논문 2006-43TC-7-3

Key Infection의 보안성 향상을 위한 개선된 키 설정 방법

(Security-Enhanced Key Establishment Scheme for Key Infection)

황 영 식*, 한 승 완**, 남 택 용**

(Young-Sik Hwang, Seung-Wan Han, and Taek-Yong Nam)

요 약

기존의 보안 메커니즘들은 센서 노드의 자원의 제약 사항들로 인해 센서 네트워크 분야에서는 적용하기 쉽지 않다. 따라서 센서 네트워크상의 보안 이슈들은 센서 네트워크의 구현에 있어서 선행적으로 해결되어야 하는 문제로 인식된다. 이런 보안 이슈들 중 키 설정은 두 노드들 간의 보안 통신을 위해 초기 단계에서 해결되어야 하는 매우 중요한 보안 요소이다. 최근 R. Anderson 등에 의해 Key Infection이라는 commodity sensor network 상의 키 설정 방법이 제안되었지만 key infection의 경우 공격자가 초기 키 설정 시간에 전송되는 키 정보를 감청할 수 있는 영역이 존재하는 본질적인 취약점을 가지고 있다. 따라서 본 논문에서는 key infection의 위험 영역을 효율적으로 줄이는 보안 메커니즘을 제안함으로써 key infection의 보안성 향상을 위한 키 설정 방법을 제안한다. 제안된 보안 메커니즘은 key infection의 위험 영역을 줄이기 위해 초기 키 설정 시에 다른 이웃 노드의 정보를 추가적으로 이용하여 공유키 쌍(pair-wise key)을 생성한다. 추가적인 키 정보를 이용함으로써 새로운 위험 영역을 얻을 수 있으며 이 영역은 기존 key infection의 위험 영역보다 면적이 감소하였기 때문에 보다 보안이 향상된 키 설정을 할 수 있다. 또한 제안된 보안 메커니즘의 안전성 평가를 위해 논리적, 수학적 관점에서 비교 평가한다.

Abstract

Traditional security mechanisms do not work well in the sensor network area due to the sensor's resource constraints. Therefore security issues are challenging problems on realization of the sensor network. Among them, the key establishment is one of the most important and challenging security primitives which establish initial associations between two nodes for secure communications. Recently, R. Anderson et al. proposed one of the promising key establishment schemes for commodity sensor network called Key Infection. However, key infection has an intrinsic vulnerability that there are some areas where adversaries can eavesdrop on the transferred key information at initial key establishment time. Therefore, in this paper, we propose a security-enhanced key establishment scheme for key infection by suggesting a mechanism which effectively reduces the vulnerable areas. The proposed security mechanism uses other neighbor nodes' additional key information to establish pair-wise key at the initial key establishment time. By using the additional key information, we can establish security-enhanced key establishment, since the vulnerable area is decreased than the key infection's. We also evaluate our scheme by comparing it with key infection using logical and mathematical analysis.

Keywords : 센서 네트워크 보안, 키 설정, Key Infection

I. 서 론

센서 네트워크는 군사용 경계, 생태 감시(monitoring)[1], 환경 감시(monitoring)와 같은 다양한 어플리케이션들을 위한 유용한 기술이다. 따라서 이런 어플리케이션들을 기반으로 하는 유비쿼터스 컴퓨팅(ubiquitous computing) 시대에서는 센서 네트워크는 핵심적인 역할을 하게 될 것이다. 하지만, 센서의 메모리, 컴퓨팅, 에너지 자원의 제한 사항, 노드의 물리적 탈취(capture), 무선 통신 매체의 사용 등으로 인해 보안 문제가 센서 네트워크 분야에서 심각하게 대두되고 있다[2].

* 학생회원, 과학기술연합대학원 정보보호공학 (University of Science & Technology)
** 정회원, 한국전자통신연구원 정보보호연구단 (Electronics and Telecommunication Research Institute)
접수일자: 2006년6월15일, 수정완료일: 2006년7월14일

모든 통신 보안 메커니즘들은 설정된 키의 보안 강도에 의존하기 때문에 키 설정은 매우 중요한 보안 사항으로 인식된다. 전통적인 네트워크분야에서 많은 키 설정 방법들이 제안되어져 왔다. 특히, 공개키 기반의 암호 방식의 경우 복잡한 키 설정 과정을 제거하여 키 설정 과정을 간략화 하였기 때문에 현재 많은 네트워크 키 설정 분야에서 사용되어 지고 있으며[3], 센서 네트워크 분야에서도 몇몇의 공개키 기반의 연구들이 제안되었다[4, 5]. 하지만, 공개키 기반의 암호 방식의 경우 고속 컴퓨팅과 다량의 메모리 및 에너지 자원을 필요로 하기 때문에 센서 네트워크 분야에 적합하지 않다. 따라서 공개키 기반 방식이 아닌 대칭키 기반 방식을 바탕으로 하는 많은 연구들이 현재 센서 네트워크상에서 연구되고 있으며, 다양한 형태의 대칭키 기반의 키 설정 방법들이 제안되었다[6, 7, 8, 9, 10, 11].

