

논문 2019-1-4 <http://dx.doi.org/10.29056/jsav.2019.06.04>

SNMP MIB 파일의 유사도 분석에 관한 연구

전병태*†

A Study on Similarity Analysis of SNMP MIB File

Byung-Tae Chun*†

요 약

컴퓨터 프로그램 분쟁 조정 해결 방법중 하나인 유사도 분석 방법은 많은 연구되어왔다. 본 논문은 MIB (Management Information Base) 파일의 정량적 유사도 분석에 관한 내용이다. 정량적 유사도란 두 컴퓨터의 소스코드 등을 분석하여 일정한 기준을 적용하여 비교한 결과를 수치로 나타낸 것을 의미한다.

분석대상 프로그램은 WiMAX CPE 장치에 대해서 SNMP 프로토콜을 사용하여 구성관리, 장애관리, 성능관리 등 네트워크 장치 관리 기능을 제공하는 프로그램이다. 여기서, WiMAX는 IEEE 802.16 무선 네트워크 표준 프로토콜을 말하며 고정형 WiMAX와 모바일 WiMAX로 구분될 수 있다. WiMAX CPE는 고객 집 또는 사무실 등 실내에 고정하여 사용하는 무선인터넷 단말기이다. 본 논문에서는 A사와 B사의 MIB 파일에 대한 유사도 분석을 수행하고, 피해회사에서 유출된 MIB 파일이 단순한 제품사양을 설명하기 위한 리스트가 아니고 그 재산적 가치가 인정될 수 있는 자료인지 여부에 대하여 분석해 보기로 한다.

Abstract

Many similarity analysis methods, one of the dispute resolution methods for computer programs, have been studied. This paper is about quantitative similarity analysis of MIB (Management Information Base) file. Quantitative similarity means that the source codes of two computers are analyzed and the results are compared with a certain standard. The source code to analyze is a program that provides network device management functions such as configuration management, fault management, and performance management using SNMP protocol for WiMAX CPE devices. Here, WiMAX refers to the IEEE 802.16 wireless network standard protocol and can be classified into fixed WiMAX and mobile WiMAX. WiMAX CPE is a wireless Internet terminal that is fixedly used in a customer's home or office.

In this paper, we analyze the similarity between MIB file of company A and company B. We will analyze whether the MIB file leaked from the damaged company is not just a list to describe the product specifications, but whether the property value can be recognized.

한글키워드 : SNMP MIB, 유사성, 유사성 분석, 프로그램, 성능

keywords : SNMP MIB, similarity, similarity analysis, program performance

1. 서 론

* 한경대학교 컴퓨터공학과

† 교신저자: 전병태(email: chunbt@hknu.ac.kr)

접수일자: 2019.05.31. 심사완료: 2019.06.15.

게재확정: 2019.06.20.

컴퓨터 프로그램 분쟁 조정[1][2]의 해결 방법 중 하나인 유사도 분석[3-5]에 관한 연구는 많이

연구되어 왔으며, 본 논문은 MIB (Management Information Base) 파일의 정량적 유사도 분석에 관한 내용이다. 정량적 유사도란 두 컴퓨터의 소스코드 등을 분석하여 일정한 기준을 적용하여 비교한 결과를 수치로 나타낸 것을 의미한다[6].

MIB 파일이란 관리자(Manager)와 대리인 (Agent) 사이에 특정한 정보를 주고받는 것이 네트워크 관리의 기본이며, 관리되어야 할 특정한 정보, 자원을 객체라 한다. 이런 객체들을 모아놓은 집합체를 MIB이라고 한다. 네트워크를 관리한다는 것은 관리 대상인 장비(익스태이션, 프린터, 파일 서버, 허브, 라우터, 스위칭 장비)들이 제공하는 MIB중에서 특정 값을 얻어와 그 장비의 상태를 파악하거나 그 값의 변경함을 의미한다. 값의 변경은 해당 MIB의 문자열(String)이나 수치를 변경시키는 것은 물론이고 값의 변경을 통해 그 장비의 상태를 변경시킬 수도 있고 그 장비에 일정한 작동을 지시, 수행할 수 있다. 즉 인터페이스의 관리값을 수정해서 해당 장비의 통신을 불가능하게 할 수도 있고 허브의 특정 포트로의 전송을 막을 수도 있다. 또한 특정 MIB의 변경을 통해 허브를 재 작동시킬 수도 있다.

