情 報 保 護 學 會 誌
第20卷 第5號, 2010. 10

스마트 그리드 환경에서의 키 관리 기술 동향 분석

최 동 현*, 원 동 호*, 김 승 주*

요 약

최근 지구 온난화와 같은 환경 문제와 에너지 소비 증가에 따른 에너지 확보의 어려움에 많은 국가들이 어려움을 겪고 있다. 이러한 에너지 확보 문제와 지구 온난화라는 문제를 해결할 수 있는 방법으로 제안된 것이 스마트 그리드 (Smart Grid) 이다. 스마트 그리드란 기존 전력망에 IT기술을 접목하여 공급자와 소비자가 양방향으로 실시간 전력정보를 교환함으로써 에너지 효율을 최적화하는 전력망이다. 기존의 폐쇄이던 전력망이 다양한 이해당사자가 참여하는 상호운용성이 보장되는 개방형 구조를 가지게 됨으로써 이에 대한 보안 기술 개발이 시급한 상태이다. 따라서 본고에서는 이러한 스마트 그리드 환경에 대해 설명하고, 이러한 환경에서의 안전한 키 관리 기술에 대한 동향을 살펴본다.

Ⅰ. 서 론

최근 지구 온난화와 같은 환경 문제와 에너지 소비 증가에 따른 에너지 확보의 어려움에 많은 국가들이 어려움을 겪고 있다. 이를 위해 태양열, 풍력 발전과 같은 친환경 에너지의 생산부터, 온난화의 원인인 CO_2 배출의 규제, 친환경 제품 사용 및 전력 에너지의 효율적인 송·배전 등과 같이 에너지와 직간접적으로 관련 분야에서 광범위하게 논의되고 있다. 이러한 논의 중 최근 들어 가장 이슈가 되고 있는 것은 스마트 그리드 (Smart Grid) 이다. 스마트 그리드란 기존 전력망에 IT기술을 접목하여 공급자와 소비자가 양방향으로 실시간 전력정보를 교환함으로써 에너지 효율을 최적화하는 차세대 전력망을 의미한다. 전력망이 스마트 그리드로 진화되면, 양방향 실시간 정보교환을 통하여 합리적 이고 효율적인 에너지 소비를 유도함으로써 고품질의 에너지 및 다양한 부가서비스의 제공이 가능해지고, 운영시스템의 개방적인 특성에 따라 신재생에너지발전, 전기차 등 청정 녹색기술의 접목 및 확장이 용이해 지게 된다 [1-4].

이러한 스마트 그리드 환경에서는 신재생 에너지인 풍력, 태양광 등이 전력계통에 연계됨으로써 전력망 연결 접점이 많아지고, 기존 폐쇄적이던 전력망에 다양한 이해당사자가 참여함으로써 상호운영성이 보장되는 개방형 구조를 가지게 됨으로써 이에 대한 보안 기술 개발이 시급한 상태이다.

본고에서는 이러한 스마트 그리드 환경의 보안 위협을 해결할 수 있는 방법 중 안전한 키 관리 기술에 대한 동향을 살펴본다.

Ⅱ. 스마트 그리드

스마트 그리드의 구성요서에 대해서는 각 국가별로 조금씩 차이가 존재한다. 이는 스마트 그리드가 개발 완료된 시스템이 아니라 개발 중인 시스템이기 때문이다. 일반적으로 스마트 그리드를 구성하기 위해 요구되는 주요 구성요소는 다음과 같다.

