The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 6, pp.147-152, Dec. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2016.16.6.147
JIIBC 2016-6-18

공장 설비 모니터링을 위한 그리드 기반 키 선분배 기법

Grid-Based Key Pre-Distribution for Factory Equipment Monitoring

조양희*, 박재표**, 양승민***

YangHui Cho*, JaePyo Park**, SeungMin Yang***

요 약 배선 작업이 어려운 공장 환경에서 설비의 상태를 모니터링하는 시스템을 구축하기위해 배포와 설치가 쉬운 무선센서 네트워크가 적합하다. 지그비는 다른 무선 통신 프로토콜에 비해 저가격, 저전력 특징을 가지고 있어 다수의 노드를 필요로 하는 모니터링 시스템에 적용하기 적합하다. 지그비 통신은 모든 프로토콜 계층이 서로 신뢰하는 OTM을 기반으로 하고 있기 때문에 디바이스 간에 암호화 보안이 필요하다. 각 노드간의 통신에 있어서 노드 인증을 보장하고, 각 노드가 관리하고 있는 비밀 정보의 노출을 최소화 해야 한다. 공장의 설비는 배포 위치가 규칙적이고 고정적이다. 공장 환경에서 센서로부터 수집되는 정보와 센서 노드에 연결되어 있는 엑츄에이터 제어 정보를 보호하기 위해 설비의 배포 환경과 유사한 이차원 그리드 기반 키 선분배 기법을 기반으로 하는 암호화 기법을 제안한다.

Abstract Wireless sensor networks that are easy to deploy and install are ideal for building a system that monitors the condition of the equipment in a factory environment where wiring is difficult. The ZigBee has characteristics of low price and low power compared with other wireless communication protocols and is suitable for a monitoring system requiring a plurality of nodes. ZigBee communication requires encryption security between devices because all protocol layers are based on OTM trusted by each other. In the communication between nodes, node authentication must be guaranteed and exposure of confidential information managed by each node should be minimized. The facilities of the factory are regular and stationary in distribution location. In order to protect the information gathered from the sensor in the factory environment and the actuator control information connected to the sensor node, we propose a cryptosystem based on the two - dimensional grid - based key distribution method similar to the distribution environment of the facility.

Key Words : ZigBee, WSN, Security, Confidential Communication

Ⅰ. 서 론

무선 센서 네트워크 기술은 배포와 설치가 쉽고 확장하기 편리해서 군사, 물류, 의료, 홈 네트워크, 농업, 건축, 산업 자동화 등 다양한 분야에서 활용되고 있다[1][2][15]. C4ISRT(Commands, Controls, Communications, Computing, Intelligence, Surveillances, Reconnaissance and Targeting) 시스템에서는 군사력, 통신 명령 또는 다양한 형태의 공격을 감지하기 위해 사용 될 수 있다[7]. 헬스 케어 분야에서는 만성 질환자의 일상 활동, 위치 추적, 상태 모니터링 및 약물 복용 등을 모니터링 하기 위해 사용 된다[8]. 서식지 모니터링, 동물 추적, 산불 감지,

*정회원, 숭실대학교 컴퓨터학과
**정회원, 숭실대학교 정보과학대학원
***정회원, 숭실대학교 컴퓨터학부
접수일자: 2016년 8월 5일, 수정완료: 2016년 12월 5일
게재확정일자: 2016년 12월 9일

Received: 5 August, 2016 / Revised: 5 December, 2016
Accepted: 9 December, 2016
*Corresponding Author: vanillo@realtime.ssu.ac.kr
Dept of Computing , SoongSil University, Korea

재난 구조와 같은 분야에서 사용된다.

무선 센서 네트워크 표준 프로토콜은 에너지 효율, 효율적인 데이터 전송 그리고 라우팅에 중점을 두고 있다. 산업용, 군사용 그리고 의료용 어플리케이션에서는 수집된 정보에 대해 보안이 요구 된다[4]. 배터리 전력을 사용하는 센서 노드의 경우 전력, 계산 능력 그리고 저장 공간이 제한되어 있고 무선 통신의 특성 때문에 전송된 데이터의 기밀성 보호에 취약하다[3]. 무선 센서 네트워크의 제한적인 환경에서 보안 요구사항을 충족하기 위해 암호 알고리즘과 에너지 효율적인 암호기법과 같은 다양한 연구가 진행되고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 지그비의 공격 유형 그리고 무선 센서네트워크 보안과 관련된 연구 기법에 대해 알아보고 3장에서는 정밀한 작업을 요하는 공장에 설치된 설비의 현재 상태를 모니터링을 하기 위해 Liu가 제안한 그리드 기반 키 선분배 기법[10]을 기반으로 지그비 무선 센서 네트워크 환경에서 모니터링되는 설비 정보의 보안을 위한 기법을 제안한다. 4장에서는 제안된 기법과 다른 기법들과 비교, 분석하고 5장에서 결론을 맺는다.