대칭키 기반의 암호 방식은 공개키 기반의 암호 방식에 비해 저속의 컴퓨팅과 소량의 자원을 필요로 하기에 현재 센서 네트워크상에서 새롭게 제안된 키 설정 방법들의 대부분은 대칭키 기반의 암호 방식을 기반으로 하고 있다. 특히 센서 네트워크에서 대칭키 기반의 암호 방식을 사용하는 대표적인 키 설정 방법들은 *Random Key Pre-distribution*[7, 8, 9, 10, 11] 과 *Commodity Sensor Network*을 정의하고 그에 맞는 키 설정을 제시한 *Key Infection*[6] 이 있다.

본 논문에서는 commodity sensor network 상의 key infection의 보안성 향상을 위한 키 설정 방법을 제안한다. 또한 향상된 보안 강도의 조사를 위해 제안된 메커니즘과 commodity sensor network 상의 대표적인 키 설정 방식인 기존의 key infection을 논리적, 수학적인 분석을 통해 비교 분석하였다.

본 논문의 구성은 다음과 같다. 우선 관련 연구로 random key pre-distribution과 key infection에 대해 II 장에서 간략하게 설명한다. III장에서는 key infection의 키 설정 과정을 보다 안전하게 하는 핵심 아이디어에 대해 다룰 것이며, IV장에서는 보안이 향상된 키 설정 방법을 보다 구체적으로 설명한다. 이어 V장에서는 제안된 방법의 안정성을 기존의 방식과 비교 분석 하였으며, 끝으로 VI장에서 결론과 함께 향후 연구에 대해 언급한다.

II. 관련 연구

센서 네트워크상의 대표적인 키 설정 방법인 random key pre-distribution의 경우 센서 노드의 메모리에 적재된 키 집합을 이용하여 각각의 센서노드들이 공통의 키들을 가질 확률을 기반으로 키를 설정한다. Random key pre-distribution 방식들은 센서 네트워크상의 키 설정을 위한 유용한 기술로 평가되고 있으나, 이들 방식들은 모든 이웃 센서들과 보안 연결을 보장하지 않으며, 단지 p 확률로 n 개의 보안 연결만을 보장한다. 또한, 센서 노드의 살포 전에 적재되는 키 집합을 저장할 많은 메모리 공간을 필요로 한다. 따라서 random key pre-distribution 방식들은 이런 측면에서 commodity sensor network에 적합하지 않다. 이런 문제를 해결하기 위해 R. Anderson 등은 센서 노드가 살포되기 전 적재되는 키 집합을 필요로 하지 않는 *Key Infection* 방법을 제안하였다[7, 8, 9, 10, 11].

Key infection은 경제적인 측면에서 고비용의 보안 메커니즘이 필요하지 않는 저비용의 보안 메커니즘이 적합한 센서 네트워크인 commodity sensor network를 정의한 후 이에 맞는 키 설정 방식을 제안 하였다. 또한 key infection 모델은 능동적인 공격자들이 일반적 네트워크에 널리 밀집해 있다고 가정하는 기존의 공격 모델과는 달리 능동적인 공격자들이 전체 commodity sensor network에 드물게 존재하는 공격 모델과 센서 노드들 사이의 키 설정 시간이 단지 수초 이내에 이루어진다는 사실을 가정하였다. 이런 가정에서 공격자들은 언제, 어디서 센서 노드들이 살포되어 키를 설정하는지를 사전에 알기는 사실상 불가능하며 공격자들이 초기 키 생성 시간에 센서 네트워크를 공격하기 위해 사전에 포획된 센서 노드를 보유하는 것 역시 쉽지 않다. 그렇기 때문에 key infection 모델은 사전에 분배된 키 집합을 메모리에 저장하기 않으며, 단지 키 설정 시간에 필요한 소량의 정보를 이용하여 키 설정 과정 시에 키 정보들을 평문 형태로 교환하여 메모리에 대한 부담을 줄이고 초기 키 설정 시간의 모든 과정들을 간결화 하였다[6]. 이런 측면에서 key infection 모델은 commodity sensor network의 특성을 잘 고려한 모델이지만 초기 키 설정 시간에 공격자가 키 정보를 도청할 수 있는 취약한 영역들이 존재한다. 따라서 key infection 모델의 초기 교차 영역을 줄일 수 있으면, 보안이 보다 더 향상된 키 설정이 가능하다. 이후 본 논문에서는 이런 취약한 영역을 '초기 교차 영역 (Initial Inter Section : IIS)' 이라고 하겠다.

III. 핵심 아이디어

Key infection 모델의 경우 commodity sensor network을 위한 간결한 초기 키 설정 방식을 다음과 같이 최초로 제안하였다: 일단 모든 센서 노드들이 살포되어지면, 각각의 노드들은 (그림 1의 노드 A) 키 값으로 k_a를 선택한 후 이 값을 주변 노드들에게 평문 형태로 전파(broadcast)한다. 이후 본 논문에서는 이런 역할을 하는 노드를 '전송자 노드(Sender node)' 라고 하겠다). 일단 키 전송이 이루어지면, 전송자 노드의 이웃 노드는 (그림 1의 노드 B) 이 키 정보를 수신한 후, 역시 키 값으로 k_{ab}를 선택한 후 이 정보를 k_a로 암호화한 $\{b, k_{ab}\}k_a$ 값을 이웃 노드들에게 전파하게 된다. 이런 과정을 거쳐 모든 센서 노드들은 공유키 쌍(pair-wise key)을 그들 이웃 노드들과 생성하게 된다. 하지만 이와 같은 key infection 모델의 경우, 전송자 노드가 키 정보를 최대 출력으로 전파하기 때문에 위의 초기 키 설정 시간에 키 정보를 도청하기 쉽다. 그림 1은 이 방식을 도식화하고 있다.

