김일성종합대학학보
(자연과학)
주체104(2015)년 제61권 제6호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 61 No. 6 JUCHE104(2015).

색페트리망에서 위치색벡토르의 도달가능성

김현정, 한도욱

론문에서는 암호학적통신규약의 안전성해석을 비롯하여 여러 분야들에서 리용할수 있는 색페트리망에서의 위치색벡토르의 도달가능성문제의 해석적표시를 새롭게 밝혔다.

선행연구[1]에서는 표적에 색을 가진 색페트리망을 정의하였고 선행연구[3]에서는 위치에 색이 있는 경우에 색벡토르의 도달가능성문제를 론의하였으나 그 풀이법에 대한 엄밀한 해석은 주지 못하였다. 또한 선행연구[2]에서는 체계의 고장진단을 위한 색페트리망을 정의하고 한가지 고장진단방법을 제기하였다.

여기서는 위치와 통로에 색이 주어진 경우에 통로의 발화조건과 위치색의 변화조건을 새로 밝힌데 기초하여 색벡토르의 도달가능성에 대한 해석적표시를 구하였다.

정의 4원조 $N=(P,\ T,\ I,\ O)$를 페트리망이라고 부른다. 여기서 $P=\{p_1,\cdots,\ p_n\}$, $n>0$은 위치들의 유한모임, $T=\{t_1,\cdots,\ t_m\}$, $m>0$은 통로들의 유한모임, $P\bigcap T=\phi$이다. $I:T\to P^{\infty}$는 매 통로를 위치들의 다중모임으로 넘기는 통로입력함수이고 $O:T\to P^{\infty}$는 매 통로를 위치들의 다중모임으로 넘기는 통로출력함수이다.

$N=(P,\ T,\ I,\ O)$에서 임의의 $p\in P$와 $t\in T$에 대하여 $\#(p,\ I(t))$, $\#(p,\ O(t))$는 각각 $I(t)$, $O(t)$에서의 위치 p의 다중도이다.

매 위치 p_i에 부아닌 옹근수 $\mu_i=\mu(p_i)$를 대응시키면 벡토르 $\mu=(\mu_1,\ \cdots,\ \mu_n)$을 페트리망의 상태벡토르 또는 상태, μ_i를 p_i의 표적 혹은 돌이라고 부른다.

임의의 통로 $t_j\in T$에 대하여 조건 $\forall p_i\in P,\ \mu_i\geq\#(p_i,\ I(t_j))$가 성립되면 t_j는 발화가능하다고 하며 t_j가 발화된 이후의 페트리망의 상태는 다음의 규칙에 따라 변화된다.

$$\forall p_i\in P,\ \mu_i'=\mu_i-\#(p_i,\ I(t_j))+\#(p_i,\ O(t_j))$$

통로들의 발화렬 $\tau=(t_{i_1},\cdots,\ t_{i_k})$에 의하여 상태가 μ로부터 μ'로 변하면 μ'는 μ로부터 도달가능하다고 말한다. 그리고 페트리망 N의 초기상태를 μ^0으로 표시한다.

N에 대하여 $D^-=(D^-(j,\ i))$, $D^-(j,\ i)=\#(p_i,\ I(t_j))$를 N의 입력행렬, $D^+=(D^+(j,\ i))$, $D^+(j,\ i)=\#(p_i,\ O(t_j))$를 N의 출력행렬이라고 부른다. 이 두 행렬은 모두 $m\times n$형행렬이다. 그리고 $D=D^+-D^-$를 변환행렬이라고 부른다.

μ'가 μ로부터 도달가능하면 련립방정식 $\mu'=\mu+x\times D$가 성립된다. 여기서 x는 μ'가 μ로부터 도달가능하게 하는 발화렬 $\tau=(t_{i_1},\cdots,\ t_{i_k})$에 통로 t_{i_j}가 나타나는 회수 즉 발화회수를 j째 성분으로 가지는 m차원벡토르로서 발화회수벡토르라고 부른다.

이제 페트리망 $N=(P,\ T,\ I,\ O)$가 주어졌을 때 넘기기 $C:P\bigcup T\to Z$를 보충한 망 $N=(P,\ T,\ C,\ I,\ O)$를 생각하고 그것을 색페트리망이라고 부른다. 여기서 $\forall p\in P,\ C(p)$는 위

치색, $\forall t \in T$, $C(t)$ 는 통로색이라고 부른다.

