情報保護學會論文誌
第13券 第5號, 2003. 10

CPN을 이용한 무선원격제어시스템의 안전성 검증

이 문 구*

Security Verification of Wireless Remote Control System Using CPN

Moon-ku Lee*

요 약

기존 웹 기반인 시스템 관리 소프트웨어 솔루션들은 시간적, 공간적 제약을 갖는다. 그리고 오류 메시지에 대한 불확실한 통보와 실시간 지원요구 및 긴급조치가 어렵다는 문제점들을 갖는다. 이러한 문제들을 해결하기 위해서 모바일 통신기기를 이용하여 원격시스템을 관리 및 모니터링하고 즉각적으로 원격지의 시스템을 제어할 수 있는 무선 원격제어 시스템을 설계 및 구현하였다. 구현된 무선 원격제어 시스템은 이러한 문제의 해결뿐만 아니라 보안의 문제도 갖고 있다. 그러므로 본 논문에서는, 무선 원격제어 시스템을 위한 보안 문제에 초점을 맞추어 진행하였으며, 설계한 보안기능은 사용자에 대한 모바일장비 사용자 인증과 대상 시스템 접근제어 기능을 갖도록 하였다. 이러한 보안 기능에 대한 안전성 검증을 위하여 각 단계에 대한 모든 가능한 상태를 표현할 수 있는 CPN(Coloured Petri Nets)을 도입하였다. 그리고 본 논문에서는 CPN 기반의 상태 불변식으로 안전성을 검증하였다. 제안한 보안 기능의 CPN 표현과 분석방법은 차후에 다른 서비스 모델의 설계와 검증에 유용한 방법이 될 수 있다.

ABSTRACT

Existing web-based system management software solutions show some limitations in time and space. Moreover, they possess such as shortcomings unreliable error message announcements and difficulties with real-time assistance supports and emergency measures. In order to solve these deficiencies, Wireless Remote Control System was designed and implemented. Wireless Remote Control System is able to manage and monitor remote systems by using mobile communication devices for instantaneous control. The implementation of Wireless Remote Control System leads to these security problems as well as solutions to aforementioned issues with existing web-based system management software solutions. Therefore, this paper has focused on the security matters related to Wireless Remote Control System. The designed security functions include mobile device user authentication and target system access control. For security verification of these security functions introduced CPN(Coloured Petri Nets) which is capable of expressing every possible state for each stage. And then in this paper was verified its security through PI(Place Invariant) based on CPN(Coloured Petri Nets). The CPN expression and analysis method of the proposed security function can also be a useful method for analyzing other services in the future.

keyword :

Ⅰ. 서 론

기존의 유선 시스템관리 소프트웨어 솔루션들은 시간적, 공간적인 제약을 갖는다. 이러한 문제들을 해결하고자 모바일 단말기(휴대폰, PDA, Smart Phone, Webpad)로 원격의 시스템을 모니터링 하고, 실시간

* 김포대학 컴퓨터계열 조교수(yeon0330@kimpo.ac.kr)

으로 무선 원격제어를 할 수 있는 시스템을 제안하였다. 제안한 무선원격제어시스템은 원격의 모바일 장비 사용자에 대한 인증과정과 대상서버에 대한 접근제어 등의 보안기능이 필요하다.

그렇기 때문에 본 논문에서는 이러한 보안 기능을 갖는 무선 원격제어 시스템을 설계하고 CPN(Coloured Petri Nets)의 상태 불변식(place invariant)을 이용하여 그에 대한 안전성을 검증하는 것을 주 목적으로 한다.

제안한 무선원격제어 시스템은 무선장비로 원격의 대상 시스템을 제어하고자 할 때, 단일 명령의 실행으로 끝나는 것이 아니라 계속적으로 대상 시스템을 모니터링은 물론 특정한 이벤트에 대한 제어를 하여야만 한다. 그러므로 제공되는 보안 시스템은 지속적으로 인증된 사용자만이 시스템에 접근제어 할 수 있도록 안전한 보안이 이루어져야만 한다. 그러나 제안하는 보안기능은 무선 시스템에 적용됨에 따라 기존의 유선상의 보안 시스템과는 달리 시스템의 실행시간을 기준으로 세션 키를 설정하여 가급적 무선장비의 한정된 용량이 부담이 되지 않는 범위 내에서 보안 프로토콜을 실행하고 이에 대한 보안기능을 설정하였다. 때문에 보안등급에 따라 실행되는 제어 명령의 데이터는 어떤 상황에서도 손실되지 않아야 하고, 실행과정이 계속 반복 순환하거나, 교착 상태가 발생하거나, 또는 데이터 충돌이 발생되는지 등에 관한 안전성을 검증하여야만 한다. 그리고 이러한 안전성은 설계한 모델이 완벽하게 시스템으로 구현되기 위해서 가장 중요한 요인이다.

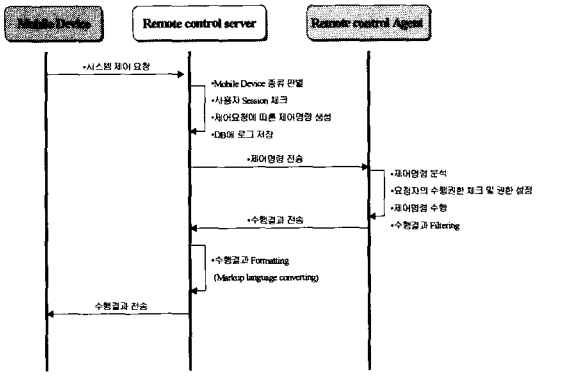
제안한 시스템의 안전성 검증을 위하여 CPN의 상태 불변식(Place Invariant)을 이용하였다. 상태 불변식은 제안한 시스템의 보안 기능이 상태불변식의 성질인 안전성, 유계성, 보존성 등을 만족하고, 발생 가능한 상태(place)와 전이의 토큰 개수가 유한적으로 정의됨으로써 설계한 보안기능에서 오버플로우(overflow)나 데드락(deadlock) 그리고 무한 루프(loop)가 발생하지 않음을 검증할 수 있다. 이러한 상태 불변식은 제안한 보안 기능의 발생 가능한 모든 경우를 CPN의 그래픽으로 표현하고 이를 기반으로 상태 불변식에 의해 안전성을 검증하게 된다. 즉, 상태 불변식 검증 방법은 모델에서 표현되는 모든 상태를 방정식으로 표현하여 입력이 요청된 토큰과 출력되는 토큰이 항상 같도록 유지되어 상태가 불변한다는 정리를 수학적으로 증명함으로써 모델의 안전성을 검증하게 된다.[8]