이런 공격자의 도청 위험을 줄이기 위해 key infection 모델에서는 *Key Whispering* 이라는 방식을 추가적으로 제안하였다. Key whispering의 경우, 각각의 노드들이 키 정보를 최대 출력으로 전파하지 않고 초기 전송 범위에서 이웃 노드들이 응답이 올 때 까지 조금씩 전송 범위를 점차 확대해나가는 전파 방식을 채택하였다. 따라서 key whispering 방식에서 공격자는 그림 2의 초기 교차 영역(IIS)에 있지 않는 한 키 정보를 도청할 수가 없게 되며, 설사 이 공간에 공격자가 있다 해도 단지 0.8% 정도의 링크수가 노출된다[6].

비록 key infection 모델에서 공격자에 의해 한 개의 센서 노드의 정보가 누출되는 파급이 0.8% 이지만, 실제적인 초기 공격의 위험은 센서 네트워크의 전체 면적에 대비 초기 교차 영역의 비율과 관계가 있다.

Key infection의 key whispering에는 두 노드의 (그림 2의 노드 A, B) key whispering 범위에 의해 생성된 초기 교차 영역(IIS)이 존재하며, 초기 교차 영역 상에서 전송자 노드는 키 정보를 평문의 형태로 전송한다. 수신자는 이 키 정보를 이용하여 공유키 쌍(pair-wise key) 정보를 전송하기 때문에 공격자가 초기 교차 영역에 존재하면 이 공유키 쌍(pair-wise key) 값은 노출된다. 따라서 key infection 모델에서 보다 강화된 보안 키 설정 과정을 얻기 위해서는 이 초기 교차 영역(IIS)을 줄여야 한다.

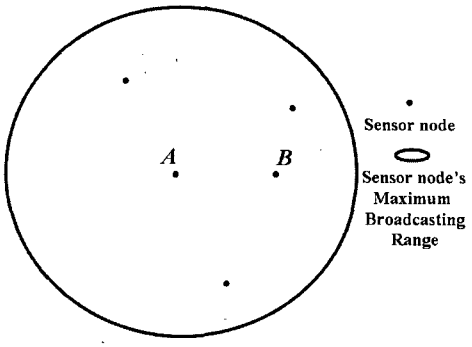


그림 1. Key infection에서의 최대 전파 (broadcasting) 방식
Fig. 1. Broadcasting method in Key Infection.

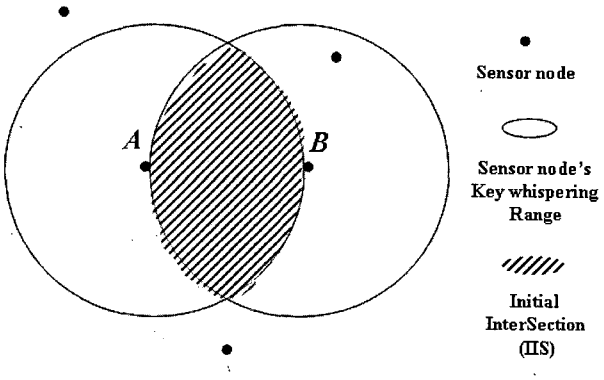


그림 2. Key infection 모델에서의 key whispering 방식
Fig. 2. Key whispering method in Key Infection.

본 논문의 주요 접근 방식에서는 key infection의 초기 교차 영역(IIS)을 줄이기 위해 다른 노드의 키 정보를 추가적으로 이용한다. 그림 2와 달리 본 방식에서는 노드 A와 B는 추가적으로 노드 A의 또 다른 이웃 노드(노드 B를 제외한 이웃 노드)로 부터 키 정보를 받는다. 추가적인 키 정보를 받게 됨으로써, 3개의 노드들 (e.g. 그림 3의 노드 A, B 와 A의 또 다른 이웃 노드 C)의 key whispering 범위에 의해 생성되어진 감소된 초기 교차 영역(Reduced-IIS)을 얻을 수 있다. 이 범위는 기존의 초기 교차 영역의 면적에 비해 감소하였기 때문에 공격자가 이 영역에 존재하여 키 정보를 도청을 할 수 있을 위험 또한 줄어들게 된다.

이런 핵심 아이디어를 가지고, VI장에서는 본 논문에서 제안한 key infection의 보안성 향상을 위한 키 설정 방식을 구체적으로 다루겠다.

IV. 보안이 향상된 키 설정

본 장에서는 III장의 핵심 아이디어를 이용하여 보안이 향상된 키 설정 방법에 대해 구체적으로 설명하

겠다.

