모바일 환경에서의 보안 기법 연구

최경호* 김정식* 임을규*

*한양대학교 정보통신학과

Study on Security Mechanism in Mobile Environments

Kyoung-Ho Choi* Jung-Sik Kim* Eul Gyu Im*

*Department of Information and Communication, Hanyang Univ.

요 약

유무선 네트워크의 발전으로 인해 언제 어디서나 자신이 원하는 작업을 할 수 있으며 정보를 얻을 수 있는 유비쿼터스 환경이 구축되고 있다. 사용자들은 이동성이 뛰어난 모바일 디바이스를 통하여 다양한 네트워크에 접속을 할 수 있으며, 이는 예전보다 더 많은 정보를 사용자가 주고받을 수 있음을 의미한다. 유비쿼터스 시대의 이동성이라는 장점은 개인 정보의 유출이 예전보다 다양한 방법으로 이루어질 수 있다는 문제점을 파생하였다. 따라서 유비쿼터스 컴퓨팅 환경이 우리 삶에 편리하면서도 안정적으로 정착하기 위해서는 적합한 보안 기술들이 고려되어야 한다. 그러나 기존의 유선네트워크가 주요 컴퓨팅 환경이었던 시절에 개발된 보안 기법들은 PC나 서버급 컴퓨터를 대상으로 만들어졌기 때문에 이동성을 우선시하기 위해 저전력 초경량을 목표로 설계된 모바일 디바이스에서는 직접적인 사용이 어려운 실정이다. 본 논문에서는 기존의 보안기법들이 모바일 환경에서 적용되기 어려운 이유를 분석하고 모바일 디바이스에 적합한 보안 알고리즘을 제안한다.

I. 서론

우리는 현재 잘 갖추어진 유선 통신 환경을 통해 원하는 정보를 얻을 수 있고, 또 원하는 작업을 필요한 컴퓨터를 사용해서 수행할 수 있다. 더욱이 최근에 많은 연구진들이 유무선 네트워크, 센서 네트워크, CDMA 망 등이 [1]통합된 환경을 연구하고 있고, 이러한 환경에서 언제 어디서나 원하는 정보를 얻을 수 있는 환경을 구축하려는 노력을 하고 있다. 따라서 미래의 정보 통신 환경은 컴퓨팅 기술과 네트워크 기술이 융합되어 사용자가 언제 어디서나 네트워크에 접속하여 원하는 정보를 얻을 수 있고, 원하는 작업을 수행할 수 있는 환경인 유비쿼터스 환경으로 진화할 것이다. 휴대폰이나 무선 인터넷을 사용할 수 있는 여러 단말기들이 일상생활에 널리 보급되어지면서 우리는 이러한 장치들을 통해서 어느 곳에서나 원하는 정보를 얻을 수 있게 되어, 정보의 이동성이 용이해 졌다. 그러나 앞서 언급했던 유비쿼터스 시대의 장점인 언제 어디서든 정보의 획득이 가능하다는 점은 장점인 동시에 정보의 유출이라는 단점이 된다. 또한 이러한 정보 유출문제 외에 개인의 프라이버시 문제가 발생하게 된다. 이러한 개인의 프라이버시는 사용자가 외부로 드러내지 않기 원하는 정보일 수 있기 때문에 이러한 정보의 유출은 유비쿼터스 환경 구현에 심각한 문제점이 될 것이다.

그렇기 때문에 유비쿼터스 환경이 우리의 삶에 편리하고 안정적으로 정착되기 위해서는 보안 기술이 필수적으로 고려되어야 한다. 즉 우리가 쉽게 휴대할 수 있는 모바일 디바이스에서의 데이터 기밀성(security)과 무결성(integrity)을 제공하는 메커니즘을 필요로 하게 된다. 이미 유선환경에서 사용되는 여러 보안 메커니즘들이 있지만, 이러한 유선환경에서 사용되는 보안 메커니즘들을 모바일 환경에 그대로 적용하여 사용하기에는 모바일 환

1)
본 연구는 한국과학재단 특정기초연구 (R01-2006-000-11196-0)지원으로 수행되었음.

