논문 20-45-08-03 The Journal of Korean Institute of Communications and Information Sciences '20-08 Vol.45 No.08
https://doi.org/10.7840/kics.2020.45.8.1338

악의적 재밍 환경의 무선 센서 네트워크에서 랜덤 액세스 메시지 길이의 최적화

정 대 교◆, 박 철 순*, 김 동 우°

Optimal Message Length in Random Access for Wireless Sensor Networks Under Jamming Attacks

Dae-Kyo Jeong◆, Cheol-Sun Park*, Dongwoo Kim°

요 약

무선 센서 네트워크(wireless sensor network)의 랜덤 액세스(random access, RA)가 진행될 때 메시지의 길이는 랜덤 액세스 처리량(throughput)에 영향을 준다. 본 논문에서는 악의적인 재밍(jamming)이 전개되고 있는 환경에서 무선 센서 네트워크의 랜덤 액세스 처리량을 분석하고 최적의 메시지 길이를 구한다.

Key Words : Random access, optimal message length, throughput, jamming attack

ABSTRACT

When random access (RA) in a wireless sensor network (WSN) is attacked by hostile jammers, the throughput of the RA is severely degraded if ordinary RA parameters are being used. In this letter, we suggest changing the message length used in RA if jamming exists. We provide a method to find an optimal message length and evaluate how much RA throughput gain is achieved with a numerical investigation in jamming environments. It shows that we achieve about 32-54% improvement in the throughput for moderate jamming environments.

Ⅰ. 서 론

최근 지능적이고 초소형의 무선 센서 장치가 광범위하게 개발됨에 따라 무선 센서 네트워크는 방위, 의료, 각종 산업에서 활용되고 있다. 무선 센서 네트워크는 무선 주파수 통신 링크를 통하여 수많은 무선 센서 장치들의 상호연결로 구성된다. 이러한 무선 주파수를 이용하는 통신 링크는 원하지 않는 간섭 신호와 잡음에 의해 신호의 품질이 급격하게 저하되는 특징을 가지고 있다. 따라서 악의적인 재밍 신호는 무선 센서 네트워크에 심각한 위협 요인이 될 수 있다[1].

이에 따라, 재밍 공격을 탐지하는 다양한 기술들에 대한 연구[2]가 이루어졌으며, 우호적인 재밍을 도입하는 연구[3]까지 활발히 이루어지고 있는 추세이다. 특히, 논문 [4]에서는 무선 센서 네트워크 환경에서 재밍 공격이 전개 될 때 랜덤 액세스의 처리량과 지연 성능을 분석한 연구가 이루어 졌다. 본 논문은 재밍이 전개되고 있는 환경에서 랜덤 액세스의 처리량을 분석하고, 처리량을 최대로 할 수 있는 최적의 메시지 길이 구하였다. 본 논문의 수치 실험은 제안한 메시지 길이를 사용하면, 재밍이 없는 환경에서 적용된 메시지 길이를 사용했을 때보다 보통의 재밍 환경에서 약 32~54% 정도의 처리량 증가를 얻을 수 있다는 걸 보여준다.

Ⅱ. 시스템 모델

그림 1은 본 논문에서 가정한 무선 센서 네트워크의 랜덤 액세스 및 공격자의 재밍 공격 과정을 나타낸 그림이다. 센서 노드는 메시지 신호를 보내기 전에 프리앰블(preamble) 신호를 헤더 센서에게 보낸다. 이때 한 개의 슬롯(slot)이 소요된다. 보내진 프리앰블 신호를 헤더 센서가 수신하게 되면 응답 신호(acknowledge signal)를 센서 노드에게 보내게 된다. 응답 신호를 수신한 센서 노드는 프리앰블 신호를 보

※ 이 연구는 방위사업청 및 국방과학연구소의 재원에 의해 설립된 신호정보 특화연구센터 사업의 지원을 받아 수행되었음.
◆ First Author : (0000-0001-5977-4156)Hanyang University Research Institute of Engineering & Technology, daekyo12@hanyang.ac.kr, Post-Doc., 정회원
° Corresponding Author : (0000-0001-5541-5738)Hanyang University Division of Electrical Engineering, dkim@hanyang.ac.kr, 정교수, 정회원
* Agency for Defense Development, csun1402@add.re.kr
논문번호 : 202003-071-B-LU, Received March 25, 2020; Revised May 11, 2020; Accepted May 11, 2020