모든 센서 노드들이 살포되어 지면 각각의 노드(그림 3의 노드 A)들은 키 k_a 값을 선택한 후 이 값을 그 노드의 첫 번째 이웃 노도(그림 3의 노드 B)에게 key whispering 방식으로 전송한다. 이 과정이 끝나면 전송자 노드에서 가장 가까이에 존재하는 첫 번째 이웃 노드는 이 키 정보를 받게 되며, 첫 번째 이웃 노드 역시 전송자 노드처럼 키 k_b 값을 선택한 후 이 값을 key whispering 방식으로 전송자 노드에게 보낸다. 전송자 노드가 k_b 값을 수신하게 되면, 전송자 노드는 첫 번째 이웃 노드 이외의 다른 이웃 노드를 key whispering 방식으로 찾게 된다. 다른 이웃 노드가 존재하면 전송자 노드는 발견된 노드에게 추가적인 키 정보를 역시 key whispering 방식으로 전송해 주기를 요청한다. 사실 다른 이웃 노드가 보내는 키 값은 공유키 쌍(pair-wise key)을 생성하기 위한 단순한 추가적 정보 값이기에 난수(random) 값을 사용한다. 이 추가적 정보가 전송되면 이 정보를 이용하여 전송자 노드와 그의 첫 번째 이웃 노드 간의 공유키 쌍(pair-wise key)을 생성한다. 하지만, 전송자 노드와 추가 정보를 제공하는 다른 이웃 노드의 위치에 대해 전송자의 첫 번째 노드는 특정 각도($2\theta_2$) 내에 존재해야 추가 정보를 수신할 수가 있다. 이는 한편으로 전송자 노드와 그의 첫 번째 이웃 노드의 위치에 대해서 다른 이웃 노드(e.g. 그림 3의 노드 C)는 또 다른 특정 각도($2\theta_1$) 내에 위치해야 한다는 것을 의미한다. 따라서 첫 번째 이웃 노드를 제외한 다른 이웃 노드들이 $2\theta_1$ 내에 존재하면 이들 노드들의 추가 키 정보를 전송자 노드와 첫 번째 노드가 수신할 수 있으며 이때 3개의 노드들에 의해 생성되는 초기 교차 영역은 기존의 면적보다 감소하게 된다. 이후 본 논문에서는 이런 추가 정보를 제공하는 노드들을 '보조 노드(Assistent node)' 라고 하겠다 (그림 3 참조).

결국 감소된 초기 교차 공간(Reduced-IIS)을 얻기 위해서는 특정 각도($2\theta_1$) 내에 있는 이 보조 노드를 찾아야 한다. 이를 위해 우선적으로 이 특정 각도에 대한 식을 유도해야 한다. 이 각도에 대한 식을 유도하기 위해 우선 전송자 노드에서 첫 번째 이웃 노드의 거리를 x라고 두며, 전송자 노드에서 보조 노드까지의 거리를 y라 두면 다음과 같은 특정 각도와 세 노드들 간의 거리(x, y)에 관한 식을 얻을 수 있다.

$$x \le y,\ a \ge 1,\ y = ax$$

$$2\theta_1 = 2\cos^{-1}(0.5/a) \tag{1}$$

또한 식 (1)을 이용하면 y/x 값과 이 특정 각도에 대한 그래프 또한 유도 할 수 있게 된다 (그림 4 참조).

최종적으로 식 (1)과 그림 4를 통해 이 특정 각도의 범위를 다음과 같이 얻을 수 있다.

$$120^\circ \le 2\theta_1 < 180^\circ \tag{2}$$

따라서 둘 이상의 이웃 노드를 가지는 각각의 전송자 노드는 아래의 p 확률로 보조 노드를 가지게 되는 것이다(식 3. 참조).

$$\frac{1}{3} \le p < \frac{1}{2} \tag{3}$$

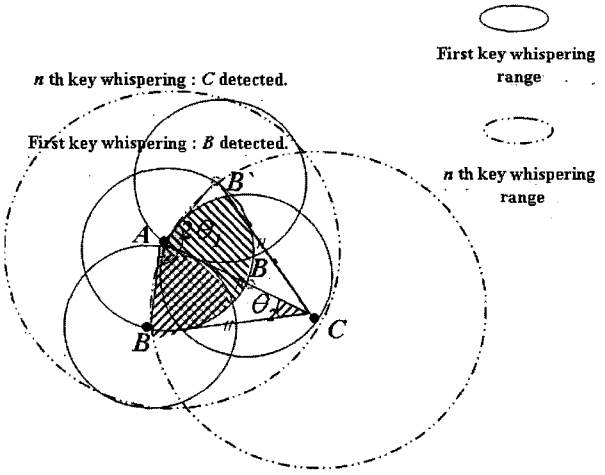


그림 3. Key infection의 보안성이 향상된 키 설정
Fig. 3. Security-enhanced key establishment scheme for Key Infection.

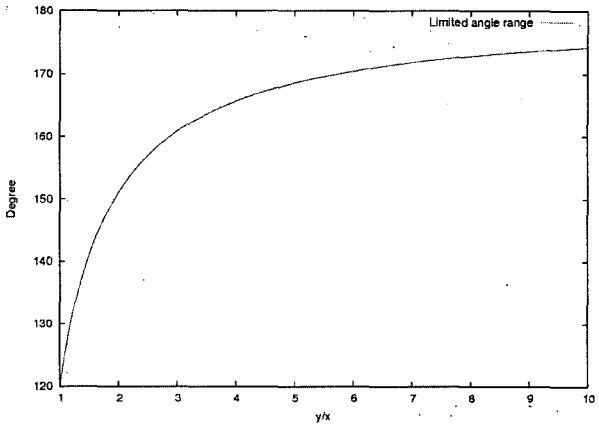


그림 4. Key infection 모델에서 초기 교차 영역(IIS)을 줄일 수 있는 특정 각도와 세 노드들 간의 거리 비의 관계 그래프
Fig. 4. Limited angle range that enable Key Infection's IIS to be reduced.