경의 여러 가지 제약들, 특히 제한된 자원 때문에 어려운 실정이다. 보안기술의 핵심 요소인 암호기술의 경우는 일반적으로 암호화 알고리즘이 다수의 연산을 필요로 하는 복잡한 수학을 기반으로 한다. 그리고 이러한 복잡한 연산은 전력 소모와도 직결되는데 모바일 디바이스 같은 경우는 유선 네트워크에서의 PC나 서버급 컴퓨터 보다 컴퓨팅 능력이 떨어지거나 전력이 충분히 공급되기 어려운 상황이다. 이와 같은 이유로 배터리로 동작되는 대부분의 모바일 디바이스가 여러 복잡한 보안 루틴을 실행하는 동안 순간적으로 배터리 전하가 고갈 될 수 있다. 이것은 시스템이 동시에 실행하는 음성통신 같은 실시간 태스크를 방해함은 물론 다수의 사용자에게 보안 위협이 될 수도 있다. 따라서 유비쿼터스 환경에서의 모바일 단말기에 적용될 수 있는 보안 기술을 고려할 때에는 저전력으로도 실행될 수 있는 초경량 보안 기법을 먼저 고려해 보아야 한다.

본 논문에서는 1장에서 기존의 모바일 환경에서의 보안 기법을 정리하고, 2장에서는 우리가 제안하는 모바일 환경에 적합한 새로운 보안 기법을 소개하며, 3장에서는 기존의 방법과 비교 분석을 하고, 4장에서 결론 및 향후계획을 제시하겠다.

II. 본문

1. 기존의 보안 기법 분석

1) WEP (Wired Equivalent Privacy)

무선 랜 표준인 IEEE 802.11에서는 보안을 위한 기법인 WEP라는 것을 제안하고 있다. WEP는 유선 랜에서 기대할 수 있는 것과 같은 수준의 접근제한과 프라이버시를 무선 랜에서도 구현하기 위해 제안된 보안 프로토콜이다. 무선 랜은 통신에 전파를 이용하기 때문에 아무런 보안장치가 없다면 전선이나 장비에 물리적으로 접근해야만 통신 내용을 도청할 수 있는 유선 통신과는 달리 유효반경 내에 위치하는 어느 누구든지 통신 내용을 도청할 수 있게 된다.[1] 이를 보안하기 위해 고안된 기술이 WEP로 설정된 WEP key를 아는 사람만을 랜으로의 접근을 허용해 원하지 않는 제3자가 무선 랜으로 접근하지 못하도록 한다. 그림 1은 WEP의 암호화 구조를 보여준다.

40비트의 RC4 secret key와 24비트의 IV(Initial Vector)를 연접하여 64비트의 seed 값을 생성한다. 이 seed 값을 RC4 기반의 WEP PRNG(Pseudo Random Number Generator)의 입력으로 사용하여 pseudo random key sequence를 생성한다. 데이터

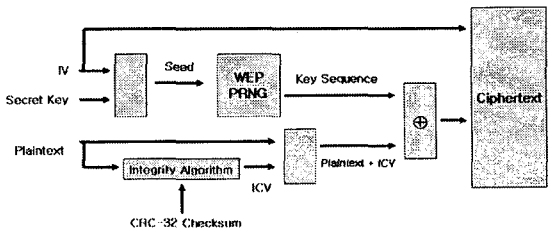

그림 1 WEP의 암호화 구조

는 데이터 무결성을 위해 평문(plaintext)에 무결성 알고리즘(CRC-32 checksum)을 사용하여 ICV(Integrity Check Value)를 생성하고, 이를 평문과 연접한다. 평문과 ICV를 연접한 값에 key sequence를 XOR하여 암호문(ciphertext)을 생성하게 되며, 이 암호문에 IV 24비트와 key sequence ID 2비트, 패딩 6비트가 추가되어 전송된다.[2]

그러나 WEP에는 몇 가지 취약점들이 발견되고 있다. 첫 번째는 RC4 스트림 암호가 같은 키를 두 번 사용한다는 특성상 발견되는 취약점으로 이 방식을 사용하는 WEP 프로토콜 또한 안전하다고 할 수 없다. 두 번째는 IV의 크기가 24비트로 매우 작아서 재생공격에 안전하지 못하다는 점이다. IV가 24비트의 길이를 가지고 있기 때문에 이는 한 패킷 당 2^{24}개의 키 중에 하나를 선택하여 전송하게 되고, 이 조합이 다 고갈되고 나면 IV를 다시 시작하게 된다. 이는 초 당 11M 비트를 전송하는 네트워크에서 5시간 이내에 가능한 키 조합이 고갈되어 질 수 있다. 세 번째는 키 스트림의 재생공격에 대한 취약성이다. 서로 다른 두 개의 메시지에 대하여 모두 같은 키와 IV 쌍으로 이루어진 키 스트림을 사용하기 때문에 관찰된 두 메시지로부터 정보를 얻어낼 수 있게 된다.