벡토르 $\delta = (C(p_1),\ C(p_2), \cdots,\ C(p_n))$, $\gamma = (C(t_1),\ C(t_2), \cdots,\ C(t_m))$ 을 각각 위치색벡토르, 통로색벡토르라고 부른다.

그러면 임의의 상태 μ 에 위치색벡토르가 일의적으로 대응된다.

색페트리망에서의 통로의 발화조건은 위치색과 통로색의 영향을 받으며 통로의 발화후에 위치색이나 통로색들이 변하는 경우와 변하지 않는 경우로 갈라진다. 여기서는 임의의 위치 $p_i \in P$ 에 대하여 위치색은 어떤 옹근수로 표현되고 임의의 통로 $t_j \in T$ 에 대하여 통로색은 $C(t_j) \in \{1,\ -1\}$ 이라고 가정한다. 또한 페트리망의 매 위치 $p_i \in P$ 에 대하여 $\mu(p_i) \neq 0 \Leftrightarrow C(p_i) \neq 0$ 이 성립된다고 가정한다.

통로의 발화조건은 $\forall p_i \in P,\ \mu_i \geq \#(p_i,\ I(t_j))$, $\forall p_i \in I(t_j),\ C(p_i) \neq 0$ 으로 놓고 t_j 가 발화한 다음에 위치색은 $\forall p_i \in I(t_j),\ C(p_i) = 0$, $\forall p_k \in O(t_j),\ C(p_k) = C(t_j) \times C(p_i)$ 로 변하며 통로색은 변하지 않는다고 가정한다.

상태의 도달가능성을 정의한것과 류사하게 위치색벡토르 δ 가 어떤 발화렬의 발화후에 δ' 로 변하였다면 δ' 는 δ 로부터 도달가능하다고 말한다.

문제는 주어진 δ 가 초기위치색벡토르 δ^0 으로부터 도달가능한가를 판정하는것이다.

이를 위하여 각각 색입력행렬, 색출력행렬이라고 부르는 다음의 $m \times n$ 형행렬들을 보자.

$$E^- = (E^-(j,\ i)) \quad \left(E^-(j,\ i) = \begin{cases} 1, & p_i \in I(t_j) \\ 0, & p_i \notin I(t_j) \end{cases}\right), \quad E^+ = (E^+(j,\ i)) \quad \left(E^+(j,\ i) = \begin{cases} 1, & p_i \in O(t_j) \\ 0, & p_i \notin O(t_j) \end{cases}\right)$$

보조정리 $N = (P,\ T,\ C,\ I,\ O)$ 에서 임의의 $t_j \in T$ 에 대하여 $|I(t_j)| \leq 1$, $|O(t_j)| \leq 1$ 이라고 할 때 δ 가 발화렬 $\tau = (t_{i_1}, \cdots, t_{i_k})$ 의 발화에 의하여 δ^0 으로부터 도달가능하면 관계식 $\delta = \delta^0 - F(\delta^0,\ i_1) - F(\delta^0,\ i_2) - \cdots - F(\delta^0,\ i_k)$ 가 성립된다. 여기서 $C(j) \in \{1,\ -1\}$ 은 고정된 상수이며 $F(\delta^0,\ j) = (e(j)E^-) \cdot (\delta^0(e(j)E^-)) + (e(j)E^+) \cdot (\delta^0(e(j)E^+)) - (C(j)e(j)E^+) \cdot (\delta^0(e(j)E^-))$.

$e(j)$ 는 j 째 성분만 1이고 나머지 성분들은 모두 0인 m 차원벡토르이다.

