전술 애드혹 네트워크에서의 비밀분산 기반 노드 인증

양지훈O, 이수진(교신저자)*
O국방대학교 국방과학학과,
*국방대학교 국방과학학과
e-mail: drain7@gmail.comO, cyberkma@gmail.com*

Secret Sharing based Node Authentication in Tactical Ad-Hoc Network

Ji-hun YangO, Soo-jin Lee(Corresponding Author)*
ODept. of Defense Science, Korea National Defense University,
*Dept. of Defense Science, Korea National Defense University

● 요 약 ●

본 논문에서는 군사용 전술통신 분야에서 활용성이 증대되고 있는 애드혹 네트워크에 적용 가능한 비밀분산 기반의 노드 인증 기법을 제안한다. 필드에 전개되기 이전에 네트워크를 형성할 각 노드는 지수형 분산비밀키과 원본비밀키를 저정하고, 필드에 배치된 이후 네트워크 형성 초기단계에서 비밀분산의 원본비밀키 정보 복원 연산을 통해 다수 노드에 대한 동시 인증을 실시한다. 그리고 인증과정에서 원본비밀키 복원 연산을 방해하는 노드를 원본비밀키 복원 연산을 수행하기 이전에 PUF값을 활용하여 탐지한다.

키워드: 전술 애드혹 네트워크, 인증, 비밀분산, PUF

I. Introduction

애드혹 네트워크는 무선을 기반으로 하기 때문에 다양한 보안취약점을 가질 수 있어 보안대책의 적용이 매우 중요하다. 특히 네트워크 형성 초기에 신뢰할 수 있는 노드들만으로 안전한 네트워크를 구성하기 위한 노드 인증이 반드시 수행되어야 한다.

애드혹 네트워크에서의 노드 인증과 관련된 선행연구들은 대부분 대칭키 암호를 기반으로 하며, 과도한 통신비용과 동일 비밀키의 계속적인 사용으로 인한 비밀키 노출 가능성이 한계로 지적되어 왔다. 공개키 암호를 기반으로 한 노드 인증의 경우 공개키 인증을 위한 인증기관의 구성이 제한된다는 한계를 가진다.

본 연구에서는 전술 애드혹 네트워크에 참여하는 노들들이 필드에 배치되기 이전에 저장하는 분산비밀키와 원본비밀키를 활용하여 다수의 노드를 동시에 인증하는 기법을 제안한다. 그리고 잘못된 분산비밀을 전송하여 인증을 방해하는 공격자를 탐지하기 위해 PUF(Physical Unclonable Function)를 활용한다.

II. Preliminaries

1. 애드혹 네트워크에서의 노드 인증 기법

대칭키 암호를 기반으로 노드를 인증하는 기법은 다중키를 기반으로 하는 기법[1]과 확률적으로 공유된 키를 인증에 활용하는 기법[2] 등이 있다. 공개키 암호를 기반으로 하는 인증 기법들은 비밀분산[3]을 이용하여 인증기관을 구성하는 방식이 주로 제안되었다.

2. 비밀분산

비밀분산에서는 일정 수 이상의 분산비밀이 모일 경우 원본비밀키나 코드를 복원할 수 있어 중요 정보의 분산저장 및 권한의 분산 등을 위해 다양하게 응용되고 있다.

3. PUF

PUF는 반도체 제조과정에서 발생하는 미세한 공정오차를 이용하여 동일한 입력에 대해 서로 다른 출력을 생성한다.[4] 때문에 특정 장치 내에 IC 칩의 형태로 장착되어 인증 및 암호 키 생성 등에 많이 활용되고 있다.

III. The Proposed Scheme

비밀분산은 민감하고 중요한 정보 혹은 비밀을 다수의 분산비밀로 나누어 여러 참여자들에게 분산 저장한다. 그리고 일정 수 이상의 분산비밀이 모이면 원본 정보 혹은 비밀이 복원된다. 본 연구에서는 이러한 비밀분산의 특성을 활용하여 ElGamal 공개키 암호가 적용된 애드혹 네트워크 환경에서 다수 노드가 참여하여 원본 비밀키의 복원을 시도한 후 올바른 원본 비밀키가 복원되면 복원에 참여한 모든 노드를 동시에 인증한다.