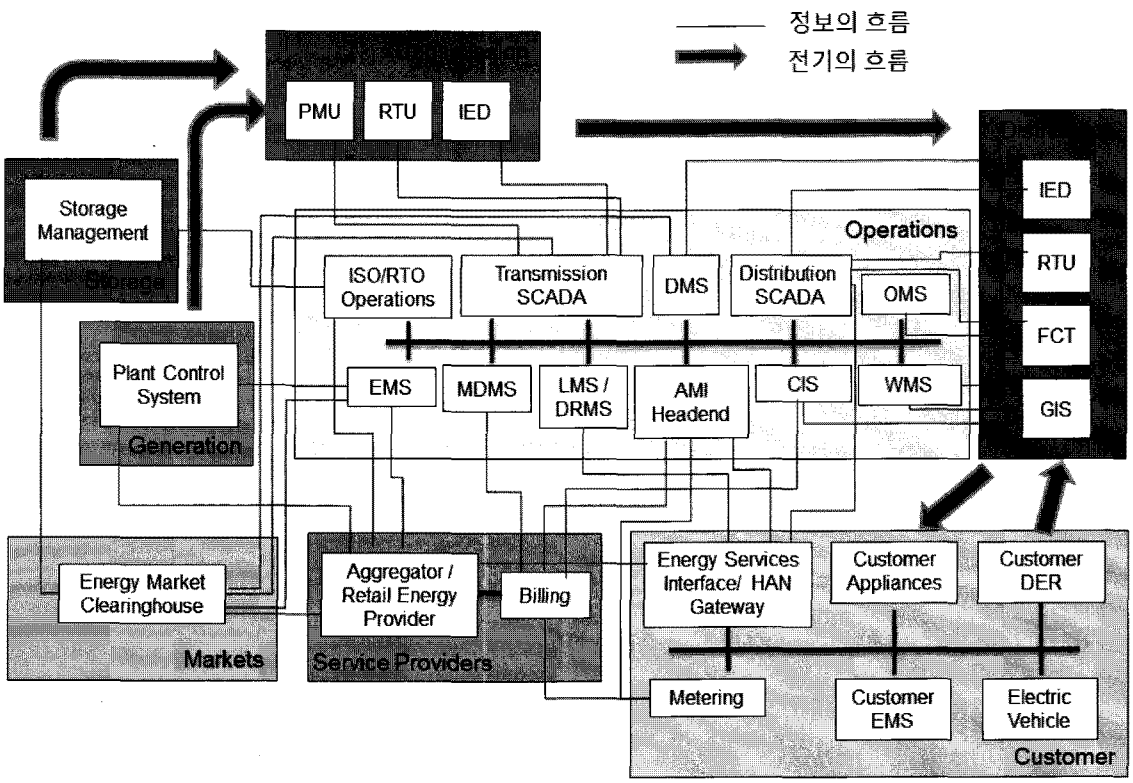
먼저 전력의 송배전 등을 안전하고 효율적으로 관리하는 SCADA와 다양한 전력 관련 정보의 전달에 사용되는 통신로, 전력의 계량과 관련된 고도화된 검침 기반 시설 (Advanced Metering Infrastructure), 사용자와 기기 간 정보 전달을 위한 시각화 기법 및 기기간의 호환성 등에 대한 인터페이스 등이 스마트 그리드의 주요 구성요소로 언급되고 있다.

이러한 스마트 그리드의 전체 구성과 그 안에서의 전기와 정보의 흐름을 표현한 것이 [그림 1]이다[5-6].

그림에서 사용된 용어는 다음과 같다.

- Customer EMS (Customer Energy Management

* 성균관대학교 정보보호연구소 ({dhchoi, dhwon, skim}@security.re.kr)