본 논문의 구성은 다음과 같다. 2장에서는 제안하는 무선 원격제어 시스템의 보안기능을 기술하고, 3장에서는 CPN의 도입목적을 기술하였다. 그리고 4장에서는 무선원격제어 시스템의 보안기능을 CPN의 아크와 노드의 형태로 표현하였으며, 5장에서는 본 연구에서 설계 및 구현된 무선원격제어 시스템의 보안기능에 대한 안전성을 검증하였다. 마지막으로 6장에서는 결론과 차후 연구방향 등을 기술하였다.

Ⅱ. 무선 원격제어 시스템의 동작과 보안 기능

2.1 무선 원격제어 시스템의 동작

모바일 장비의 특성상 기존의 세션 관리 기법으로는 세션 관리가 힘들다. 따라서 사용자 세션 관리 부분이 별도로 구축되어야 하며, 세션 ID에 해당하는 키 값은 사용자가 제어서버에 접속한 최종시간을 기준으로 하며, 이 값은 모바일 장비와 제어서버 간에 통신 시 파라미터로 전송되어 모바일 세션을 관리하도록 한다.[6] 모바일 장비와 원격지 제어 서버 그리고 에이전트가 상호 동작하는 과정은 [그림 1]과 같다. 원격지 제어서버의 웹 서버는 JSP 엔진기능이 제공되며, 모바일 장비의 종류를 판별하고, 모바일 장비로부터 시스템 제어요청(request)을 받아서 원격지 제어서버의 엔진으로 처리를 넘기고, 그 결과를 응답(response) 하는 부분을 담당한다.[1,2] 이때, 모바일 장비의 종류를 판별하고, 사용자의 세션을 체크한 후 제어 요청에 따른 제어 명령을 생성하면서 데이터베이스 연결모듈을 통하여 각종 데이터베이스 정보를 질의 및 업 데이트 모듈로 처리한다.[10] 또한 제어요청에 따른 처리내용은 데이터베이스에 로그 파일로

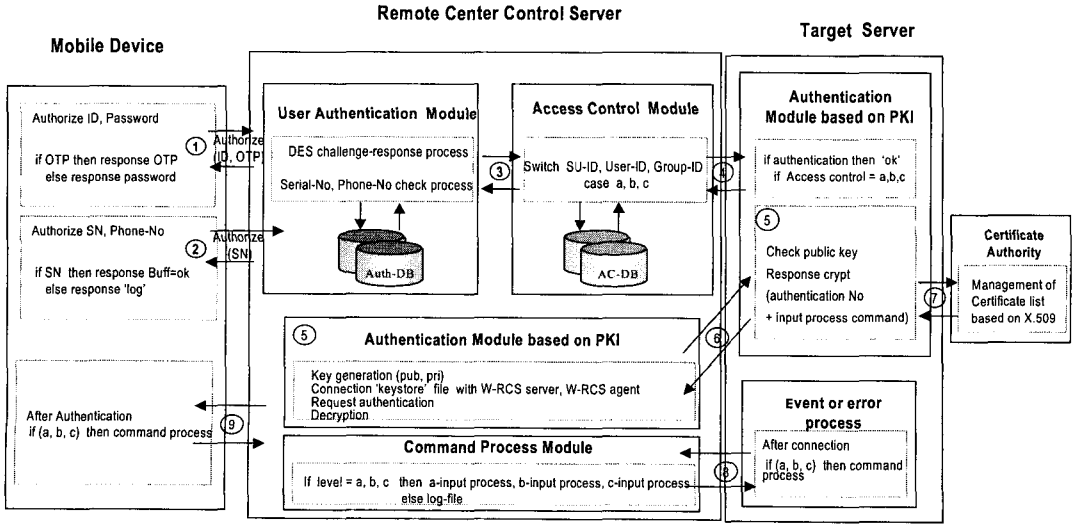


〔그림 1〕 무선원격제어 시스템의 동작

저장되고, 제어 명령은 에이전트로 전송된다. 원격지 제어서버의 에이전트 엔진은 제어명령을 분석하고 요청자의 수행권한 체크 및 권한 설정을 하기위하여 정보를 파싱(parsing)하여 정보 추출 및 객체에 저장하는 페이지 퍼메팅(Page formatting), 원격지 에이전트의 상태 체크, 이벤트 발생시 전자메일과 유선관리 시스템 전송, 사용자 세션 관리, 기타 데이터의 분석 및 가공을 위한 대부분의 로직 그리고 응용 프로토콜 인터페이스 모듈 등으로 처리과정이 이루어진다.[9] 원격지 에이전트모듈에서 각 에이전트들은 원격지 서버의 노드(host)들에 설치되며, 이는 원격지 콘솔과의 통신, 모니터링 데이터의 추출 그리고 제어명령을 분석한다. 그리고 요청자의 수행권한 체크 및 권한 설정, 제어명령 수행 그리고 수행결과를 필터링(filtering)하여 원격지 서버에 전송하도록 명령어 라인 인터페이스(Command Line Interface)를 제공한다. 원격지 제어 서버에서는 에이전트로부터 전송되어온 수행 결과를 마크업(markup language) 언어(HTML, XML 등)로 변환하는 사용자 인터페이스 과정을 갖은 후 수행결과를 모바일 장비에 전송한다. 모바일 장비에서는 사용자 인증을 위한 기본 보안기능 만 설정될 뿐 어떠한 모듈도 설치되지 않으며, 기본적으로 설치되어 있는 브라우저만 있으면 사용가능하도록 하였다. 응용 프로토콜 인터페이스에서 제공하는 기능은 대상 시스템의 유선 콘솔에서 제공하는 대부분의 모니터링 기능과 원격 제어기능을 제공할 수 있다.

