JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 19, No. 11, pp. 2195-2202, Nov. 2018

Financial Information eXchange 트래픽 시각화 연구

권성문 · 김명종 · 손태식*
아주대학교 컴퓨터공학과

Research for Visualization of Financial Information eXchange Traffic

Sungmoon Kwon · Myungjong Kim · Taeshik Shon*
Department of Computer Engineering, Ajou University, Suwon 16499, Korea

[요 약]

스마트 폰을 이용한 금융 거래와 최근의 가상화폐를 이용한 거래가 급증함에 따라 금융 네트워크의 트래픽 규모가 커지고 있다. 또한 금융을 대상으로 하는 사이버 공격과 금융 보안 사고도 증가하고 있어 이에 대한 대응방안이 필요하다. 그러나 금융 사이버 공격에 대응하는 것은 대규모 트래픽에 대한 분석이 요구되기 때문에 비용과 시간의 측면에서 쉽지 않다. 따라서 이에 대한 해결 방안으로 시각화 기법이 사용될 수 있으며 이를 위해 본 논문은 주식 거래, 가상화폐 거래 등 금융 거래에서 사용되는 프로토콜 중 하나인 Financial Information eXchange 프로토콜을 대상으로 네트워크 트래픽을 분석하고 트래픽 유형 별 주요 시각화 필드를 도출하며 시각화 방안을 제안한다.

[Abstract]

As financial transactions using smart phones and transactions using cryptocurrency have increased sharply, the traffic volume of financial networks is increasing. Financial cyber attack is also increasing, so its countermeasure is needed. However, coping with financial cyber attack is hard in aspect of cost and time because analysis of massive traffic is necessary. Therefore, visualization technique can be used as a solution to this problem. For this purpose, this paper analyzed the network traffic of Financial Information eXchange protocol, which is one of the protocols used in financial transactions such as stock trading and cryptocurrency and derived the visualization field for each traffic type and propose a visualization method.

색인어 : 금융 네트워크, 시각화, FIX 프로토콜, 사이버 보안

Key word : Cyber security, Financial network, FIX protocol, Visualization

http://dx.doi.org/10.9728/dcs.2018.19.11.2195

Received 28 October 2018; **Revised** 10 November 2018
Accepted 20 November 2018

***Corresponding Author; Taeshik Shon**

Tel: +82-31-219-3321
E-mail: tsshon@ajou.ac.kr

Ⅰ. 서 론

스마트 폰과 같은 다양한 플랫폼을 이용한 금융 거래와 가상화폐와 관련된 거래를 통해 금융 네트워크의 트래픽은 이례적으로 급증하고 있다. 네트워크 트래픽이 증가함에 따라 이에 비례하여 금융 보안사고 발생 시 분석해야 할 네트워크 트래픽의 양 또한 증가하고 있다. 국내의 2013년 3월에 발생한 방송망, 금융망 사이버테러와 국외의 2014년 7월 미국에서 일어난 JP Morgan Chase 은행의 데이터 침해 사건, 2016년 2월 방글라데시 센트럴 은행의 시스템 권한이 탈취되어 1억 달러 상당의 금액이 도난당한 사건 등 금융 네트워크의 보안 사고로 금융 네트워크 보안의 중요성이 강조되고 있다. 특히 금융 네트워크에 대한 사이버 공격은 직접적인 고객의 금전적 피해로 이어질 수 있기 때문에 이에 대응하기 위한 방안이 필요하다. 금융 네트워크에 시각화를 적용하여 모니터링을 하는 것은 보안 관제원이 중요한 데이터에 집중할 수 있기에 데이터를 보다 효과적으로 분석하여 시간과 금액을 최소화 할 수 있는 장점이 있을 뿐만 아니라 외부 네트워크에서 들어오는 패킷을 시각화하여 모니터링함으로써 인간이 한순간 분석 할 수 있는 양의 한계를 극복할 수 있다. 이러한 이유로 빅데이터로 구성된 주요 정보들에 대해 시각화한 시스템이나 프레임워크들이 등장하고 있다. 2016년 Uber社에서 발표한 오픈소스 'Deck.gl'[1]는 지도에 관한 데이터를 시각화해주는 프레임워크이며 국내 엔키아 社에서 발표한 폴스타 IIoT는 산업 빅 데이터를 머신러닝 기반으로 실시간 수집, 처리, 분석을 해주는 통합 시각화 프레임워크이다. 이 밖에도 일반적인 데이터 시각화 프레임워크로 사용되는 오픈소스 d3.js[2]가 있다.

