중요 환경 감시목적의 에너지 보유량을 고려한 라우팅 프로토콜에서의 안전한 클러스터 형성 기법

유명한*, 김장성*, 김광조*

*카이스트 정보통신공학과

A Secure Clustering Scheme over an Energy-aware Routing Protocol for Critical Conditions Monitoring Applications

Myunghan Yoo*, Jangseong Kim*, Kwangjo Kim*

*Department of Information and Communications Engineering, KAIST.

요 약

무선 센서 네트워크는 유비쿼터스 컴퓨팅 환경에서의 필수적인 기술 중의 하나이다. 하지만 네트워크가, 연산, 저장, 전력 등의 자원이 제한된 센서노드로 구성돼있기 때문에, 보안상으로 더욱 취약하다. 중요 환경 감시목적의 라우팅 프로토콜은 그 목적에 걸맞게 알려진 공격에 대해서 강건해야 함에도 불구하고 대부분의 관련 연구들은 보안 요구사항들을 만족시키지 않는다. 이에, 본 논문은 기밀성, 데이터의 무결성 체크 그리고 각 노드의 인증과 같은 보안 요구사항을 만족시키는 에너지 보유량을 고려한 라우팅 프로토콜에서의 안전한 클러스터 형성 기법을 제안한다. 또한, 제안되는 방식은 클러스터 형성 외에 추가적인 비용 없이 데이터를 취합하는 노드에 대한 비정상적 동작에 대한 감시도 지원한다.

I. 서론

다가오는 유비쿼터스 사회에서 가장 유망한 기술 중에 하나인 무선 센서 네트워크는 일상에서 뿐만 아니라 각종 인간이 접근하기 힘든 환경에서도 사람들을 도울 것으로 기대되고 있다.

이런 기대를 반영하듯이 무선 센서 네트워크에 대한 다양한 종류의 논문들[3, 4, 13, 14, 17]이 나왔다. 이중에서도 HPEQ (Hierarchical Periodic, Event-driven and Query-based) [4]은 특정 위험한 지역을 효율적으로 광범위하게 감시할 수 있어 유용하다. HPEQ의 주된 목적은, 건물의 화재, 독성 가스의 유출, 가스폭발, 그리고 심지어는 군사적 전장 등과 같은, 중요한 물리적 환경을 감시하는 것이기 때문에 실뢰성 있는 이벤트 감지 및 이의 전송이 매우 중요하다.

하지만, HPEQ는 노드간의 클러스터 형성 과정이나 감지한 데이터를 보고하는 과정에서 보안에 대한 고려를 전혀 하지 않아서 외부의 사용자가 네트워크의 구성을 파악할 수 있고, 모든 메시지들을 볼 수 있어서 악의적 의도만 있으면 메시지를 조작하거나 클러스터의 데이터 Aggregator(이하 Agr)가 되는 등의 공격이 쉽게 가능하다.

따라서 본 논문에서는 Agr 뿐만 아니라 모든 클러스터의 멤버 노드들의 인증과 메시지의 무결성, 기밀성, 최신성을 보장하는 클러스터 형성 기법을 제안한다. 제안하는 방식은 각 노드에 단지 두 개의 키와 크레덴셜(이하, *Credential*)의 저장용량만을 요구한다. 한편, 클러스터 형성 과정에서의 통신 부하 측면에서는 HPEQ보다 약간의 추가적 저장·통신비용을 요구하는데, 이는 Agr와 클러스터의 멤버 노드들의 잘못된 행동을 감시하는 감시자 노드를 지정하기에 일어나는 것이다. 하지만, 이는 보안 수준과 저장·통신비용 사이에서의 합리적인 교환이라는 것을 보일 것이다.

이를 위해, 본 논문의 2장에서는 제안되는 방식의 대략적인 전체적 모습을 설명하고 무엇을 달성했는지 보일 것이다. 3장에서는 제안된 방식에 대해 세부적으로 그림과 함께 설명하고, 4장에서는 보안 수준에 대한 분석을 할 것이다. 그리고 5장에서는 HPEQ보다 추가적으로 요구하는 저장·통신비용을 계산할 것이고, 마지막으로 6장에서는 결론에 대해 기술할 것이다.

II.아키텍처 설계

본 논문에서 제안하는 클러스터 형성 기법은 기본적으로 HPEQ [4]를 틀로 잡고 있다. 따라서, HPEQ의 구조를 먼저 살펴볼 필요가 있는데, HPEQ는 기본적으로 초기설정, Agr를 선택하고 클러스터를 형성하는 단계, 그리고 싱크로의 데이터 보고 이렇게 세 가지의 동작 단계를 가지고 있다.

