展示两台主机之间的通信白名单，如图4所示。然后进行白名单自学习时间测试，找出最佳的白名单自学习时间。自学习时间过短，不能充分学习工控系统网络特征；自学习时间过长，则会浪费工控系统资源。分别设置自学习时间为12h、24h、36h和48h进行测试，实验结果如图5所示。从图5可以看出，自学习时间小于36h时，学习到的白名单规则数随时间的增加而不断增加；超过36h时，白名单规则数量则趋于稳定。实验证明，36h是最佳的白名单自学习时间。

图 4 通信白名单

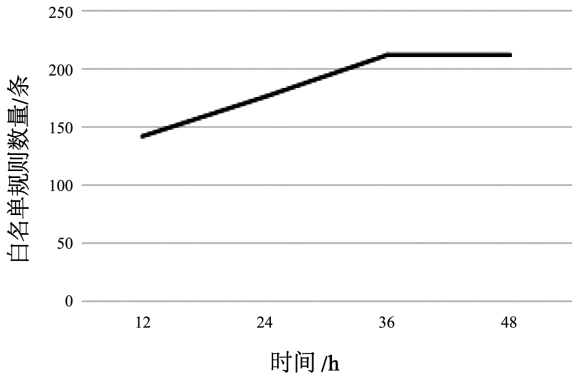

图 5 白名单自学习时间

3）复合入侵检测方法测试

异常数据包类型有两种：格式异常和行为异常。本文测试了12个S7数据包，其中2个正常数据包、8个格式异常数据包和2个行为异常数据包，实验结果如表1所示。从表1可以看出，复合入侵检测方法能有效检测出工业控制网络中的异常S7数据包。

表 1 复合入侵检测结果

异常类型	异常描述	白名单检测结果	异常行为检测
格式异常	非法 IP	告警	未检测
格式异常	非法长度	告警	未检测
格式异常	非法端口号	告警	未检测
格式异常	非法协议类型	告警	未检测
格式异常	非法函数字段	告警	未检测
格式异常	非法地址字段	告警	未检测
格式异常	非法数据字段	告警	未检测
格式异常	非法文件名字段	告警	未检测
行为异常	高频响应	未告警	告警
行为异常	PLC 异常关闭时间	未告警	告警
正常	COTP 连接包	未告警	未告警
正常	S7 正常数据包	未告警	未告警

为进一步测试复合入侵检测方法的稳定性，还进行了压力测试，即逐步增加异常攻击的强度（发包速率），记录入侵检测的检测精度。实验结果如图6所示，从图6可以看出，在异常攻击强度较高的情况下，入侵检测方法仍能保持较高的检测精度，在5000个/s的发包速率下，检测精度可以达到98.3%。

4 结束语

本文提出了一种基于深度解析和白名单自学习的工控复合入侵检测模型，并通过实验验证了该模型的有

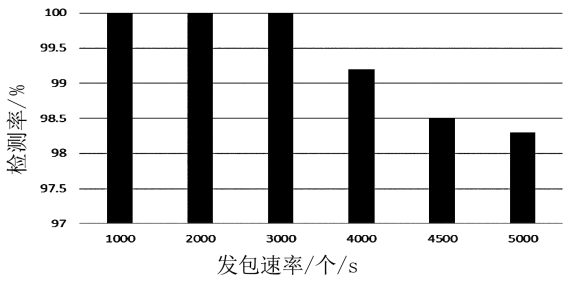

图 6 入侵检测精度

效性和检测精度。本文提出的复合入侵检测模型可用于电力系统工控网络安全技防领域，精准、高效地检测S7协议异常流量。下一步工作将进一步优化模型，提高模型精度，并搭建生产测试环境开展测试。（责编 马珂）

参考文献：

[1] XIA Chunming, LIU Tao, WANG Huazhong, et al. Current Situation and Development Trend of Information Security in Industrial Control System[J]. Information Security and Technology, 2013, 4(2): 13–18.
夏春明，刘涛，王华忠，等. 工业控制系统信息安全现状及发展趋势 [J]. 网络空间安全，2013，4（2）：13–18.

[2] SADEGHI A R, WACHSMANN C, WAIDNER M. Security and Privacy Challenges in Industrial Internet of Things[C]//ACM. 2015 52nd Annual Design Automation Conference, June 7 – 11, 2015, San Francisco, California. New York: ACM, 2015: 1–6.

[3] DRIAS Z, SERHROUCHNI A, VOGEL O. Analysis of Cyber Security for Industrial Control Systems[C]//IEEE. 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, August 5–7, 2015, Shanghai, China. NJ: IEEE, 2015: 1–8.

[4] MARCO C, EMMANUELE Z, FRANK K. Sequence–aware Intrusion Detection in Industrial Control Systems[C]//ACM. The 1st ACM Workshop on Cyber–Physical System Security, March 14–April 14, 2015, Singapore. New York: ACM, 2015: 13–24.

[5] PONOMAREV S, ATKISON T. Industrial Control System Network Intrusion Detection by Telemetry Analysis[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 13(2): 252–260.

[6] TRIVEDI M. Toward Autonomic Security for Industrial Control Systems[D]. Starkville: Mississippi State University, 2015.

[7] VASILOMANOLAKIS E, SRINIVASA S, CORDERO C G, et al. Multi–stage Attack Detection and Signature Generation with ICS Honeypots[C]//IEEE. 2016 IEEE/IFIP Network Operations and Management Symposium, April 25–29, 2016, Istanbul, Turkey. NJ: IEEE, 2016: 1227–1232.

[8] PONOMAREV S, ATKISON T. Session Duration Based Feature Extraction for Network Intrusion Detection in Control System Networks[C]//IEEE. 2016 International Conference on Computational Science and Computational Intelligence, December 15–17, 2016. Las Vegas, NV, USA. NJ: IEEE, 2016: 892–896.

[9] DUNLAP S, BUTTS J, LOPEZ J, et al. Using Timing–based Side Channels for Anomaly Detection in Industrial Control Systems[J]. International Journal of Critical Infrastructure Protection, 2016, 15: 12–26.

[10] MUTHA A, TUTEJA M R R. Secure and Efficient Approach for Multilayer Cyber Security Based on Intrusion Detection System[J]. International Journal of Advent Research in Computer and Electronics, 2015, 2(2): 33–37.

[11] GAI Keke, QIU Meikang, TAO Lixin, et al. Intrusion Detection Techniques for Mobile Cloud Computing in Heterogeneous 5G[J]. Security and Communication Networks, 2016, 9(16): 3049–3058.

[12] VINAYAKUMAR R, SOMAN K P, VELAN K K S, et al. Evaluating Shallow and Deep Networks for Ransomware Detection and Classification[C]//IEEE. Sixth International Conference on Advances in Computing, Communications and Informatics(ICACCI–2017), September 13–16, 2017, Manipal, India. NJ: IEEE, 2017: 1282–1289.

[13] CASELLI M, ZAMBON E, AMANN J, et al. Specification Mining for Intrusion Detection in Networked Control Systems[C]//USENIX Association. Proceedings of the 25th USENIX Security Symposium, August 10–12, 2016, Austin, United States. Austin: USENIX, 2016: 791–806.

[14] KWON Y J, KIM H K, YONG H L, et al. A Behavior–based Intrusion Detection Technique for Smart Grid Infrastructure[C]//PowerTech. 2015 IEEE Eindhoven PowerTech, June 29 – July 2, 2015, Eindhoven, Netherlands. NJ: IEEE, 2015: 1–6.