2.2 무선원격제어 시스템의 보안기능

본 논문에서 제안한 모바일 장비를 이용한 무선 원격제어 시스템은 모바일 장비 사용자와 원격제어 서버사이의 인증과정과 원격제어서버와 대상 서버간의 지속적인 명령어 사용 권한부여를 위한 접근제어 보안 기능이 이루어지도록 하였으며, 사용자와 대상 서버간의 인증은 공개 키 기반구조(PKI)의 X.509에 기초하도록 하였다. [그림 2]는 무선원격제어시스템의 보안기능을 도식화 한 것이다. 먼저, 무선원격제어 시스템의 보안 기능은 모바일 장비 사용자가 원격 제어서버에 접근하고자 할 때, ① 사용자의 ID를 입력하면 서버에서 일회용 패스워드 생성을 위한 챌린지 값을 전송하게 되고 일차적인 인증과정이 끝나면, ② 이차적인 인증과정으로 사용자가 소유하고 있는 모바일 장비의 일련번호(Serial Number)를 확인하는 과정으로 모바일 장비 사용자의 인증처리과정이 진행된다. 이렇게 원격제어서버에서 인증된 모바일 사용자라고 하더라도 제어하고자 하는 대상서버에 접근하여 명령어를 실행하고 시스템을 제어하려면 접근제어기능에 의하여 해당 사용자의 권한이 부여되어야 한다. ③ 접근제어에 의한 권한부여는 Super-user, Group-user, User 의 ID에 따라 접근권한을 받기위하여 데이터베이스로부터 자료를 확인한다. ④ 접근제어의 등급에 따라 권한이 부여된다. ⑤, ⑥ 이렇게 권한 부여를 할당 받은 사용자 혹은 그룹은 무선원격제어 서버와 에이전트의 요청에 따라 원격에



〔그림 2〕 무선원격제어 시스템의 보안기능

서 시스템의 명령어 사용권한을 갖기 위하여 등록된 사용자들은 암호화된 키 값을 키 스토어에서 생성한다. ⑦ 이렇게 생성된 암호화 키 값은 X.509 기반의 공개키 기반 구조(PKI)의 공인된 인증과정을 실행하는데 사용된다. ⑧ 사용자가 원격 시스템에 접속한 이후에러 혹은 이벤트에 대하여 시스템을 제어할 때도 역시 권한 등급에 의해서만 시스템을 제어할 수 있다. ⑨ 이렇게 연결이 설정된 이후에 지속되는 시스템 제어과정도 역시 주어진 권한 등급 내에서만 처리가 가능하다.

Ⅲ. CPN의 도입

본 장에서는 무선원격제어시스템의 보안기능에 대한 안전성을 검증하기 위하여 CPN을 도입하게된 목적과 CPN의 속성에 대하여 기술한다.

3.1 CPN 도입의 목적

설계한 무선원격제어시스템의 안전성을 검증하기 위하여 CPN(Coloured Petri Net)을 도입하게 된 주요 목적은 다음과 같다.[3]

- 시스템의 각 기능에 대한 흐름이 CPN의 아크와 노드 등으로 구성된 그래픽으로 표현이 가능하다.
- 시스템의 각 진행단계를 논리형식에 맞는 구문의 표현으로 정의가 가능하다.
- CPN의 성질(안전성, 위계성, 보존성)을 이용하여 시스템을 구현하기 이전에 안전성을 검증할 수 있다.

CPN은 시스템의 각 기능에 대하여 동적 특성을 검증하기 위해서 사용된다. 이중에서도 특히 데드락 발생 여부, 토큰간의 충돌 발생 여부 등 안전성(safety)을 검증할 수 있고 형평성 등도 검증할 수 있다. 또한 CPN은 그 특성 때문에 상태 수 급증 문제(state explosion problem)를 유발하지 않으면서 도달성 분석(reachability analysis)을 수행할 수 있기 때문에 여러 가지 분석 방법을 적용할 수 있는데, 본 논문에서는 정형적인 방법으로 상태 불변식(Place Invariant)을 이용하여 제안하는 모델의 안전성을 검증하고자 한다.

통합 인터페이스(Integrated Interface) 모듈은 역시 다른 유선상의 시스템 관리자들과의 연동과 사용자 요청에 대한 인터페이스 모듈을 제공한다.[10]

3.2 CPN의 구성

CPN은 다음의 요구사항을 만족하는 튜플(tuple)로 구성된다.

[정의 3.1]

CPN = $(\sum, P, T, A, N, C, G, E, I)$

$\sum$: 0이 아닌 타입의 유한 집합 형태의 컬러집합.

$P=\{P_1, P_2, \ldots, P_m\}$: 상태(Place)의 유한 집합으로 어떤 사건이 발생하기 전이나 발생한 후의 상태.

$T=\{1, t_2, \ldots, t_n\}$: 전이(Transition)의 유한집합으로 어떤 상태로 도달하기 위한 사건.

A : $A \subseteq (P\times T)\bigcup(T\times P)$를 나타내며, 흐름관계의 유한 집합으로, 전이(transition)의 흐름.

N : N은 노드(Node)의 함수 $N(a)$. 만약 근원지(source)에서 목적지(destination)로 간다면, N=(source, dest)를 표현 함.

G : 가드(Guard)의 함수

$\forall_t \in T$: $[Type(G(t))=B \wedge Type(Var(G(t))) \subseteq \sum]$

B는 바인딩요소(binding element) b의 유한 집합.

E : 간선 식 함수.

C : 컬러(Color)의 함수.

$\forall_a \in A$:

$[Type(E(a))= C(p(a))_{MS} \wedge Type(Var(E(a))) \subseteq \sum]$,

$p(a)$는 $N(a)$의 상태(place)이다.