FIX(financial information exchange) 프로토콜은 1992년에 처음으로 주식 거래 데이터를 전자적으로 기록하기 위해서 작성되었으며, 다양한 금융 상품을 거래하기 위한 국제적인 표준 프로토콜이다. FIX 거래 단체에 따르면 FIX 프로토콜은 미국, 캐나다 등 북미 지역뿐만 아니라 유럽, 중국 등 다양한 국가와 지역에서 사용되고 있으며, 현재 FIX 5.0이 최신 버전으로 사용되고 있다.[3] 또한 2015년부터는 가상화폐 거래에도 사용되고 있다. 본 논문에서는 현재 네트워크 보안을 중심으로 연구되고 있는 시각화 방법들을 살펴보고 금융 네트워크에서 주로 쓰이고 있는 프로토콜 중 하나인 FIX 프로토콜을 분석하여 시각화 연구를 진행할 때 중점으로 두어야하는 데이터에 대해 분석하고, 분석한 필드들을 기반으로 기존에 연구 중인 시각화 방법을 적용한 프레임워크를 제안하고자 한다. 본 연구의 주요 기여 사항으로는 금융 거래에 사용되는 FIX 프로토콜을 분석하여 시각화 필드를 규정함에 따라 FIX 프로토콜에 대한 네트워크 트래픽을 보다 효과적으로 분석할 수 있는 토대를 마련하여 금융 네트워크에 보안에 기여한 점에 있다.

논문의 구성은 총 5장으로 구성되었다. 2장에서는 네트워크 보안관점으로 시각화에 대한 관련 연구들에 대해서 살펴보고, 3장에서는 FIX 프로토콜에 대해 설명하며, 실제 FIX 프로토콜의 트래픽을 분석하여 트래픽 유형별 시각화를 위한 필드를 도출한 내용을 설명한다. 4장에서는 FIX 프로토콜에 대해 시각화를 적용하기 위한 방법 및 정의한 시각화 태그 필드들을 실제적으로 FIX 프로토콜 패킷에 적용한 시각화 결과를 설명한다. 마지막 5장에서는 본 논문에 대한 결론과 향후 연구를 제시한다.

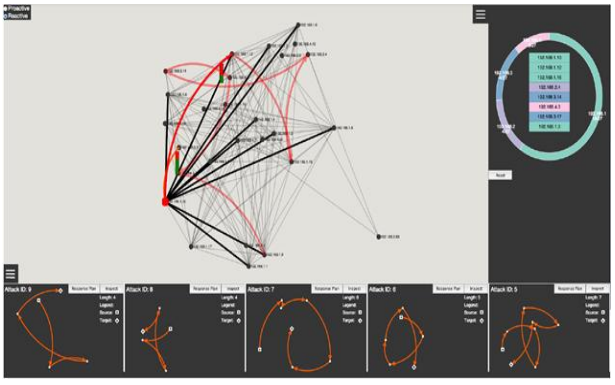

그림 1. PERCIVAL 도구
Fig. 1. PERCIVAL tool

Ⅱ. 관련 연구

시각화는 최근 이슈가 되고 있는 빅데이터를 중심으로 대량의 데이터를 효과적으로 분석하기 위해 연구되고 있는 분야이다. 시각화는 데이터를 보다 효과적으로 표현하기 위한 기법으로 네트워크 시각화에 대한 연구들이 진행 되고 있다. D. Arendt et al.[4]는 2016년에 CyberPetri 시각화 도구를 개발하여 공개하였다. CyberPetri는 연결된 네트워크의 상황을 실시간으로 분석할 수 있는 도구로 내부 네트워크의 보안을 위하여 웹서버로부터 받은 데이터를 시각화하여 나타내어 주며 IP(internet protocol)에 대한 정보를 가공하고 뷰/컬러 필터를 원형, 바 형태의 데이터 그래프에 적용하여 사용자가 시스템의 이상 징후를 효과적으로 식별할 수 있다. H. Siadati et al.[5]이 2016년에 제안한 APT-Hunter는 기업 내부 네트워크 환경에서 보안 분석가들이 악의적인 침입을 인식하는 데에 도움을 주는 도구이다. 로그인되어 있는 사용자/시스템의 로그인 패턴을 분석하고 시스템 간에 연결을 선 그래프로 표현하여 보안 분석가들이 효과적으로 식별할 수 있게 설계하였다. M. Angelini et al.[6]은 네트워커 보안에서 모니터링 관점에서 상황 인식의 중요성을 강조하였으며 PERCIVAL 시스템을 제안하였다. PERCIVAL 시스템은 내부 네트워크에서 사전 대응과 사후 대응에 대한 분석을 통해 네트워크 데이터를 Attack graph로 시각화하여 보안 분석가들이 효과적으로 보안 대응할 수 있게 설계하였다. 그림 1.은 PERCIVAL 도구에서 사후 대응에 대한 분석을 시각화한 것이며, 3개의 구역으로 나누어져 있다. 메인 화면에는 내부 네트워크 구성을 보여주며 다음 노드에서 공격에 대한 대응이 완료되었는지를 확인할 수 있게 해준다. 하단에는

