Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.6, Dec. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.6.975

3D 환경을 고려한 무선 센서 네트워크의 키 사전 분배 기법 실험 연구*

윤 혜 민,[1†] 신 수 연,[2] 권 태 경[3‡]
[1,2,3]연세대학교 정보대학원 정보보호 연구실 (대학원생, 박사 후 연구원, 교수)

An Experimental Study on Pairwise Key Pre-distribution Schemes of Wireless Sensor Networks Considering 3D Environments*

Hyemin Yun,[1†] Sooyeon Shin,[2] Taekyoung Kwon[3‡]
[1,2,3]Information Security Lab, GSI, Yonsei University
(Graduate student, Post-Doc, Professor)

요 약

무선 센서 네트워크 보호를 위해 다양한 키 분배 및 관리 기법들이 제안되었지만 대부분 2차원(2D) 환경만을 고려한 시뮬레이션 및 성능 실험을 수행하였다. 본 논문에서는 실제 환경 3차원(3D) 지형적 특성이 키 사전 분배 기법에 미치는 영향을 알아보기 위해 Full Pairwise (FP) 기법, Random Pairwise (RP) 기법, 두 가지를 결합한 Full and Random Pairwise (FRP) 기법의 성능을 2D 환경과 3D 환경에서 비교분석한다. 실험을 위해 Blender와 Unity 등의 3차원 그래픽 툴과 네트워크 시뮬레이터인 NS-3를 활용한다. 결과적으로, 실제 3차원 지형에 따라 각 기법의 성능에 차이가 있음을 확인하였으며 배치 오류를 고려한 위치 기반 분배 기법인 FRP가 여러 측면에서 가장 효율성이 높음을 확인하였다.

ABSTRACT

To protect wireless sensor networks (WSNs), various key distribution and management schemes have been proposed. However, most of them conducted simulations and experiments for performance evaluation by considering only the two-dimensional (2D) environments. In this paper, we investigate the effect of real-world three-dimensional (3D) topographic features on the key pre-distribution schemes for WSNs. For this purpose, we analyze and compare the performance of three pairwise key pre-distribution schemes in 2D and 3D environments: full pairwise (FP), random pairwise (RP), and full and random pairwise (FRP) schemes. For the experiments, we employ a network simulator NS-3 and 3D graphic tools such as Blender and Unity. As a result, we confirm that there was a difference in the performance of each scheme according to the actual 3D terrain and that the location-based FRP that considers deployment errors, has the highest efficiency in many aspects.

Keywords: Wirless sensor networks, Pairwise key pre-distribution, 2D, 3D, NS-3

Received(09. 03. 2020, Modified(11. 04. 2020), Accepted(11. 05. 2020)

* 본 연구는 고려대 암호기술 특화연구센터(UD170109E D)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

† 주저자, 2019521120@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

I. 서 론

무선 센서 네트워크(Wireless Sensor Networks, WSNs)는 계산, 메모리 및 통신 등의 자원이 제약적인 소형 저전력 센서 노드들로 구성되며, 주변 환경을 모니터링하고 정보를 수집 및 처리하는 다양한 환경, 군사 모니터링 및 헬스 케어 등의 분야에서 사용된다. WSNs는 센서 노드의 무선 통신 사용, 한정된 자원, 군사 및 적대적 지역 배치 등으로 여러 공격에 취약하여 이를 해결하기 위해 다양한 암호 키 분배 및 관리 기법들이 제안되었다[1]. 이 중 pairwise 키 사전 분배는 각 노드 쌍이 유일한 키를 가지며 다른 노드들의 신원을 확인할 수 있고 링크 손상 및 노드 캡쳐 등으로 인한 키 손상을 최소화할 수 있으며 높은 복원력을 지원하여 효율적으로 작동한다. 또한 노드 위치 정보 및 지형적 특성은 통신 및 에너지 효율, 네트워크 수명 등 다양한 부분에 영향을 미친다[2]. 위치 정보를 활용한 대부분의 키 분배 및 관리 기법들은 2차원(2D) 위치 정보만을 활용해 성능 및 효율성을 측정하는데, 실제로 WSNs가 사용될 지역의 지형 및 지물이 네트워크 배치 과정 등에 영향을 크게 미치는 요소이나 반영하지 못한다는 문제점이 발생한다. 또한 3D 환경에 노드가 배포될 경우 노드의 배치 오류 문제가 발생할 수 있기 때문에 이를 개선하기 위해서는 3차원(3D) 위치 정보를 고려해야 한다.