반면에, 제안되는 방식은, 초기설정, 안전한 클러스터 형성, 키 관리, 안전한 데이터 보고, 이렇게 네 가지 부분으로 구성되어 있다. 처음 초기설정에서는 노드들은 각자의 싱크 노드와 공유하는 고유키와 네트워크상의 전체 노드들과 공유하는 광역키를 저장하며 추가적으로 *Credential*을 저장하게 되는데, *Credential*에 대해서는 3장에서 자세히 다루고자 한다.

키 관리에서는, 광역키, 고유키, 그리고 Agr와 감시자 노드를 포함하는 클러스터 멤버들과 공유하는 클러스터키, 이렇게 세 가지가 쓰인다.

안전한 데이터 보고는, 만약에 클러스터가 안전하게 형성되어 기밀성 및 멤버 노드들에 대한 인증을 제공 한다면 자연스럽게 보장되고, 이후에는 메시지의 최신성과 전송의 성공이 추가적으로 필요하다. 그런데 원래 HPEQ는 충분한 전송 성공률을 보이고, 심지어 HPEQ의 이전 버전인 PEQ[3]에서부터 사용된 경로 복구기능을 이용해서 DoS공격의 한 종류인 재밍(Jamming) 공격에 대해서 유연하게 대처가능하다. 또한 메시지의 최신성은 논스 및 이에 대한 덧셈연산으로 보장가능하다. 따라서 본 논문에서는 안전한 클러스터 형성과 키 관리에 대해서 중점적으로 다룰 것이다.

III.제안 방식

본격적인 제안 방식에 대한 설명에 앞서서 다음 표 1은 제안 방식에서 쓰는 범례를 보여주고 있다.

표 1. 범례

REQ EN	잔여 에너지양 요청
REP_EN	잔여 에너지양 응답
SET_AGR	Agr 지정 메시지
AGR_NTF	Agr로부터 클러스터 형성의 선언
IDx	ID of node X
CN, A, I, P, N, C, S	Agr 후보, Agr, 감시자 노드, 부모 노드, 보통 노드, 모든 클러스터 멤버 노드, 싱크 노드
Nonce	논스
CK, Kx, KG	클러스터키, 노드 X의 고유키, 광역키
EKx(M)	키로 암호화된 메시지 M
Credentialx	노드 X의 익명
TR	송수신 횟수
AUTH_REQx	노드 X의 인증 토큰, *Credentialx||EKx(IDx||TR||Nonce)*
MACKx(M)	메시지 M의 인증 코드, 사용된 키는 Kx,
⇒, →	브로드캐스트, 유니캐스트 전송

3.1 Cluster Data Aggregator 선택

Agr 선택은 HPEQ와 마찬가지로 한 노드를 확률에 기반을 두어 선택하는 것으로 시작한다. 이는 확률적 기반에서 선택한 노드가 미리 탈취됐을 확률이 낮음을 가정한 것이다. HPEQ에서는 선택된 노드의 역할은 Agr를 선택하는 것에서 끝났지만, 제안 방식에서는 이 선택된 노드가 감시자 노드로서 계속 활용한다.

선택된 노드는 그의 이웃들에게 1단계 메시지인 (S1)을 브로드캐스트한다. 여기서 이웃들은 Agr의 후보군이라 칭한다. 여기서 광역키로 암호화된 메시지는 오직 네트워크를 구성하는 노드만이 복호화 할 수 있다.

$$(S1)\,[I \Rightarrow CN]\, REQ\_EN \| E_{K_G}(ID_I \| Nonce \| Amount\,of\,Energy)$$

그 후, 위의 메시지를 받은 모든 노드들이 응답을 하는 HPEQ와는 다르게, 후보군 중에서 감시자 노드보다 더많이 에너지를 가지고 있는 노드만이 아래의 메시지(S2)로 응답해준다. 여기서 논스는 원래의 논스에 1을 더하여 메시지가 최신임을 명확히 한다.

$$(S2)\,[CN \rightarrow I]\, REP\_EN \| E_{K_G}(ID_{CN} \| Nonce + 1)$$

그런 후, 만약 감시자 노드가 다른 후보군들보다 많은 양의 에너지를 가지고 있더라도, 감시자 노드는 *SET_AGR*을 비롯한 메시지(S3)를 가장 많은 에너지를 보유한 노드에게 보낸다.