이런 이론을 바탕으로 본 논문의 방식을 다시 정리해 보면 다음과 같다: 단계 1. 모든 센서 노드들이 살포되어 지면 각각의 노드(그림 3의 노드 A)들은 키 k_a 값을 선택한 후 이 값을 그 노드의 첫 번째 이웃 노도(그림 3의 노드 B)에게 key whispering 방식으로 전송한다 ($A \xrightarrow{k_a} B$). 단계 2. 이 과정이 끝나면 전송자 노드에서 가장 가까이에 존재하는 첫 번째 이웃 노드는 이 키 정보를 받게 되며, 첫 번째 이웃 노드 역시 전송자 노드처럼 키 k_b 값을 선택한 후 이 값을 key whispering 방식으로 전송자 노드에게 전송한다 ($B \xrightarrow{k_b} A$). 단계 3. 전송자 노드가 k_b 값을 첫 번째 이웃 노드로 부터 수신하게 되면, 전송자 노드는 첫 번째 이웃 노드 이외의 다른 이웃 노드를 key whispering 방식으로 찾게 된다. 만일 다른 이웃 노드가 존재하면 전송자 노드는 발견된 노드에게 추가적인 키 정보 k_n 값을 역시 key whispering 방식으로 전송해 주기를 요청한다. 만일 이들 새로 발견되는 노드들 중 보조 노드(그림 3의 노드 C)가 존재하면 이 노드는 전송자 노드와 그 노드의 첫 번째 이웃 노드는 추가적인 키 정보 k_n 값을 보조 노드로 부터 key whispering 방식으로 수신하게 된다 ($A \xleftarrow{k_n} C \xrightarrow{k_n} B$). 단계 4. 이 추가 키 정보의 수신이 이루어지면 첫 번째 이웃 노드는 키 정보와 함께 받은 보조 노드의 아이디 값인 id_c 값을 전송자 노드에게 보내어 현재 자신이 어떤 노드로 부터 추가 키 정보의 수신 여부를 알린다 ($B \xrightarrow{id_c} A$). 단계 5. 위 과정들을 통해 전송자 노드와 첫 번째 이웃 노드는 같은 키 정보 값을(k_a, k_b, k_n) 공유하게 된다 (A computes $k_{ab} = H(k_a \parallel k_b \parallel k_n)$). 단계 6. 끝으로 공유된 키의 값을 확인을 위해 두 센서 노드는 *challenge-and-response* 방식으로 키의 공유를 확인한다($A \xrightarrow{\{N\}k_{ab}} B$, $B \xrightarrow{\{N+1\}k_{ab}} A$).

위의 프로토콜 과정이 끝나면, 같은 키 정보를 이용해 전송자 노드와 첫 번째 이웃 노드는 공유키 쌍(pair-wise key) k_{ab}를 commodity sensor network 상에서 초기 키 설정 시간에 생성하게 된다.

V. 제안된 메커니즘의 안전성 평가

본 논문에서 제안된 메커니즘의 향상된 안전성 평가를 위해 우선 본 논문에서는 각각의 노드들은 적어도 두개 이상의 이웃 노드들을 가지며, 보안 측정은 단지

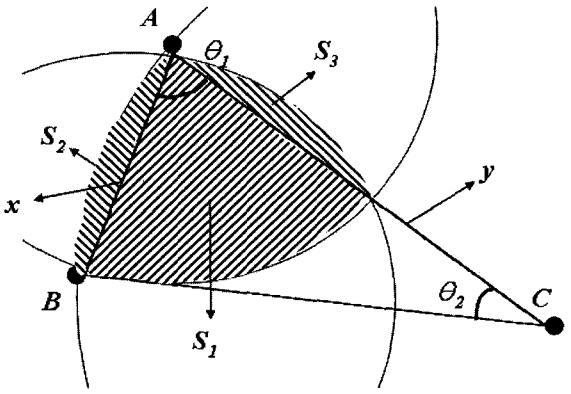


그림 5. 최대 감소된 초기 교차 영역의 넓이
Fig. 5. The maximum reduced-IIS area.

한 개의 보조 노드로 부터 추가적 키 정보를 받는 경우를 고려했다. 이런 조건하에서 본 논문에서 제시 하는 방식의 감소된 초기 교차 영역(Reduced-IIS)과 대표적인 commodity sensor network 상의 키 설정 방법인 key infection의 초기 교차 영역(IIS)을 비교함으로써 향상된 안전성을 평가한다. 더불어 본 장에는 이들 영역들과 보조 노드가 특정 각도($2\theta_2$)내에 존재할 확률을 수학적으로 계산하였다.

제안된 메커니즘에서 초기 교차 영역의 평균 감소된 면적을 구하기 위해 우선 최대로 감소된 초기 교차 영역의 넓이를 구해야 한다. 그림 5는 이와 같이 최대한으로 초기 교차 영역이 감소하는 경우를 도식화 하고 있다.

