수처리 계측제어망 Ad-hoc 적용시 데이터 신뢰성 확보를 위한 통신 프로토콜 제안

유철*, 서강도*, 최홍열*, 홍성택*, 지유철*

*K-water

The Communication protocol proposal at Ad-hoc for Water-Treatment

Yu-Chool*, Seo Gang do*, Choi Hong yeol*, Hong Sung taek*, Ji Yu chul*

*K-water

E-mail : jy231@kwater.or.kr, skgang@kwater.or.kr, hong@kwater.or.kr, sthong@kwater.or.kr, jiyuchul@kwater.or.kr

요 약

수처리 계측제어 시스템에서 네트워크의 재난대비나 유선망에 대한 백업개념 등으로 Ad-hoc 통신망 구축시 각 노드간의 송수신 데이터에 대한 높은 수준의 신뢰성과 보안성이 확보 되어야 한다. 이에 대해 일정 규모의 시설물이 집중된 폐쇄적 수처리 시설물의 FA망에 대한 Ad-hoc 통신망 구축시 일반적인 통신 프로토콜을 적용하기 보다는 사회기반 공공 설비인 수처리 시스템의 특성과 고정밀 산업플랜트와 같은 시간제약성을 고려하여, ZRP를 이용한 H-ARQ와 공정제어 명령 통신 프레임의 OTP를 활용한 별도의 특정 프로토콜을 적용함으로써 시설물 운영의 신뢰성과 보안성을 확보하고자 한다.

ABSTRACT

In concept, such as the backup of wired network and disaster prevention network of water treatment measurement and control system, reliability and security of high level of sending and receiving data between the nodes must be ensured in Ad-hoc network construction. Rather than apply the common communication protocols of Ad-hoc network construction during the FA network of closed water treatment facility with the facility of a certain scale is concentrated contrast, and high characteristics of the water treatment system infrastructure, public facilities We have developed a specific protocol another that applies the OTP of communication frame of process control commands and H-ARQ with ZRP by applying the flexibility to time constraints such as precision industrial plants to ensure the safety and property of facility operation.

키워드

AD-HOC, ZRP, H-ARQ, OTP

Ⅰ. 서 론

최근 들어 무선 통신 기술의 비약적인 발전으로 산업용 자동화 설비에도 유·무선 접목을 통한 무선 네트워크 기술 적용이 확대됨에 따라 산업용 통신망의 또 다른 형태로 자리잡아가고 있다. 이중 중요 사회 기반시설인 수처리 계측제어 시스템에서 ISM밴드를 활용한 Ad-hoc 자가망 무선 네트워크 구축시, 공통 통신 대역 사용 및 설비 집약적 시스템의 통신환경을 감안하여 엄격한 조건을 만족시키는 무선 자원의 보안성 제고와 데이터 신뢰성 확보를 위해 ZRP(Zone Routing Protocol)를 기반으로 하는 보안강화형태의 에러 정정방식 통신 프로토콜을 제안한다.[4][5][6]

Ⅱ. 본 론

Ⅱ-1. ZRP Routing 적용

Ad-hoc 통신은 다중 홉으로 이루어져 통신효율이 저하되는 특성이 있다. 또한 계층별(링크계층,

네트워크계층)로 나누어진 구조를 갖고 있으며, 이 중 링크계층에서 매체 접근 제어 프로토콜은 무선의 특징을 직접 반영하여야 하므로 유선망에 비해 더욱 복잡하며, 네트워크 계층은 유선망 라우팅 개념을 많이 도입하여 무선특성을 감안한 각 노드들에 대한 오버헤드와 Flooding양 조절, 대체경로 검색 등 주요 고려사항들이 있다.[2][5]