분석대상 프로그램은 WiMAX(Worldwide Interoperability for Microwave Access) CPE(Customer Premises Equipment) 장치에 대해서 SNMP(Simple Network Management Protocol) 프로토콜을 사용하여 구성관리, 장애관리, 성능 관리 등 네트워크 장치 관리 기능을 제공하는 프로그램이다. 여기서, WiMAX는 IEEE 802.16 무선 네트워크 표준 프로토콜을 말하며 고정형 WiMAX와 모바일 WiMAX로 구분될 수 있다. WiMAX CPE는 고객 집 또는 사무실 등 실내에 고정하여 사용하는 무선인터넷 단말기이다.

본 논문에서 다룰 유사도 분석 내용은 B사 들로부터 압수한 B사 들 유출 자료인 MIB 파일

(T&W.zip 자료중 'SNMP_v0.2.MIB' 파일)과 피해회사 제공의 MIB파일 및 연동 소스 코드(2개, 특정회사요청내용이 포함된 자료와 피해회사판매 CPE 관련 일반적 자료)를 비교하여 유출한 MIB 파일이 단순한 제품사양을 설명하기 위한 리스트가 아닌 피해회사가 판매한 CPE 제품에 일반적인 다른 기능이 포함되어 있어 그 재산적 가치가 인정될 수 있는 자료인지 여부에 대하여 분석해 보기로 한다.

2. 유사도 분석에 사용되는 도구

유사도 분석[7]에 사용되는 도구는 한국저작권위원회[8]에서 개발한 'exEyes'를 사용하여 수행하였다. 추가적으로 상세한 분석이 필요한 소스코드에 대해서는 'Notepad+', 'Excel', 'Compare It', 그리고 'explore' 소프트웨어를 사용하여 휴리스틱 방법으로 유사성을 심층 분석하였다.

표 1. 분석 도구
Table 1. Analysis Tool

비교 대상	분석 방법		사용 도구
MIB 파일	공개 여부 분석	오픈 소스 여부 확인	Google
	유사성 분석	도구를 이용하여 분석대상 소스코드의 유사성 분석	exEyes Excel
		분석인의 전문지식과 경험에 기반하는 휴리스틱 방식 병행	Notepad+ Compare It

3. SNMP MIB 파일의 유사도 분석

소스코드의 유사도는 다음과 같은 방법[9-11]으로 산정한다. 각각의 비교 대상의 기준이 되는

쪽을 A, 반대쪽을 B라 했을 때, A의 각각의 파일에 대해 '파일별 유사 줄수'를 계산한다. 즉, 하나의 A의 파일에 대해 B의 모든 파일과 각각 유사 줄 수를 산출하여 그 중 가장 큰 유사 줄 수를, 파일별 유사 줄 수로 한다. A의 모든 파일의 '파일별 유사 줄 수'의 합을 A의 전체 줄 수로 나눈 것이 전체 유사도가 된다.

3.1 A사 MIB 파일의 공개 소스코드 여부 분석

본 논문에서는 A사 MIB 파일이 인터넷 상에 공개된 소스 코드[12][13]인지를 확인하기 위하여 구글 및 SNMP MIB 전문 인터넷 사이트를 통하여 검색하였다. 검색 결과 그림 1에 도시된 바와 같이 A사 MIB 객체 43개중에서 유사한 MIB 객체가 일부 발견되었다. 그러나, 유사한 MIB 객체 수는 3개로 매우 적었고, 더욱이 이름만 동일할 뿐 전체적으로는 유사성이 낮았기 때문에 A사 MIB 파일은 공개 소스 코드가 아니라고 판단된다.



그림 1. 공개 SW 여부 분석

Fig. 1. Analyze whether it is open SW

3.2 유출된 MIB 파일이 피해회사가 판매한 제품에 다른 기능이 포함되었는지 여부

네트워크 장치를 개발할 때 네트워크 장치의 순수 기능뿐만 아니라 네트워크 장치 관리 기능도 반드시 구현해야 한다. 네트워크 장치 관리 기능을 SNMP 프로토콜을 사용하여 구현하는 통상적인 개발 절차를 살펴보면, 개발자는 먼저 네트워크 장치의 현재 구동 상태 정보(예, 성능정보, 장애 이벤트 등)와 네트워크 장치의 동작 변경을 위해 네트워크 관리자가 변경할 수 있는 정보(예, 구성정보, 계정정보 등) 등을 MIB(MIB)으로 정의해야 한다.