I : 초기화 함수로서, 다음의 닫힌 식 P 로부터 정의. $\forall_p \in P$: $[Type(I(p))= C(p)_{MS}]$

가드 함수 G는 변환 t와 대수형의 식 즉, 술어를 사상한다. $G(t)$의 모든 변수는 $\sum$에 속하는 데이터 타입을 가져야만 한다. 모든 노드의 집합을 표시하기 위해서 $X=P\bigcup T$를 사용한다. 그리고 CPN 구조의 이웃 요소들 사이의 관계를 기술하는 많은 함수를 정의한다. 각 함수의 이름은 함수의 범위를 나타내며, P는 상태에 사상되고, A는 간선의 집합에 사상된다. 컬러집합은 CPN모델에서 사용되는 유형, 연산 함수들을 결정한다. 각 컬러집합은 적어도 한 개의 요소를 갖고 있다고 가정한다. 상태(P), 전이(T)와 간선(A)은 집합 P, T, A의 조합으로 정의된다. 상태, 전이, 그리고 간선을 갖는 집합은 유한해야 한다. 노드 함수는 첫 번 요소가 출발 노드이고, 두 번째가 목표 노드인 쌍을 각 간선으로 사상한다.

[정리 3.1]
가중치 함수(weight function) W 가 상태(place)의 흐름을 나타내기 위한 필요충분조건은 W 가 상태(place)의 불변식(invariant)을 결정하는 (i)과 (ii)를 만족하여야만 한다.

(i) 다음의 조건을 만족하는 필요충분조건인 경우 W 는 상태의 흐름(flow)이라고 말한다.

$$\forall (t, b) \in BE :$$
$$\sum_{p \in P} W_p(E(p, t)\langle b\rangle) = \sum_{p \in P} W_p(E(t, p)\langle b\rangle). \text{----(1)}$$

W_p는 모든 $p \in P$ 에 대한 가중치의 집합이다.
BE 는 모든 바인딩 엘리먼트(binding element)들의 집합이고, 바인딩 엘리먼트는 (t, b)의 쌍으로 이루어지며, $t \in T$ 그리고 $b \in B(t)$이다.

(ii) 다음의 조건을 만족하는 필요충분조건인 경우 W 는 상태 불변식(place invariant)을 결정한다고 말한다:

$$\forall M \in [M_0\rangle : \sum_{p \in P} W_p(M(p)) = \sum_{p \in P} W_p(M_0(p)). \text{(2)}$$

W가 상태(place)의 흐름(flow)이라고 가정할 때, $M_1[Y\rangle M_2$가 $W(M_1) = W(M_2)$임을 증명한다면 제안하는 모델의 안전성을 검증하게 된다.

[증명]
Y 는 초기 마킹 M_1에서 진행되는 단계를 표현한다. 그리고 Y 단계는 $\forall p \in P$:
$\sum_{(t, b) \in Y} E(p, t)\langle b\rangle \le M(p)$ 의 필요충분조건을 만족하는 마킹 M 에서 진행가능 하다. 마킹 M_1에서 진행가능한 Y단계가 발생하면 마킹 M_1은 다른 마킹 M_2로 변경되며, 다음과 같이 표현 된다:

$$\forall p \in P:\ M_2(p)$$
$$= (M_1(p) - \sum_{(t, b) \in Y} E(p, t)\langle b\rangle) + \sum_{(t, b) \in Y} E(t, p)\langle b\rangle. \quad ①$$

첫 번째 합은 제거된 토큰들을 나타내고, 두 번째 합은 추가된 토큰들을 나타낸다. Y단계의 발생에 의해서 M_2는 M_1에서 직접 도달가능하며, $M_1[Y\rangle M_2$ 같이 표현된다.

식①에 의해서 [정리 3.1]의 식(1)을 적용하면 식②와 같다.

$$\sum_{p \in P} W_p(M_2(p) + \sum_{(t, b) \in Y} E(p, t)\langle b\rangle)$$
$$= \sum_{p \in P} W_p(M_1(p) + \sum_{(t, b) \in Y} E(t, p)\langle b\rangle). \quad ②$$

가중치 함수(weight function)의 선형성(linearity)으로부터 식③을 얻을 수 있다:

$$\sum_{p \in P} W_p(M_2(p)) + \sum_{p \in P} \sum_{(t, b) \in Y} W_p(E(p, t)\langle b\rangle)$$
$$= \sum_{p \in P} W_p(M_1(p)) + \sum_{p \in P} \sum_{(t, b) \in Y} W_p(E(t, p)\langle b\rangle). \quad ③$$

흐름 성질(flow property)로부터 식④를 얻을 수 있다:

$$\forall (t, b) \in BE: \sum_{p \in P} W_p(E(p, t)\langle b\rangle)$$
$$= \sum_{p \in P} W_p(E(t, p)\langle b\rangle). \quad ④$$

식④는 식⑤와 같이 적용 된다:

$$\sum_{(t, b) \in Y} \sum_{p \in P} W_p(E(p, t)\langle b\rangle)$$
$$= \sum_{(t, b) \in Y} \sum_{p \in P} W_p(E(t, p)\langle b\rangle). \quad ⑤$$

식⑤는 식⑥과 같이 다시 작성할 수 있다:

$$\sum_{p \in P} \sum_{(t, b) \in Y} W_p(E(p, t)\langle b\rangle)$$
$$= \sum_{p \in P} \sum_{(t, b) \in Y} W_p(E(t, p)\langle b\rangle). \quad ⑥$$

위의 식에서 두 개의 $\sum$는 위의 식과 동일하기 때문에 식 ⑦과 같은 결론을 얻을 수 있다:

$$\sum_{p \in P} W_p(M_2(p)) = \sum_{p \in P} W_p(M_1(p))$$
즉, $W(M_2) = W(M_1)$이다. ⑦

다음에 $M \in [M_0\rangle$을 도달 가능한 마킹(marking)이라고 하고, σ 를 M_0에서 시작해서 M으로 끝나는 발생순서라고 하자. 위의 결과를 σ의 $M_i[Y_i\rangle[M_{i+1}$의 각 단계에 적용하면 $W(M) = W(M_0)$이라는 결론을 얻을 수 있다. 그러므로 [정리 3.1]의 (i)이 증명된다.