예상되는 공격 경로를 나타내어 준다. 우측에는 관리자들이 적용된 공격 경로에 대한 리뷰를 할 수 있다. IDS RainStorm[7]은 침입 탐지 시스템에서 생성되는 많은 양의 경보 데이터를 시스템 관리자가보다 효율적으로 관리하기 위해서 네트워크 내에 경보 활동을 시각적으로 보여준다. x축으로는 알람의 패턴과 색상의 변화로 인해 경보 알람을 나타내고, y축으로 네트워크 IP 주소를 제공해 경보 알람의 위치를 제공한다.

네트워크 보안 관점에서 시각화에 대한 연구는 기존에 존재하던 시스템에 시각화 도구를 통합하는 방법으로 진행되고 있으며, IP 주소, 포트 번호, 공격 패턴, 라우팅 방법 등을 기준으로 다양하게 연구되고 있다.[7] 시각화 연구들은 적용된 분야가 다르지만 각각에 내부 네트워크에 대해서 시각화를 적용하여 시스템의 이상 유무를 판단하거나 공격에 대해서 인식하는 데에 도움을 주는 도구들이다. 그러나 급증하는 금융 네트워크를 분석하기 위한 시각화 도구를 위한 연구는 진행되고 있지 않아 금융 네트워크 프로토콜 분석을 통해 금융 네트워크 맞춤형 시각화 연구가 필요하다.

Ⅲ. FIX 프로토콜 분석 및 시각화 필드 도출

3장에서는 금융 네트워크에서 금융 상품들을 거래하기 위해 사용되는 주요 프로토콜 중 하나인 FIX 프로토콜에 대하여 분석하며 FIX 트래픽 분석에 기반한 트래픽 유형별 시각화 필드를 도출한 내용을 설명한다.

3-1 FIX 프로토콜 분석

1) FIX 프로토콜 구조

초기의 FIX 프로토콜은 주주들 간의 직접적인 메시지 교환을 가능하게 함으로써 주식거래 활동의 편의를 도모하기 위해 사용되었지만, 프로토콜이 발전됨에 따라 다양한 기능들이 확장되었다. FIX 프로토콜은 세션(session)과 응용(application) 두 계층으로 정의되고, 세션 계층은 데이터 전송에 대한 기능을 담당하며, 응용 계층은 데이터 내용을 담고 있다. FIX 프로토콜은 아래 그림 2.와 같이 각 구매자와 판매자의 FIX 엔진 사이에서 Logon, Orders, Allocations 등의 메시지를 TCP(transmission control protocol)/IP 계층 위에서 주고받으며 통신을 수행한다.

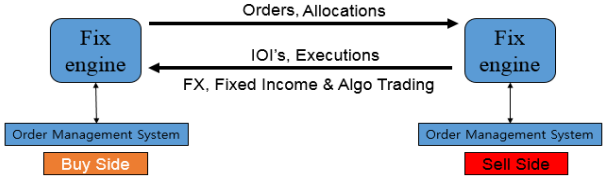

그림 2. FIX 프로토콜 통신
Fig. 2. FIX protocol communication

표 1. FIX 프로토콜 기본 필드
Table 1. Basic field of FIX protocol

Tag	Description
8	BeginString
9	BodyLength
35	MsgType
10	Checksum

FIX 프로토콜의 형식은 “Tag=Value" 형식으로 XML(extension markup language) 형식 또한 지원한다. 주로 사용되는 데이터 형식이 "Tag=Value" 형식이기 때문에 본 논문에서는 XML 형식은 다루지 않는다. FIX 프로토콜은 표 1.과 같은 필드를 기본적으로 포함하여 Header, Body, Trailer 세 부분으로 구성되며 각 부분을 시작하는 BeginString 필드와 체크섬 필드는 필수적이다. FIX 프로토콜은 현재 5.0 버전을 기준으로 1~1139 번까지의 태그가 정의되어 있으며, 기업들 간 통신을 위한 사용자 정의 유형 5000~9000번의 태그 번호가 사용 가능하다.[8]

2) FIX 통신 트래픽 분석

실제 FIX 프로토콜 시뮬레이션 통신 트래픽을 분석한 결과 FIX 통신 유형은 크게 Logon, Heartbeat, 브로커의 IoI(indication of interest), 구매자의 Order 명령 및 ExecutionReport 명령으로 나뉠 수 있다.