작성된 MIB 파일은 자동화 도구를 사용하여 C와 C++와 같은 컴퓨터 프로그램 소스 코드로 변환되고, 개발자는 그 자동 생성된 소스 코드를 확장하여 구현을 완료하는 것이 통상적인 개발 절차이다. 네트워크 장치에서의 MIB 개발은 소프트웨어에서 데이터베이스 스키마의 개발과 비유될 정도로 중요하게 간주되어야 한다. 따라서 MIB 파일의 기능은 단순히 제품 사양을 설명하기 위한 리스트가 아니다. MIB 파일은 WiMAX CPE 등 네트워크 장치를 개발할 때 중요 요소 중 하나인 네트워크 장치 관리 기능을 제공함을 볼 수 있다.

A사 MIB 파일은 관리자 구성정보, WiMAX 구성정보, WiMAX 성능정보, RF(Radio Frequency) 정보, MAC 통계 정보, WiMAX 성능 정보, LAN 정보 등 총 43개의 맵 객체를 통해 WiMAX CPE에 대한 네트워크 장치 관리 정보를 정의하고 있다.

A사 MIB 파일에서, 각각의 MIB 객체(예, WiMAX의 IP address MIB 객체 정보, RF의 RSSI MIB 객체 정보 등) 하나하나는 비록 기존의 네트워크 시스템에서 취득될 수 있기 때문에 독특한 다른 기능이 포함되어 있다고는 할 수 없다. 그러나 MIB 객체들이 모여서 구성된 하나의 A사 MIB 파일은 A사 WiMAX CPE 장치만의

관리를 위해 개발된 프로그램이기 때문에 다른 MIB 파일과 구별될 수 있는 차별된 특별한 정보라고 판단된다.

A사 MIB 파일은 그림 2에 도시된 바와 같이 IANA(Internet Assigned Numbers Authority)라는 공식 인터넷 할당번호 관리 기관에 사설(private)로 등록되어 있었다. 즉, A사 MIB 파일 최상위 객체가 IANA에 등록 되어 있었으며(<http://www.oid-info.com/>), 여기서 private(4)은 사설을 의미한다. 또한 앞서 기술한 바와 같이, 인터넷상에서 A사 MIB를 검색하였지만 발견되지 않았다.

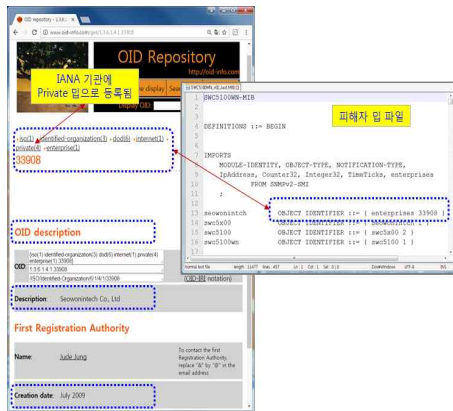


그림 2. IANA 기관에 사설(private) MIB으로 등록된 A사 MIB

Fig. 2. Analysis of victims' MIB registered privately in IANA institution

분석결과를 종합하면, MIB 파일은 네트워크 장치 관리 기능을 제공하는 프로그램 중요 구성 요소 중 하나이며, A사 의 WiMAX CPE 장치만을 관리하기 위해 작성되었기에 다른 MIB 파일과 구별되는 유일한 프로그램 판단된다.

또한 A사 의 MIB 파일은 개발하는데 있어서 WiMAX CPE 장치 관리를 위한 요구사항 분석과 설계, 그리고 구현 등 적지 않은 시간과 노력

이 투자되었다고 사료되며, 외부에 공개하지 않은 사설 MIB으로 개발되었기 때문에 재산적 가치가 인정될 수 있는 자료인 것으로 판단된다.

3.3 A사 와 B사 의 MIB 파일간 소스코드 유사성 분석

A사 MIB 파일의 재산적 가치 유무의 판단에 앞서, A사 와 B사 의 MIB 파일간에 소스코드 유사성이 있는 지를 판단하기 위하여 MIB 파일을 비교 분석하였다.

분석 결과, A사 MIB파일 과 B사 MIB파일 간 평균 유사도는 원본 기준일 경우에는 89.3%(392 라인의 A사 소스코드 중에서 350 라인이 유사함)로 분석되었다. 결과를 요약하여 나타낸 것이 표 2이다.