본 논문에서는 3D 지형적 특성이 키 사전 분배 기법의 성능에 미치는 영향을 알아보기 위해 2D와 3D 환경을 고려하여 실험을 진행한다. 특히 배치 오류에 대해 저항성을 가지는 pairwise 키 사전 분배 기법에 초점을 두었으며 이 중 결정론적인 기법인 Full Pairwise (FP) 기법[3], 확률론적 기법인 Random Pairwise (RP) 기법[3]과 FP와 RP의 장점 및 노드 위치 정보를 활용하는 하이브리드 방식인 Full and Random Pairwise (FRP) 기법[4]의 성능을 비교 분석한다.

II. Pairwise 키 사전 분배 기법

2.1 FP 키 사전 분배 기법

FP[3]은 네트워크에 존재하는 모든 노드들이 다른 노드들과 통신하기 위해 pairwise 비밀 키를 저장한다. 네트워크 크기가 n인 경우 각 센서 노드들은 자신 이외의 다른 모든 노드들과의 통신을 위해 $n-1$ 개의 키가 필요하며 전체 네트워크를 위해서는 총 $n(n-1)/2$ 개의 pairwise 키가 필요하다. 키 연결률은 한 노드가 주변의 노드들과 1개 이상의 키를 공유할 확률로 키 연결률이 1이라는 의미는 네트워크 전체의 노드들이 모두 주변 노드들과 공유키를 가지고 안전한 링크를 확립한다는 것을 의미한다. FP는 이론상 키 연결률은 1이며, 단일 노드에 저장되어있는 키가 노출되어도 다른 노드들 간 통신에는 영향을 끼치지 않아 높은 저항성을 가진다. 그러나 네트워크 규모가 증가하면 각 노드에 저장되어야 하는 키와 전체 네트워크에서 필요로 하는 키의 크기 및 개수가 증가하므로 메모리 비용도 급증하는 문제점이 존재한다.

2.2 RP 키 사전 분배 기법

RP[3]은 각 센서 노드가 주변 노드와 키 공유를 통해 안전한 링크를 확립할 확률 p를 이용하여 FP가 가지는 메모리 비용 문제를 해결하기 위해 제안된 기법이다. 각 노드는 확률 p와 네트워크 크기 n을 바탕으로 전체 키 풀에서 랜덤하게 선택한 n_p개의 pairwise 키를 저장한다. 공유한 키를 탐색하기 위해 각 노드들이 본인의 노드 ID를 브로드캐스트하고 통신 범위 내에 존재하는 이웃 노드들 중 공통으로 가진 키를 저장한 노드들이 응답하면서 안전한 링크를 확립한다. RP는 확률 $p=0.5$, 노드 개수 $x=100$이면 각 노드 당 키 링 사이즈가$(x\times p)-1 = 49$이고, FP는 키 링 사이즈가 $x-1 = 99$가 된다. 따라서 FP보다 메모리 비용 측면에서 효율적이며 노드 캡쳐 공격에 대한 면에서 저항성이 우수하다. 하지만 확률 p에 따라 키 연결률이 매우 낮아지는 단점이 존재한다.

2.3 FRP 키 사전 분배 기법

FRP[4]는 FP와 RP를 결합한 하이브리드 방식으로 기존 기법의 한계점인 배치 오류에 대한 저항성을 가지며 동시에 통신 간섭으로 인한 키 연결성과 네트워크 복원력 문제를 개선하였다. 또한 키 확립 이후 노드 캡쳐 공격 발생 시에도 완벽하게 네트워크를 회복할 수 있으며 적은 메모리 및 통신비용, 높은 키 연결률, 안전성, 확장성을 모두 확보하였다. 총 3단계로 동작하며, 먼저 노드 배포 전에 배치될 그리