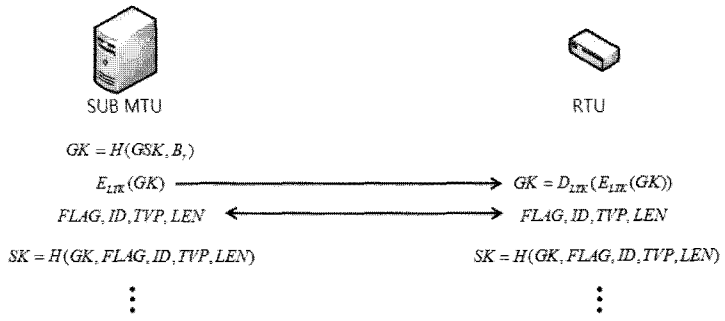
〔그림 1〕 스마트 그리드 구성도

System) : 고객 에너지 관리 시스템으로 고시된 전력 가격에 따라 전력 사용량을 조절하고, 잉여 전력을 판매함

- EMS (Energy Management System) : 전력의 수요에 맞게 효율적인 전력 생산이 가능하도록 관리하는 시스템
- PCS (Plant Control System) : 발전소를 관리하는 시스템
- DMS (Distribution Management) : 배전을 관리하는 시스템
- LMS/DRMS (Load Management System/Demand Response Management System) : 전력의 송배전 데이터와 각 가정의 전력 사용량을 분석하고 이를 관리하는 시스템
- OMS (Outage Management System) : 단전을 관리하는 시스템
- WMS (Work Management System) : 수리가 필요한 작업을 관리하는 시스템
- CIS (Customer Information System) : 고객 정보를 관리하는 시스템
- GIS (Geographic Information System) : 지리 정보를 제공하는 시스템
- FCT (Field Crew Tools) : 무선 통신이 가능한 단말기로 배전과 고객, 지리정보를 이용하여 작업자가 이를 활용하여 단전 등의 기타 수리를 진행함
- ISO/RTO (Independent System Operator/Regional Transmission Oraganization) : 독립 시스템 운영기관/지역 송전 기관
- PMU (Phasor Measurement Unit) : 송전과정의 electrical wave를 측정하는 장치
- IED (Intelligent Electronic Device) : RTU와 동일한 기능을 수행함

Ⅲ. 키 관리 기술 동향

현재 이러한 스마트 그리드와 관련하여 안전한 키 관리 기술이 연구되고 있는 분야는 SCADA와 AMI 부분이다. 본 고에서는 SCADA에서의 키 관리 기술에 대해



〔그림 2〕 SKE에서 세션키 생성 과정

살펴보고자 한다.

3.1 SKE(Sandia Key Management) [7]

SKE는 SANDIA에서 연구한 키 관리 프로토콜이다. SKE에서 사용되는 통신 방식은 [그림 2]에서 보는 것처럼 SUB-MTU(SUB-Master Terminal Unit) 와 RTU(Remote Terminal Unit) 또는 MTU와 RTU사이의 통신에서 사용되는 C-S(Controller to Subordinate)와 SUB-MTU사이의 통신에 사용되는 P2P 통신으로 구분한다. SKE에서 제안된 주요한 통신 전략은 C-S통신 즉 제어장치와 종속장치간의 통신이다. 만약 SUB-MTU와 RTU사이의 통신이라면 여기서 SUB-MTU가 제어장치가 되고 RTU는 종속장치가 된다. SKE에서 제어장치와 종속장치 사이에 사용되는 키는 다음과 같다.

- LTK(Long Term Key) : 각각의 제어장치와 종속장치 사이에 수동적으로 배포된 키로 GK를 생성하는데 사용된다.
- GSK(General Seed Key) : KDC에 의해서 생성된 랜덤한 비트열로 GK를 생성할 때 사용된다. 여기서 KDC(Key Distribution Center)는 MTU와 HMI와 같이 물리적으로 안전한 곳에 설치되며 SCADA 시스템에서 사용할 키를 관리하는 역할을 한다.
- GK(General Key) : 제어장치와 종속장치 사이에 공유된다. 이것은 제어장치에 의해서 생성되며 GSK와 LTK를 사용한다. 이것은 제어장치에서 생성되어 LTK로 암호화되어서 종속장치로 전송된다.
- SK(Session Key) : 실제로 전송하려고 하는 데이터를 암호화하는데 사용되는 키 이다.

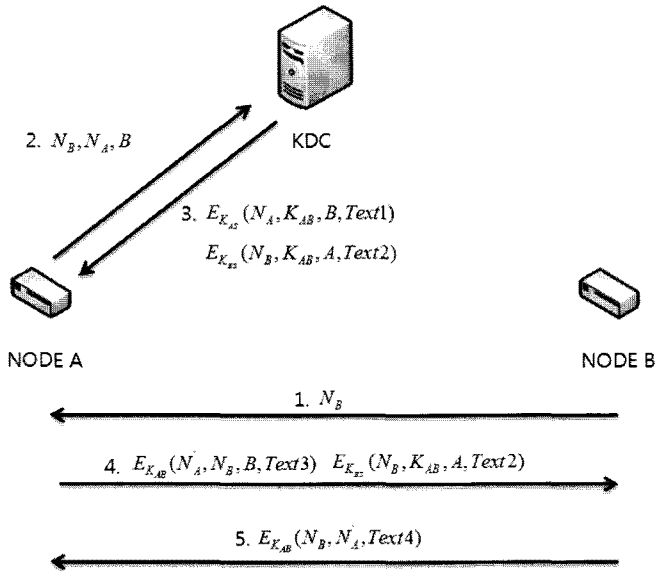
여기서 KDC는 시스템에서 각각의 장치들이 사용하는 키를 관리하는 기능을 한다. 제어장치와 종속장치는 LTK를 공유하고 있다. 제어장치는 KDC로부터 받은 GSK와 자신이 생성한 랜덤한 비트 열 Br을 해쉬 하여 GK를 생성한다. 이렇게 생성된 GK는 LTK로 암호화하여 종속장치로 전송한다.