네트워크계층 라우팅 프로토콜은 크게 Table driven방식과 On-demand 방식으로 나누어진다. 하지만 Table driven방식은 Ad-hoc환경에서 다수 문제점이 있어 실제로는 많이 사용되지 않고 있으며, 대부분 Ad-hoc 프로토콜은 On-demand 방식에 근간을 두고 있다. 대표적인 On-demand 프로토콜은 AODV(Ad-hoc On Demand Distance Vectoe Routing), TORA(Temporally Ordered Routing Algorithm), DSR(Dynamic Source Routing) 등이 있으며, 이들 프로토콜은 Mobile 환경에 적합한 특성을 갖고 있다. 본 고에서는 일정 지역내에서 고정된 노드들 간의 AD-HOC 통신망을 고려할 때, Hybrid방식(Table driven + On-demand)의 라우팅 기법을 연구 대상으로 하였다. Hybrid방식 라우팅 프로토콜 중 대표적인 것은 ZRP(Zone Routing Protocol)가 있으며, ZRP는 Routing Zone 내부영역에서 Table driven방식을 사용하고 Routing Zone 외부영역에서는 On-demand방식을 사용하는 라우팅 기법이다.[1]

일반적인 ZRP는 무선통신망에서 설정된 홉 수 내에서 해당 목적지가 나타나면 설정된 홉 수내에서 목적지를 찾으며, 실패시 최종 메시지 수신 노드에서 다시 해당 목적지에 대한 Routing Table을 검색, 메시지를 송출하는 방법을 목적지에 도달할 때까지 반복적으로 수행한다.

하지만, 수처리 시설물 특성상 지역적으로 국한된 점을 감안할 때, ZRP를 수행하는 각 노드의 Routing Table에 미리 해당 주변 노드 및 중앙국에 대한 주소를 입력하여 메시지 요청 발생시 별도의 검색 없이 직접 통신할 수 있도록 구성하며, 사고발생 등의 돌발상황시 중앙의 통신감시장비(예:SCADA서버 등)는 유선에서 무선으로 즉각 중단없이 망절체가 이루어지게 한다.

Ⅱ-2. H-ARQ 에러정정 기법 적용

무선통신에서 효과적인 데이터 송수신을 위해 에러 정정 부호화를 사용하는 것은 일반적인 사항이다. 이 중 대표적인 것이 ARQ(Automatic Repeat Request)이며 ARQ는 FEC(Forward Error Correction)에 비해 구조가 단순하고 높은 신뢰도를 제공하나 채널 비트 오율 증가에 따라 정보처리율이 떨어지는 단점이 있다. 이러한 단점을 보완하기 위해 채널 부호화 방식과 재전송 방식을 결합한 방식을 H-ARQ(Hybrid ARQ)라 하며, FEC 방식으로 오류 정정을 수행한 후 다시 오류를 검출하여 데이터 에러가 있을 경우 재전송을 요구하는 방식으로 Type 1, Type 2로 구분된다. 이 중 Type 1 H-ARQ는 각 블럭에서 오류 정정 및 오류 검출을 위해 1개 또는 2개의 부호를 사용하여 부호화하고 수신기에서 오류가 검출되지 않을 경우 다음 과정으로 전달하고 오류가 검출되면 재전송을 요구한다.

Type 2 H-ARQ는 첫 번째 전송에서 재전송 요구가 발생하면 다음 전송에서 Redundancy를 증가시켜 전송하는 방식으로 수신된 비트와 보내고자 하는 비트를 결합한 새로운 블럭을 전송하며 일반적으로 현재 3세대 이동통신에서 사용되고 있다.[3][7][8]

본 고에서는 수처리 계측제어 시스템 특성을 감안하여 데이터의 신뢰성에 중점을 두어 TYPE 1 H-ARQ를 기반으로 하는 에러 정정 기법 적용을 제안 한다.

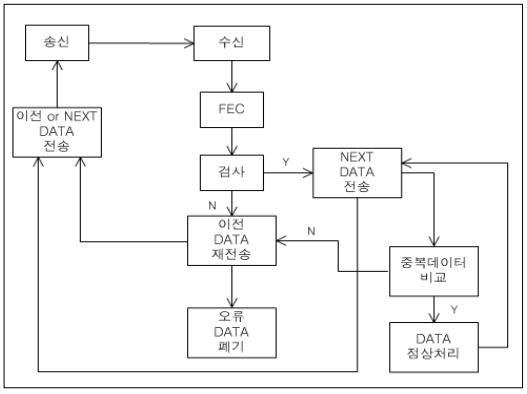

그림 1. 에러 정정 흐름도

무선통신 환경에서 Fading 발생과 ISM밴드에서 다른 무선설비와 혼신 등 송수신 데이터 에러발생에 대해 H-ARQ로 처리하도록 한다.