II. 관련 연구

1. 지그비 공격 유형

지그비 공격 유형은 물리적 공격, 키 프로비저닝 공격 그리고 리플레이 공격이 있다.

많은 수의 지그비 디바이스가 디바이스를 켜면 메모리에 저장되어 있는 암호키를 램으로 로드하여 사용한다. 공격자는 오픈소스 또는 하드웨어와 소프트웨어 툴을 사용하여 메모리에서 램으로 로드되는 키를 물리적으로 탈취할 수 있다.

지그비 네트워크는 업데이트를 쉽게 하기 위해 OTA(Over the Air)키 전달 방식을 사용한다. 이 키는 디바이스가 네트워크에 조인되지 않고 연결하려는 경우 또는 키 로테이션이 발생할 때 한번 전송된다. 이때 키를 평문으로 보내기 때문에 보안에 취약하다.

재생 공격은 원격에서 이루어지며 지그비 디바이스가 권한이 없는 행동을 하도록 한다. 공격자는 키 로테이션이 발생할 때까지 트래픽과 패킷을 감시한다. 공격자는 패킷을 복호화하지 못해도 캡쳐된 패킷을 네트워크의 다른 디바이스로 전달할 수 있다.

지그비 네트 지그비는 모든 프로토콜 계층이 서로 신뢰하는 OTM(Open Trust Model)을 기반으로 하고 있다. 따라서 지그비 디바이스 간에 암호화 보안이 필요하다[11].

2. 무선 센서 네트워크 보안 관련 연구

데이터 탐색 및 배포 프로토콜은 무선 센서 네트워크를 배치한 후에 센서 노드에 저장된 프로그램 또는 파라메타를 갱신하는 프로토콜이다. 기존의 데이터 탐색 및 배포 프로토콜은 중앙 집중형 접근방식으로 베이스 스테이션과 노드 사이의 연결이 끊어지면 기능을 수행 할 수 없다. Di-Drip은 네트워크 소유자가 다수의 네트워크 사용자에게 다른 특권을 부여할 수 있고 센서 노드에게 직접 데이터 항목을 배포할 수 있는 보안 기능을 가지는 분산 데이터 탐색 및 배포 프로토콜이다[5].

일반적인 네트워크에서 사용하는 디피 헬만(Diffie-Hellman) 알고리즘과 공개키 기반 기법과 같은 키 동의 기법은 저장 공간이 제한된 센서 노드에는 적합하지 않다. 이러한 단점을 극복하기 위해 배포 위치가 정적인 센서 노드를 위한 랜덤 키 선 분배 기법이 제안되었다. 이 기법은 배포 후에 이웃노드로부터 공통 비밀 키를 찾을 수 있다[6].

랜덤 Pair-wise기법에서 각각의 노드는 키 풀에서 정해진 수의 키를 선택한다. 두 통신 노드는 공유키를 비밀키로 사용하고 공유키가 없으면 중개노드를 통해 키를 찾는다[9].

위치 기반 Pair-wise기법은 크기가 N인 네트워크에서 노드를 $N^{-1/2}$X $N^{-1/2}$ 그리드의 교차점에 분배하고 그리드의 열과 행을 따라 다항식을 할당한다. 동일한 다항식을 공유하는 두 개의 노드는 그 다항식으로부터 공통키를 생성하고 공유하는 다항식이 없으면 중개노드를 통해 키를 생성 한다[10].

키 사전 분배 기법의 경우 공유키(Shared Key)를 확인 하는 단계에서 공유키를 가지고 있는 노드가 위장 데이터를 전송하거나 다른 노드로 가장하여 데이터를 전송할 수 있다. 또한 공격자에게 키 체인(Key Chain)노출되는 경우에 대부분의 비밀키가 노출될 수 있다.

각 노드간의 통신에 있어서 노드 인증을 보장하고, 각 노드가 관리하고 있는 비밀 정보의 노출을 최소화해야 한다. 또한 공격자에 의해 야기되는 통신과 계산 오버헤

드를 최소화해야 한다.

Ⅲ. 이차원 그리드 기반 키 분배 기법

제안하는 기법은 다항식 기반 키 분배 기법을 기반으로 지그비 통신의 특성을 이용한다. 부피가 크고 무거운 공장의 설비의 경우, 한번 설치되면 고정된 곳에 위치한다. 제안하는 기법은 공장 설비 배포 환경과 유사한 그림 1과 같은 2차원 그리드를 이용한다. 네트워크의 크기가 N인 경우, 그리드는 $2n$개의 다항식을 가지는 nxn 길이의 x,y축을 가진다. 여기서 n = $\sqrt{N}$을 의미한다. 유한체 F_q상의 m차 다항식 $f(x,y)$를 생성한다. 여기서 q는 암호화 키를 수용할 수 있는 충분히 큰 소수를 의미한다.

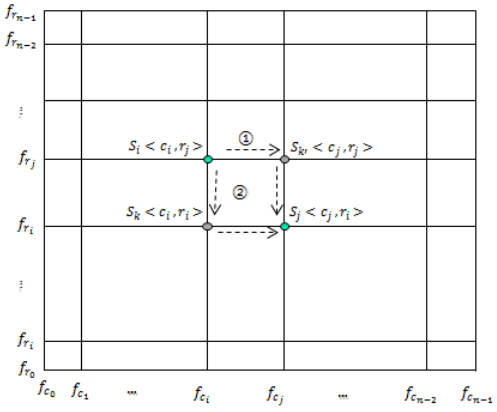

그림 1. 이차원 그리드 그래프
Fig. 1. Two-Dimensional Grid Graph

지그비 노드는 그리드 교차점에 배치되고 i번째 열과 j번째 칼럼이 교차하는 교차점의 좌표 정보는 (x_i, y_j)로 표현한다. 그리드에서 i번째 열의 다항식은 $f_{r_i}(x,y)$, i번째 칼럼의 다항식은 $f_{c_i}(x,y)$ 으로 표현한다. 센서 노드가 좌표 (x_i, y_j)에 위치했을 때, 키 관리 서버는 다항식 f_{r_i}와 f_{c_i}를 센서노드에 배포한다. 센서의 좌표는 센서 ID로 암호화된다. 유효한 좌표는 $\log_2 n$비트의 이진 문자열로 표현 될 수 있다. 좌표 (x_i, y_j)로부터 만들어진 센서 ID S_{id} = $< c_i, r_j >$로 표기한다.

1. 키 할당

키 관리 서버는 m차 다항식 $2n$개를 생성한다. 그리드의 교차점 (x_i, y_j)에 위치한 센서의 ID는 $< c_i, r_j >$이다. 키 관리 서버는 센서 노드에게 ID와 교차점에 해당하는 다항식을 할당한다.

$$K_d = \{S_{id}, f_{c_i}, f_{r_j}, P_{CNT}\} \quad (1)$$

할당된 다항식은 지그비 코디네이터가 네트워크 구성 시에 동적으로 할당한 네트워크 주소 $NADDR_{id}$ 로 암호화하여 배포한다.

$$EK_d = e_{NADDR_{id}}(K_d) \quad (2)$$

2. 다항식 탐색

인접한 노드와 서로 공유하고 있는 공유키를 확인 하는 절차를 수행한다. 배포된 키를 네트워크 주소 $NADDR_{id}$ 로 복호화한다.

$$K_d = e^{-1}_{NADDR_{id}}(EK_d) \quad (3)$$

센서 노드 i는 센서 노드 j와 공유키를 찾기 위해 센서 ID를 확인한다. $r_i = r_j$ 인 경우, 노드 i와 j는 다항식 f_{r_i}를 공유한다. $c_i = c_j$인 경우, 노드 i와 j는 다항식 f_{c_i} 를 공유한다. 공유하는 다항식이 없는 경우 이웃 노드를 통한 경로 탐색을 수행한다.

3. 경로 탐색

센서 노드 i와 센서 노드 j가 공통키를 찾기 못할 경우, 두 노드와 공통키를 갖는 제 3의 센서 노드 k를 탐색하여 키를 설정할 수 있다. 그림 1 의 ①번 센서노드 k'의 $< c_i, r_j' >$ ②번 센서노드 k의 $< c_i', r_j >$ 로부터 $< c_j, r_i >$를 찾는다.

4. 데이터 키 생성

센서 노드는 배포된 키와 송신 노드에서 수신 노드로 보내는 메시지 카운터 MSG_{CNT}와 데이터 키로 비밀키를 생성한다.

$$K = f(MSG_{CNT}, K_d) \quad (4)$$

데이터의 평문 $M = (M_1, M_2, \cdots, M_l)$을 비밀키 K를 사용하여 암호문 $C = (C_1, C_2, \cdots, C_l)$ 을 만

든다.

$$C = e_k M \quad (5)$$

송신 노드는 COUNT, EK_d 그리고 암호문을 전송한다. 수신 노드는 공식(3)으로 K_d를 구하고 공식 (4)로 K를 구한다. 암호화된 데이터를 K로 복호화 해서 평문을 얻는다.

$$M = e_k^{-1} C \quad (6)$$

Ⅳ. 비교 분석

표 1은 N개의 노드로 구성된 센서 네트워크에서 그리드 기반의 키 선 분배 기법을 사용하는 기법들과의 비교를 보여준다.

표 1. 다른 기법들과 비교
Table 1. Comparison with other Schemes

Schemes	Computation	Memory	Connectivity
GBS[10]	SBP Evaluation	ID + 2 SBP	$\frac{2}{N^{1/2}-1}$
Our Scheme	SBP Evaluation	ID + 2 SBP	$\frac{2}{N^{1/2}-1}$
3D-GBS [13]	SBP Evaluation	ID + 3 SBP	$\frac{3}{N^{2/3}+N^{1/3}+1}$
HGBS [12]	SBP Evaluation	ID + n SBP	1

대칭 이변량 다항식(SBP:Symmetric Bivariate Polynomial)을 사용하는 2차원 그리드 기반의 기법 GBS[10], 3차원 그리드 기반의 기법 3D-GBS[13] 그리고 계층적 그리드 기법 HGBS[12]와 비교한다.

1. 연결성

연결성은 네트워크 노드가 자신이 가지고 있는 정보를 가지고 단일 홉으로 통신 할 수 있는 확률을 말한다. 제안하는 기법의 연결성은 그림 2에서와 같이 3D-GBS와 HGBS기법에서의 단일 홉 연결성보다 작고 GBS기법과 같은 $\frac{2}{N^{1/2}-1}$의 연결성을 가진다. 제안하는 기법은 3D-GBS와 HGBS기법에 비해 연결성에서 좋은 결과를 보인다.

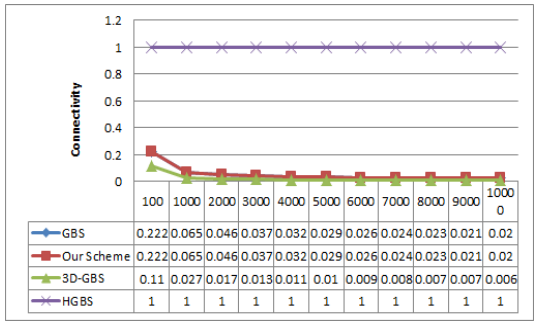

그림 2. 단일 홉의 연결성
Fig. 2. Connectivity of single hop

2. 메모리 오버헤드

메모리 오버헤드는 네트워크 구성 시에 할당받은 네트워크 주소 $NADDR_{id}$로 암호화한 키를 배포하고, 배포된 키로 데이터 키를 동적으로 생성하여 사용하기 때문에 $NADDR_{id}$와 데이터 키는 고려하지 않는다. 따라서 다항식 $x^0, x^1, \cdots x^m$의 계수 $a_0, a_1, \cdots, a_m$를 저장하기 위해 메모리는 $(m+1)\lg(q)$비트가 필요하다[14]. 다항식의 차수 m과 소수 q에 따른 메모리 오버헤드는 그림 3에서 확인할 수 있다. 차수 m과 소수 q가 커질수록 메모리 오버헤드도 커진다.

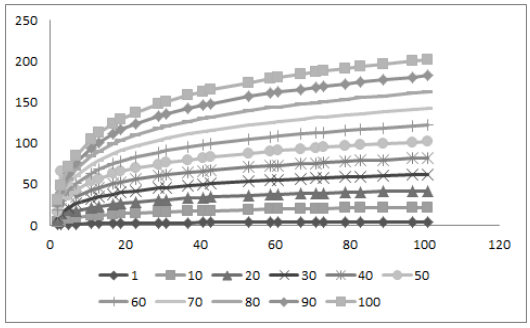

그림 3. 메모리 오버헤드
Fig. 3. Memory Overhead depended on Degree

3. 연산 오버헤드

연산 오버헤드는 m차 다항식의 확인이 필요하다. $n = \sqrt{N}$일 때, $m = \alpha \times n^2$ 차수의 다항식을 확인하기 위해 $2m$-2의 연산이 필요하다. 차수 m에 따른 다항식의 연산 회수는 그림 4와 같이, 차수가 커질수록 연산 회수가 비례적으로 증가한다.

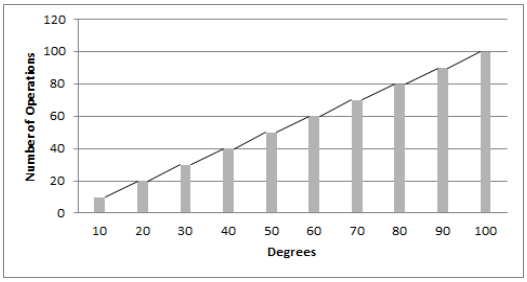

그림 4. 연산 횟수
Fig. 4. Number of Operations

메모리 오버헤드와 연산 회수는 시스템의 성능에 직접적으로 영향을 주기 때문에 적용하려는 대상 프로세서의 성능에 따라 다항식의 차수 m와 소수 q의 범위를 정하여 사용하여야 한다.

4. 위장 공격 및 재전송 공격

무선 통신은 위장 공격과 재전송 공격에 취약한 점이 있다. 무선 구간에서 탈취한 데이터를 재전송 하거나 정상적인 노드로 위장하는 공격이 가능하다. 제안한 기법에서는 키 분배 과정에서 패킷 카운트 P_{CNT}를 포함하여 동적으로 생성된 네트워크 주소로 암호화하여 전송한다. 무선 통신 구간에 데이터가 노출되어도 암호화 알고리즘을 알아야 정보를 확인 할 수 있다. 또한, 탈취한 메시지를 재전송을 하여도 패킷 카운트 P_{CNT}의 값이 변하지 않았으므로 무시된다.

V. 결 론

본 논문에서 제안한 기법은 2차워 그리드 기법 GBS와 연결성, 메모리 오버헤드 그리고 연산 오버헤드에서 비슷한 성능을 가지면서 보안의 위협에 노출되어 있는 무선 통신에서 악의적인 공격자로 부터의 위장 공격이나 재전송 공격 공격을 방지할 수 있다. 지그비 통신의 특성인 네트워크 구성 시마다 새로 설정되는 네트워크 주소를 이용해 배포키를 암호화하기 때문에 메모리에 ID를 저장하여 메모리로부터 ID정보가 노출되는 물리적 공격과 키 프로비저닝 공격을 방지할 수 있다. 또한 동적으로 생성되는 데이터 키와 메시지 카운터를 이용하여 데이터를 암호화하여 전송하므로 재생 공격을 방지할 수 있다.

본 논문에서 제안한 기법은 공장 설비 모니터링 환경과 같이 센서 노드의 위치가 규칙적이고 센서 노드에 엑츄에이터가 연결되어 노드를 배포하기 전에 위치 정보를 관리 서버가 가지고 있는 지그비 무선센서 네트워크 어플리케이션에서 무선 통신 구간에서 악의적인 공격으로부터 센서로부터 수집되는 정보와 엑츄에이터 제어 정보에 기밀성, 무결성 그리고 가용성을 제공할 것으로 기대된다.

향후 필요한 과제는 실제 지그비 무선 센서 네트워크 환경에서 제안된 기술을 구현하는 것이다.

References

[1] Akyildiz, Ian F., et al., "Wireless sensor networks: a survey", Computer networks 38.4, (2002) pp. 393-422.

[2] Rajesh K. M., et al., "Efficient Patient Monitoring for Multiple Patients Using WSN", In Advances in Mobile Network, Communication and its Applications (MNCAPPS), 2012 International Conference on. IEEE, pp.87-90, 2012. DOI: https://doi.org/10.1109/mncapps.2012.23

[3] Hyunjue Kim and Jong-Moon Chung., "USN Security Enhancement Using System IDs", Journal of the Institute of Electronics Engineers of Korea.,, Vol. 46, No. 2, (2009) pp.73-80

[4] Hosein Marzi and Arash Marzi, "A Security Model for Wireless Sensor Networks", Computational Intelligence and Virtual Environments for Measurement System and Applications (CIVEMSA), 2014 IEEE International Conference on. IEEE, (2014).

[5] Daojing H., et al., "Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks", Parallel and Distributed Systems, IEEE Transactions on 26.4, pp.1129-1139, 2015. DOI: https://doi.org/10.1109/tpds.2014.2316830

[6] Wenliang D., et al., "A Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge", INFOCOM 2004. Twenty-third AnnualJoint conference of the IEEE computer and

communications societies. Vol. 1. IEEE, 2004.
DOI: https://doi.org/10.1109/infcom.2004.1354530

[7] Martincic, F. and Schwiebert L., "Introduction to Wireless Networking", Handbook of Sensor Networks: Algorithms and Architectures. Hoboken, NJ, USA: John Wiley & Sons, 2005.
DOI: https://doi.org/10.1002/047174414x.ch1

[8] Alemdar, H. and D. Ersoy. "Wireless Sensor Networks for Healthcare: A Survey", Computer Networks 54.15, pp.2688-2710, 2010.
DOI: https://doi.org/10.1016/j.comnet.2010.05.003

[9] Eschenauer, L., Gligor, V.D. "A Key-management Scheme for Distributed Sensor Networks", In:ACM CCS, pp.41-47, 2002.
DOI: https://doi.org/10.1145/586110.586117

[10] Liu, D., Ning, P. "Establishing pairwise keys in distributed sensor networks", In ACM CCS, pp.52-61, 2003.
DOI: https://doi.org/10.1145/948117.948119

[11] ZigBee Alliance., "ZigBee-2007 Specification.", ZigBee Document 05347r17.Jan. (2008).

[12] Mohaisen, A., Nyang, D., "Hierarchical grid-based pairwise key pre-distribution scheme for wireless sensor nets", In: EWSN, pp.83 - 98, 2006.
DOI: https://doi.org/10.1007/11669463_9

[13] Liu, D., et al, "Establishing Pairwise Keys in Distributed Sensor Networks." ACM Trans. Inf. Syst.Secur. 8, pp.41 - 77. 2005.
DOI: https://doi.org/10.1145/1053283.1053287

[14] Hwang, J., Kim, Y., "Revisiting random key pre-distribution schemes for wireless sensor networks", In: SASN, pp.43 - 52, 2004.
DOI: https://doi.org/10.1145/1029102.1029111

[15] Young-Il Kim., "A Study on Data Processing Methodology of Picking System using Zigbee Wireless Communication", The Journal of the institute of Internet, Broadcasting and Communication, Vol. 13, No. 6, (2013) pp.269-274

저자 소개

조 양 희(정회원)

- 2001년 : 숭실대학교 컴퓨터학부 학사
- 2011년 : 숭실대학교 컴퓨터학과 석사
- 2014년 : 숭실대학교 컴퓨터학과 박사 수료

<주 관심분야 : 임베디드 시스템, 센서 네트워크, 보안, 원격 모니터링 시스템>

박 재 표(정회원)

- 1998년: 숭실대학교 컴퓨터학과 석사
- 2004년: 숭실대학교 컴퓨터학과 박사
- 2008년 ~ 2009년: 숭실대학교 정보미디어 기술 연구소 전임연구원
- 2010년 ~ 현재: 숭실대학교 정보과학대학원 교수

<주 관심분야 : 컴퓨터 통신, 보안, 암호학, 멀티미디어 통신>

양 승 민(정회원)

- 1978년 : 서울 대학교 전자공학과 학사
- 1983년 : Univ. of South Florida 전산학과 석사
- 1986년 : Univ. of South Florida 전산학과 박사
- 1987년 ~ 1991년 :Univ. of Texas at Arington 조교수
- 1993년 ~ 현재 : 숭실대학교 컴퓨터학부 교수

<주 관심분야 : 실시간 임베디드 시스템, 결함 허용, 센서 네트워크, 운영체제 >