이렇게 해서 제어장치와 종속장치가 공유하고 있는 GK가 생성되고 각 세션마다 해당 GK로 세션키를 생성한다. 세션키 SK는 공유하고 있는 GK, FLAG, ID, 시간변수 TVP, 그리고 메시지길이 LEN을 해쉬 하여 생성한다. GK가 공격자에 의해서 공격 받게 된다면 제어장치가 다시 GK를 생성하여 업데이트 한다.

SUB-MTU간의 통신은 P2P통신으로 키 교환을 위해 공개키 암호 알고리즘을 사용한다. KDC는 각각의 SUB-MTU에게 공개키와 개인키 쌍을 할당한다. SUB-MTU는 이렇게 받은 키쌍을 이용하여 통신하고자 하는 SUB-MTU와 키 교환 알고리즘을 이용하여 CK(Common Key)를 공유한다. CK는 C-S에서 GK와 같은 역할을 하게 된다.

3.2 SKMA [8]

Queensland University of Technology에서 연구해서 발표한 SKMA는 SCADA 시스템을 위한 키 관리 방식이다. SKE가 공개키 암호 알고리즘을 사용하는 반면 SKMA는 대칭키 암호 알고리즘으로만 이루어져 있다는 장점이 있다. 여기서 노드는 RTU, SUB-MTU,

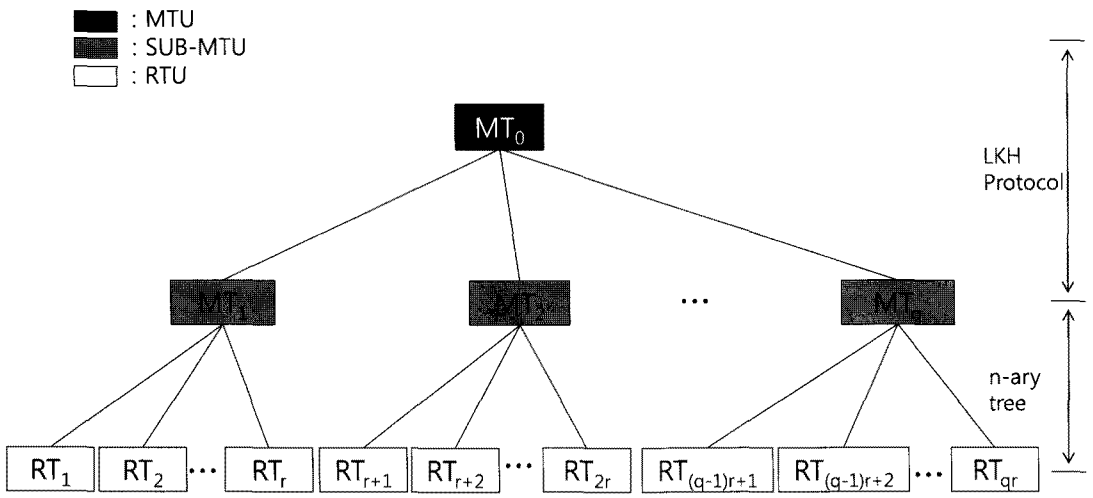


〔그림 3〕 SKMA 키 관리 방식

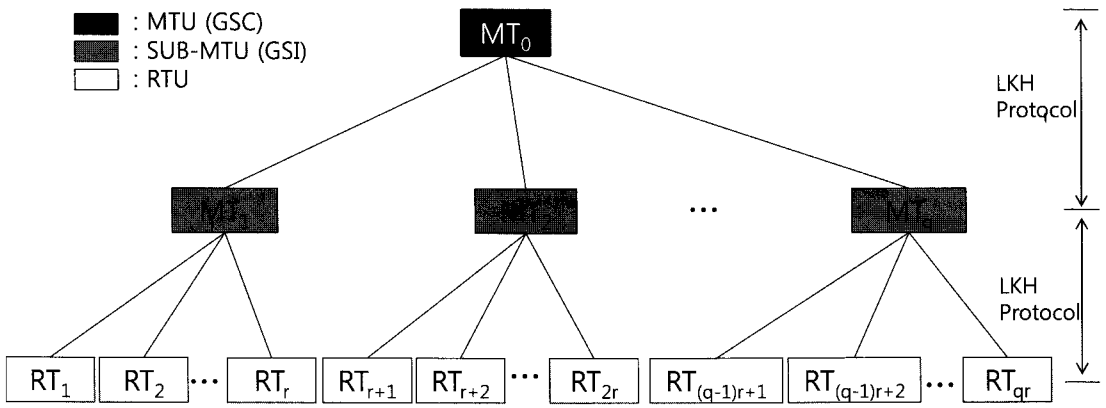
MTU 모두 될 수 있다. SKMA에서 사용되어지는 키는 다음과 같다.