드 좌표에 따라 키 개수를 계산하고 이에 맞는 키 링을 키 풀에서 도출하여 저장하는 키 사전 분배 단계를 거친다. 이후 동일 영역에 있는 노드는 FP, 인접 영역에 있는 노드는 RP로 키를 공유하는 공유키 발견 단계를 수행한다. 여기서 키 링 사이즈인 m을 계산하기 위해 먼저 p_c와 r_a를 이용해 $p' = p_c - (1-r_a)/r_a$ 를 계산한다. p_c는 인접 영역에 있는 이웃 노드와 랜덤한 pairwise 키를 설정하기 위해 사전에 정의한 확률이며 r_a는 임의로 정한 노드의 통신 범위가 인접 영역에 속할 확률, p'은 인접 영역의 두 노드가 연결될 확률이다. p_c=0.5, r_a=0.75로 가정했을 때 p'은 0.33이다. 또한, 동일 지역에서는 $x-1$개의 노드와 키를 공유하며 α가 인접 지역의 개수일 때 노드 위치에 따라 $\alpha x p' (\alpha \in 3,5,8)$개의 노드와 키를 공유한다. 각 노드는 α = 8일 때 최대 개수의 노드와 키를 공유할 수 있으므로 최대 $m = n + 8\lfloor xp' \rfloor - 1$ 의 키 링이 생성된다. p' = 0.33, x = 100일 때 키 링 사이즈는 각 노드 당 $m/x \fallingdotseq 3.63$으로 FP, RP와 비교했을 때 메모리 비용 측면에서 훨씬 효율적임을 알 수 있다. 마지막으로 2단계에서 키를 확립하지 못한 경우 이미 키를 확립한 이웃 노드의 도움을 받아 경로키를 확립하는 단계로 이루어진다. 결론적으로 FRP는 FP와 RP에 비해 메모리 비용 측면에서 높은 효율성을 가진다.

III. 실험 방법 및 결과

본 실험에서는 2D 환경을 가정해 시뮬레이션이 이루어진 기존의 키 사전분배 기법[1]들의 성능이 실제 지형에서는 어떤 영향을 받는지 알아보기 위해 실제 지형을 고려한 3D 환경에서 성능을 분석한다.

3.1 실험 방법

NS-3[5] 시뮬레이션을 통해 2D 환경과 3D 환경을 모두 고려하여 세 가지 키 사전분배 기법의 성능을 비교분석하였으며 Table 1은 실험 환경을 보여준다. RP와 FRP의 연결 확률 p_c는 0.5로 가정하였고 r_a는 0.75로 가정하였다. FRP의 경우에는 그리드 기반의 위치 정보를 활용하므로 전체 배포 지역을 4x4 그리드로 분할하고 그리드 당 노드 수를 9개로 가정하였다.

Table 1. Experimental environment

OS	Ubuntu 18.04.3
CPU	Intel i7-8700 (3.20GHz)
Memory	13.71 GB RAM
Number of nodes	144
Deployment area	$100m^3$
Transmission range of node	$20m$

3D 환경의 경우에는 여러 가지 유형의 실제 지형을 고려하기 위해 산(mountain), 협곡(valley), 평지(plain), 세 가지 지형을 선택하였다. 실제 지형 이미지를 획득하기 위해 terrain.party 사이트를 활용하였으며[6] 3D 지형으로 변환하기 위해 Blender 2.82[7]를 활용했다. Blender를 사용하여 나온 결과물 중 raw 파일을 Unity[8]에 로드하고 노드 생성 후 지형에 배포하였고 이 때 노드가 지형에 닿을 때 x, y, z 좌표를 텍스트 정보로 변환 저장하여 배포 후 노드 위치 데이터를 획득했다.

Fig. 1.의 왼쪽은 지형별 Blender로 변환한 3D 지형 이미지를 보여주며 오른쪽은 Unity에서 지형별 노드 배포의 예를 보여준다. 2D 환경의 경우에는 Unity의 단순한 사각형 평면에 노드를 배포 후 위치 데이터를 획득하였다. 두 환경 모두 노드별로 특정 위치에서 공중 배포하는 것으로 가정하였다.