증명 통로 t_j 가 발화한 결과에 δ^0 으로부터 위치색벡토르 δ 가 도달되였다고 하면

$\delta = \delta^0 - (e(j)E^-) \cdot (\delta^0(e(j)E^-)) - (e(j)E^+) \cdot (\delta^0(e(j)E^+)) + (C(j)e(j)E^+) \cdot (\delta^0(e(j)E^-)) = \delta^0 - F(\delta^0,\ j)$

가 성립된다. 여기서

$F(\delta^0,\ j) = (e(j)E^-) \cdot (\delta^0(e(j)E^-)) + (e(j)E^+) \cdot (\delta^0(e(j)E^+)) - (C(j)e(j)E^+) \cdot (\delta^0(e(j)E^-))$

임을 고려하면 웃식은 $\delta = \delta^0 - F(\delta^0,\ j)$ 로 표시된다. 이것은 론문에서 제기한 페트리망에 대한 제한조건 $|I(t_j)| \leq 1$, $|O(t_j)| \leq 1$ 과 E^-, E^+ 의 정의를 고려하면 곧 나온다.

이것을 일반화하여 δ 가 통로들의 $\tau = (t_{i_1}, \cdots, t_{i_k})$ 의 발화에 의하여 δ^0 으로부터 도달되였다고 하면 $\delta = \delta^0 - F(\delta^0,\ i_1) - F(\delta^0,\ i_2) - \cdots - F(\delta^0,\ i_k)$ 가 성립된다.(증명끝)

정리 색페트리망 $N = (P,\ T,\ C,\ I,\ O)$ 에서 임의의 통로 $t_j \in T$ 에 대하여 $\#(p_i,\ I(t_j)) \leq 1$, $\#(P_i,\ O(t_j)) \leq 1$ 이라고 가정하고 위치색벡토르 δ 가 초기위치색벡토르 δ^0 으로부터 도달가능하다면 다음의 련립방정식이 만족된다.

$$\begin{cases}\mu' = \mu^0 + x \times D \\ \delta = \delta^0 - F(\delta^0,\ i_1) - F(\delta^0,\ i_2) - \cdots - F(\delta^0,\ i_k) \\ x \geq 0,\ \text{옹근수}\end{cases}$$

$$F(\delta^0,\ j) = (e(j)E^-)\cdot(\delta^0(e(j)E^-)) + (e(j)E^+)\cdot(\delta^0(e(j)E^+)) - (C(j)e(j)E^+)\cdot(\delta^0(e(j)E^-))$$

여기서 상태 μ^0과 μ는 각각 위치색벡토르 δ^0과 δ에 대응하는 상태이다.

증명 증명하려는 련립방정식의 의미를 따져보면 그것은 색페트리망에서 어떤 발화렬 τ가 있어서 상태 μ가 초기상태 μ^0으로부터 도달가능하고 그때 대응하는 위치색벡토르는 δ^0으로부터 δ에로 도달가능해야 한다는것을 의미한다.

그런데 상태 μ^0으로부터 μ에로의 도달가능성의 필요조건은 $\mu' = \mu + x \times D$라는것이 이미 증명되여있고 그때의 발화렬에 의하여 δ가 δ^0으로부터 도달가능하기 위한 필요조건은

$$\delta = \delta^0 - F(\delta^0,\ i_1) - F(\delta^0,\ i_2) - \cdots - F(\delta^0,\ i_k),$$

$$F(\delta^0,\ j) = (e(j)E^-)\cdot(\delta^0(e(j)E^-)) + (e(j)E^+)\cdot(\delta^0(e(j)E^+)) - (C(j)e(j)E^+)\cdot(\delta^0(e(j)E^-))$$

라는것이 앞의 보조정리에서 증명되였다. 따라서 정리는 증명되였다.(증명끝)

한가지 응용실례로서 DH열쇠공유규약의 안전성판정문제를 보기로 한다.

DH열쇠공유규약은 다음과 같다.

송신자 A와 B는 씨수 p를 선택하고 Z_p에서의 생성원소 g를 선택하여 공유한다.

송신자 A는 $x \in Z_p$를 비밀로 선택하고 $Y_A = g^x \bmod p$를 계산하여 B에게로 보낸다.

수신자 B는 $y \in Z_p$를 비밀로 선택하고 $Y_B = g^y \bmod p$를 계산하여 A에게로 보낸다.

A와 B는 각각 열쇠 $k = Y_B{}^x \bmod p$, $k = Y_A{}^y \bmod p$를 계산하여 열쇠를 공유한다.

DH열쇠공유규약에 대한 공격은 다음과 같다.

