방향 네트웍에서 안전한 통신 프로토콜

권우철 좌경룡

한국과학기술원 전자전산학과

Perfectly Secure Communaton n Dected Networks

Woo-Cheol Kwon Kyung-Yong Chwa

Dept. of Electral Engeeng and Computer Sence, KAIST

요약

본 논문에서는 방향 네트웍에서 안전한 통신 프로토콜을 연구한다. 본 논문은 Dolev 등의 방법[6]을 따라 일반적인 네트웍을 한 쌍의 전송자와 수신자가 여러개의 채널을 통해 연결되어 있는 모델로 단순화한다. Dolev 등은 채널이 모두 양방향이거나 또는 방향이 모두 전송자에서 수신자인 경우만 다루었으나 여기서는 양방향과 단방향 채널이 동시에 존재하는 경우를 다룬다. 단방향 채널에는 전송자에서 수신자로의 방향 뿐만 아니라 그 역방향으로만 통신이 가능한 채널도 포함된다. 본 논문은 정보이론적으로 안전한 통신이 가능하기 위한 필요충분조건을 구하고 효율적인 알고리즘을 제시한다. 이 알고리즘은 단순화한 모델에서의 채널을 정점분리 경로로 대응시켜 일반적인 방향 네트웍에 적용될 수 있다.

1 서론

분산 컴퓨팅에서 통신의 보안은 매우 중요한 문제이다. 네트웍에서 두 노드간의 통신은 일반적으로 다른 노드들과 이들 사이의 채널을 거치는 간접 경로를 통해 이루어진다. 이 경우 다른 노드들의 도청에 의해 통신하는 두 노드의 프라이버시가 침해당할 수 있게 된다. 이때 고의적으로 통신을 방해하는 노드나 채널이 존재할 경우 문제는 더욱 복잡해진다.

이러한 경우 정보이론적으로 안전하고 에러를 허용하지 않는 통신 프로토콜은 Dolev 등에 의해 처음으로 제시되었다[6]. Dolev 등은 일반적인 네트웍에서 통신의 보안 문제를 전송자와 수신자만을 고려해 단순화시켜 SMT(Secure Message Transsn) 문제로 정의하였다. SMT 문제에서 전송자와 수신자는 n개의 채널로 서로 통신을 할 수 있다고 가정한다. 이때 각 채널은 일반적인 네트웍에서 전송자와 수신자를 잇는 정점 분리 경로(vertex sjo t path)에 해당한다. 계산 능력의 제한이 없는 adversary가 σ개의 채널을 차지해 이들을 통해 메세지에 대한 정보를 얻으려 하고 ρ개의 채널을 변조하여 수신자가 정확하게 메세지를 전달받는 것을 방해하려 한다고 하자. 이러한 가정 아래 Dolev 등은 각 채널에서 단방향, 즉 전송자에서 수신자 방향으로만 정보 전달이 가능할 경우 $n \geq \sigma + 2\rho + 1$이, 또 각 채널에서 양방향으로 통신이 가능할 경우 $n \geq \sigma + \rho + 1$이 안전한 통신을 위한 필요충분조건임을 보이고 효율적인 알고리즘을 제시하였다.

본 논문에서는 단방향 채널과 양방향 채널이 혼재해 있는 모델에서의 안전한 통신을 고려한다. 이때 단방향 채널은 전송자에서 수신자로만 통신이 가능한 채널뿐 아니라 그 역방향으로만 통신이 가능한 채널도 포함한다. 본 논문은 이렇게 확장된 모델에서 안전한 통신이 가능하기 위한 필요충분조건을 보이고 효율적인 알고리즘을 제시한다. 본 논문의 알고리즘은 방향 네트웍에서의 통신 문제에 응용될 수 있다.

이외에 안전한 통신을 정보이론적 관점에서 다룬 연구로는 다음과 같은 것들이 있다. Sayeed와 Abu-Amara는 [6]과 동일한 모델에서 좀 더 효율적인 알고리즘을 제시하였다[10]. Frankl 과 Yung은 hypergraph에서 pass e adversary에 대해 안전한 통신이 가능하기 위한 필요충분조건을 보이고 알고리즘을 제시한 바 있다[8]. mult cast graph에서 통신의 보안 문제가 [7, 12]에서 다루어졌다. 그리고 [3, 2]에서는 그래프의 위상이 프로세서에게 알려져 있지 않은 경우 통신의 보안 문제에 대해 고려하였다.