2. 필드 배치 전 준비단계

전술 애드혹 네트워크에 참여하는 모든 노드는 기본적으로 PUF가 장착되어 있다. 보안관리자는 각 노드에 장착된 PUF를 통해 CRP(Challenge-Response Pair) 테이블을 생성한다. 그리고 전술 애드혹 네트워크에 참여할 노드들이 사용할 생성자 g와 소수 p를 공개한다. 각 노드는 개인키로 사용할 x를 선택하고, 자신의 공개키 $pk^i(g^x \bmod p)$를 계산하여 보안관리자에게 보고한다.

보안관리자는 임의의 Lagrange 다항식 F(x)를 선택한 후, 각 노드로부터 보고받은 공개키를 이용하여 각 노드에 분배할 분산비밀(K_i)을 계산한다. 분산비밀의 계산이 완료되면 보안관리자는 분산비밀과 원본비밀을 지수형태(g^{Ki}, g^K)로 변환한 후 각 노드에 분배한다. 이상과 같은 과정을 거쳐 각 노드는 공개키/개인키 쌍, 분산비밀 및 원본비밀을 가지게 되며, 작전에 투입될 노드들의 CRP 중 일부를 추가로 저장한다.

3. 필드 배치 후 인증단계

필드에 배치된 노드들은 네트워크 형성 초기 단계에서 인증을 수행하기 위해 자신의 공개키와 지수 형태의 분산비밀, 그리고 사전에 개별 노드에 저장된 PUF CRP의 Response값(R_i)에 의사난수생성 알고리즘에 의해 생성된 난수(RN)를 결합한 값의 해시값[$H(R_i \| RN)$] 을 브로드캐스팅한다. 각 노드들은 네트워크 내의 다른 노드들이 브로드캐스팅한 데이터를 수신한 후, 먼저 각 노드에 해당하는 Challenge 값을 CRP 테이블에서 찾는다. 이후 매칭되는 R_i 값과 난수를 결합한 값을 해시한 후 수신된 값과 비교하여 일치하는 노드들이 전송한 분산비밀 정보만을 이용하여 원본비밀의 복원을 시도한다.

원본비밀의 복원이 완료된 후 자신이 저장하고 있는 원본비밀과 일치할 경우 원본비밀 복원에 참여한 모든 노드는 정당한 노드로 인증할 수 있게 된다. 비밀분산을 이용한 노드 인증 과정은 Fig. 1에서 보는 바와 같다.

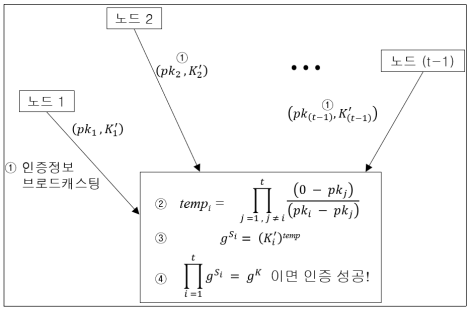

Fig. 1. 비밀분산 기법을 이용한 인증 과정

IV. Conclusions

본 연구에서는 중요 정보의 분산저장이나 권한 분산에 활용되어 왔던 비밀분산을 이용하여 한 번의 통신만으로 (t-1) 개의 노드를 동시에 인증할 수 있는 효율적인 인증기법을 제시하였다. 그리고 원본비밀의 복원을 위한 계산을 수행하기 전에 PUF CRP 값을 활용하여 인증과정을 방해할 수 있는 공격자를 탐지하고 배제하는 방안을 추가로 제시하였다.

향후에는 제안된 접근방법의 효율성을 입증하기 위해 통신비용과 연산비용 등을 분석하고, 인증 이후 단계에서 안전한 통신을 위해 사용할 세션키를 설립하는 방안 등에 대해 연구를 진행할 예정이다.

REFERENCES

[1] S. Zhu, S. Setia, and S. Jajodia, “LEAP : Efficient Security Mechanism for Large-Scale distributed Sensor Networks, in Proceedings of the 10th ACM Conference on Computer and Communications Security(CCS ’03), Washington D.C, Oct, 2003.

[2] H. Chan, A. Perrig, and D. Song, “Random Key Pre-distribution Schemes for Sensor Networks,” in the Proceedings of IEEE 2003 Symposium on Security and Privacy, Berkeley, CA, 2003.

[3] A. Shamir, “How to share a secret,” Communications of the ACM, 22(11), pp. 612-613, 1979.

[4] U. Rührmair and D. E. Holcomb, “PUFs at a Glance,” In Proc. of the conference on Design, Automation & Test in Europe(DATE '14), 2014