Logon 명령은 사용자 간의 새로운 세션을 생성하기 위해 사용된다. 주로 구매자 및 클라이언트 측에서 Logon 메시지를 전송하여 세션을 요청하며, 브로커 및 서버 측에서는 전송 받은 Logon 메시지를 검사하여 세션 연결 여부를 결정한다. 세션 연결을 승인하는 경우 동일한 구조의 Logon 메시지를 전송하나 세션 연결을 거부하는 경우 Logout 메시지를 전송한다. 세션이 생성됨과 동시에 시퀀스(sequence) 번호는 1로 초기화되며 Logon 수행 중에 클라이언트의 Heartbeat 주기 또한 설정한다. Heartbeat 명령은 클라이언트가 다른 명령을 보내지 않고 있으나 세션을 현재도 사용 중임을 서버에 알리는 명령으로, 최후의 메시지 전송으로부터 Logon 과정에서 설정된 주기가 지날 때마다 전송한다. 목적 자체가 단순하기 때문에 Heartbeat 메시지의 데이터는 주소 값과 메시지 전송 시의 시간 값 외에는 포함하고 있지 않다. 브로커가 전송하는 IoI 명령은 현재 브로커가 구입과 매각에 관심이 있는 상품들을 전송하는 명령이다. 거래 목적 아이템의 고유 번호, 이름, 통화 단위와 가격, 수량, 거래 유효 시간, 판매 및 구매 여부 등 해당 아이템의 거래를 위한 각종 정보를 포함하고 있으며 관심 상품 목록을 주기적으로 구매자에게 전송한다. Order 명령은 구매자가 원하는 아이템에 대해 판매 또는 매입을 수행하는 명령으로 구매 명령에 대한 고유 번호, 이름, 수량, 판매 및 구입여부, 명령 및 전송 시간 등을 담고 있다. Order 명령이 처리됨에 따라 이에 대한 응답으로 ExecutionReport 명령이 브로커로부터 전송되며 Order 명령의

해당 품목 주문 수량이 많은 경우 다수의 ExecutionReport 명령으로 처리 과정을 리포팅하기도 한다. 이 경우 각 ExecutionReport 명령마다 거래 진행에 따른 잔여 거래 수량이 감소되어 전송되며 마지막 ExecutionReport는 잔여 거래 수량이 0으로 전송된다.

3-2 FIX 프로토콜 시각화 필드 도출

FIX 프로토콜의 하위 계층인 TCP/IP 계층의 IP 주소나 포트 번호 값은 단일 패킷으로 비정상행위 탐지에 활용 될 수 있다. 그러나 응용 계층의 FIX 프로토콜의 패킷은 단일 패킷만으로 비정상행위를 탐지하기가 쉽지 않아 일련의 패킷에 대한 분석이 필요하다. 따라서 앞 3-1 소절에서 분석된 5 항목의 트래픽 유형에 대해 일련의 패킷을 분석하기 위해 요구되는 시각화 필드를 도출하였으며 표 2. ~ 표 6.는 트래픽 유형별 시각화 필드와 각 필드에 대한 설명을 정리한 것이다.

표 2. 시각화 필드 – Logon 메시지
Table 2. Visualization field – Logon message

Tag Number	Tag Name	Description
49	SenderCompID	Assigned value used to identify firm sending message
52	SendingTime	Time of message transmission
56	TargetCompID	Assigned value used to identify receiving firm
108	HeartBtInt	Interval of heartbeat message

표 3. 시각화 필드 – Heartbeat 메시지
Table 3. Visualization field – Heartbeat message

Tag Number	Tag Name	Description
49	SenderCompID	Assigned value used to identify firm sending message
52	SendingTime	Time of message transmission
56	TargetCompID	Assigned value used to identify receiving firm

표 4. 시각화 필드 – IoI 메시지
Table 4. Visualization field – IoI message

Tag Number	Tag Name	Description
27	IOIQty	Quantity of IOI
34	MsgSeqNum	Integer message sequence number
35	MsgType	Message format is privately defined between sender and receiver
44	Price	Price of IOI item
49	SenderCompID	Assigned value used to identify firm sending message
52	SendingTime	Time of message transmission (always expressed in UTC)
54	Side	Buy (1), Sell (2)
55	Symbol	Name of IOI item
56	TargetCompID	Assigned value used to identify receiving firm

