**국민대학교 컴퓨터공학부**

**창의 소프트웨어 프로그램 1기 동계 훈련**

**개별 프로젝트**

**Traffic backup method in High-Speed network**

**for Cyber Black box**

**Department of Computer Engineering, Kookmin University**

**20113328 Ji-man Jeong**

1. **서론**

**1). 프로젝트 선정 이유**

**2). 프로젝트 목적**

**3). 프로젝트의 중요성**

1. **본론**
2. **연구 진행 방향**

1). 실험 절차

1. **실험 및 검증**

1). One by One.

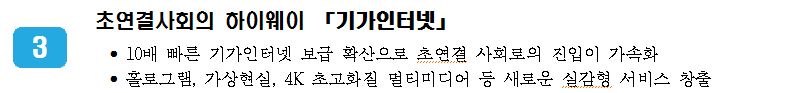
2). Batch (Multi Thread).

3). De-Duplication technique.

1. **결론**
2. **실험 결과**
3. **추후 연구 사항**
4. **서론**

**1). 프로젝트 선정 이유**

**C:\Users\Administrator\Desktop\캡처1.PNG**

****

[ 그림 1-1 KISA 보도자료 ]

최근 인터넷 네트워크의 속도는 급격하게 빨라지고 있다. 기가 단위로 통신하는 네트워크는 우리에게 많은 편리함을 주고 있다. KISA에서 발표한 2015년 인터넷 및 정보보호 10대 산업이슈 전망을 살펴보면[그림 1-1], 기가 인터넷이 3위에 뽑힐 정도로 중요한 이슈로 자리잡았다.

또한 최근에는 사이버 블랙박스라는 개념이 도입되었는데, 이는 네트워크 상에 존재하는 모든 패킷들을 저장소에 저장하여, 사이버 공격을 받았거나 패킷들의 정보를 필요로 할 때, 분석하는 것을 의미한다. 패킷들을 분석하여 어떤 방식으로 공격이 시행되었는지 알 수 있으며, 이를 통해 다음 공격을 예상하고 (군집도 비교) 방어책을 마련할 수 있기 때문에, 사이버 블랙박스 또한 매우 중요한 이슈로 자리잡고 있다.

그러나 빠르게 성장하는 네트워크 통신에 비해 하드웨어에 데이터를 저장하는 속도는 한계를 보이고 있다. 물리적인 한계에 부딪혀 저조한 상승률을 보이는 저장 기술을 위해 새로운 기술이 필요하기 때문에 새로운 기술을 생각해 보고자 프로젝트로 선정하였다.

**2). 프로젝트 목적**

프로젝트 목표는 다음과 같다.

기가바이트 단위로 통신하는 네트워크 망에서 트래픽을 실시간으로 저장소에 저장할 때, 네트워크 통신의 속도와 저장소에 저장하는 속도의 차이에서 발생하는 문제점을 여러가지 방법으로 해결하고, 실제로 적용해본다. 이를 통해 사이버 블랙박스를 위한 새로운 저장 기술을 제시한다.

**3). 프로젝트의 중요성**

최근 악성 공격의 빈도수는 점차 증가하는 추세이며, 다양하게 진화하고 있어 기존의 방어체계로는 모두 방어하기 어렵다. 따라서 패킷들을 모두 저장하고 분석하여 새로운 공격에 대한 방어책을 마련하고, 더불어 다음 공격을 예측하는 것은 매우 중요하다. (사이버 블랙박스) 따라서 이 프로젝트는 매우 의미가 있다..

1. **본론**

**1.연구 진행 방향**

1). 실험 절차

본 프로젝트를 진행하기 전해 구현해야 할 모듈이 하나 있다.

서버-클라이언트 모델로 동작하는 패킷 전송 모듈인데, 이는 사용자가 원하는 속도로 패킷을 전송할 수 있도록 구현 하여야 한다. 따라서 맨 처음으로 이 모듈을 구현하고 실제로 잘 동작하는지 테스트 해본다.

기본 모듈이 구현이 되면 다음과 같은 방법으로 실험을 진행한다.

a). One by one : 패킷을 1개 읽고, 그 1개를 바로 저장하는 방식

b). Batch (multi thread) : 패킷을 저장하는 버퍼공간을 적절한 사이즈로 구성한뒤, 한 쓰레드에서 패킷을 읽고, 다른 쓰레드에서 버퍼가 꽉 차면 버퍼에 있는 데이터를 저장소에 저장한다.

c). De-Duplication : 패킷의 중복도와 유사성을 체크한 뒤, DRE system에 주로 사용되는 Chuncking 방식을 통해 데이터를 줄여서 저장해 본다.

각각의 단계를 거치면서 최대 얼마의 속도까지 가능한지 알아보고 정리한다.

**2.실험 및 검증**

1). One by One.

2). Batch (Multi Thread).

3). De-Duplication technique.

1. **결론**