Ⅱ-3 OTP를 이용한 명령어 인증 방법

사회기반시설의 계측제어시스템에서 무선설비 운영은 그 특성상 높은 보안성이 요구된다. 특히, 공공시설물에서 설비에 대한 주요 공정제어 데이터가 전송되는 환경에서 무선통신 도입시 국가주체의 보안담당기관을 통해 해당 시스템에 대해 보안성 검토를 받아야 한다. 따라서, 무선통신에서의 보안성 확보는 현재 공공기관에서의 무선설비 도입시 가장 중요한 이슈이다.[10][11]

수처리시설에서 SCADA(Supervisory Control and Data Acquisition)시스템 관점의 데이터를 분류해 보면 공정감시를 위한 현장 RCS(Remote Control System)의 취득 데이터와 공정제어를 위한 SCADA서버에서 하위 계층 설비로의 명령 송신 데이터로 크게 나누어 볼 수 있다.

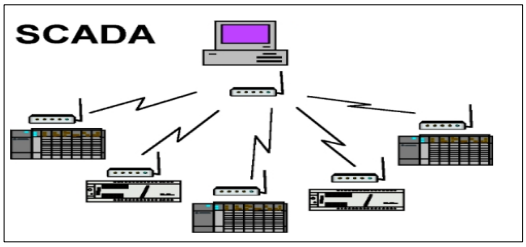

그림 2. SCADA 시스템 개략도

여기서, 보안성 관점으로 판단하면 데이터 취득보다는 명령 송신에 대해 데이터 전송과정에 신중할 필요가 있다. 자칫 외부 침입자들에 의해 Spoofing 등 해킹으로 무선 통신망을 통해 주요 밸브 및 약품투입 설비 등 수처리설비에 잘못된 가동 명령어가 전송되면 큰 사고로 이어질 수 있다. 따라서 평소 공공기관 등은 국가보안기관으로부터 각종 보안실무 감사나 지도를 받고 이에 상응한 설비를 도입하도록 되어 있다.

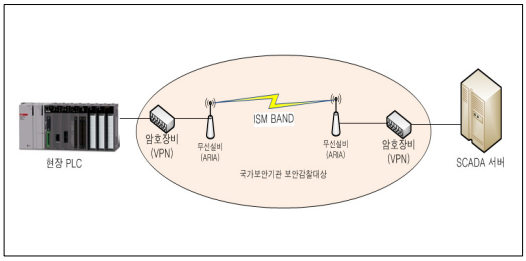

그림 3 수처리 무선시스템 도입시 보안성 검토 대상

이에 따라 일반적으로 사이버테러 등에 대비하여 국가보안기관에서 검증을 받은 VPN, 방화벽 장비 등을 이용하여 해당 통신구간에 대해 데이터 터널링 기법이나 방화벽을 설치하여 안전한 데이터 송수신이 이루어지는데 주요 국가공공기관들은 주로 국가공인 암호 알고리즘 중 하나인 ARIA(Academy, Research Institute, Agency)를 기반으로 사용중이다.

본 고에서는 위의 일반적인 보안장치와 병행하여 수처리 무선 통신시스템 환경에서 상위 시스템과 하부 설비 간 전송되는 데이터에 대해 보안성을 강화하고자 OTP(One Time Password)를 이용한 명령어 진실 판단 방안을 제안한다.

일반적으로 OTP 기법에는 S/KEY 방식, 챌린지 리스펀스 방식, 시간 동기화 방식, 이벤트 동기화 방식 등이 있다. 이 중 이벤트 동기화 방식은 시간 동기화 방식이 갖고 있는 단점을 극복한 방식으로써 인증서버와 사용자 토큰 간에 시간 정보를 일치시킬 필요가 없으면서도 잘 알려진 암호 알고리즘을 사용하기 때문에 안전성이 높은 방식이다. 이벤트 동기화 방식은 시간 정보 대신 인증서버와 인증 횟수(Counter) 기록을 공유하고 인증 횟수를 일회용 패스워드 생성시 입력 값으로 활용한다.