표 5. 시각화 필드 – Order 메시지
Table 5. Visualization field – Order message

Tag Number	Tag Name	Description
11	ClOrdID	Unique order ID
34	MsgSeqNum	Integer message sequence number
35	MsgType	Message format is privately defined between sender and receiver
38	OrderQty	Quantity of order item
49	SenderCompID	Assigned value used to identify firm sending message
52	SendingTime	Time of message transmission (always expressed in UTC)
54	Side	Buy (1), Sell (2)
55	Symbol	Name of order item
56	TargetCompID	Assigned value used to identify receiving firm

표 6. 시각화 필드 – ExecutionReport 메시지
Table 6. Visualization field – ExecutionReport message

Tag Number	Tag Name	Description
11	ClOrdID	Unique order ID
14	CumQty	Quantity of processed amount
32	LastQty	CumQty of last execution report
34	MsgSeqNum	Integer message sequence number
35	MsgType	Message format is privately defined between sender and receiver
38	OrderQty	Quantity of order item
49	SenderCompID	Assigned value used to identify firm sending message
52	SendingTime	Time of message transmission (always expressed in UTC)
54	Side	Buy (1), Sell (2)
55	Symbol	Name of order item
56	TargetCompID	Assigned value used to identify receiving firm
151	LeavesQty	Remaining quantity of order item

Logon 메시지에서는 Heartbeat 주기를 저장하여 추후 Heartbeat 명령의 정상 동작 유무를 파악하여 Heartbeat를 이용한 서버의 자원 소모를 노린 비정상 메시지 전송을 탐지 할 수 있을 것이다. IoI 메시지에서는 해당 아이템에 대한 필드들을 기록하여 가격의 변동을 모니터링해야 한다. IoI 리스트가 많은 경우 특정 품목에 대한 IoI 메시지 주기는 길어질 수 있으며 이 경우 단 하나의 비정상 가격의 IoI 메시지가 구매자로 하여금 혼동을 일으킬 수 있다. 따라서 IoI 품목 별로 정보를 저장하고 추이를 모니터링하여 비정상적 가격 변동을 통한 비정상 거래 내역이 탐지 가능해야 한다. Order과 ExecutionReport는 실제 금융 거래 내역을 나타내므로 최대한 상세한 정보의 기록이 필요하다. 특히 고유 거래 ID는 금융사고 발생 시 금융 거래 내역을 역추적 하는데 필수적인 사항이며, 금융 거래 시간은 소비자

의 거래 시간 패턴 분석에도 활용 될 수 있다.

그리고 공통적으로 시간 값과 금융 트랜잭션의 경우 ID 값을 기록함으로써 금융 사고가 발생했을 시 해당 시간의 해당 사건의 분석이 가능해야 한다.

Ⅳ. FIX 프로토콜 시각화

이어서 4장에서는 3장에서 분석한 시각화 필드들을 시각화하기 위한 방안과 수행 결과를 설명한다.

4-1 시각화 방안

FIX 프로토콜 시각화를 위해 구성한 시스템의 동작 순서는 그림 3.과 같다. 대상 네트워크에서 수집된 네트워크 패킷 파일인 Pcap(packet capture) 파일에 대해서 각 필드에 대해서 파싱을 하여 CSV(comma-separated values) 파일을 생성한다. 다음 단계로는 TCP/IP와 FIX 프로토콜에 대해서 파싱된 CSV 파일을 분석하여 시각화를 진행한다. PCAP 파일을 파싱하여 CSV 파일을 생성하기 위해 Python 2.7.13와 dpkt 1.9.1을 사용하였으며, 시각화를 적용하기 위해 웹 기반 라이브러리 d3.js를 사용하였다. 그리고 시각화 대상 패킷으로는 WireShark에서 제공하는 FIX 프로토콜 시뮬레이션 패킷[9]을 사용하였다.

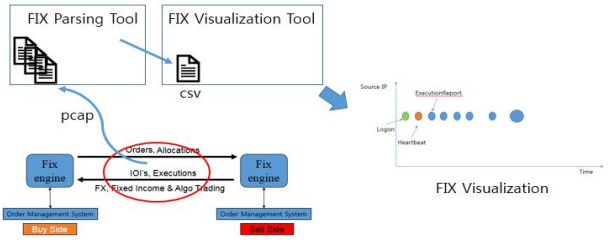

그림 3. Visualization 절차
Fig. 3. Visualization procedure

```
fix = tcp.data.split("\x01")
msg_ty = find_tag(fix,'35')
data['Msg_Type'] = msg_type(msg_ty)
msg_count(msg_ty);
SenderCompID = find_tag(fix,'49')
data['SenderCompID'] = SenderCompID
TargetCompID = find_tag(fix,'56')
data['TargetCompID'] = TargetCompID
MsgSeqNum = find_tag(fix,'34')
data['MsgSeqNum'] = MsgSeqNum
SendingTime = find_tag(fix,'52')
data['SendingTime'] = SendingTime
OrderQty = find_tag(fix,'38')
data['OrderQty'] = OrderQty
Price = find_tag(fix,'44')
data['Price'] = Price
data['tcp_checksum'] = tcp.sum
writer.writerow(data)
```