이번에는 [정리 3.1]의 (ii)를 증명하기 위해서 W의 상태 불변식을 결정하고 CPN이 동작하지 않는 바인딩 구성요소는 가지고 있지 않다고 가정하자. 이것은 각 바인딩 구성요소 (t, b)가 적어도 도달 가능한 하나의 M_1을 가지고 있다는 것을 의미한다. M_2를 $M_1[t, b\rangle M_2$에 의해 결정되는 마킹이라고 하자. 앞과 유사한 순서에 의해 $W(M_2) = W(M_1)$이 식⑧과 같이 적용됨을 알 수 있다:

$$\sum_{p\in P} W_p(E(p, t)\langle b\rangle) = \sum_{p\in P} W_p(E(t, p)\langle b\rangle). \quad ⑧$$

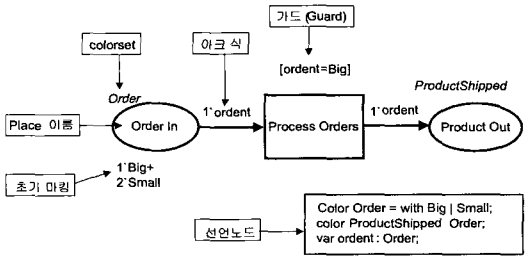
그러므로 [정리 3.1]의 (ii)가 증명됨을 알 수 있다.

Ⅳ. CPN을 이용한 안전성 검증

본 장에서는 무선원격제어 시스템에서 제안하는 각 보안기능들을 CPN으로 표현하였다.

4.1 무선원격제어 시스템 보안기능의 CPN 표현

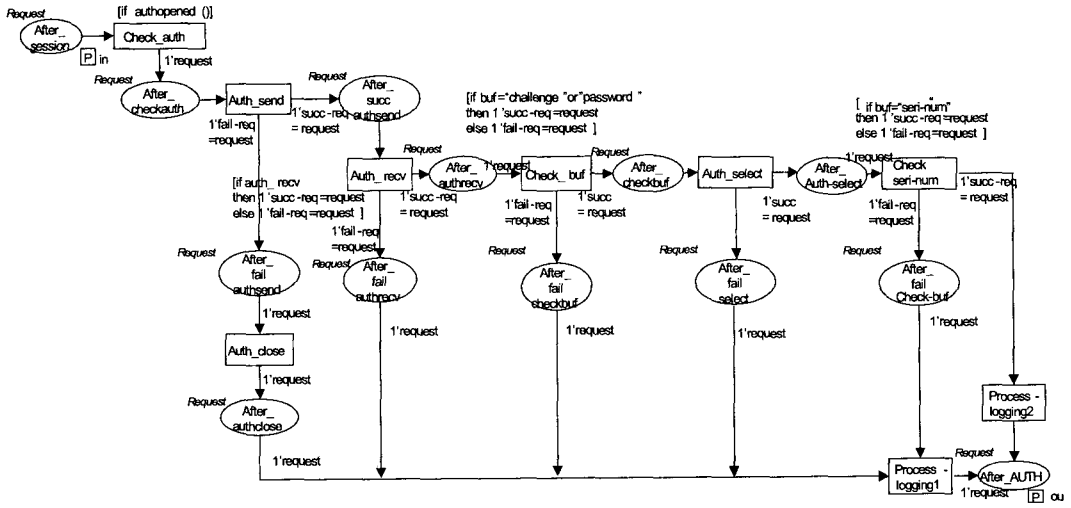
CPN의 표현방법은 [그림 3]과 같으며, 칼라셋(color set)은 토큰의 타입을 나타낸다. 아크식은 아크의 표현값을 나타내고, 가드(Guard)식은 전이의 조건을 나타낸다. 초기 마킹은 플레이스에서 표현되어, 초기의 토큰값을 나타내며, 선언노드는 현재 페이지에서 사용하는 칼라와 변수를 선언한다.[4~7]



〔그림 3〕 CPN의 표현방법

4.2 사용자 인증 기능의 CPN 표현

모바일 장비 사용자가 원격제어서버에 접근하려면 원격제어서버로부터 사용자 인증과정을 갖게 된다. 인증을 위한 매개변수(argument)로 사용자의 ID를 입력하게 된다. 만약 인증이 이미 실행되었다면 "Authentication = 1"로 설정이 되어서 인증과정을 종료하고 다음단계의 보안과정이 진행된다. 인증과정이 실행되지 않은 사용자는 일회용패스워드(one time password)방식으로 패스워드를 전송하여 패스워드 스니핑(sniffing)과 같은 도청으로부터 보호된다. 일차적인 인증과정이 진행되고 나서, 사용자가 소유하고 있는 모바일 장비의 일련번호가 서버에 등록된 일련번호와 일치하는지를 검증받게 된다. 이러한 과정이 실행됨으로 해서 도난으로 인한 사용자의 오류를 사전에 막을 수 있다. 사용자의 인증기능 처리과정을 CPN의 그래픽 표현으로 도식화 하면 [그림 4]와 같다. 초기 마킹 플레이스는 "Check_auth"가 실행되며, 이때 가



〔그림 4〕 사용자인증기능

드 식(즉, 전이의 조건)에서는 인증과정이 이루어졌었는지를 체크한다. 인증과정이 이루어지지 않았었다면, 다음 플레이스에서는 "Auth_send"로서 이증과정이 실행된다. 이때 인증이 성공적으로 실행되면 오더(Order In)는 "After_succ_authentication"상태가 되고, 인증과정이 실패하면 "After_succ_authentication"단계로 전이되며, 다음 플레이스가 실행되도록 표현된다.[3~7]