2) WPA (Wi-Fi Protected Access)

WPA는 Wi-Fi 무선 랜 사용자를 위해 개발된 무선 랜 보안 표준 중 하나이다. WEP는 복잡하지 않은 가정용으로는 아직도 유용하지만 대량의 메시지 흐름으로 암호화키가 보다 빨리 발견될 수 있는 기업용으로는 충분치 않은 것으로 판단된다. WPA는 WEP보다 정교한 데이터 암호화를 제공하고, 사용자 인증이 다소 불충분했던 WEP와는 달리 완전한 사용자 인증 기능을 제공한다.[3] WPA는 TKIP(Temporal Key Integrity Protocol) 암호화와 802.1x/EAP(Extensible Authentication Protocol)인증에 기반을 두고 있다.

WPA는 개인 및 소규모 무선 랜 환경에 적합한 WPA Personal(WPA-PSK)과 보다 규모가 큰 무

선랜에 적용 가능한 WPA Enterprise(WPA-EAP) 구조로 나누어진다. WPA-PSK 방식은 기존의 WEP 보다 한층 더 보안이 강화된 무선 랜을 구성할 수 있는 방법으로 WEP가 가지고 있던 문제점 중 하나인 기존 40 비트의 키 길이를 128비트로 늘이고, 암/복호화 키가 동일 BSS에서 공유되는 방식에서 벗어나 사용자 별, 네트워크 세션 별, 전송되는 프레임 별로 키를 달리하는 TKIP (Temporal Key Integrity Protocol) 방식을 채택하여 외부의 공격자가 네트워크 도청을 수행하여 수집한 데이터를 기초로 WEP 키를 추출하는 공격에 대한 저항력을 가지도록 하였다. 그 결과 WEP에서 암/복호화 키가 정적이며, 데이터 유출에 의한 공격에 취약했던 점에 비해 WPA-PSK 방식은 암/복호화 키를 요건에 따라서 정교하고 신속하게 생성/갱신하기 때문에 암/복호화 키를 추출하기 위한 데이터 수집단계가 사실상 힘들어지게 된다. WPA Enterprise(WPA-EAP) 방식은 WPA-PSK가 기존 WEP의 암/복호화 키 관리 방식을 중점적으로 보완한 방식인데 비해서 WPA-Enterprise는 사용자 인증영역까지 보완한 방식이다. WPA-EAP는 인증/암호화를 강화하기 위해서 다양한 보안 표준 및 알고리즘을 채택하였는데, 유선 랜 환경에서 포트 기반 인증 표준으로 사용되는 IEEE 802.1X 표준과 이와 함께 다양한 인증 메커니즘을 수용할 수 있도록 IETF의 EAP 인증 프로토콜을 채택하였다. EAP 인증 프로토콜에는 EAP-MD5, EAP-TLS, EAP-TTLS, EAP_SRP, PEAP, LEAP등이 있다. 아직까진 공중 무선 랜 사업자들은 EAP-MD5 수준의 초보적인 인증방법을 주로 사용하고 있는 실정인데, EAP-MD5는 사용자 패스워드와 ID만으로 인증 허가를 내려주기 때문에 보안성이 떨어지는 단점이 있다.