그림 4. Python pcap 파일 파싱 코드
Fig. 4. Python pcap file parsing code

```
d3.csv("Data/fixStat.csv",type, function (d){
    nv.addGraph(function() {

        var chart = nv.models.pieChart()
                .x(function(d) { return d.MsgType })
                .y(function(d) { return d.Count })
                .showLabels(true)
                .labelThreshold(.05)
                .labelType("percent")
                .donut(true)
                .donutRatio(0.35)
                .valueFormat((d3.format(".0f")))
            ;
        d3.select("#pie_chart_0")
            .datum(d)
            .transition().duration(350)
            .call(chart);
        return chart;
    });
});
```

그림 5. 시각화 코드
Fig. 5. Visualization code

1) Python pcap 파일 파싱

FIX 프로토콜은 TCP/IP 계층을 통해 메시지를 전송한다. TCP와 IP 계층 관련 필드를 dpkt 라이브러리에 따라 파싱을 수행한다. 그 후 TCP payload를 그림 4.와 같이 '\x01'을 토큰으로 나누어 각 태그마다 값을 읽어 각 태그의 값과 메시지를 저장하여 CSV 파일을 생성하였다.

2) 시각화

그림 5.는 Python 파싱 코드로 생성된 CSV 파일을 입력으로 받아 d3 라이브러리를 사용하여 파이 그래프를 생성하는 코드이다. d3 라이브러리는 웹브라우저 상에서 시각화하기 위해 사용되는 자바스크립트 라이브러리이다. HTML5(hyper text markup language 5)와 CSS(cascading style sheet) 등을 기반 해 구현되어 있으며 Datameer와 뉴욕 타임즈가 시각화를 할 때 활용하고 있다. CSV 파일의 헤더 메시지 타입과 데이터를 읽어 시각화한다. FIX 프로토콜 시각화 방법은 전체적인 FIX 메시지의 종류를 분석하기 위해 통계적인 정보를 쉽게 나타낼 수 있는 원형 그래프와 시간에 따른 전체적인 FIX프로토콜 분석을 통해 3장에서 도출한 FIX 시각화 태그들을 나타내는 그래프로 나누어진다. FIX 프로토콜 메시지는 메시지 유형에 따라 메시지의 역할이 달라진다. FIX 메시지의 종류를 분석하기 위한 원형 그래프는 통신의 특성상 Logon/Logout, HeartBeat 메시지의 비율이 낮고 Execution Report, NewOrderSingle, IOI 등의 비율이 높다. 시간에 따른 전체적인 FIX 프로토콜을 분석해 도출한 시각화 태그를 이용한 그래프는 프로토콜 특성상 빈도가 낮은 메시지가 가지고 있는 필수 태그에 따라 메시지를 교환하고 있는 지에 대한 확인이 필요하고, 거래 정보에 따른 금융 상품의 종류, 가격, 양 등의 추가적인 태그들을 나타낼 수 있는 그래프여야만 한다.