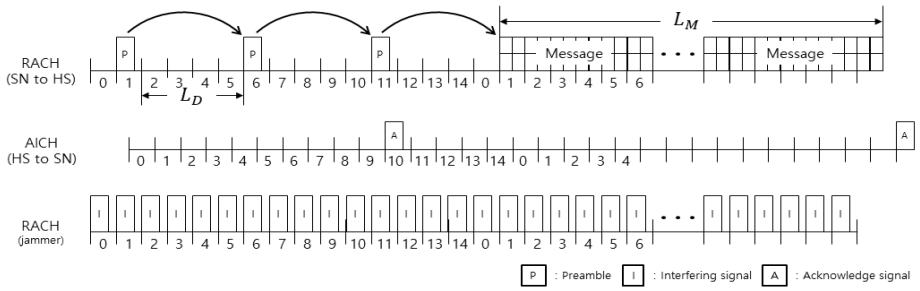

그림 1. 무선 센서 네트워크의 랜덤 액세스 과정 및 공격자의 재밍 공격
Fig. 1. Random access process and jamming attack in wireless sensor networks

내고 난 다음 슬롯으로부터 L_D 슬롯만큼 지연한 후 메시지 신호를 L_M 슬롯 동안 전송을 하고 메시지 수신에 성공하면 헤더 센서는 센서 노드에게 L_D 슬롯 안에 응답 신호를 보내고 랜덤 액세스 과정은 종료된다. 그러나 센서 노드가 보낸 프리앰블 신호 또는 메시지 신호에 대한 응답 신호를 수신하지 못한 경우 센서 노드는 L_D 슬롯만큼 지연한 후 다시 프리앰블 신호를 보낸다. 공격자는 매 슬롯 마다 재밍 신호를 발생시킨다.

Ⅲ. 무선 센서 네트워크의 랜덤 액세스 처리량 분석

3.1 프리앰블과 메시지 신호의 파워 캡쳐

프리앰블 신호를 P, 메시지 신호를 M으로 나타내고, 이를 통칭할 때 $U \in \{P, M\}$로 표기하고, 재밍 신호는 J로 나타낸다고 하자. P_U는 프리앰블 혹은 메시지 신호의 수신파워, P_J는 재밍 신호의 수신파워, σ^2는 잡음 파워, 그리고 β_U는 프리앰블 및 메시지 신호를 성공적으로 수신하기 위해 필요한 신호 대 간섭 잡음비라 하자. 각각의 수신파워가 평균 μ_U인 지수분포를 따른다고 가정하면, 헤더 노드가 각 슬롯에서 프리앰블 신호 및 메시지 신호의 수신에 성공할 확률은 아래 식 (1)과 같이 구할 수 있다[4].

$$\begin{aligned} D_U &= \Pr\left\{\frac{P_U}{P_J+\sigma^2} \geq \beta_U\right\} \\ &= \int_0^\infty e^{-\frac{\beta_U(x+\sigma^2)}{\mu_U}} \frac{e^{-\frac{x}{\mu_J}}}{\mu_J} dx \\ &= \frac{e^{-\frac{\beta_U\sigma^2}{\mu_U}}}{\mu_J}\left(\frac{\beta_U}{\mu_U}+\frac{1}{\mu_J}\right)^{-1}. \end{aligned} \tag{1}$$

3.2 무선 센서 네트워크의 랜덤 액세스 처리량

랜덤 액세스에는 세 가지의 사건이 존재한다. 프리앰블 전송을 실패할 경우는 $1-D_P$의 확률로 발생하고, 1 슬롯이 소모된다. 프리앰블 전송에 성공하고, 메시지 전송에서 성공 혹은 실패할 경우는 각각 $D_P D_M^{L_M}$와 $D_P(1-D_M^{L_M})$의 확률로 발생하고, 두 경우 모두 $1+L_D+L_M$ 슬롯이 소모된다. 그리고 각 사건과 사건사이는 L_D 슬롯만큼 지연이 발생한다. 랜덤 액세스를 시도해서 총 t번 실패하고 $t+1$번 때 성공하였고 랜덤 액세스에 사용된 총 슬롯 수분에 메시지에 사용된 슬롯을 처리량(throughput)이라고 가정하면, 무선 센서 네트워크에서 랜덤 액세스에 대한 평균 처리량(throughput)은 식 (2)와 같이 나타낼 수 있다[4].

$$\begin{aligned} T(L_M) = &\sum_{t=0}^{\infty}\sum_{a=0}^{t}\binom{t}{a}(1-D_P)^{t-a}\left\{D_P(1-D_M^{L_M})\right\}^a D_P D_M^{L_M} \\ &\times \frac{L_M}{t-a+(1+L_D+L_M)(a+1)+L_D(t+1)}. \end{aligned} \tag{2}$$

Ⅳ. 메시지 길이 최적화

메시지의 길이가 길어지면 메시지의 절대적 양은 증가하나 수신에 성공해야 될 슬롯이 증가함에 따라 재밍이 전개되는 환경에서 헤더 센서가 메시지 수신에 실패할 확률이 높아진다. 그러므로 최적의 메시지 길이를 설정해야 한다. 최적의 메시지 길이를 찾기 위해 식 (2)의 랜덤 액세스의 처리량을 미분하면 다음과 같은 식을 얻는다.

$$\Lambda(L_M)=\frac{dT}{dL_M}=\sum_{t=0}^{\infty}\sum_{a=0}^{t}\binom{t}{a}\frac{(1-D_P)^{t-a}D_P^{a+1}}{\delta}$$
$$\times\Big[D_M^{L_M}\left(1-D_M^{L_M}\right)^a+D_M^{L_M}L_M\ln(D_M)\left(1-D_M^{L_M}\right)^a$$
$$-\frac{D_M^{L_M}L_M\left(1-D_M^{L_M}\right)^a(a+1)}{\delta}$$
$$-D_M^{2L_M}L_M a\ln(D_M)\left(1-D_M^{L_M}\right)^{a-1}\Big], \quad (3)$$

여기서 $\delta=t-a+(1+L_D+L_M)(a+1)+L_D(t+1)$ 이다. $\Lambda(L_M)=0$이 되는 L_M을 찾고 L_M은 양의 정수를 가져야 하므로 찾은 L_M의 올림과 버림 값을 각각 랜덤 액세스의 처리량에 대입하여 큰 처리량을 가지는 값을 최적의 L_M으로 결정하면 최적인 L_M에 대한 표현은 다음과 같다.

$$L_M^*=\arg\max\left(T\left(\lceil\Lambda^{-1}(0)\rceil\right),T\left(\lfloor\Lambda^{-1}(0)\rfloor\right)\right). \quad (4)$$

V. 수치적 결과

본 논문에서 수치적 결과를 관찰하기 위하여 $\sigma^2=1$, $\beta_U=0.5$, $L_D=4$로 가정하였다. 그림 2는 식 (4)를 이용하여 재밍 신호의 평균 수신 파워 μ_J에 대하여 최적의 L_M을 나타낸 것이다. 이 그림을 통해서 알 수 있듯이 μ_J가 0일 때의 최적 메시지 길이가 RA신호의 파워 증가에 따라 3, 5, 6인 것에 비해, μ_J가 2일 때는 1, 2, 3으로 감소한다. 재밍 신호의 평균 수신 파워가 증가함에 따라, 혹은 프리앰블이나 메시지 신호의 파워가 감소할수록 최적 메시지의 길이는 감소해야 한다.

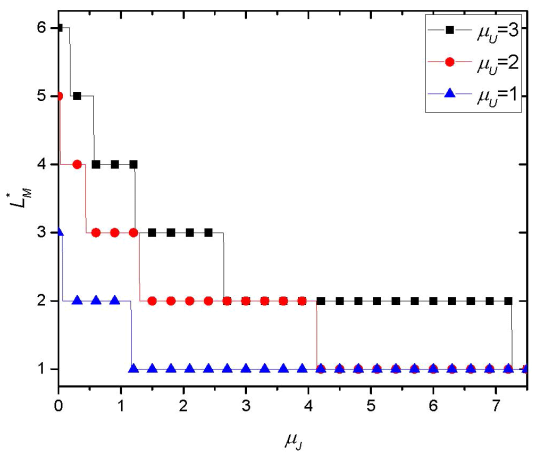

그림 2. 재밍 신호의 평균 파워에 따른 최적 메시지 길이
Fig. 2. The optimal length of the message signal for the average power of the jamming signal

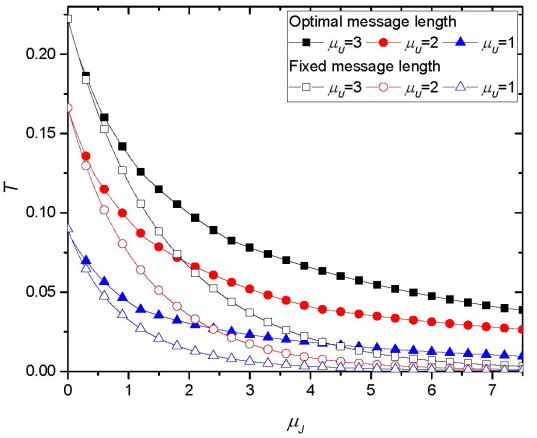

그림 3. 최적 메시지 길이를 사용한 재밍 신호의 평균 파워에 따른 랜덤 액세스의 처리량
Fig. 3. Throughput of random access using the optimal length of the message signal for the average power of the jamming signal

그림 3은 식 (4)에서 구한 최적 메시지 길이를 식 (2)에 대입하여 구한 랜덤 액세스의 처리량과 재밍이 없는 환경에서 구한 최적 메시지 길이(그림 3에서 fixed message length라고 표현)를 적용한 처리량을 비교해본 그림이다. 재밍 신호의 평균 파워가 증가할수록 재밍 신호를 고려한 최적 메시지 길이를 사용한 것과 재밍이 없는 환경에서 구한 최적 메시지 길이 3, 5, 6을 사용한 것의 처리량 차이는 평균 재밍 파워가 증가함에 따라 점점 증가하는 것을 확인할 수 있다. $\mu_J=2$를 고려하면, 재밍 신호를 고려한 메시지 길이의 선택이 처리량에 있어서 $\mu_U=3$에서는 약 51%, $\mu_U=2$에서는 약 91%, $\mu_U=1$에서는 약 121% 증가한다. $\mu_J=7.5$로 재밍 시도가 크게 증가하여 최적메시지 길이가 1로 설정되는 경우에도 μ_U의 크기에 따라 11-16배의 처리량 증가를 얻을 수 있다.

VI. 결 론

본 논문에서는 재밍이 존재하는 환경에서 무선 센서 네트워크의 랜덤 액세스 처리량을 분석하고 처리량 관점에서 메시지 길이를 최적화하였다. 재밍 신호의 평균 파워가 증가할수록 최적 메시지 길이는 감소하는 것을 수치적 결과를 통하여 확인하였다. 그리고 재밍을 고려한 최적 메시지 길이를 사용하면 그렇지 않을 때 보다 상당한 처리량의 증가를 얻을 수 있다는

것을 알 수 있다. 실제 무선 센서 네트워크에서는 재밍 신호 이외의 간섭 신호가 일정량으로 분포하므로, 본 논문의 최적 메시지 길이에 의한 처리량 향상 결과는 실제보다 과대하게 평가되었을 수 있다. 이에 대한 추가 연구가 필요하고, 또한 재밍 파워를 항상 모니터링 하는 시스템과 이를 이용하여 적응적으로 메시지 길이를 변화시키는 시스템에 대한 연구도 추가적으로 필요하다.

References

[1] J. Kim, E. Kim, and J. Lee, “Jamming technology in military communications,” *KICS Info. & Commun. Mag.*, vol. 26, no. 3, pp. 32-40, Feb. 2009.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” in *Proc. 6th ACM Int. Symp. Mobile ad hoc Netw. and Comput.*, pp. 46-57, Urbana-Champaign, IL, USA, May 2005.

[3] D.-K. Jeong, I. Kim, and D. Kim, “Optimal pricing and power allocation for collaborative jamming with full channel knowledge in wireless sensors networks,” *Sensors*, vol. 17, no. 11, pp. 1-18, Nov. 2017.

[4] D.-K. Jeong, J.-H. Wui, and D. Kim, “Random access performance of distributed sensors attacked by unknown jammers,” *Sensors*, vol. 17, no. 11, pp. 1-17, Nov. 2017.