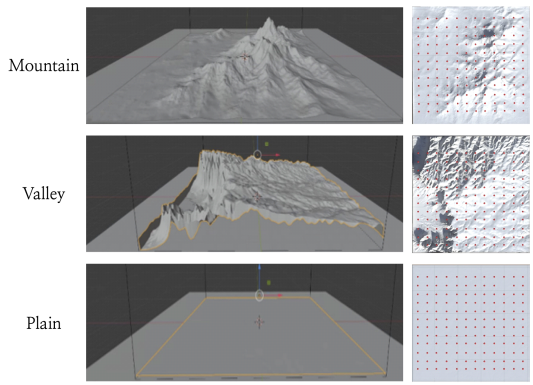


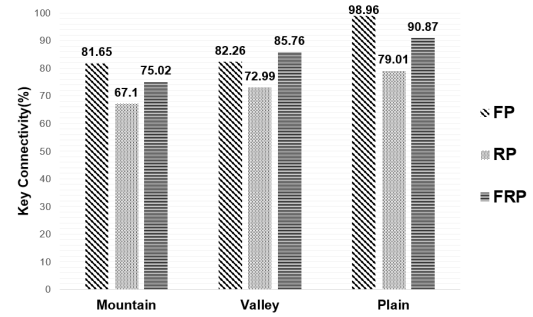
Fig. 1. 3D terrain and node deployment

1) FP, RP 기법은 위치 기반을 고려하지 않은 기법으로 실험 진행

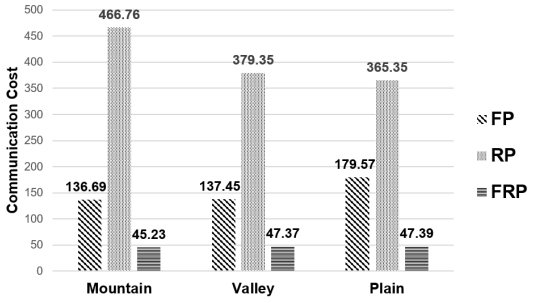
3.2 실험 결과

NS-3 시뮬레이션을 통해 2D 및 3D 환경에서의 FP, RP, FRP의 성능을 분석하였다. 획득한 2D 및 3D 좌표는 모두 NS-3 시뮬레이터 내에서 동일한 소스 코드로 처리하였고, 성능 지표는 전체 키 연결률(key connectivity)과 통신비용(communication cost)을 사용하였다. 키 연결률은 키 확립 후 연결된 노드의 비율로 전체 키 연결률을 의미한다. 통신비용은 배포 후 키 확립 동안 각 노드가 주변 노드와 주고받은 통신 메시지를 카운트 한 후 노드 별 평균값을 계산한 값이다. Pairwise 키 사전분배 기법은 계산 비용이 별도로 발생하지 않으며 통신비용이 에너지 효율성에 큰 영향을 미친다. 일반적으로 데이터 전송 중 에너지 소모가 매우 크기 때문에[8] 통신비용은 에너지 효율성과 밀접한 관계를 가지는 중요한 성능 지표다. 키 연결률은 높을수록, 통신비용은 낮을수록 성능이 우수한 것을 의미하며 메모리 비용은 이론적으로 계산 가능하여 측정하지 않았다.

Table 2는 2D 환경에서 각 기법의 NS-3 시뮬레이션을 10회 반복한 결과의 평균이며, Table 3는 3D 환경에서 NS-3 시뮬레이션을 10회 반복한 평균, Fig. 2는 3D 환경에서 3가지 지형별로 각 기법의 NS-3 시뮬레이션을 10회 반복하여 측정한 평균 키 연결률(Fig. 2(a))과 통신비용(Fig. 2(b))이다.



(a) Key connectivity by terrain



(b) Communication cost by terrain

Fig. 2. Performance test by terrain

3D 환경에서의 FP, RP, FRP의 키 연결률 평균은 각 87.62%, 73.03%, 83.88%이며 통신비용 평균은 각 151.24, 403.82, 46.66로 2D 환경과 비교했을 때 키 연결률과 통신비용 모두 감소하였다. 이는 실제 지형을 고려했을 때 지형이 직접적으로 Pairwise 키 사전분배 기법에 영향을 미치며 통신비용은 성능이 증가한 것이 아닌 지형이 데이터 전송에 영향을 준다는 것을 의미한다. 이 부분은 모든 기법에서 평지보다 산과 협곡 지형에서 통신비용이 감소하는 것을 통해 확인할 수 있다. 지형별로 비교했을 때는 평지보다 산과 협곡에서 성능이 좋지 않았으며, 기법별로 비교했을 때는 FP가 키 연결률이 가장 높으나 통신비용이 상대적으로 높은 편이었다. RP는 2D 환경과 마찬가지로 지형과 상관없이 가장 낮은 성능을 보였으며 FRP는 상대적으로 높은 키 연결률을 가지고 메모리 비용도 낮으며 통신비용은 FP의 3배, RP의 8배 이상 낮아 에너지 효율성 측면에서 매우 우수함을 알 수 있다. 2D 환경[Table 2]와 3D 환경[Table 3]의 평균값을 비교했을 때, 모든 기법에 대하여 2D 환경의 키 연결률이 더 높았고, 통신 횟수는 3D 환경에서의 성능이 더 좋았다. 또한 2D 환경과 3D 환경의 평지[Table 3]에서의 성능을 비교하였을 때 FP를 제외한 두 기법에서 키 연결률은 평지에서 더 높았으며 통신 횟수는 세 기법에서 모두 평지에서 성능이 더 우수함을 확인

Table 2. Performance on 2D environment

Performance Metric	FP	RP	FRP
Key connectivity(%)	99.75	75.97	89.23
Communication cost	175.93	467.57	47.55
Storage size(byte)	1165.1	1157.07	227.09

Table 3. Performance on 3D environment

Performance Metric	FP	RP	FRP
Key connectivity (%)	82.26	72.99	85.76
Communication cost	137.45	379.35	47.37
Storage size(byte)	1150.89	1142.89	209.67

할 수 있다.