- Long term node-KDC key: 이 키는 node와 KDC 사이에 공유되는 키로 통신을 위해 키를 설정할 때 사용된다.
- Long term node-node key : 노드와 노드사이에 공유되는 키 이다.
- Session Key : 메시지를 암호화 하는데 사용되는 키 이다.
- Node-KDC Key : 이 키는 수동적으로 설치되며, node와 node사이의 키를 생성할 때 사용된다.

Node-KDC 키는 노드가 시스템에 배포되기 전에 설치된다. 새로운 노드가 추가될 때 node-node 키가 [그림 3]과와 같은 과정을 통해서 교환된다.



〔그림 4〕 ASKMA 키 관리 구조



〔그림 5〕 ASKMA+ 키 관리 구조

위와 같이 SKMA에서는 서버와 노드 A, 노드 B간의 3자간 키 확립 프로토콜을 사용하는데 이는 ISO 11770-2 메커니즘 9를 기본으로 한다 [9]. 통신에서 데이터를 암호화하는데 사용되는 세션키는 3자간 키 확립 프로토콜로 얻은 node-node 키와, 타임스탬프(세션의 유지기간에 기반을 둔)값의 해쉬하여 생성한다.

키 철회 메커니즘은 KDC에 의해서 수행되어진다. 키가 공격당했다는 사실을 자동적으로 알려주는 알고리즘은 현재 없다. 다만 시스템을 모니터링하다 이상행동을 발견하면 해당 노드와 관련된 키를 철회 한다. KDC 해당 노드의 키가 철회 되었다는 사실을 다른 모든 노드에게 알려야한다. 이때 사용되는 메시지는 각각의 노드와 KDC간의키로 암호화해서 전송되어진다.

3.3 ASKMA [10]

2008년에 Choi 등이 제안한 논문으로 LKH (Logical Key Hierarchy) 구조를 이용한 방식이다. 제안하는 방식의 핵심은 RTU와 SUB-MTU사이의 키는 n-ary 방식으로 구성하고 SUB-MTU와 MTU 사이는 binary tree로 구성하는 것이다. 이를 그림으로 표현하면 [그림 4]와 같다.

제안된 방법은 SKE 와 SKMA 방식이 broadcasting을 지원하지 못하는 반면에 ASKMA는 이를 지원하는 장점을 가지고 있다. 또한 이러한 키 관리 구조를 통해 RTU에 저장되는 키의 수를 최소화 하여 성능상의 제약을 가지고 있는 RTU에 계산상의 많은 부하가 걸리는 것을 방지하였다.

3.4 ASKMA+ [11]

2010년에 Choi 등이 제안한 논문으로 이전에 제안한 ASKMA에 효율성을 보다 향상시킨 논문이다. 제안하는 핵심아이디어는 다음과 같다. 먼저 키 관리 구조를 MTU와 SUB-MTU 그리고 SUB-MTU와 RTU로 나누고 각각의 키 관리 구조를 LKH(Logical Key Hierarchy) 구조로 구성하는 것이다. 그리고 이 두 개의 구조를 Ioulus Framework를 이용하여 연결시키는 방식을 제안하고 있다. 구조는 [그림 5]와 같다.

제안하고 있는 방식은 RTU와 SUB-MTU간의 키 관리를 보다 효율적으로 사용이 가능하게 하였다. 또한 각각의 SUB-MTU가 분리됨으로써 서로 영향을 주지 않아 더욱더 효율적이게 되었다.