$$(S3)\,[I \rightarrow A]\, SET\_AGR \| E_{K_G}(ID_I \| Nonce + 2)$$

비록 감시자 노드가 Agr를 선택했지만, 아직

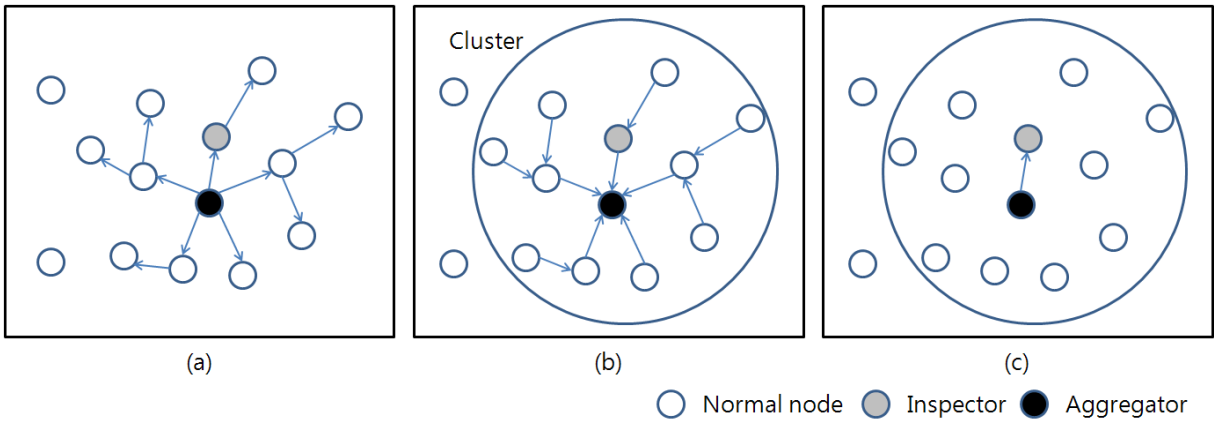

그림 1. 클러스터 설정

선택한 노드를 신뢰할 수 있다고 보기는 어렵다. 왜냐하면, 탈취된 노드가 자신의 남은 에너지양을 과장해서 알려줬을 가능성이 있기 때문이다. 따라서 감시자 노드는 클러스터 설정단계에서 이에 대한 인증을 싱크에게 요청한다.

3.2 클러스터 설정

Agr로 지정된 노드는 자신이 Agr임을 알림과 동시에 주위 노드들에게 클러스터를 형성하도록 메시지(S4)를 보낸다. 이를 받은 주위 노드들은 홉 카운트을 하나씩 깎아서 0이 될 때까지 메시지(S4)를 보내고 자신이 부모노드가 되고 받은 노드는 자식노드가 된다.

$$(S4)\,[A \Rightarrow N]\, AGR\_NTF \| E_{K_G}(ID_A \| newNonce)$$

홉 카운트가 0일 때 메시지(4)를 받은 자식노드는 자신의 인증 토큰을 부모 노드에게 보낸다. 이 인증 토큰(*AUTH_REQ*)은, *Credential*과 TR, 이 두 가지 요소로 구성되어 있다. *Credential*은 클러스터의 구성원 리스트를 외부로부터 보호하기위한 것으로 각 노드의 ID와 논스가 합쳐져서 싱크의 고유키로 암호화된 것이다. TR은 노드의 송수신 횟수로, 이는 싱크가 각 노드의 에너지양을 계산하기위한 송수신 각각 8비트씩의 총 16비트 길이의 인자이다. 만약 횟수가 8비트 길이를 넘기면 초기화 되나, 이는 싱크가 에너지양을 계산하는 데는 문제가 되지 않는다.

$$(S5)\,[N \rightarrow P]\, AUTH\_REQ_N$$

자식 노드들로부터 응답을 받은 부모 노드는 자신의 인증 토큰을 붙여서, 더 상위의 부모에게 전송한다.

$$(S6)\,[P \rightarrow A]\, AUTH\_REQ_P \| AUTH\_REQ_{N_1} \| \ldots$$

결국 Agr가 모든 인증 토큰을 모으게 되는데, 이 과정은 위의 그림 1에 묘사되어있다. 토큰들을 모은 Agr는, 모은 메시지들에 자신의 *Credential*과 메시지의 MAC을 더하여 (S7)과 같이 감시자 노드에 보낸다.

$$(S7)\,[A \rightarrow I]\, AUTH\_REQ_1 \| \ldots \| AUTH\_REQ_n \| Credential_A \| MAC_{K_A}(M)$$