4-1 시각화 검증

FIX 프로토콜 시각화는 그림 6.과 같이 두 개의 영역으로 나

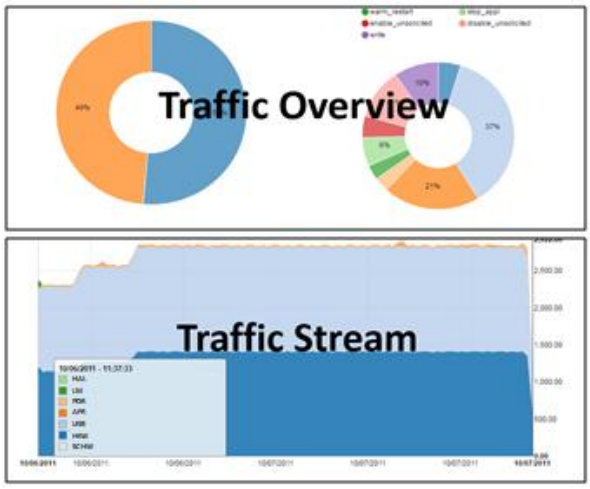

그림 6. 시각화 뷰
Fig. 6. Visualization view

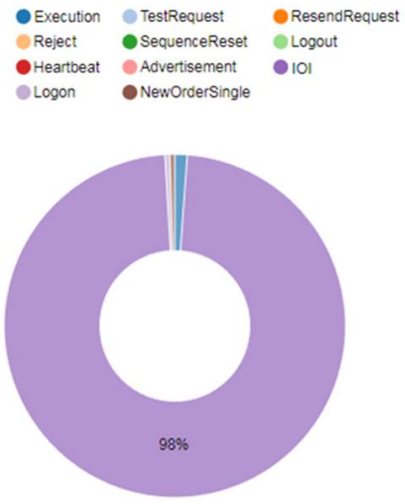

그림 7. FIX 프로토콜 메시지 유형 통계 그래프
Fig. 7. FIX protocol message type statistic graph

누어서 설명할 수 있다. FIX 프로토콜 메시지 유형에 따른 통계를 나타내어 주는 영역과 TCP/IP 계층의 IP, 포트 번호 및 FIX 프로토콜을 분석해 도출한 시각화 태그를 시간에 따라 나타내어 주는 영역이다.

그림 7.은 FIX 프로토콜의 메시지 유형에 따른 통계를 나타내어 주는 그림으로 실험으로 사용된 트래픽 메시지 종류의 대부분이 IoI인 것이 확인된다. 이다음 가장 많은 분포를 보이는 메시지는 ExecutionReport 메시지로 ExecutionReport 메시지는 주문에 대한 영수증이나 변경 사항, 주문 상태, 거래 후 수수료 계산 등에 대한 정보를 가지고 있다. 샘플 데이터에서의 Order 수량이 컸기 때문에 Order 처리가 여러 번에 나뉘어 실행되어 다주 ExecutionReport 메시지가 전송되었기 때문에 두 번째로 높은 메시지 사용 빈도수를 보였다. 그 다음 높은 분포를 보이는 Heartbeat 메시지는 Logon 메시지에서 서로 합의한 HeartBtInt 시간에 따라 주기적으로 메시지를 교환해 통신 링크의 상태를 확인하고, 메시지의 마지막 문자열이 수신되지 않은 시기를 식별하기 위해 사용되었다.

일련의 FIX 패킷 데이터를 시각화하는 것은 특정 IoI의 값의 일련의 흐름 외에도 그림 8.와 같은 패킷 단위의 시각화를 수행하였다. x축은 시간, y축은 IP 주소 값을 의미하며 이를 통해 비정상 주소에 대한 데이터 통신이 시각적으로 확인이 가능하다. 이외에도 각 FIX 메시지 유형별로 포인트의 모양을 다르게 하였으며, 주로 사용되지 않는 포인트의 경우 기본 값으로 설정하여 각 패킷의 특성을 시각적으로 바로 알아 볼 수 있도록 하였다. 또한 상세 값이 필요한 경우 값을 확대하여 마우스를 오버 시 해당 포인트의 상세 데이터 값을 출력하도록 하여 FIX 프로토콜에 대한 정보를 한눈에 알 수 있게 표현하였다. 이와 같이 FIX 프로토콜을 여러 그래프로 시각화하여 나타냄으로써 로그로 나타내던 시스템과는 다르게 네트워크의 특성을 직관적으로 파악할 수 있는 장점이 있어 금융 보안사고 발생 시 특정 시간대의 정보 분석이나 네트워크 트래픽을 모니터링하여 사전에 공격에 대응에 활용될 수 있을 것이다.