4.3 접근제어기능의 CPN 표현

사용자 인증과정으로 모바일 장비 사용자가 원격지 제어서버로부터 인증되었다면, 다음 단계는 명령어를 입력하여 대상 시스템을 제어하는 것이다. 제어서버로부터 인증된 사용자라도 대상 시스템에 접근하여 제어하려면 명령어 입력을 위한 권한을 부여받아야 한다. 이는 사용자의 등급에 따라 명령어 입력 권한에 제한을 두어 인가되지 않은 사용자가 원격에서 대상 서버를 제어할 수 없도록 하고, 사용자의 등급에 따라 시스템을 제어 하도록 하여 사용자의 오용 또는 남용에 의하여 시스템이 제어되지 않도록 하기 위함이다. 때문에 인증된 사용자의 권한부여를 위하여 접근제어 데이터베이스를 체크한다. 이때 원격지 서버 데이터베이스에 설정되어 있는 보안 등급을 확인하고자 사용자의 ID에 따라 사용자를 SuperUser-ID, Group-ID, User-ID로 분류하고, 모바일 장비의 일련번호 혹은 폰 넘버를 체크한다. 또한, 정상적으로 접근제어가 허용된 사용자라도 루트(root)권한이 있는지를 확인한 후 명령어 사용 권한을 부여받게 된다. 만약 보안등급이 설정되지 않은 사용자가 권한부여를 할당받고자 접속하였다면, 접근이 허용하지 않고 로그파일만 남기고 접근권한 제어과정이 종료하게 된다. 접근제어(AC : Access Control)는 주체 및 객체의 보안 등급에 근거하여 주체의 객체에 대한 접근을 제어하는 방법으로, 주체 및 객체의 보안 등급에 따라 접근제어를 하므로, 세밀한 접근제어가 가능하여 보안에 대한 높은 신뢰성을 제공한다. 설계된 접근제어 기능의 안전성을 검증하기 위한 CPN 표현은 [그림 5]와 같다.

V. 무선원격제어 시스템의 안전성 검증

본 장에서는 무선 원격제어 시스템의 안전성 여부를 CPN(Coloured Petri Nets)의 상태 불변식(Place Invariant)을 이용하여 검증하고자한다.

5.1 접근제어 기능의 안전성 검증

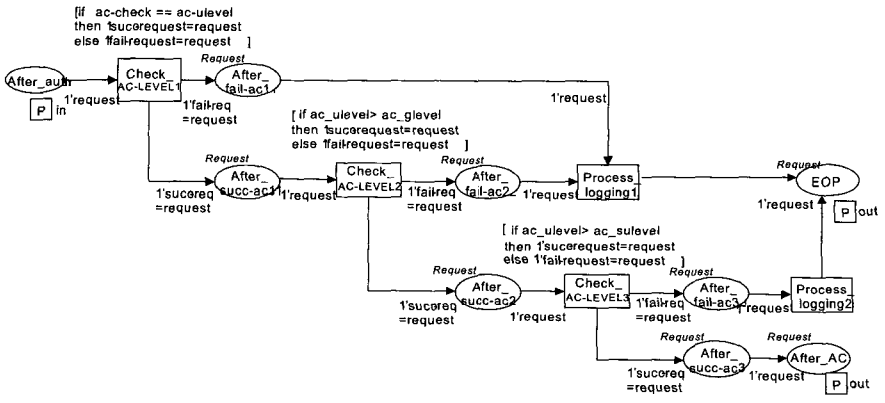
본 장에서는 무선원격제어시스템의 보안기능 중에서 접근제어 기능에 대하여 상태 불변식으로 그 안전성을 검증하고자 한다.

안전성을 검증하기 위해서 접근제어 기능의 처리과정은 다음과 같이 4가지 도달 가능한 상태로 표현할 수 있다.

① $M_{After-Auth}$
$[\ Y_{Chek-AC-LEVEL1}\ Y_{Process-logging}\rangle\ M_{EOP}$

② $M_{After-Auth}[\ Y_{Chek-AC-LEVEL1}$
$Y_{Chek-AC-LEVEL2}\ Y_{Process-logging1}\rangle\ M_{EOP}$

③ $M_{After-Auth}$
$[\ Y_{Chek-AC-LEVEL1}\ Y_{Chek-AC-LEVEL2}$
$Y_{Chek-AC-LEVEL3}\ Y_{Process-logging2}\rangle\ M_{EOP}$



〔그림 5〕 접근제어(AC) 기능 처리과정

④ $M_{After-Auth}[\ Y_{Chek-AC-LEVEL1}\ Y_{Chek-AC-LEVEL2}\ Y_{Chek-AC-LEVEL3}\rangle\ M_{After-AC}$

첫 번째 도달 가능한 상태 ①의

$M_{After-Auth}$

$[\ Y_{Chek-AC-LEVEL1}\ Y_{Process-logging}\rangle\ M_{EOP}$은 식(a)와 같이 표현 할 수 있다.

$M_{After-auth}[\ Y_{Chek-AC-LEVEL1}\rangle\ M_{After-fail-acl}[\ Y_{Process-logging}\rangle\ M_{EOP}$ (a)

식(a)에서

$M_{After-auth}[\ Y_{Chek-AC-LEVEL1}\rangle\ M_{After-fail-acl}$이

$W(M_{After-auth}) = W(M_{After-fail-acl})$ 와

$\sum_{p\in P} W_p(E(p,t)\langle request\rangle) = \sum_{p\in P} W_p(E(t,p)\langle request\rangle)$

임을 증명하면 무선 원격제어 시스템의 보안 기능에서 접근제어 기능이 안전성이 있음을 검증하게 된다.

(a)는 [정리 3.1]에 따라 식 ①'를 얻을 수 있다.

$$\forall p\in P:\ M_2(After-fail-acl) = (M_1(After-auth) - \sum_{(t,b)\in Y} E(p,t)\langle request\rangle) + \sum_{(t,b)\in Y} E(t,p)\langle request\rangle \quad ①'$$

첫 번째 합은 제거된 토큰들을 나타내고, 두 번째 합은 추가된 토큰들을 나타낸다.