Agr로부터 메시지(S7)를 받은 감시자 노드는 Agr를 선택할 때 Agr로부터 받은 *REP_EN*와 자신의 고유키로 생성한 MAC을 덧붙인 메시지(S8)을 싱크에게 HPEQ에서의 초기 설정을 통해 설정한 멀티홉 경로로 보낸다.

$$(S8)\,[I \rightarrow S]\, AUTH\_REQ_C \| REP\_EN \| \| Credential_I \| MAC_{K_I}(M)$$

마지막으로 싱크는 받은 메시지를 인증하는데, 만약 싱크가 예측한 노드들의 남은 에너지양과 Agr가 알린 양이 비슷하고, 각 노드의 송수신 횟수가 정상적인 범위내에 있다면 적법한 노드라 간주하여, 클러스터키와 각 노드별로 새로운 *Credential*을 생성하여 각 노드의 고유키로 암호화하여 적법한 노드에게 송신한다.

$$(S9)\,[S \Rightarrow C]\, Credential_X \| E_{K_X}(CK \| newCredential_X)$$

IV.보안 분석

제한 방식은 클러스터를 형성하는 동안 여러 암호학적 도구를 통해 메시지의 기밀성, 최신성, 무결성을 제공한다. 또한, 누적적인 통계 계산을 통한 에너지감시를 적용하여 탈취된 노드가 악의적으로 활동할 수 있는 여지를 줄였다. 만약 Agr로 선택된 노드가 의심된다면, 싱크는 감시자 노드를 Agr로 재설정하고 이에 대한 라

우팅 정보를 마지막 단계인 메시지(S9)에 삽입하여 클러스터 멤버들에게 알려줄 것이다.

V.성능분석

5장에서는 HPEQ에 암호학적 도구들을 사용함으로써 발생한 추가적 저장·통신비용을 설명한다. 처음으로 저장 비용을 알아보면, 일반적으로 쓰이는 128비트 키길이의 AES를 사용하고, SHA-1을 해쉬함수로 사용하면 각 노드는 표 2와 같이 68바이트의 적은 용량만 필요하다는 것이다.

표 2. 센서 노드에 탑재되는 도구들의 크기

데이터	크기(byte)
광역키	16
고유키	16
크레덴셜	20
클러스터키	16
합계	68

또한, 본 논문에서는 가장 에너지 소모가 심한 통신비용도 고려하였다. 통신비용의 요소로는 통신 반경과 송신 메시지 길이인데[9], 본 논문에서는 HPEQ와 구조는 같다고 가정하여, 메시지 길이에 따른 화만 살펴보고자 한다. 표 3은 제안방식에서 쓰는, 각 메시지를 구성하는 요소들의 길이를 정의한 것이다.

표 3. 메시지 요소들의 크기

메시지 요소	크기(byte)
키	16
해쉬된 메시지	20
논스	6
ID	3
에너지잔량	2
TR	2

표 4는 원래 HPEQ에서 제안 방식의 각 단계에 추가로 덧붙여진 메시지 길이다. w, x, y, z는 각각 *REQ_EN, REP_EN, SET_AGR, AGR_NTF*로서, 원래 HPEQ에서 쓰인 메시지이다. [5]에 따르면, 8에서 24바이트 길이의 메시지를 송신하는 데는 거의 무시할 정도로 에너지 소모 증가량이 미미하다. 따라서 4단계까지는 HPEQ와 거의 비슷한 에너지를 소모한다고 할 수 있다. 5단계에서는 약간의 추가 통신비용이 있다. 왜냐하면, 24바이트를 송신하는 것보다 32바이트 길이의 메시지를 송신하는 것이 약 33.55%의 에너지가 더 소모되기 때문이다[5]. 이후에는 보안 수준이 높아진데 따른 필연적인 추가적인 통신 부하가 더욱 있는데, 이는

표 4. 각 단계에서 송신되는 메시지 길이

단계	메시지 길이 (byte)	
	각 요소 분해	총합
S1	w+3+6+4+3(패딩)	w+16
S2	x+3+6+7(패딩)	x+16
S3	y+3+6+7(패딩)	y+16
S4	z+3+6+7(패딩)	z+16
S5	16+3+2+6+5(패딩)	32
S6	(n+1)*32	(n+1)*32
S7	C*32+16+20	C*32+36
S8	C*32+36+y+16+20	C*32+y+72
S9	16+16+16	48

24바이트의 길이로 쪼개서 여러 번 송신하는 것이 현명할 것이다.