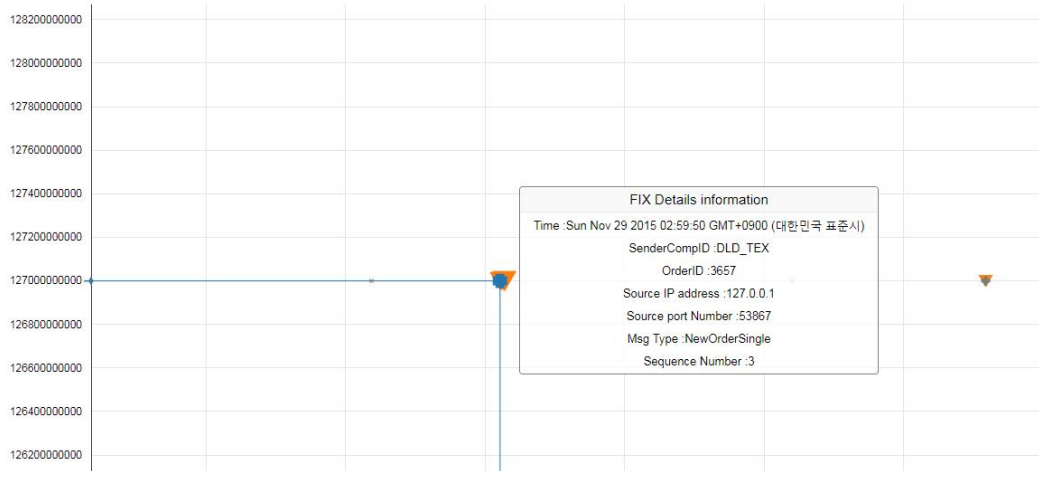

그림 8. FIX 스트림 데이터 시각화 및 상세 정보
Fig 8. FIX stream data visualization and detail information

Ⅴ. 결 론

본 논문에서는 금융 거래에서 사용되는 FIX 프로토콜에 대한 시각화를 적용하여 보안 관제원이 Log만으로는 분석하기 힘든 데이터를 효과적으로 분석 및 모니터링을 할 수 있도록 시각화 태그를 규정하고 시각화 방법을 설계하고 구현하였다. 특히 FIX 프로토콜의 트래픽 유형별로 주요 시각화 필드를 도출하여 효과적인 FIX 프로토콜 시각화에 활용 될 수 있으며 각 환경에서 다르게 사용 되는 FIX 프로토콜을 분석하여 추가적인 필요 필드를 추가함으로써 이상 거래에 대한 분석 가능할 것으로 예상된다. 많은 데이터들이 오가는 시스템에서는 효율적인 보안 관제를 위해서 시각화를 적용하는 것은 네트워크가 확장됨에 따라 필수적인 요구 사항이 되고 있어 FIX 프로토콜을 사용하는 금융 네트워크에서 제안하는 방법론이 활용 될 수 있을 것이다. 향후 연구에서는 FIX 프로토콜을 사용하는 네트워크 상의 실제 금융 보안 사고를 분석하여 제안하는 시각화 기법이 효과적으로 사용될 수 있음을 보이는 연구를 수행할 예정이다.

감사의 글

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2018-2016-0-00304)

참고문헌

[1] DECK.GL [Internet]. Available: https://uber.github.io/deck.gl/#/

[2] D3 library [Internet]. Available: https://d3js.org/

[3] FIX Trading Community [Internet]. https://www.fixtrading.org/overview/

[4] Arendt, Dustin, et al. "CyberPetri at CDX 2016: Real-time network situation awareness." Visualization for Cyber Security (VizSec), 2016 IEEE Symposium on. IEEE, 2016.

[5] Siadati, Hossein, Bahador Saket, and Nasir Memon. "Detecting malicious logins in enterprise networks using visualization." Visualization for Cyber Security (VizSec), 2016 IEEE Symposium on. IEEE, 2016.

[6] Abdullah, Kulsoom, et al. "Ids rainstorm: Visualizing ids alarms." (2005): 1.

[7] Shiravi, Hadi, Ali Shiravi, and Ali A. Ghorbani. "A survey of visualization systems for network security." IEEE Transactions on visualization and computer graphics 18.8 (2012): 1313-1329.

[8] FIX Trading Community, Financial information exchange protocol Version 5.0 Service Pack 2, 2011.

[9] FIX traffic sample captures [Internet]. Available: https://wiki.wireshark.org/SampleCaptures#Financial_Information_eXchange_.28FIX.29

권성문(Sungmoon Kwon)

2013년 : 아주대학교 컴퓨터공학과 (학사)
2013년~현 재 : 아주대학교 대학원 컴퓨터공학과 석박사통합과정
※관심분야 : 제어시스템 보안, 비정상행위 탐지, 스마트그리드 보안, 네트워크 보안

김명종(Myungjong Kim)

2016년 : 아주대학교 컴퓨터공학과 (학사)
2016년~현 재 : 아주대학교 대학원 컴퓨터공학과 석사과정
※관심분야 : 금융 보안, 비정상행위 탐지, 네트워크 보안, 시각화

손태식(Taeshik Shon)

2000년 : 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년 : 아주대학교 정보통신전문대학원 졸업(석사)
2005년 : 고려대학교 정보보호대학원 졸업(박사)
2004년~2005년: University of Minnesota 방문연구원
2005년~2011년: 삼성전자 통신/DMC 연구소 책임연구원
2017년 ~2018년 : Illinois Institute of Technology 방문교수
2011년~현 재: 아주대학교 정보통신대학 사이버보안학과 부교수
※관심분야 : 산업제어시스템 보안, 비정상행위탐지, 디지털 포렌식