WPA_PSK는 오프라인 PSK 공격(Offline PSK Dictionary Attack)에 취약점을 보이는 것으로 알려져 있다. 이는 TKIP의 PTK(Pairwise Transient Key)를 생성하는데 사용되는 PMK (Pairwise Master Key)가 패스프레이즈(passphrase)와 SSID와 SSID의 길이의 조합으로 생성되었다는 점에 기인한다. 패스프레이즈와 SSID, SSID의 길이가 연결된 스트링은 256 비트를 생성하기 위해 4096번 해쉬 한다. 패스프레이즈는 캐릭터 당 약 2.5비트의 보안 강도를 가지고 있다. 그러므로 n 바이트의 패스프레이즈는 2.5n + 12비트의 보안을 가진 키와 동일한 효과를 가지고 있어 패스프레이즈는 비교적 보안 강도가 낮다. 따라서 짧은 길이의 패스프레이즈를 통해 생성된 키들은 사전 공격에 취약하다. 20 캐릭터 미만의 길이에서 유추된 키는 사전 공격을 당할 수 있다. 4단계 키 교환 프레임의 해쉬값 생성을 위해 PTK를 사용함으로 공격자는 해쉬값에 대한 오프라인 사전 공격을 감행할 수 있으며, 8 캐릭터 미만의 패스프레이즈는 사용자가 사전에서 쉽게 선택하여 공격을 시도할 수 있다.[4] 이 공격은 WEP 공격보다 쉽게 감행할 수 있다.

3) RSN (Robust Security Network)

RSN[5]은 상호인증을 통한 접근제어, 동적인 키 갱신과 강력한 암호 알고리즘을 사용한 새로운 형태의 보안 구조이다. RSN 네트워크를 구축하며 무선 랜 보안요소 중 사용자 인증, 접근제어, 권한 검증, 데이터 기밀성, 데이터 무결성 등 5가지 보안요소를 만족한다. WPA 보안기법과 다른 점은 보다 강력한 암호 알고리즘인 CCMP 알고리즘을 기본 알고리즘으로 정의하고 있으며, 장기적인 관점에서 암호 알고리즘 처리 모듈을 하드웨어 칩셋으로 구현하고자 노력한다는 것이다. 국제표준이 안정화되는 시점에서 칩셋 제조업체의 하드웨어적인 구현이 뒷받침되어야 함으로 실제 일반 사용자들이 널리 사용할 수 있기까지는 상당한 시일이 걸릴 것으로 예측되며, 현재 사용되고 있는 액세스 포인트와 무선랜 카드는 모두 교체되어야 할 것이다. 표 1은 세 가지 보안 기법의 특징을 비교하고 있다.

	WEP	WPA	RSN
Encryption	RC4	RC4	AES
Key Management	None	EAP	EAP
Key Size	40/104 bit	128 bit	128 bit
Data/Header Integrity	CRC32 / None	Michael Algorithm	CCM
Key Life	24 bit	48 bit	48 bit
Replay Protection	None	IV	IV

표 1 기존 보안 기법의 특징 비교

2. 제안하는 모바일 보안 기법

앞선 1장에서 언급했던 기존의 무선 랜 환경에서 사용되고 있던 보안 기법들은 여러 보안상의 문제와 함께 저전력의 연산을 요구하는 모바일 디바이스에는 적합하지 않은 단점을 보여주었다. 2장에서는 저전력의 연산을 요구하는 모바일 디바이스 환경에 맞는 알고리즘을 제안한다. 제안되는 알고리즘은 크게 세션키 교환 부분과 데이터 분류 및 암호화 그리고 데이터 전송 부분으로 구성된

다. 그림 2는 제안하는 알고리즘의 전체적인 구조를 보여준다.