본 논문의 구성은 다음과 같다. 2절에서는 모델과 용어를 정의하고 3절에서는 알고리즘을 소개한다. 4장에서는 하한을 보이고 마지막으로 5절에서는 향후연구과제를 제시한다.

2 모델과 용어 정의

이 절에서 정의하는 모델과 용어의 대부분은 [6]을 따른 것이다.

메세지를 보내려고 하는 프로세서를 S(Sender), 메세지를 전달받을 프로세서를 R(Rece er)이라 하자. S와 R은 확률적 튜링 기계(Probab Turg mache) 로서 이들을 연결하는 채널을 통해 동기화(synchrozed) 된 통신을 할 수 있다. 채널은 단방향 채널과 양방향 채널로 나뉘며 S에서 R로만 정보 전달이 가능한 채널을 $S \rightarrow R$ 채널, 그 역은 $R \rightarrow S$ 채널 , S와 R 양쪽 방향으로 정보 전달이 가능한 채널은 $S \leftrightarrow R$ 채널로 부르기로 한다. 앞으로 l은 $S \rightarrow R$ 채널의 수, m은 $R \rightarrow S$ 채널의 수, n은 $S \leftrightarrow R$ 채널의 수를 가리키기로 한다. 그리고 $S \rightarrow R$ 채널은 $x_1, x_2, \ldots, x_l$, $R \rightarrow S$ 채널은 $y_1, y_2, \ldots, y_m$로 라벨이 붙여져 있다고 가정한다. S가 전송하려고 하는 메세지 M은 원소의 개수가 $2(l+m+n)$ 보다 큰 소수 p인 유한체(finite field) Q에 확률분포 Π로 분포한다고 하자. 그리고 때때로 편의상 $Q = Z_p$로 생각한다.

Dolev 등은 adversary를 A_L(steng adversary), A_D(sruptg adversary)로 구분한다. A_L은 $|L| \leq \sigma$인 채널의 집합 L을 선택하여 L에 속하는 채널을 통해 전달되는 정보를 읽어 M에 대한 정보를 알아내려 한다. A_D는 $|D| \leq \rho$인 채널의 집합 D를 선택하여 D에 속한 채널을 통해 전달되는 정보를 임의로 변조해 R이 정확히 M을 전달받는 것을 방해한다. adversary의 계산능력에는 제한이 없고 S와 R이 사용하는 프로토콜을 완전히 알고 있는 것으로 간주한다. 또한 adversary는 D와 L에 속할 채널을 프로토콜의 수행 도중 선택할 수 있다. 이때 $D \subseteq L$ 혹은 $L \subseteq D$라 가정하는 것을 포함가정(contamen t assumpn) 이라 한다. 본 논문에서는 항상 포함가정을 가정할 것이다. 또 A_L과 A_D는 통신이 가능하며 프로토콜의 수행 도중 서로 협력할 수 있다고 가정한다. 이 경우 실제 adversary는 하나만 존재하는 것과 같아진다. 따라서 본 논문에서는 편의상 때때로 A_L과 A_D를 따로 구분하지 않

고 하나의 adversary A가 σ개의 채널을 엿들을 수 있고 ρ개의 채널을 변조할 수 있는 것으로 생각할 것이다. 이러한 가정은 여러 문헌에서 고려된 secrecy와 reliability 에 관한 상황 중 최악의 상황으로 볼 수 있다[5, 1, 4, 9]. 또 A_L이 A_D와 통신을 할 수 있다고 가정하게 되면 A_L은 $D \cup L$에 속한 채널을 읽을 수 있게 되므로 실제 A_L이 읽을 수 있는 채널의 수는 $max\{\sigma, \rho\}$가 된다. 따라서 본 논문에서는 앞으로 일반적으로 $\sigma \geq \rho$라 가정할 것이다. 본 논문의 adversary 모델은 [6]의 주요 결과가 가정하고 있는 adversary 모델과 일치한다. 실제로 A_D와 A_L의 통신 가능 여부 혹은 포함 가정의 유무에 따라 secrecy와 reliability 는 크게 영향을 받는다. 이에 대한 자세한 논의는 [6]을 참고하기로 한다.