그림 5를 보면 최대 감소된 초기 교차 영역은 S_1, S_2, S_3로 이루어져 있기 때문에 최대로 감소된 초기 교차 영역을 구하기 위해서는 이들 각각의 영역의 면적을 계산해야 한다.

우선, S_1 지점의 면적은 다음과 같다.

$$\left(\frac{\theta_1}{360}\right)\times\pi\times\left(r_{A-B}=x\right)^2=\left(\frac{\theta_1}{360}\right)\times\pi\times x^2 \tag{4}$$

S_2 지점의 면적은 아래와 같다.

$$\begin{aligned}&\left(\frac{\theta_2}{360}\right)\times\pi\times\left(r_{A-C}=y\right)^2\\&-\left(\frac{\left(r_{A-B}=x\right)\times\sqrt{4\times\left(r_{A-C}=y\right)^2-\left(r_{A-B}=x\right)^2}}{2}\right)\\&=\left(\frac{\theta_2}{360}\right)\times\pi\times y^2-\left(\frac{x\times\sqrt{4\times y^2-x^2}}{2}\right)\end{aligned} \tag{5}$$

마지막으로 S_3 지점의 면적은 또한 다음과 같이 구할

수 있다.

$$\frac{1}{6}\times\pi\times(r_{A-B}=x)^2-\frac{\sqrt{3}}{4}\times(r_{A-B}=x)^2 \\ =\frac{1}{6}\times\pi\times x^2-\frac{\sqrt{3}}{4}\times x \tag{6}$$

식 (4), (5) 그리고 (6)을 다 더하면 최종적으로 최대 감소된 초기 교차 영역의 면적을 식 (7)과 같이 구할 수 있다.

$$x\le y, a\ge 1, y=ax \\ \frac{\cos^{-1}\left(\frac{0.5}{a}\right)\times x^2}{2}+\frac{\left(\pi-2\cos^{-1}\left(\frac{0.5}{a}\right)\times(ax)^2\right)}{2} \\ -\frac{x\times\sqrt{4\times(ax)^2-x^2}}{4}+\frac{1}{6}\times\pi\times x^2-\frac{\sqrt{3}}{4}\times x^2 \tag{7}$$

첫 번째 이웃 노드의 거리를 1 이라 가정하면 식 (7)을 간소화 한 식 (8)을 얻을 수 있게 된다.

$$\frac{\cos^{-1}\left(\frac{0.5}{a}\right)}{2}+\frac{\left(\pi-2\cos^{-1}\left(\frac{0.5}{a}\right)\times a^2\right)}{2}-\frac{\sqrt{4a^2-1}}{4} \\ +\frac{1}{6}\times\pi-\frac{\sqrt{3}}{4} \tag{8}$$

이제 제안한 메커니즘의 최대 감소된 초기 교차 영역과 key infection의 초기 교차 영역을 식 (8)을 이용하여 비교 할 수 있다. 그림 6은 본 논문의 방식의 초기 교차 영역의 비율이 key infection의 초기 교차 공간의 비율 보다 낮은 것을 보여 주고 있으며 이는 초기 설정 시간 때 본 논문이 제안된 방식이 더 안전하다는 것을 보여 주고 있다. 조금 더 상세히 살펴보면 그림 7에서 보여 지는 것과 같이 최대로 감소된 초기 교차 영역의 면적이 30%에서 43%에 이르는 것을 알 수 있다. 하지만 이런 측정값들은 최대 감소된 교차 공간의 값이기 때문에 평균적으로 감소된 교차 영역의 면적 값을 구하기 위해 최소 감소된 교차 영역의 면적이 0 이기에 최대 감소한 영역 면적의 값을 반으로 나누어야 한다. 따라서 평균적으로 감소된 초기 교차 영역의 면적 값은 15%에서 21.5%가 되고 이것은 또한 초기 키 설정 과정에서 나타날 수 있는 위험을 15%에서 21.5% 줄이게 되는 것을 의미한다.

더 정확한 값을 구하기 위해서는 보조 노드가 전송자 노드의 이웃 노드로 존재할 확률을 고려돼야 한다. 이 확률을 우선 p 라고 할 때, 이웃 노드들의 수를 m 이라 정의 하면 m 개의 이웃 노드들 중 한 개 이상의 보조 노드가 존재할 확률 를 구해야 한다. 이 경우 첫 번째 이웃 노드를 제외한 각각의 이웃 노드는 '이 이웃 노드가 보조 노드인지? 아닌지?'에 대한 *Bernoulli trial*을 따르게 된다. 따라서 k의 보조 노드가 m-1 개의 이웃 노드들(이웃 노드들 중 첫 번째 이웃 노드를 제외한 노드들) 중 존재할 확률은 $n = m-1$, $1/3\le p<1/2$ (식 (3)을 참조)라는 식과 함께 *binomial* 확률에 의해 식 (9), (10)을 얻을 수 있다[12].

$$p_{\min}=\frac{1}{3} \\ P_{\min}[N\ge 1]=1-P_{\min}[N<1] \\ =1-\binom{n}{k}P_{\min}^{0}(1-P_{\min})^n \tag{9}$$