Y단계의 발생에 의해서 M_2는 M_1에서 직접 도달가능하며, 식①'에 [정리 3.1]의 (i)를 적용하면 식②'과 같다.

$$\sum_{p\in P} W_p(M_2(After-fail-acl) + \sum_{(t,b)\in Y} E(p,t)\langle request\rangle) = \sum_{p\in P} W_p(M_1(After-auth) + \sum_{(t,b)\in Y} E(t,p)\langle request\rangle) \quad ②'$$

식②'은 가중치 함수(weight function)의 선형성(linearity)으로부터 다음 식③'을 얻을 수 있다.

$$\sum_{p\in P} W_p(M_2(After-fail-acl)) + \sum_{p\in P}\sum_{(t,b)\in Y} W_p(E(p,t)\langle request\rangle) = \sum_{p\in P} W_p(M_1(After-auth)) + \sum_{p\in P}\sum_{(t,b)\in Y} W_p(E(t,p)\langle request\rangle) \quad ③'$$

식③'은 흐름 성질(flow property)로부터 다음 식④'을 얻을 수 있다.

$$\forall (t,b)\in BE\ :\ \sum_{p\in P} W_p(E(p,t)\langle request\rangle) = \sum_{p\in P} W_p(E(t,p)\langle request\rangle) \quad ④'$$

식④'는 식⑤'와 같이 적용된다.

$$\sum_{(t,b)\in Y}\sum_{p\in P} W_p(E(p,t)\langle request\rangle) = \sum_{(t,b)\in Y}\sum_{p\in P} W_p(E(t,p)\langle request\rangle) \quad ⑤'$$

식⑤'는 다음 식⑥'과 같이 다시 작성할 수 있다.

$$\sum_{p\in P}\sum_{(t,b)\in Y} W_p(E(p,t)\langle request\rangle) = \sum_{p\in P}\sum_{(t,b)\in Y} W_p(E(t,p)\langle request\rangle) \quad ⑥'$$

위의 식⑥'에서 두 개의 $\sum$는 위의 식과 동일하기 때문에 다음 식⑦'과 같은 결론을 얻을 수 있다.

$$\sum_{p\in P} W_p(M_2(After-fail-acl)) = \sum_{p\in P} W_p(M_1(After-auth))$$

즉, $W(M_{After-fail-acl}) = W(M_{After-auth})$이다. ⑦'

다음에 $M_{EOP}\in[\ M_{After-auth}\rangle$을 도달 가능한 마킹(marking)이라고 하고, σ를 $M_{After-auth}$에서 시작해서 M_{EOP}으로 끝나는 발생순서라고 하자. 위의 결과를 σ의

$M_{After-auth}$

$[\ Y_{Chek-AC-LEVEL1}\ Y_{Process-logging}\rangle\ M_{EOP}$

의 각 단계에 적용하면 $W(M_{EOP}) = W(M_{After-auth})$이라는 결론을 얻을 수 있다.

그러므로 [정리 3.1]의 (i)이 증명된다.

이번에는 $\sum_{p\in P} W_p(E(p,t)\langle b\rangle) = \sum_{p\in P} W_p(E(t,p)\langle b\rangle)$를 증명하기 위해서 W의 상태 불변식을 결정하고,

무선원격제어 시스템의 보안기능(접근제어)은 CPN이 동작하지 않는 바인딩 구성 엘리먼트는 가지고 있지 않다고 하자. 이것은 각 바인딩 엘리먼트 (t, b)가 적어도 도달 가능한 하나의 M_1을 가지고 있다는 것을 의미한다. $M_{After-fail-acl}$을 $M_{After-auth}[t, b\rangle M_{After-fail-acl}$에 의해 결정되는 마킹이라고 하자.

여기서 t와 b를 다시 정의하면, t는 전이(transition)의 엘리먼트(element)이고, b는 바인딩(binding) 엘리먼트이다. 즉, [그림 5]에서 첫 번째 발생가능한 단계 $Y_{Chek-AC-LEVEL1}$의 가드 식 $G(t)$는 $G(t)$=(ac-ulevel>ac-glevel)이며, 사용자의 등급(user-id)과 그룹 사용자 등급(group-id)에 따라서 바인딩 엘리먼트<b>값이 suc-request 또는 fail-request로 결정된다. 단 suc-request와 fail-request 그리고 request는 동일한 request의 컬러 타입을 갖는다.

따라서, $M_{After-auth}[t, b\rangle M_{After-fail-acl}$에서 t의 조건식에서 사용자의 등급이 그룹사용자 등급보다 낮다면 b는 fail-request로서 $M_{After-fail-acl}$상태의 마킹값을 갖게 된다.

그러므로,

$M_{After-fail-acl}$는 $M_{After-auth}[t, b\rangle M_{After-fail-acl}$에 의해 결정되는 마킹이므로, 앞서 증명된 결과에 따라서 $W(M_{After-fail-acl}) = W(M_{After-auth})$가 [정리 3.1]의 (ii)에 따라 다음 식(2)에 적용되어, ⑧'와 같이 증명된다.

$$\forall M \in [M_0\rangle : \sum_{p\in P} W_p(M(p)) = \sum_{p\in P} W_p(M_0(p)). \quad (2)$$

$$\sum_{p\in P} W_p(E(p, t)\langle request\rangle) = \sum_{p\in P} W_p(E(t, p)\langle request\rangle) \quad ⑧'$$

또한 CPN의 속성 중에서 보존성 성질에서 전이(transition)의 입력 토큰의 수는 출력 토큰의 수와 같아야 한다. 즉, $|I(t_i)| = |O(t_i)|$이므로 무선원격제어 시스템의 접근제어 보안기능에서 전이(transition)의 조건식 $G(t)$에 따라 입력 토큰의 개수와 출력 토큰의 개수가 같으므로 전이 불변식(transition invariant)이 상태 불변식과 같은 방법으로 증명될 수 있으므로 무선원격제어 시스템의 접근제어 기능은 안전성이 있음이 증명된다.

강제적 접근제어 기능의 각 도달 가능한 상태들은 다시 세부적으로 다음과 같이 정의 할 수 있다.

