

빌딩 보안 네트워크상의 정보폭주 방지를 위한 분류 알고리즘에 관한 연구

김계국*, 서창옥**

A study on the classification algorithm in order to information explosion prevention in building security network

Kye-Kook Kim*, Chang-Ok Seo**

요 약

출입 보안 시스템에서 과도한 이벤트 발생으로 인해 네트워크가 마비되는 경우가 종종 발생된다. 이때 이벤트 발생 원인을 분석하고 이를 대처하기 위해서는 많은 시간이 소요되며 그 시간동안 ACU와 출입보안 서버와의 연결이 끊어지게 되어 출입 현황 및 출입자 정보의 갱신 등을 실시간으로 처리할 수 없게 된다. 본 논문에서는 이벤트에 의한 정보폭주를 방지하기 위하여 분류알고리즘을 제안하였다.

Abstract

The whole network system is paralyzed due to excess event of security server once in a while. If that happens, We have to analyze the cause of events, the time will require when we deal with a matter. All the while, ACU(ACCESS CONTROL UNIT) and security server are off, We can not treat about information retrieval of people who come to building with real time. In this paper, we suggested classification algorithm in order to prevent of information explosion.

▶ Keyword : 정보폭주(information explosion), 분류알고리즘(classification algorithm)

• 제1저자 : 김계국
• 접수일 : 2005.09.26, 심사완료일 : 2005.11.09
* 국립원주대학 전자통신과 교수, ** 건국대학교 대학원 박사과정생

I. 서론

과거에는 출입보안시스템의 규모가 크지 않아 RS232C나 rs422등을 사용하여 출입보안시스템(6)을 운용하였으나 오늘날에는 출입자의 수가 증가하고, 이에 따른 출입보안시스템도 매우 복잡해지고 있는 추세이다.

이로 인해 과거에 사용하던 RS232C나 RS422과 같은 통신에서 네트워크를 이용하는 통신으로 바뀌고 있으며, 복잡하고 다양한 정보를 전송하는 이더넷 통신 속에 출입보안시스템의 정보도 함께 흐르고 있다.

한 선로에 여러 가지 정보가 동시에 전송되고 있어 어느 한쪽에서 과도한 정보를 전송 할 경우에는 통제가 불가능하게 되어 정보 폭주 상태가 초래된다.

본 논문에서는 출입보안시스템의 과도한 이벤트 발생으로 인해 정보 폭주가 일어나는 것을 미연에 방지하기 위해 상대적 중요성(relative importance)과 절대적 중요성(absolute importance)에 의한 마스킹 분류 알고리즘을 제안하였다.

II. 출입통제 시스템 구성

출입보안서버는 인터넷망을 통해 들어오는 ACU에 관한 이벤트 정보를 수집관리하고 지령을 내리는 업무를 하게 된다.

각각의 ACU와 의 통신 프로토콜은 출입보안시스템에 의해 폴링(Polling)을 하게 되는데 이때 ACU의 상태를 하나씩 출입보안서버로 보내주게 된다.[1]

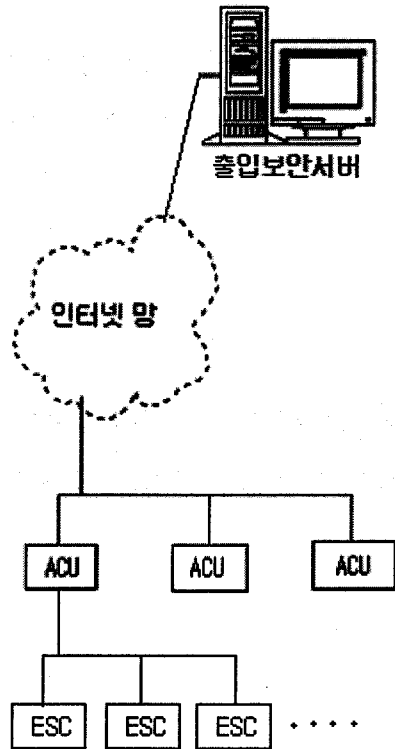


그림 2-1 출입보안시스템
Fig 2-1 Security system

ACU의 상태응답이 없을 때에는 3회에 걸쳐 재전송을 시도 하여 상태요구를 하며 그래도 응답이 없으면 출입보안시스템에서 ACU의 에러를 관리자에게 알리게 된다.

