

## 캡스톤 18 조 회의록

프로젝트명	O24Sec	팀명	앨러리를 찾아서
회의 시간	3 월 12 일 16:00 - 18:00		
장소	국민대학교 미래관 7 층 K 랩		
참석자	김민송, 장우혁	서기	김민송
안건	<ul style="list-style-type: none"> <li>• 현재까지 진행사항 및 앞으로 추가로 진행해야 하는 부분</li> <li>• 현재 프로젝트 진행사항에 대한 검증 필요성</li> <li>• 프로젝트에 대한 전체적인 문서작성</li> </ul>		
회의 내용	<p>📌 현재까지 진행 사항 확인</p> <ol style="list-style-type: none"> <li>1. 객체 별 이벤트 분리: 기동으로 쓰일 규칙을 몇 개 만들어 놓은 상태 <ul style="list-style-type: none"> <li>- B 클래스 대역 별 상대 통신 대역 카디널리티(내부/외부)</li> <li>- 유사 대역에 대해 같게 (내부/외부) 처리하기</li> <li>- 사용된 포트를 통해 서버/클라이언트 구분하기</li> </ul> </li> <li>2. 암호화 패킷 분리: 코드까지 작성된 상태 <ul style="list-style-type: none"> <li>- Entropy 임계 값을 정할 수식이 필요했는데 이 경우 전체적으로 샘플링을 통해 가장 많이 수용시킬 수 있는 수식을 설정해서 적용시켜 놓은 상태</li> </ul> </li> <li>3. 이벤트 클러스터링: 여러가지 실험을 통해 잘 되는 내용을 찾으면서 사용할 기법 선별 중 <ul style="list-style-type: none"> <li>- 현재 패킷 이벤트에서 페이로드를 두고 각 Byte 를 특징으로 하여 무작정 클러스터링을 하는 방법을 시도 중 (데이터의 사이즈가 너무 커서 물리적제약으로 인해 전체 데이터를 사용하는데 어려움)</li> <li>- 페이로드 사이즈가 패킷 별로 상당한 크기차이를 보이기 때문에 현재 0 패딩을 통해 모두 1600byte 로 맞추어서 실험 진행 중</li> </ul> </li> </ol> <p>📌 추가 목표 사항</p> <ul style="list-style-type: none"> <li>- 유사도에 대한 스터디 필요: 이벤트 전체에 대한 유사도 검증이 필요하기 때문에 1:1 1: N 의 유사도가 아닌 전체 데이터에서 유사도를 얻어 낼 수 있는 방법</li> <li>- 만약 클러스터링으로 구분이 잘되어 집합을 나타낼 수 있게 된다면 Apriori Algorithm(연관 규칙 분석)을 통해 각 집합에서 연관된 규칙을 뽑아내서 어떤 규칙이 있는지 클러스터별로 확인할 수 있게 할 수 있을지 테스트</li> </ul>		

	<p>☞ 현재 프로젝트 진행사항에 대한 검증 필요성</p> <p>앞서 1 번기술(서버/클라이언트-내부/외부 분리)과 2 번기술(암호화 패킷 분리)를 통해 3 번기술(클러스터링을 통한 재 라벨링)을 진행할 때 선행되는 전 처리 기술에서 정확도가 낮으면 뒤에 적용시킬 기술의 정확도에서도 문제가 생길 수 있기 때문에 지금까지 만들어 놓은 기술에 대한 정확도 검증을 해야함</p> <p>1 번 기술: 현재 데이터를 5 월~9 월까지로 규칙을 만들어서 코드를 만들어 놓았기 때문에 4 월이나 포함되어 있는 월중 하나를 빼고 검증용 데이터를 만들어 정확도에 대한 검증 진행</p> <p>2 번 기술: 마지막 수식 설정 과정에서 검증을 통해 데이터 기반의 수식을 만들었기 때문에 다른 4 월 데이터를 통해 검증 진행</p> <p>☞ 프로젝트에 대한 전체적인 문서작성</p> <ol style="list-style-type: none"> <li>1. 수행보고서 (UseCase, 선행기술, 필요 기술 등 내용을 포함해서 수정)</li> <li>2. GIT PAGE, 개인 레포지터리 구축 작성</li> <li>3. 각자 완성한 기술에 대해 보고서화 시켜 전체 보고서에 합치기</li> <li>4. 만들어 놓은 기술 실행시킬 수 있는 코드화</li> </ol>
프로젝트 진행사항	
서기의 의견	<p>학기가 시작되고 동시에 캡스톤을 진행해 보니 둘 다 현재 20 학점 넘게 듣고 있는 수업이 생각보다 크게 다가왔다. 그래서 각 주당 꼭 해야 할 최소 목표를 정해 놓고 목표에 대해서는 꼭 완수 하겠다는 목표를 가지고 진행을 해야 할 것 같다. 그리고 무작정 개발이 아닌 각 단계의 모듈에 대한 검증도 철저히 해서 뒤에 나올 결과물에 대한 신뢰성을 높이는 것도 중요할 것 같다.</p>