① $M_{After-auth}$
$[\ Y_{Chek-AC-LEVEL1}\ Y_{Process-logging}\rangle\ M_{EOP}$
$M_{After-auth}[\ Y_{Chek-AC-LEVEL1}\rangle\ M_{fail-acl}$
$M_{fail-acl}[\ Y_{Process-logging}\rangle\ M_{EOP}$

② $M_{After-Auth}[\ Y_{Chek-AC-LEVEL1}$
$Y_{Chek-AC-LEVEL2}\ Y_{Process-logging1}\rangle\ M_{EOP}$
$M_{After-suc-acl}$
$[\ Y_{Chek-AC-LEVEL2}\rangle\ M_{After-fail-ac2}$
$M_{After-fail-ac2}[\ Y_{Process-logging1}\rangle\ M_{EOP}$

③ $M_{After-Auth}$
$[\ Y_{Chek-AC-LEVEL1}\ Y_{Chek-AC-LEVEL2}$
$Y_{Chek-AC-LEVEL3} - Y_{Process-logging2}\rangle\ M_{EOP}$
$M_{After-auth}[\ Y_{Chek-AC-LEVEL1}\rangle\ M_{After-suc-acl}$
$M_{After-suc-acl}[\ Y_{Chek-AC-LEVEL2}$
$Y_{Chek-AC-LEVEL3}\rangle\ M_{After-fail-ac3}$
$M_{After-fail-ac3}$
$[\ Y_{Chek-AC-LEVEL3}\rangle\ Y_{Process-logging2}\rangle\ M_{EOP}$

④ $M_{After-Auth}[\ Y_{Chek-AC-LEVEL1}$
$Y_{Chek-AC-LEVEL2}\ Y_{Chek-AC-LEVEL3}\rangle\ M_{After-AC}$
$M_{After-Auth}[\ Y_{Chek-AC-LEVEL1}\rangle\ M_{After-suc-acl}$
$M_{After-suc-acl}[\ Y_{Chek-AC-LEVEL1}$
$Y_{Chek-AC-LEVEL2}\rangle\ M_{After-suc-ac2}$
$M_{After-suc-ac2}[\ Y_{Chek-AC-LEVEL3}\rangle\ M_{After-AC}$

무선원격제어 시스템의 보안 기능 중에서 접근제어기능은 4단계의 도달 가능한 상태로 표현 하였으며, 도달 가능한 상태 중에서 첫 번째 단계의 상태를 CPN으로 표현한 다음, 상태 불변식

$M_{After-auth}$
$[\ Y_{Chek-AC-LEVEL1}\ Y_{Process-logging}\rangle\ M_{EOP}$

에 대하여 안전성을 검증하였다. 같은 방법으로 도달 가능한 나머지 3단계와 CPN으로 표현된 사용자 인증기능도 상태 불변식으로 표현이 가능하며, 같은 방법으로 안전성을 검증할 수 있다.

Ⅵ. 결 론

본 연구는 모바일 단말기로 이동 중에도 원격지의 시스템을 모니터링 할 뿐만 아니라 문제가 발생되면 즉각 모바일 단말기로 장애통보를 해주거나, 원격지의 시스템에 바로 접근해서 문제를 해결 할 수 있는 원격제어 기능을 제공할 수 있는 무선 원격제어 시스템에 대한 보안 기능을 설계하였다. 제안하는 보안 기능은 모바일 장비 사용자가 원격지 서버에 접속하기 위하여 강력한 인증과정을 수행하도록 하고, 원격지 서버로부터 인증된 사용자라도 대상 서버에 접속하여 명령어를 원격에서 입력하려면 명령어 사용에 대한 권한을 부여 받기위한 접근제어기능을 수행해야만 한다. 이러한 보안기능은 실제 구현에 앞서 설계된 보안 기능들에 대한 안전성을 검증하고자 CPN 기반의 상태 불변식을 이용하였다. 상태 불변식은 CPN을 이용해서 시스템의 각 기능에 대한 흐름을 그래픽으로 표현이 가능하고, 그래픽으로 표현된 모든 가능한 상태를 방정식으로 표현하여 입력이 요청된 토큰과 출력되는 토큰이 항상 같도록 유지되어 상태가 불변한다는 정리를 수학적으로 증명함으로써 모델의 안전성을 검증한다. 이러한 CPN기반의 상태 불변식을 이용한 안전성 검증은 유선과 무선 시스템 통합을 위한 구현과정을 실행하기 이전에 안전성을 검증할 수 있는 효율적인 방법이 될 수 있다.

참 고 문 헌

[1] Dr. Mikael Sjodin 2002 *"Remote Monitoring and Control Using Mobile Phone"*, 2002.

[2] http://www.cis.upenn.edu/~bcpierce/courses/629/papers/Concordia-White paper, *"Mobile Agent Computing"*, 2002.

[3] Analysis of CP-nets, *http://www.daimi.aau.edu/CPnets/intro/analysis.htm*, December 1997.

[4] *Design/CPN Overview of CPN ML Syntax*, Meta Software, 1993.

[5] *Design/CPN Programmer's Manual for X-Windows Version 2.0*, Meta Software, 1993.

[6] *Design/CPN Reference Manual for X-Windows Version 2.0, Meta Software*, 1993.

[7] *Design/CPN Occurence Graph Manual for X-Windows Version 2.0*, Meta Software, 1993.

[8] Kurt Jensen, *"Colored Petri Nets. Basic Concepts, Analysis Methods and Practical Use"*. Volume 1, 2, 3: Basic Concepts, EATCS monographs on Theoretical Computer Science, Springer-Verlag 1992.

[9] Dr. Mikael Sjodin 2002 *"Remote Monitoring and Control Using Mobile Phone"*, 2002.

[10] Carles Arehart, Nirmal Chidambaram, etc. *"Professional WAP"* Wrox. 2000.

[11] James F. Kurose and Keith W. Ross, *"Computer Networking"*, Addison Wesley 2nd-Edition, 2002.

〈著者紹介〉

이 문 구 (Moon-ku Lee) 정회원

1984년 : 숭실대학교 전자계산학 (학사)
1993년 : 이화여자대학교 대학원 전산교육학 (석사)
2000년 : 숭실대학교 대학원 컴퓨터시스템 (공학박사)
2000년 3월~현재 : 김포대학 컴퓨터계열 조교수
<관심분야> 네트워크 프로그래밍 및 보안, 인터넷 보안, 시스템 보안, 암호화 알고리즘, 전자상거래 보안, 침입탐지 및 차단시스템