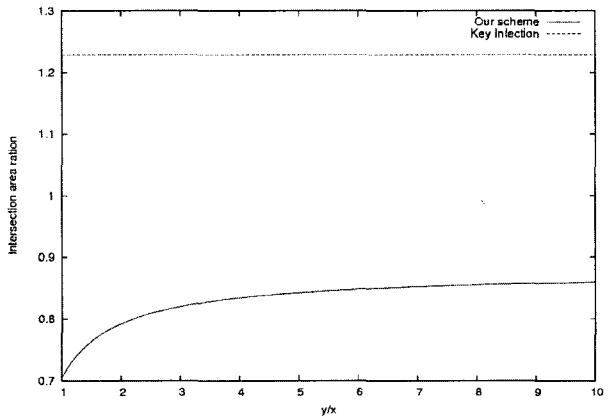


그림 6. 초기 교차 영역의 면적 비교 그래프
Fig. 6. Comparison of IIS area ratio.

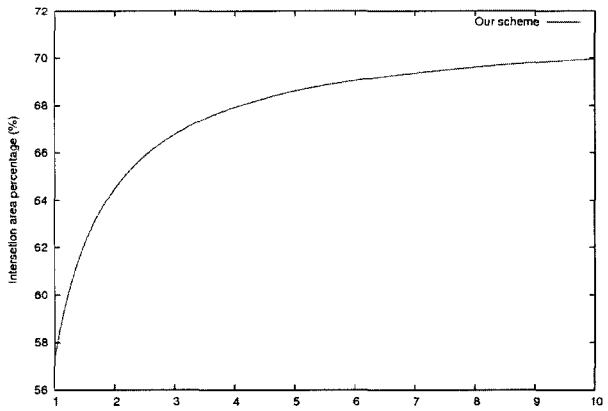


그림 7. 제안된 메커니즘과 key infection 방식을 비교 시 초기 교차 영역의 비율(%) 비교 그래프
Fig. 7. IIS area percentage when our scheme is compared with Key Infection.

$$p_{\max} = \frac{1}{2}$$

$$P_{\max}[N \geq 1] = 1 - P_{\max}[N < 1]$$
$$= 1 - \binom{n}{k} P_{\max}^{0} (1 - P_{\max})^{n} \quad (10)$$

식 (9), (10)을 이용하면 평균적으로 감소된 초기 교차 영역에 대한 식 (11)을 구할 수 있다.

$$15P_{\max}(\%) < Average\ Reduced\text{-}IIS \leq 21.5P_{\min}(\%) \quad (11)$$

보다 명확한 이해를 위해 실례적인 commodity sensor network 환경을 다음과 같이 가정하고 제안된 메커니즘의 계산해 보았다.

제안된 센서 네트워크 환경 : 100 개의 센서 노드들이 가로 세로 $62m$ 크기의 정사각형 지역에 분포하며 commodity sensor network을 형성하고 있다. 각각의 노드들은 $10m$의 전파 전송 범위를 가지고 있다. 이런 환경 하에서는 각각의 노드들은 평균 7.0736 개의 이웃 노드들을 가진다 (이 값은 위 가정된 환경을 구현한 소프트웨어 시뮬레이션 환경의 결과 값을 통해 얻어 졌다.).

위의 환경 하에서의 식 (9), (10)을 적용하면 식 (12)를 구할 수 있다.

$$p_{\min} = \frac{1}{3}$$

$$P_{\min}[N \geq 1] = 1 - P_{\min}[N < 1] = 1 - \binom{n}{k} P_{\min}^{0} (1 - P_{\min})^{n}$$

$$= 1 - (1 - \frac{1}{3})^{6} = 0.9122$$

$$p_{\max} = \frac{1}{2}$$

$$P_{\max}[N \geq 1] = 1 - P_{\max}[N < 1] = 1 - \binom{n}{k} P_{\max}^{0} (1 - P_{\max})^{n}$$

$$= 1 - (1 - \frac{1}{2})^{6} = 0.9844$$

$$0.9122 \leq P < 0.9844 \quad (12)$$

식 (11), (12) 조합하면 위에서 제시된 commodity sensor network 환경 하에서의 평균적으로 감소된 초기 교차 영역을 값을 아래와 같이 얻을 수 있게 된다.

$$14.7656(\%) < Average\ Reduce\text{-}IIS \leq 19.6123(\%) \quad (13)$$

결론적으로 key infection의 보안성 향상을 위한 키 설정 방법을 적용함으로써 공격자가 초기 키 설정 단계에서 도청할 수 있는 key infection의 초기 교차 영역을 줄이게 되어 기존의 key infection 방식에 비해 보다 향상된 키 설정 안전성을 얻게 되었다.

VI. 결 론

센서 노드의 제약 사항 때문에 센서 네트워크 분야에서는 보안 문제가 중요하게 인식되고 있다. 이 중 센서 네트워크상의 키 설정은 매우 중요한 문제이며 본 논문에서는 이를 위해 commodity sensor network 상의 대표적인 키 설정 방법인 key infection을 개선한 새로운 키 설정 방법을 소개 하였다.

제안된 방법은 추가적인 키 정보를 위해 추가 정보를 제공하는 보조 노드를 이용하였다. 추가적인 키 정보를 이용함으로써 전송자 노드와 그 노드의 첫 번째 이웃 노드 그리고 보조 노드에 key whispering에 의해 새롭게 생성된 초기 교차 영역을 얻게 되었다. 이 새로운 영역은 key infection의 초기 교차 영역 보다 감소하였기 때문에 공격자가 초기 키 설정 시간에 키 설정 정보를 도청할 수 있는 여지를 줄이게 되었다. 초기 키 설정 시간에 생성된 키는 이후의 모든 보안 과정에 사용되기에 초기 교차 영역을 줄임으로써 보다 보안성이 향상된 commodity sensor network 상의 키 설정 방식을 얻게 되었다. 향상된 보안의 측정을 위해 수학적으로 제안된 방식과 기존의 key infection 방식을 비교하였으며 이 결과를 통해 본 논문의 방식이 commodity sensor network 상에서 보다 보안성이 향상된 키 설정을 제공하는 것을 증명 하였다.

추가적으로 n 개의 보조 노드들의 키 정보를 이용하여 키를 생성할 경우 보안 향상에 대한 연구가 이루어져야 할 것이다. 많은 수의 추가적 보조 노드들을 이용하여 키 설정을 할 경우 초기 교차 영역이 점점 감소되어 메커니즘의 보안성은 향상되지만 키 설정 시간의 증가, 송수신 메시지들의 증가로 인해 메커니즘은 복잡해지게 된다. 반면 작은 수의 추가적 보조 노드들을 이용할 경우, 송수신 메시지 수가 적기 때문에 에너지 자원의 절약, 낮은 컴퓨팅 연산 등의 간결한 메커니즘을 유

지할 수 있다. 따라서 n 개의 보조 노드들의 키 정보를 이용할 경우 복잡성 대 간결성과 같은 교환 조건(trade-off)이 발생할 수 있으며 이 경우에 다양한 설정들에 대한 효율성 측면 문제들 역시 차후 연구로 병행되어야 할 것이다.

참 고 문 헌

[1] R. Szewxzyk, E. Osterwell, J. Polastre, M. Hamiltom, A. Mainwaring, and D. Estrin, "Habitat Monitoring", Communication of the ACM, Vol. 47, No. 6, June, 2004.

[2] E. Shi, A. Perrig, "Designing Secure Sensor Networks. IEEE Wireless Communications", December, 2004.

[3] W. Diffle, M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November, 1976.

[4] Y. H. Lee, V. Phadke, A. Deshmukh, and J. W. Lee, "Key Management in Wireless Sensor Networks", European Workshop on security in Ad-Hoc and Sensor Networks (ESAS 2004), LNCS 3313, Heidelberg, Germany, August 6, 2004.

[5] G. Gaubatz, J-P. Kaps, and B. Sunar, "Public Key Cryptography in Sensor Networks-Revisited", European Workshop on security in Ad-Hoc and Sensor Networks (ESAS 2004), Germany, August 6, 2004.

[6] R. Anderson, H. Chan, A. Perrig, "Key Infection: Smart Trust for Smart Dust", IEEE International Conference on Network Protocols (ICNP 2004), 2004.

[7] L. Eschenauer, V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks", Conference on Computer and Communications Security. Proceedings of the 9th ACM conference on Computer and communications security 2002, USA. 2002.

[8] H. Chan, A. Perrig, D. Song, "Random Key Predistribution Schemes for Sensor Networks", IEEE Symposium on Research and Privacy, 2003.

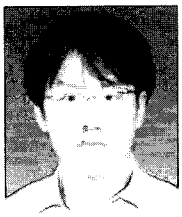
[9] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Pairwise Key Pre-Distribution Scheme for wireless sensor networks", In ACM conference on Computer and Communications Security (CCS), 2003.

[10] R. Blom, "An Optimal Class of Symmetric Key Generation Systems", In EUROCRYPT 84, 1985

[11] J. M. Hwang, Y. D. Kim, "Revisiting Random Key Pre-distribution Schemes for Wireless Sensor Networks", SASN'04, Washington, DC, USA, October, 2004.

[12] A. Leon-Garcia, Probability and Random Processes for Electrical Enigneering, 2nd ed. MA: Addison-Wesley Publishing Company, Inc., 1994.

저 자 소 개



황 영 식(학생회원)
1998년 울산대학교 정보통신 공학과 학사 졸업.
1998년~현재과학기술연합대학원 정보보호공학과 석사과정.
<주관심분야 : 암호 프로토콜, 센서 네트워크 보안, 네트워크 보안 등>

한 승 완(정회원)
1994년 전남대학교 전산학과 학사 졸업.
1996년 전남대학교 전산통계학과 석사 졸업.
2001년 전남대학교 전산통계학과 박사 졸업.
2001년~현재 한국전자통신연구원 정보보호연구단, 정보보호원천연구팀 선임 연구원.
<주관심분야 : 네트워크 보안, 알고리즘, 계산 이론 등>

남 택 용(정회원)
1987년 충남대학교 계산통계학과 학사 졸업.
1990년 충남대학교 계산통계학과 석사 졸업.
2005년 한국외국어대학교 전자정보공학과 박사졸업.
1987년~현재 한국전자통신연구원 정보보호연구단 보안게이트웨이연구팀 팀장(책임연구원)
<주관심분야 : 정보보호, 인터넷, 이미지 마이닝 등>