이제 두 매개변수 σ와 ρ를 이용하여 SMT를 엄밀히 정의하도록 한다. ew_A^P는 A가 프로토콜 P의 수행도중 얻을 수 있는 모든 정보라고 하고 프로토콜 P를 이용해 유한체 Q에서 확률분포 Π로 분포하는 M을 전송할 때 ew_A^P의 확률분포를 $\hat{\Pi}(A, M, P)$라고 하자.

정의 1 $(\sigma, \rho) - SMT$ *(Secure Message Transmission)*

S가 유한체 Q에서 확률분포 Π로 M을 임의로 선택하여 프로토콜 P를 이용하여 R에게 전송할 때 $|L| \leq \sigma$, $|D| \leq \rho$ 인 모든 A에 대해 다음을 만족한다.

- *Secrecy* $\forall M' \in Q, \hat{\Pi}(A, M', P) = \hat{\Pi}(A, M, P)$
- *Reliability* *R은 정확히 M을 전달받는다.*

특히 S와 R이 $S \rightarrow R$ 채널로만 연결되어 있을 경우 1-way $(\sigma, \rho) - SMT$ 라 하고 $S \leftrightarrow R$ 채널로만 연결되어 있을 경우 2-way $(\sigma, \rho) - SMT$ 라 부른다.

S에서 R로 정보를 전달할 수 있는 채널의 수가 2ρ보다 큰 경우 S는 모든 채널을 통해 같은 메세지를 보내고 R은 다수의 채널에서 일치하는 값을 선택하면 항상 reliability 를 보장할 수 있다. 이러한 방법을 사용하여 메세지를 전달하는 것을 S가 R로 공개적으로 메세지를 전송한다고 부르기로 한다.

3 알고리즘

이 절에서는 단방향 채널을 충분히 활용하는 알고리즘을 제시한다. l개의 $S \rightarrow R$ 채널과 m개의 $R \rightarrow S$ 채널로 구성되어 있는 모델을 생각하고 $l \geq 2\rho + 1$, $l + m \geq \sigma + \rho + 1$, $l + 2m \geq \sigma + 2\rho + 1$라 가정한다. 이러한 조건들은 실제로 $(\sigma, \rho) - SMT$가 가능하기 위한 필요조건임을 다음 절에서 보일 것이다.

이 알고리즘은 보안을 위해 Sham 의 비밀분산기법[11]을 사용한다. S는 랜덤 패드를 숨길 다항식 $f(x) \in Q[x]$을 선택하는 작업의 일부를 R에게 분산시킨다. 편의상 여기서는 $m \leq \sigma$라 가정한다. 알고리즘을 기술할 때에는 이러한 가정을 사용하지 않을 것이다. R은 $s_1, s_2, \ldots, s_m$을 랜덤하게 선택하여 각 y 를 통해 S에게 보낸다. S가 실제로 받은 값들이 $s'_1, s'_2, \ldots, s'_m$라 하자. S는 $t_1, t_2, \ldots, t_{\sigma-m}$와 패드 r을 랜덤하게 선택한다. 그리고 이들을 모두 보간하는 σ차의 다항식 $f(x) \in Q[x]$를 찾는다. 즉 $R \rightarrow S$ 채널을 통해 받은 n개의 난수를 $f(1), f(2), \ldots, f(m)$의 값으로 하고 $t_1, t_2 \ldots, t_{\sigma-m}$을 $f(m+1), f(m+2), \ldots, f(\sigma)$의 값으로 한다. 마지막으로 $f(0)$을 랜덤 패드 r로 둔다. S는 $f(1+m), f(2+m), \ldots, f(l+m)$를 $S \rightarrow R$ 채널을 통해 R에게 보낸다. R은 자신이 보낸 점과 S에게서 받은 점을 모두 보간할 수 있는 차수 σ인 다항식 $g(x) \in Q[x]$ 를 찾는다. 이 때 S와 R은 랜덤 패드를 숨긴 다항식 $f(x)$의 $\sigma+1$개 이상의 보간점들을 공유하게 된다. 결국 S가 $f(x)$를 랜덤하게 선택하여 $\sigma+\rho+1$개의 $S \rightarrow R$ 채널을 통해 보간 점들을 보내는 것과 같아진다.

adversary의 변조로 인해 R이 보간 다항식 $g(x)$를 찾는데 실패한 경우 R은 모든 y 들을 통해 "FAIL" 신호를 S에게 보낸다. 우선 $R \rightarrow S$ 채널 중 D에 속하지 않는 채널이 하나 이상 존재하는 경우를 생각하자. 가정에 의해 $R \rightarrow S$ 채널중 적어도 하나는 변조가 불가능하므로 "FAIL" 신호가 S에게 전달될 수 있다. S가 "FAIL" 신호를 받으면 R에게서 받은 정보와 R에게 보내려 한 정보를 공개적으로 R에게 전달한다. R은 S가 보낸 정보를 이용해 변조가 발생한 채널을 새로 발견할 수 있게 되고 다음부터 이 채널을 통한 정보를 무시하고 보간 다항식을 찾는다. 이러한 과정을 한번 할때마다 D에 속한 채널을 새로 채널을 찾아낼 수 있으므로 이 과정을 많아도 ρ번 반복하게 되면 R은 D에 속한 채널을 완전히 알아내게 된다. 그러면 이후의 보간 다항식을 항상 성공적으로 찾아낼 수 있으므로 S는 R에게 안전하게 랜덤 패드를 전달할 수 있게 된다.

모든 $R \rightarrow S$ 채널이 D에 속하는 경우에는 A가 "FAIL" 신호를 전달하지 않음으로써 R이 랜덤 패드를 전달받는데 실패할 수도 있다. 이를 대비해 S는 알고리즘의 마지막에 [6, 10] 등에서 제시한 1-way $(\sigma, \rho - m) - SMT$를 위한 알고리즘을 사용해 M을 R에게 전달한다. 여기서 $R \rightarrow S$ 채널이 모두 D에 속하므로 $S \rightarrow R$ 채널 중 D에 속하는 채널은 $\rho - m$개가 된다. 따라서 이 경우 R은 안전하게 M을 얻을 수 있다.

마지막으로 R이 보간 다항식을 찾아 랜덤 패드 전송에 성공했지만 A가 거짓 "FAIL" 신호를 S에게 보내어 메세지 전송을 방해하는 경우를 생각한다. 이때 실제 보간 다항식을 찾는데 실패한 회수가 ρ번 이상이면 R은 D에 속하는 모든 채널을 찾아낼 수 있다는 사실을 이용하여 S는 한 $R \rightarrow S$ 채널이 보내는 "FAIL"신호를 ρ번만 인정한다. 이렇게 하면 반복 회수를 $n\rho$번으로 제한할 수 있다.

다음은 알고리즘의 기술이다. 입력의 X와 Y는 각각 $S \rightarrow R$ 채널과 $R \rightarrow S$ 채널의 집합이다. X_{val} 와 Y_{val} 는 각각 X와 Y로 초기화한다. **1waySMT**$(X, \sigma, \rho, Q,$ **pw ate to** $S : M)$는 $S \rightarrow R$ 채널의 집합 X를 통해 M을 전송하는 1-way $(\sigma, \rho) - SMT$ 알고리즘이다. 이러한 알고리즘은 [6, 10]에서 예를 제시한 바 있다. **GeneralSMT**에서 사용하는 모든 연산은 항상 유한체 Q에서의 연산이다.

GeneralSMT$(X, Y, \sigma, \rho, Q,$ **1waySMT, pw ate to** S : $M,$ **pw ate to** $R : X_{val}, Y_{val})$

1. R은 $s \in Q$를 각 $y \in Y_{val}$ 를 통해 R에게 보낸다.
2. S가 s'를 각 $y \in Y$를 통해 받는다. 이때, S는 y 의 모든 행동을 Q의 원소로 해석한다.

S는 $r \in Q$와 $t_1, t_2, \ldots, t_{\max\{0,\sigma-m\}} \in Q$를 랜덤하게 선택하여 다음을 만족하는 $\max\{\sigma, m\}$차의 다항식 $f(x) \in Q[x]$를 찾는다.

$$f(\ ) = \begin{cases} r & = 0 \\ s' & = 1, 2, \ldots, m \\ t_{\ -m} & = m+1, \ldots, \max\{\sigma, m\} \end{cases}$$

3. S는 $f(\ +m)$를 각 $x \in X$를 통해 보내고, $(f(l+m+1), \ldots, f(l+m+\max\{0, m-\sigma\}))$ 를 공개적으로 R에게 보낸다.
4. R은 u를 각 $x \in X_{val}$ 를 통해 받고, $(v_1, \ldots, v_{\max\{0,m-\sigma\}})$를 공개적으로 받는다.

R은 다음을 만족하는 $\max\{\sigma, m\}$차의 다항식 $g(x) \in Q[x]$를 찾는다.

$$g(\ ) = \begin{cases} s & y \in Y_{val} \\ u_{\ -m} & x_{\ -m} \in X_{val} \\ v_{\ -l-m} & = l+m+1, \ldots, l+m+\max\{0, m-\sigma\} \end{cases}$$

만약 R이 이러한 $g(x)$를 찾는데 실패하면 Y에 속하는 모든 채널을 통해 "FAIL"을 S에게 보낸다.

5. S가 "FAIL"을 전송한 회수가 ρ 이하인 채널을 통해 "FAIL"을 받으면 단계 1 에서 5 를 통해 얻은 모든 정보를 R에게 공개적으로 보낸다.

그렇지 않을 경우, S는 ("*SUCCEED*", $r + M$)을 공개적으로 전송하고 **1waySMT**$(X, \sigma, \max\{0, \rho - m\}, Q, M)$을 수행한 후, 종

료한다.

6. R이 $("SUCCEED", M')$을 공개적으로 전달받은 경우, R은 $M = M' - g(0)$ 을 계산하거나 S가 보낸 **1waySMT** 정보를 이용해 M을 얻고 종료한다.

그렇지 않을 경우, R은 S가 공개적으로 보낸 정보를 통해 faulty 채널을 찾아내어 이를 X_{val} 나 Y_{val} 에서 제거한다.

7. S와 R은 **GeneralSMT** $(X, Y, \sigma, \rho, Q, \mathbf{1waySMT}, M, X_{val}, Y_{val})$ 를 재귀적으로 수행한다.

소정리 3.1 **GeneralSMT**는 $(\sigma, \rho) - SMT$의 *secrecy* 조건과 *reliability* 조건을 만족한다.

증명 생략

이제 n개의 양방향 채널도 포함하는 경우를 생각하자. 이때에는 **GeneralSMT**에서 공개적으로 메세지를 전송할 때에는 양방향 채널을 $S \to R$ 채널로 사용하고 나머지의 경우에는 $R \to S$ 채널로 사용하여 **GeneralSMT**를 시뮬레이션할 수 있다. 따라서 우리는 다음의 정리를 얻는다.

정리 2 $l+n \geq 2\rho+1, l+m+n \geq \sigma+\rho+1, l+2m+2n \geq \sigma+2\rho+1$이면 $(\sigma, \rho) - SMT$를 위한 효율적인 알고리즘이 존재한다.

4 하한 증명

이 절에서는 $(\sigma, \rho) - SMT$가 가능하기 위한 채널 수의 하한을 고려한다. Dolev 등은 단방향 채널들로만 이루어진 경우와 양방향 채널로만 이루어진 경우에 $(\sigma, \rho) - SMT$가 가능하기 위한 채널 수의 하한을 보였다. 다음은 그들의 결과를 본 논문의 표기를 따라 다시 적은 것이다.

정리 3 (Dolev *et al.*) *1.* $S \to R$ 채널만 있는 경우

$l \geq \sigma + 2\rho + 1$ 은 *1-way* $(\sigma, \rho) - SMT$가 가능하기 위한 필요충분조건이다.

2. $S \leftrightarrow R$ 채널만 있는 경우

$n \geq 2\rho + 1, n \geq \sigma + \rho + 1$은 *2-way* $(\sigma, \rho) - SMT$가 가능하기 위한 필요충분조건이다.

본 논문에서는 $S \to R$ 채널, $R \to S$ 채널, 그리고 $S \leftrightarrow R$ 채널을 모두 포함하는 모델에 대한 하한을 보인다.

소정리 4.1 $l+n \leq 2\rho$ 이면 *reliability* 를 보장하는 메시지 전송 프로토콜이 존재하지 않는다.

증명 생략

소정리 4.2 $l+m+n \leq \sigma+\rho$ 이면 $(\sigma, \rho) - SMT$는 불가능하다.

증명 생략

소정리 4.3 $l+2m+2n \leq \sigma+2\rho$이면 $(\sigma, \rho) - SMT$는 불가능하다.

증명 생략

따라서 정리 2와 소정리 4.1,4.2, 그리고 4.3에 의해 우리는 다음 정리를 얻는다.

정리 4 $l+n \geq 2\rho+1, l+m+n \geq \sigma+\rho+1, l+2m+2n \geq \sigma+2\rho+1$는 $(\sigma, \rho) - SMT$ 를 위한 필요충분조건이다.

5 향후연구과제

모든 채널이 양방향으로 통신이 가능한 네트웍에서는 전송자와 수신자를 분리하는 vertex cut V의 원소 개수가 $\sigma + \rho + 1$일 경우 [6]의 증명을 확장하여 $(\sigma, \rho) - SMT$가 불가능함을 보일 수 있음을 쉽게 관찰할 수 있다. 따라서 이 경우 $(\sigma, \rho) - SMT$가 가능한 경우 항상 단순화된 모델의 채널을 시뮬레이션할 정점 분리 경로의 존재를 보장할 수 있다. 이와는 달리 채널에서 정보가 한 쪽으로만 전송되는 방향 네트웍에서는 이와 같은 주장이 성립하지 않는다. 일반적인 방향 네트웍에서 안전한 통신이 가능하기 위한 타이트한 하한을 찾는 것은 앞으로의 연구 과제이다.

참고 문헌

[1] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th ACM STOC*, pages 1–10, May 1988.

[2] M. Burmester and Y. Desmedt. Secure communication in an unknown network with byzantine faults. *Eletronic Letters*, 34(8):741–742, 1998.

[3] M. Burmester, Y. Desmedt, and G. Kabatianski. Trust and security: A new look at the byzantine generals problem. In *DIMACS series in discrete mathematics and theoretical computer science 38*, pages 75–83, 1998.

[4] C. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditional secure protocols. In *Proceedings of the 20th ACM STOC*, pages 11–19, May 1988.

[5] B. Chor, S. Goldwasser, S. Micali, and A. Wigderson. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Proceedings of the 26th IEEE FOCS*, pages 383–395, May 1985.

[6] D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *JACM*, 40(1):17–47, 1993.

[7] M. Franklin and N. Wright. Secure communication in minimal connectivity models. In *Advances in Cryptology, Proceedings of EUROCRYPT'98*, pages 346–360, 1998.

[8] M. Franklin and M. Yung. Secure hypergraphs: Privacy from partial broadcast. In *Proceedings of the 27th ACM STOC*, pages 36–44, 1995.

[9] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the 21th ACM STOC*, pages 73–85, 1998.

[10] H. Sayeed and H. Abu-Amara. Efficient perfectly secure message transmission in synchronous networks. *Information and Computation*, 126:53–61, 1996.

[11] A. Shamir. How to share a secret. *CACM*, 22(6):17–47, 1979.

[12] Y. Wang and Y. Desmedt. Secure communication in broadcast channels: The answer to franklin and wright's question. In *Advances in Cryptology, Proceedings of EUROCRYPT'99*, pages 446–458, 1998.