표 2. A사와 B사의 MIB 파일 유사도 분석
Table 2. Comparison of MIB file similarity Analysis between A and B

A사		B사		유사도	
MIB 파일명	라인수	MIB 파일명	라인수	유사 라인수	유사도 (%)
SWC. MIB	392	SN.M IB	324	350	89.3

유사하다고 도출된 MIB 파일 소스코드를 심층 분석한 결과 B사 가 추가한 소스 코드도 일부 분 있었지만, 대부분의 소스코드는 MIB 객체 이름 뿐만 아니라 주석까지 동일한 것으로 분석되었다. 따라서 B사 의 MIB 파일은 A사 의 MIB 파일을 의거하여 작성된 것으로 판단된다. MIB 파일의 소스 코드 유사성 분석은 그림 3에서 보여주고 있다.



그림 3. MIB 파일의 소스 코드 유사성 분석
Fig. 3. Source code similarity analysis of MIB file

4. 결 론

본 논문에서 수행한 유사도 분석 결과를 정리 하면 다음과 같다. A사 와 B사 간 MIB 파일에 대한 유사성 분석 결과, 원본 기준 방식 89.3% 유사성이 분석되었다.

유출된 MIB 파일의 재산적 가치 유무에 대한 분석 결과, 유출된 MIB 파일은 네트워크 장치관리를 제공하는 프로그램 중요 구성 요소로서, A 사 의 WiMAX CPE 장치만을 관리하기 위해 작성되었기에 다른 MIB 파일과 구별되는 유일한 프로그램으로 판단된다. 또한 유출된 MIB은 개발하는데 있어서 적지 않은 시간과 노력이 투자 되었다고 사료되며, 외부에 공개하지 않은 사설 MIB으로 개발되었기 때문에 재산적 가치가 인정 될 수 있는 자료인 것으로 판단된다.

참 고 문 헌

- [1] 이성훈, 조광문, “소프트웨어 개발에서의 분쟁조정을 위한 표준화 방안”, 한국콘텐츠학회 춘계 종합학술대회 논문집, pp.406-409, 2005.
- [2] 김도완, 윤영선, “SW 소스코드 저작권보호를 위한 통합 가이드”, 컴퓨터프로그램보호위원회, Apr. 2009.
- [3] 방효근, 신동명, 정태명, “소프트웨어 복제 감정을 위한 유사도 및 복제도 평가방법에 관한 연구”, 한국소프트웨어감정평가학회 제 2회 추계 학술발표대회 논문집, pp.9-15, 2003.
- [4] Backer, B. and Manber, U., “Deducing similarities in java sources from byte codes”, USENIX ATEC, pp.15-18, 1999.
- [5] 방효근, 신동명, 정태명, “소프트웨어 포렌식 : 프로그램 소스코드 유사성 비교 및 분석을 중심으로”, 디지털 포렌식 연구 창간호, Nov. 2007.
- [6] 김시열, “컴퓨터프로그램 저작권 유사도론”, 세창출판사, 2018.
- [7] Baker, B., “On Finding Duplication and Near-Duplication in Large Software Systems”, WCRE, pp.96-95, 1995.
- [8] exEyes, 2015. <http://www.copyright.or.kr>
- [9] Liu, C., Chen, C., Han, J., and Yu, P., “GPLAG : Detection of Software Plagiarism by Program Dependence Graph Analysis”, KDD, pp.872-881, 2006.
- [10] 이규대, “유사성 비교에서 세부항목 설정 기준”, 한국소프트웨어감정평가학회 논문지, 12권 1호, pp.21-26, Jun. 2016.
- [11] S. Marcus and M. Vosgerau, “ClassifyHub : An Algorithm to classify GitHub Repositories”, Join Artificial Intelligence, Springer, Cham, pp.373-379, 2017.
- [12] Black Duck, “The tenth annual future of open source survey”, Black Duck Software, Oct. 2016. <http://www.blackducksoftware.com/2016-future-open-source>
- [13] 김종배, 조재홍, 김태열, “오픈 소스 SW비즈니스 모델”, 한국통신학회지(정보와 통신), 35권 5호, pp.52-59, May 2018.

————— 저 자 소 개 —————



전병태(Byung-Tae Chun)

2001년 2월 고려대학교 박사
1989~1896년 한국과학기술연구원 연구원
1996~2004년 ETRI 선임연구원
2004.2.~현재 국립 한경대학교
컴퓨터공학 교수
2013.8.~현재 한국저작권위원
SW분석전문위원
2019.1.~현재 한국지식정보학회
논문지편집위원장
2004.2.~현재 한국SW감정평가학회 이사
2015.12.10. 제10회 대한민국 로봇 대상
산업통상자원부 장관상
<주관심분야> 영상처리, 로봇 HRI