수처리 무선 시스템에서 상위 시스템이 하위 시스템으로 명령 전송시 해당 명령어에 대한 검증을 위해 이벤트 동기화 방식의 OPT를 이용하여 명령어 실제 여부를 판단하도록 한다.

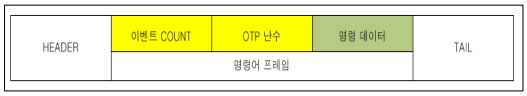

그림 4. OTP를 이용한 명령 데이터 프레임 구조

상위시스템에서 이벤트 동기화 OTP를 이용하여 명령어를 하위 설비에 송신한다고 하면, 우선 상하위설비 각각의 OTP를 카운터 '0' 으로 세팅한다. 상위시스템에서 일회용 비밀번호를 생성하기 위해 OTP 카운터 값을 '1' 로 증가시키고, 이 값을 OTP의 정해진 비밀키를 이용해서 암호화한다. 암호화 된 결과 값을 명령어 프레임에 이벤트 카운트 숫자와 함께 프레임을 생성하여 하위 설비에 송신한다.

이벤트 카운트와 일회용 패스워드를 전달받은 하위 설비에서는 명령 데이터 프레임에서 카운터 값을 알아내고 자기 OTP의 카운터 값을 '1' 로 증가 시킨 후, 상위 시스템과 약속된 비밀키를 활용해 일회용 패스워드를 생성하여 상위 시스템으로부터 받은 카운터 값과 비교하여 인증 성공/실패 여부를 판단한다. 그 후 매 상호 명령 수신시마다 OTP 카운터 값이 1씩 증가되어 저장되기 때문에 카운터 값이 매번 일치하여 성공적인 인증이 수행될 수 있다.

또한, OTP 생성알고리즘은 HMAC-SHA1, HMAC-SHA256, 3DES, AES, SEED, HIGHT 등이 있으며, 이 중 국가공인 암호알고리즘인 SEED 128Bit를 적용하여 생성 메커니즘을 제작하도록 한다.[9]

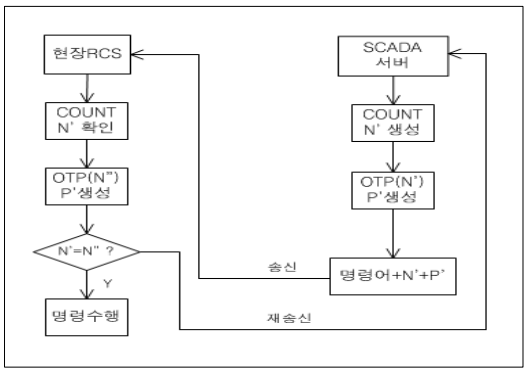

그림 5. 이벤트 동기화OTP를 이용한 명령어 처리 흐름도

시간 동기화 OTP 방식이 상위시스템의 인증 서버와 하위 설비의 OTP 토큰 사이에 시간을 일치시켜야 하는 것처럼, 이벤트 동기화 방식에서는 카운터 값을 상위 시스템과 하위 설비 OTP

토큰 사이에 일치시켜야 정상적으로 인증이 수행된다. 이벤트 동기화 방식에서 생길 수 있는 문제점은 사용자 오류나 무선 통신 에러 또는 기타 이유에 의해 일회용 패스워드가 생성되어 상위 시스템의 카운터 값과 하위 설비의 OTP 토큰의 카운터 값이 맞지 않는 경우에 발생할 수 있다.