이때 ACU의 상태를 받기 위한 폴링명령은 "GetAcu"이며 ACU의 상태 데이터 포맷은 1바이트의 STX(Start of Text)와 8바이트의 ACU번호, 7 바이트의 ACU상태 데이터, 7바이트는 출입자카드번호 1바이트의 BCC(Block check Character), 1바이트의 ETX(End of Text)로 구성되어 있다.[1]

출입용에 사용되는 출입자카드번호는 RF카드 스마트카드등의 종류가 있는데, 비접촉형 카드인 RF카드를 주로 사용한다. 요즘은 스마트 카드도 비접촉형이 생산되고 있으므로 많이 사용하는 추세이다.

즉 1바이트의 STX와 8바이트의 ACU번호, 7바이트의 ACU상태 데이터, 7바이트의 출입자카드번호 1바이트의 BCC, 1바이트의 ETX로 구성된 데이터를 출입보안서버로 보내게 된다.

STX(1)	ACU(8)	ACU status(7)	ID card (7)	BCC(1)	ETX(1)
--------	--------	---------------	-------------	--------	--------

단, 여기서 ACU의 상태는 7바이트로 표기하나 경우에 따라서는 최고 600바이트까지도 발생되는 경우가 있다.

여기서 BCC는 보통 사용하는 방식인 비트검사방식인 ACU번호부터 IDCARD 까지 XOR한 값을 BCC에 저장한다.

출입보안시스템에서 폴링방식을 사용하는 것은 폴링 중에 각각의 ACU에서 응답이 없을 때는 ACU와의 연결 상태가 좋지 않음을 즉시 알 수 있어 제어용에 많이 사용 된다.

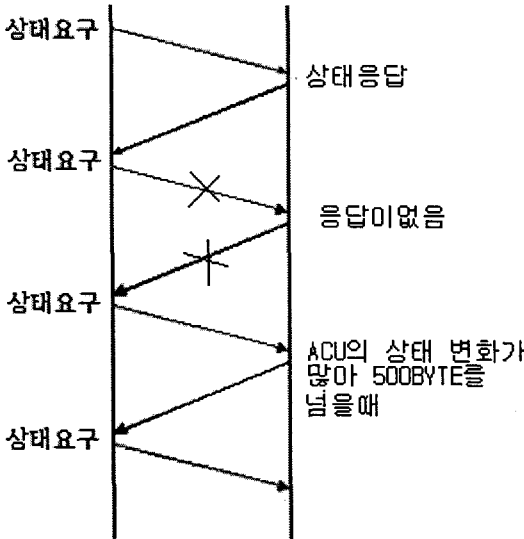


그림 2-2 출입보안시스템 원리
Fig 2-2 Principle of security system

(그림 2-2)에서 출입보안서버가 ACU의 상태를 요구하면 ACU는 현재의 상태를 출입보안 서버로 전송하게 된다.

네트워크의 선로 상태가 좋지 않을 경우에는 ACU는 출입보안서버의 의도를 알 수 없어 ACU는 응답을 하지 않게 된다. 이때 특정시간동안 기다려도 응답이 없을 때는 3회정도 시도해보고 네트워크상태가 불량하다고 관리자에게 알리게 된다.

ACU의 상태 변화가 많아 상태 데이터의 길이가 500바이트를 넘을 경우 일반적인 전송 바이트보다 약 50배 가량 길어진 데이터를 네트워크를 통해 계속적으로 전송하게되므로 네트워크 폭주가 일어 날수 있는 확률이 매우 높아지게 된다.