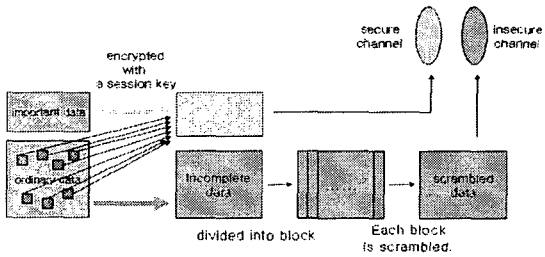

그림 2 모바일 보안 알고리즘 구조

1) 세션키 교환

모바일 디바이스 환경에 적합한 초경량 암호화 기법의 구현을 위해 데이터는 중요한 데이터와 중요하지 않은 데이터로 분류하여 각각 secure channel과 insecure channel을 통하여 전송되게 된다. secure channel을 통해 전송되는 데이터는 암호화가 되어 전송되게 되는데 경량 암호화를 위해 private-key 암호화 알고리즘으로 암호화를 해야 한다. 따라서 제안하는 알고리즘에서는 public-key 암호화 알고리즘을 이용하여 secure channel에서 사용하게 될 세션키(session key)를 교환하는 과정이 필요하게 된다. 공개키 방식에서 가장 널리 사용되는 알고리즘으로 RSA가 있으나, 이는 긴 길이의 키를 사용하여 모바일 디바이스 환경에서 사용하기에는 많은 제약이 따른다.[6] 이에 RSA에 비해 키 길이를 혁신적으로 줄인 타원 곡선의 원리를 이용한 타원곡선암호화(ECC : Elliptic Curve Cryptosystem) 알고리즘을 사용할 수 있다. 표 2는 두 알고리즘의 키 길이를 비교하고 있다. 따라서 우리가 제안하는 알고리즘에서 세션키 교환을 위해 사용할 public-key 암호화 알고리즘은 타원곡선암호화 방식을 사용한 ECDH(Elliptic Curve Diffie-Hellman Key Exchange)방식을 사용하기로 한다.

ECC	RSA	RSA/ECC 키 길이 비교
106	512	4.83 : 1
132	768	5.82 : 1
160	1024	6.40 : 1
211	2048	9.71 : 1
600	21000	35.0 : 1

표 2 ECC와 RSA의 키 길이 비교

2) 데이터 분류 및 암호화

전체 데이터를 암호화할 경우 모바일 디바이스의 특성상 전력 및 연산문제가 발생할 수 있기 때문에 데이터의 보안 강도에 따라 상이한 보안 레벨을 적용하는 메커니즘이 필요하다. 즉, 데이터의 분석을 통하여 제한된 일부 데이터에 대해서만 암호화와 복호화를 수행한다. 암호화를 수행해야 하는 데이터의 분류는 데이터의 중요도에 따라 분류를 해야 하는데 중요도의 판단은 사용자의 판단에 의해 분류하는 방법, 사전에 정한 규칙에 따라 분류하는 방법, 컴파일러를 통하여 분류하는 방법을 생각해 볼 수 있다. 이렇게 분류된 데이터 중 보안이 필요한 데이터들은 ECDH 방식으로 분배된 세션키를 사용하여 암호화를 수행하는데, 암호화 방식으로 AES(Advanced Encryption Standard) private-key 암호화 방식을 사용한다.[7] 이에 반해 보안이 필요 없는 일반 데이터들은 암호화를 수행하지 않고 일정 블록으로 나눈 뒤 간단한 XOR 연산을 기반으로 하는 스크램블을 수행한다. 이때 스크램블 알고리즘을 공개해야 하는데 이럴 경우 공격자가 언스크램블 알고리즘을 통해 원본 데이터를 쉽게 얻을 수 있다는 문제점이 있다. 이 문제의 해결방안으로는 일반 데이터의 일정하지 않은 위치의 블록들은 secure channel로 전송을 하여 공격자가 언스크램블 알고리즘으로 원본 데이터를 얻더라도 완전한 데이터를 얻을 수 없는 방법을 사용할 수 있다. 또는 스크램블 알고리즘의 사용 시 간단한 키를 사용하고, 이 키를 secure channel로 전송하는 방법을 사용할 수 있다.

3) 데이터 전송

중요도에 의해 분류된 데이터들은 AES 암호화 방식으로 암호화하여 보안 강도를 높인 secure channel과 간단한 스크램블 연산으로 최소한의 보안 강도를 유지하는 insecure channel을 통해 각각 전송된다. 수신측에서는 secure channel을 통해 전송된 데이터는 ECDH를 통해 미리 전송된 세션키를 사용하여 복호화 하고, insecure channel을 통해 전송된 데이터는 간단한 언스크램블 연산으로 원본 데이터를 얻게 된다.

3. 기존 기법과의 비교 분석

우리가 제안한 암호화 방식은 아직 컨셉을 제안하는 수준이라 구현이 되지는 않은 상태이다. 따라서 직접적인 성능 비교를 할 수는 없었으나 WEP의 경우는 여러 가지 보안상의 문제점이 있었으며, 저전력의 초경량 모바일 디바이스 환경에는 적합하지 않은 부분이 있었다. 특히 같은 키를

두 번 이상 사용하는 RC4 스트림 암호화의 사용은 다음과 같은 문제를 가지고 있다. 암호를 생성하기 위한 키 스트림 비트를 K1, K2, K3라 가정할 때 sender는 이 키 스트림을 평문 스트림인 P1, P2, P3와 XOR 연산을 하여 암호문 스트림 C1, C2, C3를 생성한다.