IV. 결 론

본 논문에서는 WSN이 배포되는 실제 지형이 Pairwise 키 사전 분배 기법의 성능에 미치는 영향을 알아보기 위해 NS-3 시뮬레이터를 활용하여 실험하였다. 3가지 특징적인 지형을 고려하여 3D 환경에서 FP, RP, FRP의 키 연결률 및 통신비용을 측정한 결과, 지형에 따라 성능에 차이가 있고 그 중 FRP가 실제 지형에서 가장 좋은 효율성을 가짐을 확인하였다. 또한, 2D 환경과 3D 환경에서의 성능을 비교한 결과 3D 환경에서 키 연결률은 약간 낮으나 통신 횟수 성능이 훨씬 우수하므로 실제 환경에서도 위 기법들을 유용하게 사용할 수 있을 것으로 판단된다. 향후, 3D 환경에서의 배치 오류 및 지형에 대한 영향에도 성능과 안전성이 높은 키 사전 분배 기법을 연구하고 다양한 지형에서의 추가적인 실험 분석을 할 예정이다.

References

[1] S. Zhu, S. Setia, S. Jajodia, "LEAP+: Effic ient security mechanisms for large-scale distributed sensor networks," ACM Transac tions on Sensor Networks (TOSN), vol. 2, Issue 4, pp 500-528, Nov. 2006

[2] F. Anjum, "Location dependent key manage ment using random key pre-distribution in sensor networks," In Proceedings of the 5th ACM workshop on Wireless security, pp. 21-30, Sep. 29. 2006

[3] KookMin University Industry Academic Cooperation Foundation, "Application Model Deployment of key Management Schemes in Ubiquitous Sensor Network", KISA, Sep. 2009

[4] T. Kwon, JH. Lee, JS. Song, "Location-Based Pairwise Key Predistribution for Wireles s Sensor Networks" IEEE Transactions on Wireless Commuications, Vol. 8, Issue. 11, pp 5436-5442, Nov. 2009

[5] A, A, Kumar, S. V. Rao, and D. Goswami(2013, June). Ns3 simulator for a study of d ata center networks. In 2013 IEEE 12th In ternational Symposium on Parallel and Dis tributed Computing (pp. 224-231). IEEE.

[6] OpenStreetMap, "terrain.party", accessed Aug 11, 2020, terrain.party

[7] Blender, "Blender Developer Document ation ,https://wiki.blender.org/wiki/Main_Page, accessed Aug 11, 2020,

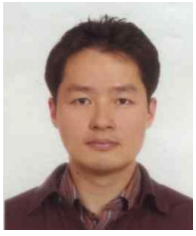
[8] The Unity team, "Unity User Manual (2019.4 LTS)", https://docs.unity3d.com/Ma nual/index.html, accessed Aug 11, 2020

[9] M. Elshrkawey, S. M. Elsherif, and M. E. Wahed, "An Enhancement Approach for Reducing the Energy Consumption in Wireless Sensor Networks,", Journal of King Saud University-Computer and Information Sciences, Vol. 30, Issue 2, p. 259-267, 2018.

〈저 자 소 개〉

윤 혜 민 (Hyemin Yun) 학생회원
2019년 2월: 서울여자대학교 정보보호학과 졸업
2019년 3월~현재: 연세대학교 정보대학원 석사
〈관심분야〉 정보보호, 디지털 포렌식, 암호 등

신 수 연(Sooyeon Shin) 정회원
2004년 2월: 세종대학교 컴퓨터공학과 학사
2006년 2월: 세종대학교 컴퓨터공학과 석사
2012년 2월: 세종대학교 컴퓨터공학과 박사
2012년~2013년: 세종대학교 Post-Doc
2013년~현재: 연세대학교 박사후 연구원
〈관심분야〉 암호 프로토콜, 정보보호, 사용자 인증, 컴퓨터 및 무선 네트워크 보안, 유저블 보안 등



권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1995년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C Berkely Post-Doc
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호 프로토콜, Usable Security, 소프트웨어/시스템 보안, 기계학습과 보안 등