네트워크의 정보폭주의 근본원인인 ACU상태변화에 따른 데이터의 과대 발생으로 인한 폭주가 일어난다. 이 데이터를 임의적으로 제거할 경우 중요한 데이터를 잃어버리는 경우가 발생하게 된다. 그래서 데이터의 신뢰성에 따라 가중치를 주어 상대적중요성과 절대적중요성에 따라 선택적으로 제거 또는 보존등을 통하여 ACU가 출입보안서버로 데이터를 전송하게 된다.

III. 상대적중요성과 절대적중요성

출입보안시스템에서 정보 폭주는 ACU에서의 과다한 이벤트 발생이 원인이 된다.

이 이벤트의 발생을 제거하면 정보 폭주는 없앨 수 있으나 출입보안시스템에서의 이벤트는 매우 중요한 역할을 하고 있어 발생을 억제하거나, 무작위로 삭제할 수는 없는 일이다. 그래서 이벤트의 마스킹준위를 정하여 그 준위에 의해 이벤트를 출입보안서버로 전송시킨다.

출입보안시스템에서 주로 발생될 수 있는 이벤트는 설치한 장소에 따라 조금씩 다르나 보통 출입문이 계속 열려 있을 경우 발생하는 이벤트, 각종 센서에서 발생하는 잠음성 이벤트, 문열림 상태 이벤트, 출입문개폐기 불량 이벤트, 출입카드 이벤트, 강제출입문개폐 이벤트, 장치파손 이벤트, 전력선 단선 이벤트 등등 무수히 많은 이벤트를 ACU에서 출입보안서버로 전송하게 된다.

한 개의 ACU에 여러 개의 ESC(Entrance Sensor and Controller)가 연결되어 있는데 [2], ESC에서 발생된 상태를 ACU가 판단하여 출입보안서버로 전송하게 된다.

여기서 발생하는 이벤트들은 그 중요성에 따라 절대적중요성과 상대적중요성 으로 나뉘어 지며 그의 비중에 따라 이벤트를 삭제, 보존, 전송 등을 수행하게 된다.

절대적중요성	상대적중요성
전력선단선이벤트	도어열림이벤트
출입카드정보	노이즈성이벤트
강제출입문개폐이벤트	개폐불량이벤트
—	—
—	—

그림 3-1 절대적중요성과 상대적중요성
Fig 3-1 Absolute importance and relative importance

절대적중요성에 해당되는 이벤트라 함은 ACU에서 발생 되는 이벤트 중에 출입보안시스템에서 가장 기초가 되는 이벤트로서 절대적으로 잃어버려서는 안되는 이벤트들의 모임을 의미하며, 상대적 중요성은 출입보안에서 절대적 중요성을 제외한 모든 이벤트의 묶음을 의미한다. 예를 들면 절대적중요성에는 전력선단선, 출입카드정보, 강제출입문개폐 등이 있으며, 상대적 중요성에는 문열림, 잠음성 이벤트, 출입문 개폐불량 이벤트등으로 나뉘어 질수 있다.

출입보안 시스템에서의 절대적 중요성은 항상 전송이 가능해야 하며 어느 하나라도 누락해서는 안되는 데이터이다.

하지만 상대적 중요성은 경우에 따라서는 몇 분이 지난 후에 데이터를 전송하든지 아니면 몇 일후에 데이터를 출입보안서버로 전송을 하여도 된다. 이러한 데이터들을 가려 낼 수 있는 방법을 본 논문에서 제안하였다.

우선 절대적중요성에 관한 데이터는 출입보안시스템을 설치한 장소에 따라 관리자와 의논하여 정의를 해 놓은 것이므로 언제나 출입보안서버에서 요구할 경우 ACU는 데이터를 전송 시켜 주어야 한다.

절대적중요성에 관련된 이벤트들은 ACU내부의 알고리즘에 의해 가장 우선처리 되며, 출입보안서버와 네트워크가 단선되었다 하더라도 다른 통신망을 이용하여 출입보안서버로 이벤트를 전송하도록 시스템이 구성되어져있다.

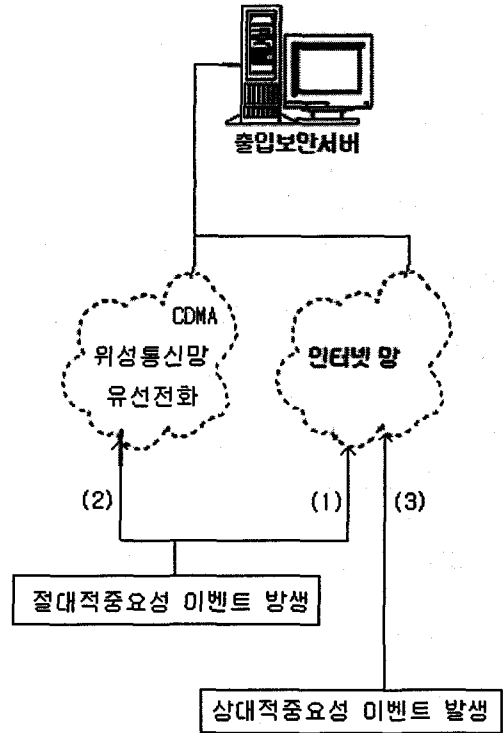


그림 3-2 전송방식
Fig 3-2 Transfer method

(그림 3-2)는 절대적 중요성과 상대적 중요성의 네트워크 망상용과 네트워크의 통신 두절이 발생 되었을 때 다른 통신망을 통해 출입보안서버에 절대적 중요성의 이벤트를 출입보안서버로 보내는 방법을 보여주고 있다.

IV. 마스킹분류법

출입보안시스템에서 정보 폭주에 영향을 주는 이벤트는 절대적 중요성과 상대적 중요성에 따른 이벤트이다.

절대적 중요성에 따른 이벤트는 실시간으로 출입보안서버에 데이터를 전송해야 하나 상대적 중요성에 따른 이벤트는 실시간 정보를 출입보안서버에 전송하지 않아도 된다.

이벤트	상대적중요성준위
도어열림이벤트	2
노이즈성이벤트	4
개폐불량이벤트	6
—	—

그림 4-1 상대적 중요성 준위 예
Fig 4-1 Example of relative importance level

상대적 중요성을 가지는 이벤트들 중에 그 중요도를 정하여 테이블을 만들고, 중요도가 높은 순서대로 실시간으로 전송을 한다.

네트워크의 트래픽이 폭주(burst traffic)로 접근해 갈 때 상대적중요성 중에 중요도가 낮은 이벤트부터 전송을 제한해야 한다.

트래픽상태가 좋지 않을 때 중요도가 낮은 이벤트 데이터를 중요도가 높은 이벤트 데이터와 같이 전송할 경우 트래픽에 영향을 줄 수 있으므로 현재 출입보안서버와 ACU 간의 네트워크의 정보 상태를 분석해서 상대적 중요성에 해당 되는 이벤트들을 분리해 내야 한다.

이렇게 네트워크상의 트래픽량에 따라 상대적중요 성준위를 적용하여 이벤트를 분류해내는 것을 마스킹(Masking) 분류법이라 하였다.

출입보안서버에서 ACU로 상태요구를 하면 ACU는 상태 응답을 출입보안서버로 전송한다.

출입보안서버는 정해진 시간에 ACU의 트래픽량을 측정하기 위해 트래픽측정용 패킷을 요구한다.

ACU는 전송속도 측정에 영향을 주지 않도록 트래픽측정용 패킷전송을 어떤 처리보다 가장 우선하게 전송한다.

출입보안서버는 전송속도를 측정 한 후 ACU에 측정 한 값을 보낸다.

ACU는 트래픽에 관련된 정보를 출입보안서버로부터 받은 후 서버의 상태 요구시에 마스킹분류법에 따라 전송하게 된다.

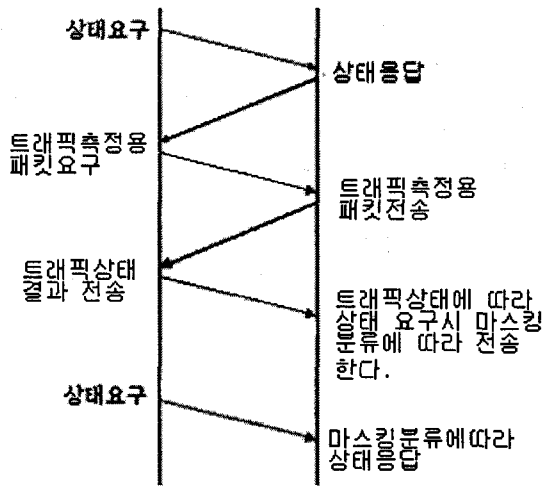


그림 4-2 정보량에 따른 마스킹분류법
Fig 4-2 Masking method by amount of information

V. 실험 및 고찰

출입보안서버는 HP ProLiant DL740을 사용하였고, ACU는 모토로라 32BIT 프로세서인 MPC860을 베이스로 하여 설계 하였으며, 사용된 OS는 Linux 커널을 포팅 하였다. MPC860 메인보드는 기본메모리에 SDRAM 64M 바이트로 설계하였으며, Flash메모리는 8M바이트를 2개 사용하여 1개는 커널 및 부트로더(boot loader)를 올렸고, 다른 하나는 MTD(Memory Technology Device)를 가능하게 하여 Flash메모리를 외장 하드 디스크 처럼 사용할 수 있도록 하였다. MTD를 사용함으로써 원격으로 제어용 프로그램을 자유롭게 바꿀 수 있게하였다. 데몬(Daemon)은 FTP 서버 데몬 과 Tenet 데몬을 올렸으며, 이 또한 원격으로 ACU를 직접관리 하기 위함 이다. ACU는 건물 내에 설치되어 있으며 48개의 ACU를 설치하였다. 알고리즘을 수정 할 경우에는 출입보안서버에서 원격으로 각각의 ACU에 적용될 수 있도록 하였다.

같은 라우터 내에 트래픽을 유발시킬 수 있는 PC를 5대 설치하였으며 각각 네트워크를 통한 동영상 및 과도한 패킷을 전송할 수 있도록 설치를 하였다.

전송속도는 100MBPS가 가능하도록 선로를 포선 하였으나 각각의 ACU와 서버와의 설치 거리가 멀어 전송속도는 평균 30MBPS정도가 되었다.

실험을 위해 ACU의 센서중에 출입문도어 센서를 상대적 중요성 순위 10으로 하였고, 비상스위치를 3으로 하였다. 그리고 절대적중요성에 해당되는 출입자 정보 카드는 ACU에서 주기적으로 발생하도록 하였다.

정보가 평균 30MBPS가 되는 것을 서버에서 확인이 가능했으며 20MBPS 이하가 될 때 상대적중요성순위가 5에서 10사이의 이벤트를 전송 보류하도록 하였고, 10MBPS 이하가 될경우에는 2에서 10사이의 이벤트를 전송 보류하도록 하였다.

VI. 결론

출입통제시스템에 연결된 ACU들에서 서버로 보내는 이벤트의 데이터량 과다로 인하여 정보폭주가 발생한다. 네트워크상의 전송속도가 저하될 때 ACU에서 서버로 보내는 이벤트량을 줄여 네트워크상의 폭주를 막기 위해 제안한 마스킹분류법을 적용하였다.

트래픽이 정상상태에서(30MBPS)는 상대적중요성에 해당되는 이벤트가 모두 서버에 전송되었다. 3대의 PC에서 동영상을 전송할 경우 전송속도가 평균 18MBPS되었을 때 상대적중요성 순위가 10에 해당되는 이벤트가 서버에서 관측되지 않고, ACU에 보관되는 것을 확인하였으며, 트래픽도 19MBPS로 상승되었다.

나머지 2대의 PC에서 과도한 패킷을 유발시켜 평균트래픽이 8MBPS가 되도록 하였다. 상대적중요성 순위가 3에 해당되는 이벤트가 서버에서 관측되지 않고, ACU에 보관되었으며 트래픽도 10MBPS로 상승되는 것을 알 수 있었다.

트래픽에 영향을 주는 요소들을 모두 제거한 후에는 전송속도가 30MBPS로 정상화되었으며, ACU에 보관되었던 상대적중요성의 이벤트들도 출입보안서버로 보내지는 것을 확인할 수 있었다.

본 논문에서 제안한 마스킹분류법을 이용하면 출입보안시스템의 정보 폭주 원인을 근본적으로 해결 할 수 있어 통신망을 안정적으로 운영할 수 있다.

참고문헌

- [1] 서창욱, 김계국 "지능형 빌딩시스템의 성능 개선에 관한 연구" 한국통신학회논문01-26-12T
- [2] 서창욱, 김계국 "빌딩 출입 보안 시스템의 정보폭주 방지방법에 관한 연구" 한국컴퓨터정보학회 논문지 VOL.9.NO.1
- [3] Kane, J.W., and Kodlick, M.R. "Access denial systems: Interaction of delay elements." SAND83-0362 1983: 7.
- [4] Sena, P.A. "Security vehicle barriers." SAND84-2593 1985: 12-54
- [5] Baker, D.R. "Curriculum Design." In Davies, S.J., and Minion, R.R., eds., Security Supervision: Theory and Practice of Asset Protection. Boston: Butterworth-Heinemann, 1999: 127-133
- [6] Gerard Honey. "Electronics Access Control"
- [7] Fischer, R.J., and Green, G. Introduction to security, 6th ed. Boston: Butterworth-Heinemann, 1998: 84-92
- [8] Hertig, C.A. "Considering Contract Security." in Davies, S.J., and Minion, R.R., eds., Security Supervision: Theory, and Practice of Asset Protection. Boston: Butterworth-Heinemann, 1999: 227-229
- [9] International Telecommunications Union (ITU). Recommendation X.200, 2000, Available at: <http://www.itu.int/publications/telecom.htm>
- [10] Mackworth, N.H. "Researches on the measurement of human performance." In Sinaiko, H.W., ed., Selected Papers on Human Factors in the Design and Use of Control System. New York: Dover, 1961: 174-331

저 자 소개



김 계 국

1954년 8월 24일 제주 우도 출생
 원광대학교 전자공학과 졸업
 숭실대학교 대학원 전자공학과 졸업
 (석사)
 건국대학교 대학원 전자공학과 졸업
 (박사)
 원광대학교 전자공학과 강사
 건국대학교 전자공학과 강사
 한국컴퓨터정보학회 이사
 한국정보기술학회 이사
 문예지 시마을 신인상으로 시인등단
 현재 국립 원주대학 전자통신과 교수
 <관심분야> 고주파회로, 원격제어
 시스템, 출입통제시스템.



서 창 옥

1965년 4월 15일 생
 1990년 서울산업대학교 전자공학과
 공학사
 1993년 건국대학교 산업대학원 전
 자공학과 공학석사
 2001년 건국대학교 대학원 전자공
 학과 박사과정수료
 2001~2003년 (주)가드텍 연구소
 수석연구원
 2003년~11월 현재 메이슨기술 대표
 <관심분야> 신호처리, 로봇지능, 출입
 통제시스템