$Ci = pi \oplus ki \ (i = 1,2,3, \ldots)$

반대로 receiver는 암호문 스트림 C1, C2, C3와 키 스트림 K1, K2, K3를 XOR 하여 평문 스트림 P1, P2, P3를 복호한다.

$Pi = ci \oplus ki \ (i = 1,2,3, \ldots)$

만약 악의적인 도청자가 i번째 비트의 평문 값을 알아냈다고 가정하면 암호문 스트림은 아래의 식에 의해 i 번째 비트의 키 값을 알아낼 수 있을 것이다.

$Ki = ci \oplus pi$

우리가 제안한 보안 알고리즘에서는 WEP나 WPA 등에서 사용되는 스트림 암호화 기법인 RC4 대신에 블록 암호화 기법인 AES를 보안을 필요로 하는 데이터의 암호화에 사용한다. AES는 RC4에 비해 속도는 약간 느리지만 RC4를 사용함으로써 발생하는 취약점을 피할 수 있다. 또 전체 데이터를 암호화 하는 것이 아니라 중요하다고 판단되는 일부 데이터만을 암호화하기 때문에 속도면에서 크게 뒤떨어지리라 생각하지 않는다. WEP나 WPA 보다 개선되어진 RSN의 경우에는 보안에 초점을 맞춰 개발되어 강력한 암호화 알고리즘을 가지고 있지만, 모바일 디바이스 환경에는 적합하지 않으며 암호 알고리즘 처리를 하드웨어적인 관점에서 해결하려 하기 때문에 기존의 디바이스들을 교체해야 하는 문제점이 있다.

4. 결론 및 향후 계획

기존의 무선 네트워크 보안 기법들은 너무 강한 보안 기법을 찾다보니 모바일 디바이스 환경에는 적합하지 않게 되거나 보안 강도는 다소 약하지만 효율성이 뛰어난 RC4 스트림 암호화 기법을 사용하여 보안상 취약한 문제점을 가지고 있었다. 무선 네트워크 보안 기법 중 모바일 환경에 적합한 암호화 기법은 보안상으로 취약하지 않으면서 초경량 저전력 이어야 한다는 제약사항이 있다. 본 논문에서는 기존 보안 기법들의 단점을 보완하는 모바일 보안 알고리즘의 개념을 제시하였다. 향후 연구 목표로는 제안하는 보안 알고리즘을 구현 하여 기존의 보안기법과 성능을 비교해볼 예정이다.

참고문헌

[1] Borsc, M and Shinde, H, "Wireless security & privacy", Personal Wireless Communications, 2005. ICPWC 2005. 2005 IEEE International Conference on 23-25 Jan. 2005 Page(s):424 - 428

[2] Hassan, H.R. and Challal, Y, "Enhanced WEP: An efficient solution to WEP threats", Wireless and Optical Communications Networks, 2005. WOCN 2005. Second IFIP International Conference on 6-8 March 2005 Page(s):594 - 599

[3] Prasithsangaree, P. and Krishnamurthy, P., "Analysis of tradeoffs between security strength and energy savings in security protocols for WLANs", Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th Volume 7, 26-29 Sept. 2004 Page(s):5219 - 5223 Vol. 7

[4] Wi-Fi-Alliance, "Wi-Fi Protected Access (WPA) Standard," 2002.

[5] Sithirasenan, E. and Zafar, S., Muthukkumarasamy, V., "Formal Verification of the IEEE 802.11i WLAN Security Protocol", Software Engineering Conference, 2006. Australian 18-21 April 2006 Page(s):181 - 190

[6] "RSA Cryptographic Challenges," http://www.rsasecurity.com/rsalabs/challenges/

[7] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," 1998.

[9] P. Prasithsangaree and P. Krishnamurthy, "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," Proc. IEEE Global Communications Conference (Globecom'03), Sanfrancisco, CA, 2003.

[10] "Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode" http://www.linuxjournal.com/article/8312