표 1. 칩기반 OTP 알고리즘 분류 (출처:TTA)

사용용도	권고 알고리즘	암호키 길이 (비트)	보안강도 (비트)
중요정보 저장	SEED	128	128
	HIGHT	128	128
정보 전송	SEED	128	128
	HIGHT	128	128
생성 알고리즘	HMAC-SHA1	162	162
	HMAC-SHA256	256	256
	3DES	168	112
	AES	128/256	128/256
	SEED	128	128
	HIGHT	128	128

이 경우 일반적인 이벤트 동기화 방식에서 사용하는 카운터 값의 오차 범위(카운터~카운터 +16 범위를 일반적인 오차 범위로 허용함)를 정해 범위 내에 들어올 경우 사용자 인증을 허용하는 방법과 오차 범위를 벗어날 경우 연속된 2회의 일회용 비밀번호가 올바른 값으로 판단될 경우 사용자 인증을 허용하는 방식으로 문제점을 극복하면 된다.[9]

Ⅲ. 결 론

무선 기반의 수처리 시스템을 실제 적용하기 위해서는 무선 환경의 영향 및 설비 환경등의 외적인 요소를 먼저 고려하여야 한다. 일반적으로 유선망보다 무선망에서 외부유입에 의한 잡음과 각종 다발성 페이딩등의 혼신 현상 발생이 다양할 것이고, 유선에서보다 무선에서 데이터 에러와 소손이 상대적으로 많이 발생할 것이다. 하지만, 무선망에서의 전송 에러는 일시적인 반면 유선 채널에서의 전송 에러는 원인규명이 어렵고 발생근원을 파악하기 힘든 면(케이블 절단, 설비 부분 훼손, 고장등)등의 치명적인 경우가 대부분이다. 이를 극복하기 위해 유선망이 구축하기 힘든 환경에서 ISM밴드을 이용한 자가망 형식의 Ad-hoc망 구축이 효과적인 대안이 될 수 있으며, 이를 적용시 사회기반시설에 대한 보안과 데이터 신뢰성을 유선망 수준으로 끌어올릴 수 있는 새로운 프로토콜이나 응용계층 등 프로세싱의 재변형이 필요하다고 사료된다.

또한, 백업망으로써 기존 유선망과 연동시 신뢰성을 증가시킬 수 있는 데이터 검증 이중화 및 정확도가 높은 경로 라우팅과 통신 오류, 의도적인 침입자에 의한 통신 프레임 변조 등에 대해 효과적인 보안성 강화를 통한 주요 설비의 오동작이나 사고를 방지할 수 있도록 향후 무선 통신망의 무결점, 무순단 운영성과 무선망에서도 유선망과 동일한 데이터 신뢰성 및 보안성 향상 기법 등이 중요한 연구 대상이 될 것이다.

참고문헌

[1] 윤동심, 강희조, 재난 구조를 위한 MANET에서의 ZRP라우팅 제안. 한국정보기술학회 2010하계 p132-134
[2] 김종천, 김영용, Telecommunications Review 제12권3호 Ad Hoc 통신망 프로토콜 개발동향 p298-311 2002.5
[3] 김학관,장주욱, 애드혹 네트워크에서의 성능 향상을 위한 분할 전송 기법 2009.02
[4] 이원희, 유명식, 전자공학회지 제39권 제11호, 산업용 실시간 제어시스템을 위한 무선통신 기술 및 시스템 제어기 연구동향 p36-46 2012.11
[5] 권혜연 외5, 전자통신동향분석 제18권 2호 이동 Ad Hoc 네트워크 기술 동향 p 11-24 2003.04
[6] 김동성, 월간 전자부품, 산업용 통신망을 위한 무선 통신 기술의 현황 및 분석 2006.04
[7] 박은찬, KOSEN Expert Review, 무선 ad-hoc 통신망을 위한 혼잡 제어 Communications magazine, vol 43, no. 3, pp. 27-32,. Mar. 2005. 5
[8] 신재욱 외2, 전자통신동향분석 제18권 6호, 이동 Ad Hoc 네트워크에서의 Flooding 기술 2003.12
[9] 한국정보통신기술협회, 일회용패스워드 알고리즘 프로파일 기술보고서 2012
[10]국가사이버안전센터, http://service2.nis.go.kr/
[11] 금융보안연구원 2010년 OTP 보안과 최신 인증기술 전망 세미나 개최결과 및 발표자료 2010.06