① 공격자 E는 A와 B사이에 교환되는 Y_A와 Y_B를 전송도중에 절취하여 Y_A를 Y'_A로, Y_B를 Y'_B로 바꾸어서 B와 A에게 전송한다.

② A와 B는 Y'_B와 Y'_A에 의하여 열쇠를 공유한다.

DH열쇠공유규약에 대한 공격과정을 페트리망으로 모형화하면 그림과 같다.

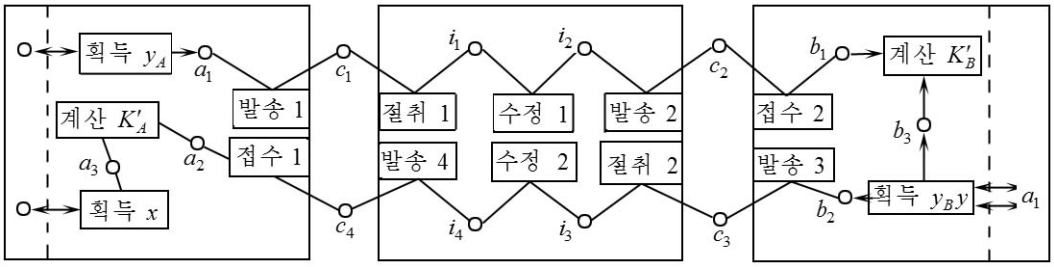

그림. 공격과정에 대한 페트리망의 모형화

여기서 론의하는 위치는 $p_1 = a_1$, $p_2 = c_1$, $p_3 = i_1$, $p_4 = i_2$, $p_5 = c_2$, $p_6 = b_1$, $p_7 = b_2$, $p_8 = c_3$, $p_9 = i_3$, $p_{10} = i_4$, $p_{11} = c_4$, $p_{12} = a_2$이며 통로는 t_1=발송 1, t_2=절취 1, t_3=수정 1, t_4=발송 2, t_5=접수 2, t_6=발송 3, t_7=절취 2, t_8=수정 2, t_9=발송 4, t_{10}=접수 1이다.

위치색모임은 $C=\{M_1, -M_1, M_2, -M_2, 0\}$이고 통로색은 $C(t_3)=C(t_8)=-1$이고 나머지 모든 통로들은 색이 1이다. 여기서 $M_1=Y_A$, $M_2=Y_B$, $-M_1=Y'_A$, $-M_2=Y'_B$를 의미하며 0은 아무런 정보도 도달되지 않았다는것을 의미한다.

초기위치색벡토르는

$$\delta^0=(M_1, 0, 0, 0, 0, 0, M_2, 0, 0, 0, 0, 0)$$

이며 이것은 A와 B가 각각 값 Y_A와 Y_B를 계산하여 발송준비단계에 있다는것을 의미한다.

그리고 위치색벡토르

$$\delta=(0, 0, 0, 0, 0, -M_1, 0, 0, 0, 0, 0, -M_2)$$

는 Y_A와 Y_B가 전송도중에 공격자에 의하여 Y'_A와 Y'_B로 변경되여 B와 A에게 전달되였다는것을 의미한다.

따라서 δ가 δ^0으로부터 도달가능하다면 주어진 열쇠공유규약은 안전하지 못한것으로 된다.

δ^0에 대응되는 초기상태는 $\mu^0=(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$이며 δ에 대응되는 상태는 $\mu=(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$이다.

이것을 론문에서 밝힌 조건에 의하여 계산하면 옹근수풀이가 존재하고 따라서 불안전상태에 도달할수 있다는 결론을 얻는다.

따라서 DH열쇠공유규약은 안전하지 못하다.

참 고 문 헌

[1] 박경철 등; 페트리망체계의 기본, 공업출판사, 36～37, 1994.

[2] P. Pawlewski et al.; Applications, In-Tech, 333～350, 2010.

[3] Long Shi Gong et al.; 计算机仿真, 22, 6, 2005.

주체104(2015)년 2월 5일 원고접수

Investigation for Reachability of Place Color Vector on the Colored Petri Net

Kim Hyon Jong, Han To Uk

The colored Petri net are used in determining security of cryptographycal protocols.

We construct the analytical notation for reachability of place color vector on the colored Petri net.

Key word: place color vector