Ⅳ. 결론

본고에서는 스마트그리드 환경에 대해 살펴보고 이에 따른 키 관리 방식에 대해 살펴보았다. 현재까지는 스마트 그리드 중 전력의 송배전과 관련된 SCADA와 관련된 키 관리에 대한 연구가 진행되어 있는 상황이지만 그 외 부분의 경우 연구가 미흡한 상황이다. 따라서 보다 안전한 스마트 그리드 환경을 만들기 위해 이와 관련한 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] 독고지은, 유지연, 이숙연, 임종인, 이경복, "스마트 그리드에서의 소비자 참여와 보안 이슈", 정보보호

학회지, 제19권 제 4호, pp. 21-35, 2009미국 전력 사업의 문제점", Aisa-Pacific Review, 08. 2009.

[2] 이일우, 박완기, 박광로, 손승원, "스마트 그리드 기술 동향", 한국통신학회지 (정보와통신), 제26권 제9호, pp. 24-33, 08. 2009.

[3] 전용희, "지능형 전력망과 정보보호", 정보보호학회지, 제19권 제4호, pp. 66-71, 08. 2009.

[4] 이정준, "AMI 기술 동향", 조명·전기설비, 제23권 제6호, pp. 27-31, 12. 2009.

[5] NIST, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0", NIST. Special Publication, 01. 2010.

[6] NIST, "Smart Grid Cyber Security Strategy and Requirements", Draft NISTIR 7628, 02. 2010.

[7] C. Beaver, D. Gallup, W. Neumann, and M. Torgerson, "Key Management for SCADA", 2002. [Online]. Available: http://www.sandia.org/scada/documnets/013252.pdf

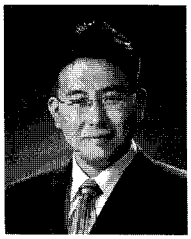
[8] R. D. Colin, C. Boyd, J. Manuel, and G. Nieto, ""KMA-A key management architecture for SCADA systems,"" in Proc. 4th Australasian Inf. Security Workshop, Vol.54, pp. 138-192, 2006.

[9] Information Technology - Security Techniques - Key Management - Part 2: Mechani는 Using Symmetric Techniques ISO/IEC 11770-2 International Standard, 1996.

[10] D. Choi, H. Kim, D. Won, and S. Kim, "Advanced Key Management Architecture for Secure SCADA Communications", IEEE Transactions on Power Delivery, Vol.24, No.3, pp. 1154-1163, 2009.

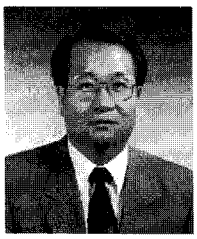
[11] D. Choi, S. Lee, D. Won, and S. Kim, "Efficient Secure Group Communications for SCADA", IEEE Transactions on Power Delivery, Vol.25 No.2, pp. 714-722, 2010.

〈著者紹介〉



최 동 현 (Dong Hyun Choi)
학생회원

2005년 성균관대학교 정보통신공학부 졸업(학사)
2007년 성균관대학교 대학원 전자전기컴퓨터공학과 졸업(공학석사)
2010년 성균관대학교 대학원 휴대폰학과 졸업(공학박사)
<관심분야> 암호이론, 모바일 보안, 보안성 평가, DRM, SCADA



원 동 호 (Dong Ho Won)
종신회원

1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1992년~1994년 성균관대학교 전자계산소 소장
1995년~1997년 성균관대학교 교학처장
1997년~1998년 정보화추진위원회 자문위원 (발령 정보화추진위원회 위원장 국무총리)
1999년~2001년 성균관대학교 정보통신대학원 원장
2002년~2003년 한국정보보호학회 회장
2002년~2004년 대검찰청 컴퓨터 범죄 수사 자문위원
2002년~2004년 성균관대학교 연구처장
2002년~2003년 감사원 IT 감사 자문위원
2002년~2004년 산학연 정보보안협의회 회장
2005년~현 재 정보보호인증기술연구소 소장
2005년~2008년 한국정보보호진흥원 이사
2009년~현 재 성균관대학교 BK21 사업단장
<관심분야> 암호이론, 정보이론, 정보보호

김 승 주 (Seungjoo Kim)
종신회원

1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년: 한국정보보호진흥원 팀장
2004년~현재: 성균관대학교 정보통신공학부 교수
2001년~현재: 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년~현재: 교육인적자원부 유해정보차단 자문위원, 디지털 콘텐츠유통협의체 보호기술워킹그룹 그룹장
2007년~현재: 대검찰청 디지털수사 자문위원, KISA VoIP 보안기술 자문위원, 기술보증기금 외부 자문위원, 전자정부 서비스보안위원회 사이버침해사고대응 실무위원회 위원
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET