6LoWPAN에서의 네트워크 관리 기법 연구

한선희*, 정성민*, 정태명**
성균관대학교 전자전기컴퓨터공학과*
성균관대학교 정보통신공학부**
{shhan, smjung}@imtl.skku.ac.kr*, tmchung@ece.skku.ac.kr**

A Study on the Technique of the Network Management for 6LoWPAN

Sun-Hee Han*, Sung-Min Jung*, Tai-Myoung Chung**
Dept. Electrical and Computer Engineering, Sungkyunkwan Univ.*
School of Information & Communication Engineering, Sungkyunkwan Univ.**

요 약

센서 네트워크는 다수의 센서노드를 통해 특정한 요청에 대한 정보를 수집하고 공유하는 네트워크이다. 센서 네트워크에는 많은 수의 센서들이 존재하기 때문에 센서노드를 관리하고 모니터링 하기 위한 효율적인 방법이 필요하다. 센서 네트워크에 IPv6를 적용한 기술로써 6LoWPAN이 있다. SNMP 사용 등 IP를 이용함으로 얻을 수 있는 다양한 장점이 있지만 센서의 배터리 용량과 메시지 사이즈가 제한적이기 때문에 메시지 사이즈가 큰 기존의 SNMP를 그대로 적용하기는 어렵다. 따라서 센서 네트워크에서 제한된 배터리 용량과 메시지 사이즈에 적용할 수 있는 효율적인 네트워크 기법이 필요하다. 본 논문에서는 네트워크 관리 프로토콜인 SNMP를 경량화 하여 6LoWPAN 환경에서도 적합한 방안을 제안하였다. 특히, SNMP 버전 중 SNMPv1, v2보다 보안성이 강화된 SNMPv3을 경량화 하여 6LoWPAN에 적합하고 보안적인 네트워크 관리를 위한 기법을 제안한다.

1. 서론

센서 네트워크는 주변 상황을 인지하기 위한 센싱 기능과 정보처리 능력, 무선 통신 능력을 갖춘 여러 센서 디바이스를 통해 원하는 정보를 수집하고 응용 서비스에 그 정보를 전달하는 네트워크이다[1]. 센서 네트워크는 유비쿼터스를 위한 핵심 기술로써 환경 감시, 시설 모니터링, 도로 교통 트래픽 검사 등 여러 응용분야에서 폭 넓게 적용될 수 있어 센서 네트워크에 대한 관심이 점차 높아지고 있다. 하지만 많은 수의 센서 노드가 조밀하게 분포되어 있고, 토폴로지의 변화가 매우 빈번하게 일어나는 특성을 갖고 있어 네트워크 관리가 필수적으로 요구된다. 센서 네트워크에는 Non-IP기반 ZigBee와 IP기반 IPv6 over Low Power WPAN(6LoWPAN)이 있다. 본 논문에서는 6LoWPAN 네트워크에서 효율적이고 보안성이 강화된 SNMPv3 압축 방식을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 센서 네트워크의 특징에 대한 설명과 네트워크 관리 기법인 Simple Network Management Protocol(SNMP)에 대해 설명하고, 6LoWPAN에 대해 설명한다. 3장에서는 SNMP를 6LoWPAN에 적용할 때 문제점에 대해 기술한 후 그 문제점을 해결하기 위해 6LoWPAN에 적용할 수 있도록 SNMPv3을 경량화 하는 기법을 제안한다. 4장에서는 결론으로 마무리 한다.

2. 관련 연구

2.1 센서 네트워크

센서 네트워크는 무선 통신을 이용하여 센서 네트워크를 구성하여 통신하여 정보를 수집하고 공유하는 네트워크이다. 센서 네트워크는 <표1>과 같은 특징을 갖고 있다[1].

<표 1> 센서 네트워크의 특징

종류	특징
Fault tolerance	결함이 생기더라도 다른 경로를 이용하여 네트워크 토폴로지를 유지함
Salability	한 번에 다수의 노드와 통신 가능
Low-cost	노드의 비용은 저렴함
Low-power consumption	제한된 배터리 용량 때문에 운영에 있어서 에너지 사용 최소화해야함
Environment	센서는 열악한 환경에서도 문제없이 동작해야함

2.2 Simple Network Management Protocol(SNMP)

SNMP는 네트워크상의 장비를 관리하고 감시하기 위한 목적으로 정의된 응용 계층에서 사용되는 표준화된 프로토콜이다[2]. SNMP는 통신망을 관리하기 위해 통신망의 구성요소들이 저장되어 있는 관리정보베이스(MIB,

Management Information Base)를 통해 디바이스들의 정보를 제공하는 역할을 한다. TCP/IP 기반의 네트워크 관리는 <표 2>와 같은 특징을 갖고 있다.

<표 2> TCP/IP 네트워크 관리 특징

기능	특징
Topology Management	네트워크상의 호스트들이 어떤 구조를 이루고 있는지 구성을 나타낼 수 있음
Performance Management	네트워크 사용량, 에러율, 처리속도, 응답시간 등 성능 분석에 필요한 통계정보를 얻어낼 수 있음
Device Management	시스템정보(CPU, MEMORY, DISK 사용량)를 얻어올 수 있음
Security Management	정보의 제어 및 보호 기능, 최근 버전인 SNMPv3은 특히 정보보호를 위한 기능이 향상됨

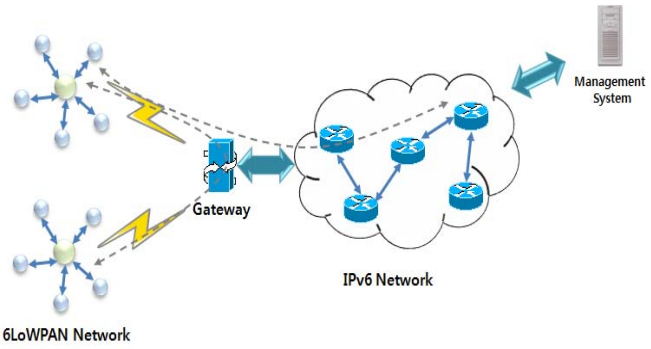
TCP/IP 기반의 네트워크와는 다르게 6LoWPAN에서는 <표 3>과 같은 네트워크 관리 기능을 제공해야 한다[7].

<표 3> 6LoWPAN의 네트워크 관리 특징

기능	특징
Passive monitoring	데이터 분석을 위한 네트워크 상태 정보를 수집하고 관리
Fault detection monitoring	문제가 발생했는지 알아내기 위해 네트워크의 상태 정보를 수집하고 관리
Reactive monitoring	발생한 이벤트를 검출하기 위한 네트워크 상태 정보를 수집하고, 네트워크에 자동으로 구성하고 관리함

2.3 IPv6 over Low Power WPAN(6LoWPAN)

6LoWPAN은 저전력 센서 네트워크에서 Internet Protocol(IP)을 사용하기 위한 RFC 4944로 표준화 되었다. 6LoWPAN의 MAC/PHY계층은 IEEE 802.15.4 기반으로 이루어져 있으며 MAC/PHY계층과 네트워크 계층 사이에 IPv6패킷의 효율적인 전달을 위해 IPv6의 헤더를 압축하는 Adaptation Layer를 정의하였다. 6LoWPAN은 Adaptation Layer를 통해 무선 센서 장치가 직접 IPv6 주소를 가지고 인터넷 망과 연동함으로써 별도의 센서 노드용 운영체제를 사용하지 않고도 6LoWPAN 망의 센서 노드와 인터넷 망의 호스트 간 단대단(End-to-End) 통신을 가능하게 해 준다. 즉, 복잡한 프로토콜 변경이나 관리 없이 단말간의 통신이 가능하다. (그림 1)은 6LoWPAN 네트워크 관리가 이루어지는 구조를 나타낸다[4]. 6LoWPAN 네트워크에서는 센서노드 간에 통신할 수 있고, Management System에서 정보를 요청할 때 Gateway는 IPv6 네트워크에서 인식할 수 있도록 연동 후 정보를 Management System으로 전달한다.



(그림 1) 6LoWPAN 네트워크 관리 구조

3. SNMPv3 경량화 방식 제안

3.1 6LoWPAN에서 SNMP 지원의 문제점

IEEE 802.15.4는 적은 전력소비와 낮은 비용의 특징을 만족시기 위해 전송할 수 있는 최대 패킷의 크기는 127바이트이다. 하지만 SNMP 메시지의 최소 사이즈는 484바이트로 이 사이즈는 6LoWPAN에 사용하기 위해서 여러 번의 메시지 교환이 필요하기 때문에 효율적이지 못하다[9]. 따라서 6LoWPAN에 SNMP를 사용하기 위해서는 SNMP 메시지 사이즈를 줄여야 한다.

본 논문에서는 SNMP 버전 1~3 중에서 버전 3을 경량화 하였다. 버전 1은 6LoWPAN 환경에 적합하지 않은데 그 이유는 버전 1에서는 Routing Table에 많은 열이 존재 할 경우에 전체 테이블을 읽으려고 한다면 요청과 응답 메시지를 여러번 반복하여 수행하여야 한다. 이러한 작업은 저전력인 센서 네트워크에 적합하지 않는 요소로써 요청할 때마다 전력을 소비하는 양을 줄이기 위해 교환되는 패킷의 수를 최소화 하여야 한다. 또한 버전 1에서는 전송중인 데이터의 비밀성을 해치거나, 내용을 위조하는 공격에 대응하는 기능을 제공하지 못한다. 따라서 이러한 문제점을 보완하기 위해 버전 2가 표준화 되었다. 버전 2는 큰 테이블의 값들을 한 번의 요청으로 가져 올 수 있지만 보안의 측면을 강화하기 위해 버전 3이 표준화 되었다. 버전 3은 데이터 재전송 방지 기능, 위장 방지, 무결성 보장 기능, MIB에 대한 접근 통제 기능들이 추가되어 SNMP 버전 2보다 더 안전한 통신망 관리 기술을 제공한다[5]. 따라서 본 논문에서는 6LoWPAN에서 네트워크 관리를 하기 위한 방법으로 SNMPv3을 이용한 관리 방식을 제안한다.

3.2 SNMPv3 경량화 방식

기존 SNMP가 제공하는 기능을 센서 네트워크에 적용하기 위해서는 SNMP 메시지의 크기를 줄이고, SNMP 메시지 교환을 최소화 하여 적용할 수 있다.

본 논문에서 제안하는 방식은 기존의 프로토콜 수정 없이 SNMP 메시지의 크기만 줄임으로써 센서 네트워크의 특징에 적합한 네트워크 관리 방식이다. <표 4>는 SNMPv3의 메시지 구성을 나타낸 것으로써 총 9개의 필드로 이루어져 있고 17 bytes 크기로 구성된 5개의 필드

와 가변적인 크기로 구성된 4개의 필드로 구성되어 있다 [6],[8].

<표 4> SNMPv3 메시지 구성

필드명	크기 (bytes)	설명
msgVersion	4	SNMP 버전을 나타내는 필드
msgID	4	두 개의 SNMP 객체 간에 요청과 응답메시지를 연결하기 위한 유일한 식별자
msgMaxSize	4	메시지를 송신할 때 최대 크기
msgFlags	1	reporttableFlag : Report-PDU 수신 여부 privFlag : 암호화와 인증여부 authFlag : 보안수준
msgSecurity Model	4	적용할 보안 모델
msgSecurity Parameters	Variable	보안 모델에 적용하기 위한 파라미터
context EngineID	Variable	context는 MIB에 속하는 일부로써 SNMP 관리 도메인 안에서 유일하게 식별되는 값
contextName	Variable	PDU 안에 있는 관리 정보를 담고 있는 특정 context를 나타내는 이름
PDU	Variable	<PDU Type> GetRequest : 객체 목록 값 요청 GetNextRequest : 다음 값 요청 Response : 관리자 요청의 응답 SetRequest : 객체 목록 값 설정 GetBulkRequest : 다중 값 요청 InformRequest : 관리자가 다른 관리자의 특정 관리 정보 요청 Trap : 요구되지 않은 정보 전송 <Request ID> 응답과 요청을 매치하기 위해 사용되는 식별자 <Error Status> 요청의 결과 에러가 없으면 0, 에러가 있으면 0이 아닌 값으로 에러 상태 값을 알려줌 <Error Index> Error Status 필드의 숫자가 0이 아닐 때(에러 존재), 에러가 발생된 객체를 가리킴

<표 4>와 같은 메시지 구조에서 SNMP 트래픽의 양을 줄이기 위해 각각의 필드 크기를 다음과 같이 줄이는 방식을 제안한다.

- msgVersion(Message Version Number) : 버전을 나타내는 필드로서 현재 버전은 4가지로 나뉘고, SNMPv1은 0, SNMPv2c는 1, SNMPv2p, v2u는 2, SNMPv3은 3의 값을 갖고 있다. 현재 모든 버전이 사용되지만 SNMPv3은 이전 버전과 호환되기 때문에 SNMPv3의 압축한 형태의 버전인 Compressed SNMPv3의 버전을 4로 추가하여 0~4의 값을 표현할 수 있는 2bits로 줄일 수 있다.
- msgID(Message Identifier) : 이 필드는 request에 해당하는 response를 식별하고, 네트워크에 중복된 메시지를 식별하는 기능을 제공하는 필드로 1byte면 충분하다[3].
- msgMaxSize(Maximum Message Size) : User-based security model인 SNMPv2c에서 2bytes가 사용되는데 v3에서도 2bytes로 사용한다[6].
- msgFlags(Message Flags) : 기존 SNMPv3에는 reporttableFlag, privFlag, authFlag가 각각 1bit의 크기이고, 예약 공간으로 5bits가 설정되어 있는데 메시지를 최소화하기 위해 예약 공간을 삭제하고 3bits로 줄였다.
- msgSecurityModel(Message Security Model) : 적용할 보안 모델의 값을 나타내는 필드로 SNMPv1은 1의 값, v2는 2, v3은 3의 값을 나타낸다[6]. 이것은 0~3까지 나타낼 수 있는 2bits로 줄일 수 있다.
- msgSecurityParameters(Message Security Parameters) : 이 필드는 msgAuthoritativeEngineID, msgAuthritative-EngineBoots, msgAuthoritativeEngineTime 파라미터를 사용하여 재전송 방지에 사용하는 필드와, msgUserName, msgAutheriticationParameters 파라미터로 위장방지와 무결성 보장을 제공하는 필드, msgPrivacyParameters 파라미터로 정보 노출 방지하는 필드로 구성 되어 있다.
- contextEngineID : MIB에 속하는 일부의 값을 context라고 하고 해당하는 context의 값을 식별하기 위해 사용되는 값으로 해당 context를 처리하기 위해 보내지는 필드이다.
- contextName : PDU와 연관된 특정 context의 이름을 나타내는 필드이다.
- PDU : PDU는 PDU Type, Request ID, Error Status, Error Index로 구성되어 있고, PDU Type은 총 9가지가 있고 0~8의 숫자로 총 3bits로 나타낼 수 있다. Request ID는 1byte로 줄이고, Error Status는 0~18까지 에러 코드가 정의되어 있는데, 이것을 나타내기 위해서는 5bits면 충분하다. Error Index는 에러가 발생된 곳을 가리키는 필드로, 1byte로 줄인다. 따라서 PDU의 총 사이즈를 24bits로 압축하였다.

이와 같은 방식으로 기존 SNMPv3 메시지를 <표 5>와 같이 압축하였다.

<표 5> SNMPv3 메시지 압축

필드명	기존 크기	압축 크기
msgVersion	4bytes	2bits
msgID	4bytes	8bits
msgMaxSize	4bytes	16bits
msgFlags	1bytes	3bits
msgSecurity Model	4bytes	2bits
msgSecurity Parameters	Variable	Variable
context EngineID	Variable	Variable
contextName	Variable	Variable
PDU	Variable	PDU Type : 3bits Request ID : 8bits Error Status : 5bits Error Index : 8bits

4. 결론

본 논문에서는 6LoWPAN 환경에 SNMP를 적용하기 위해 메시지의 크기를 줄이는 방안을 제안하였다. 기존의 SNMPv3 메시지에서 사이즈가 Variable인 msgSecurityParameters, contextEngineID, contextName 필드를 제외하고, 17bytes를 7bytes의 사이즈로 줄였다. 본 논문에서는 기존에 제안된 SNMPv1과 v2의 메시지를 압축한 방식에서 제공하지 못했던 접근통제 기능, 데이터의 재사용 방지 기능, 정보노출 등의 기능이 추가되어 더 강화된 보안서비스를 제공하는 SNMPv3 메시지 사이즈를 경량화 함으로써 센서 네트워크의 네트워크를 관리하기 위한 기법을 제안 하였다. 이후에는 6LoWPAN에서 네트워크를 관리하기 위해 본 논문에서 제안한 경량화된 SNMPv3을 바탕으로 성능을 평가하고, 성능 평가를 기반으로 더 최적화된 SNMPv3 경량화 기법을 제안 할 것이다.

ACKNOWLEDGMENT

본 논문은 중소기업청에서 지원하는 2010년도 산학연공동기술개발사업(No. 00044301)의 연구수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] J. Yick, B. Mukherjee, D. Ghosal, "Wireeless sensor network survey," Computer Networks, pp. 2292-2330, 2008.

[2] D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," RFC 3444, 2002.

[3] Haksoo Choi, Nakyoung Kim, Hojung Cha, "6LoWPAN-SNMP: Simple Network Management Protocol for 6LoWPAN," IEEE Computer Society, pp. 305~313, 2009.

[4] H. Mukhtar, Kim Kang-Myo, S.A Chaudhry, A.H Akbar, Kim Ki-Hyung, Seung-Wha Woo, "LNMP-Management Architecture for IPv6 based low-power Wireless Personal Area Network(6LoWPAN)," NOMS, pp. 417~424, Aug. 2008.

[5] U. Blumenthal, B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)," RFC 3414, 2002.

[6] SNMP, http://www.tcpipguide.com/, Mar. 2011.

[7] W L. Lee, A. Datta, R. Cardell-Oliver, "Network Management in Wireless Sensor Networks," Handbook on Mobile Ad Hoc and Pervasive Communications.

[8] 서상원, "네트워크 보안 관리, SNMP," maso, pp. 304~311, Feb. 2008.

[9] N. Kushalnagar, G. Montenegro, C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," RFC 4919, Aug. 2007.