통신횟수 측면에서 보면, 본 논문에서 제안한 방식은 메시지(S7)을 제외하고는 HPEQ와 통신횟수가 같게 하여 추가되는 통신비용을 최소화하였다.

VI.결론

본 논문에서는 HPEQ라는 중요 환경 감시 목적의 프로토콜에 암호학적 도구들을 사용하여 보안 요구사항을 만족하고자 시도하였다. 또한, 싱크에서 각 노드로부터 계속적으로 보고되는 그들의 남은 에너지양의 누적적 통계 계산을 통하여 Agr을 포함하는 모든 센서 노드를 인증하여 악의적 목적으로 탈취된 센서 노드의 활동을 억제할 수 있다. 또한, 제안된 방식은 기본이 되는 프로토콜인 HPEQ로부터 추가되는 저장·통신비용을 최소화하였다.

추후에는 제안한 방식과 비슷한 목적의 방식들과의 비교를 추가할 것이고, 제안 방식을 센서노드들로 구현하여 실험해볼 것이다.

[참고문헌]

[1] A. Boukerche, I. Chatzigiannakis, and S. Nikoletseas, A New Energy Efficient and Fault-tolerant Protocol for Data Propagation in Smart Dust Networks using Varying Transmission Range, In 37th ACM/IEEE Annual Simulation Symposium - ANSS, 2004.

[2] P. Banerjee, D. Jacobson, And S. N. Lahiri, Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks, Proceedings of 6th IEEE International Symposium on

Network Computing and Applications (NCA 2007), 2007.

[3] A. Boukerche, R. W. N. Pazzi, And R. B. Araujo, A fast and reliable protocol for wireless sensor networks in critical conditions monitoring applications, International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems (MSWIM'04), 2004.

[4] A. Boukerche, R. W. N. Pazzi, And R. B. Araujo, HPEQ - A Hierarchical Periodic, Event-driven and Query-based Wireless Sensor Network Protocol, Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05), 2005.

[5] C. Chang, D. J. Nagel, and S. Muftic, Measurement of Energy Costs of Security in Wireless Sensor Nodes, Proceedings of ICCCN 2007, 2007.

[6] I. Chatzigiannakis, S. Nikoletseas, and P. Spirakis, A Comparative Study of Protocols for Efficient Data Propagation in Smart Dust Networks, In Proc. 2nd ACM .POMC 2002, 2002.

[7] L. Eschenauer and V. D. Gligor, A key management scheme for distributed sensor networks, In 9th ACM conference on Computer and communications security, 2002.

[8] D. Estrin, R. Govindan, J. Heidemann, Embedding the Internet, Communication ACM 43, 2000

[9] W. Heinzelman, A. Chandrakasan, And H. Balakrishnan, Energy-efficient communication protocol for wireless sensor networks, Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS'00), 2000.

[10] J. Ibriq and I. Mahgoub, A Secure Hierarchical Routing Protocol for Wireless Sensor Networks, Communication systems (ICCS 2006), 10th IEEE Singapore International Conference on, 2006.

[11] J. Ibriq and I. Mahgoub, A Hierarchical Key Establishment Scheme for Wireless Sensor Networks, Advanced Information Networking and Applications, (AINA '07). 21st International Conference on, 2007.

[12] G. Khanna, S. Bagchi, and Y. Wu, Fault Tolerant Energy Aware Data Dissemination Protocol in Sensor Networks, IEEE DSN, 2004.

[13] C. Karlof and D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, Elsevier's Ad-Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 2003.

[14] S. Lindsey and C. S. Raghavendra, PEGASIS: Power Efficient GAthering in Sensor Information Systems, in the Proceedings of the IEEE Aerospace Conference, 2002.

[15] A. Manjeshwar, and D. P. Agrawal, APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks, in the Proceedings of the 2nd IPDPS'02, 2002.

[16] S. Nikoletseas, I.Chatzigiannakis, A. Antoniou, H. Euthimiou, A. Kinalis, And G. Mylonas, Energy Effcient Protocols for Sensing Multiple Events in Smart Dust Networks, Proc. 37th Annual ACM/IEEE ANSS'04, 2004.

[17] L. Oliveria, H. Wong, M.Bern, R. Dahab, And A.A.F. Lourerio, SecLEACH: A Random Key Distribution Solution for Securing Clustered Sensor Networks, In the Fifth IEEE International Symposium on Network Computing and Applications (NCA'06), 2006.

[18] M. Younis, M. Youssef, and K. Arisha, Energy-Aware Routing in Cluster-Based Sensor Networks, in the Proceedings of the 10th IEEE/ACM MASCOTS' 02, 2002.