http://dx.doi.org/10.3745/KIPSTC.2011.18C.4.207

익명성을 제공하는 RSSI기반 V2V 메시지 인증기법

서 화 정[†] · 김 호 원[††]

요 약

지능형 차량 네트워크(VANET)는 차량 간 (V2V, Vehicle to Vehicle) 또는 차량과 노변장치간 (V2I, Vehicle to Infrastructure)의 통신을 통해 서비스를 제공하는 기술이다. 지능형 차량 네트워크는 통신을 통해 유통되는 정보의 중요성을 고려해 볼 때 메시지의 인증 및 보안은 필수적인 요건이다. 현재 VANET의 보안성을 향상시키기 위해 다양한 인증기법이 연구되고 있다. 그중에서도 RAISE scheme은 차량 밀집환경에서의 인증을 익명으로 수행한다. 하지만 스킴에 사용된 기법인 k-anonymity는 익명성을 제공하는 대신 차량의 ID를 얻기 위해 불필요한 전수조사 연산을 수행해야 한다. 본 논문에서는 차량 간의 통신에 사용되는 무선 신호세기의 특성을 이용하여 위치기반 인증 및 암호화 기법을 제시하며 알고리즘의 정확도를 향상시키기 위해 3차원 상에서의 위치 선정 기법을 적용한다.

키워드 : VANET, RSSI, 인증, 익명성

A Message Authentication Scheme for V2V message based on RSSI with anonymity

Seo, Hwa-Jeong[†] · Kim, Ho-Won[††]

ABSTRACT

Vehicular Ad Hoc Network(VANET) is a communication technology between vehicles and vehicles(V2V) or vehicles and infrastructures(V2I) for offering a number of practical applications. Considering the importance of communicated information through VANET, data authentication, confidentiality and integrity are fundamental security elements. Recently, to enhance a security of VANET in various circumstances, message authentication is widely researched by many laboratories. Among of them, Zhang. et. al. is an efficient method to authenticate the message with condition of anonymity in dense space. In the scheme, to obtain the vehicular ID with condition of anonymity, the k-anonymity is used. However it has a disadvantage, which conducts hash operations in case of determining the vehicular ID. In the paper, we present a location based algorithm using received signal strength for the location based authentication and encryption technique as well, and to enhance the accuracy of algorithm we apply a location determination technique over the 3-dimensional space.

Keywords : VANET, RSSI, Authentication, Anonymity

1. 서 론

VANET(Vehicle Ad-hoc Network)통신은 무선 통신 기능을 지원하는 지능형 차량들 간 그리고 차량과 노변장치들 간의 통신을 통해 수집된 정보를 가공하여 운전자에게 다양한 응용 서비스를 제공한다. 안전한 주행을 위해 제공되는 교통사고 발생, 갑작스런 기상 변화, 도로의 결빙 상태 그리고 차량의 거리와 속력이 있다[1]. 지능형 차량 서비스는 도로상에 설치된 RSU(Road SIde Unit)와 차량에 탑재된 OBU(On Board Unit) 상호간에 정보를 교환하며 서비스에 필요한 정보를 제공한다.

현재 연구기관과 대학에서 VANET상에서의 RSU와 OBU간의 보안 통신에 대한 연구가 진행되고 있다. 연구의 중점은 통신에 사용되는 메시지의 크기와 수를 줄여서 보다 효율적인 통신이 가능하도록 하는데 있다. 지금까지는 메시지의 익명성에 대한 연구는 활발히 진행되지 않았다. 2008년 발표된 Zhang et. al.에서는 VANET 보안 통신에서 메시지 전송 시에 자신의 ID를 사전에 분배받은 메시지와 난수를 통해 생성하여 전송하는 방식으로 진행되었다[2]. 수신자는 송신자의 ID정보를 통해 메시지의 근원지를 확인했다. 하지만 이는 공격자가 메시지를 스니핑하게 될 경우 해당

※ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2010-0026621).
† 준 회 원 : 부산대학교 컴퓨터학과 석사과정
†† 종신회원 : 부산대학교 컴퓨터학과 조교수
논문접수 : 2011년 2월 10일
수 정 일 : 1차 2011년 5월 11일
심사완료 : 2011년 5월 11일

메시지의 송신지에 대한 정보를 알 수 있는 문제가 있다. 같은 해에 발표된 RAISE schem은 RSU의 역할증대를 통한 VANET상의 통신량, 계산량을 줄여주며 k-anonymity기법을 통해 익명성까지 제공하는 메시지 인증 기법을 제안하였다[3]. 하지만 스킴에서 사용된 k-anonymity기법은 모든 메시지에 대한 ID값을 해시연산을 통한 전수조사를 통해 알아보는 비효율적인 측면을 가진다.

본 논문에서는 k-anonymity를 통한 비효율적인 메시지 인증대신 RSSI기반 아이디 방식을 통해 불필요한 연산을 줄이고 보다 빠르고 정확하게 차량의 ID를 찾아내는 알고리즘을 제시한다. 또한 해당 알고리즘의 정확도를 높이기 위해 현실 세계와 동일한 3차원 상에서의 위치선정기법을 적용한다.

본 논문은 다음과 같이 구성된다. 2장에서는 k-anonymity와 RSSI기반 거리계산 알고리즘 그리고 3차원 상에서의 위치 선정기법에 대해 기술한다. 3장에서는 제안하는 시스템 모델 및 기법에 대해 설명한다. 4장에서는 제안하는 기법의 안전성과 효율성을 분석하고 마지막으로 5장에서는 본 논문의 결론을 내린다.

2. 관련 연구

2.1 k-anonymity

k-anonymity는 K개의 차량이 PID(Pseudo-ID)를 사용하여 익명통신을 제공한다. 따라서 제삼자는 VANET상에서 통신하는 차량의 ID를 확인하는 것이 불가능하다. 반면에 RSU의 경우 자신이 가진 모든 key값에 대해 적합한 값이 나올 때까지 전수조사를 수행하여 차량의 ID를 확인한다. 따라서 차량은 익명성을 보장받는 가운데 RSU와 안전한 통신이 가능하게 된다. 하지만 차량이 밀집된 지역에서 k개의 차량이 RSU와 통신을 하게 되는 경우 전수조사의 복잡도는 $O(k^2)$ 이다.

2.2 RSSI기반 거리측정 알고리즘[4]

<표 1>에서는 RSSI를 통한 거리 계산 시 사용되는 용어를 설명한다.

<표 1> 용어 정리

표 기	정 의
n	신호 전파 상수
d	거리
A_R	1미터상에서의 RSSI 값

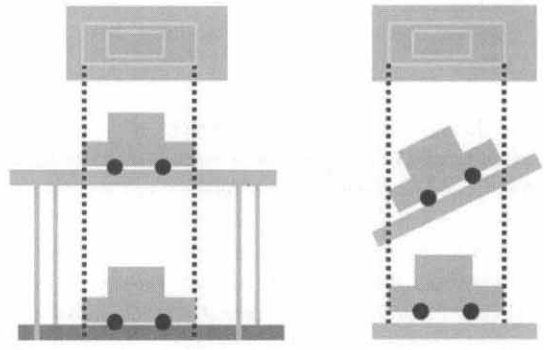
RSSI값은 전송되는 통신에서 측정되는 전파의 전송세기를 의미한다. RSSI값은 메시지 송신부와 수신부의 거리가 가까울수록 높게 나타난다. 식 (1)와 (2)는 RSSI값의 변환을 통해 거리를 구하는 식을 나타낸다. 공식에 사용된 용어는 신호에 특성에 따른 전파 상수값인 n, 상호간의 거리가 1미터인 경우의 RSSI 값 A_R 그리고 측정된 RSSI값을 이용하여 센서간의 거리를 계산하는 공식이다.

$$RSSI = -(10n\log d + A_R) \tag{1}$$

$$d = 10^{-\frac{RSSI + A_R}{10n}} \tag{2}$$

2.3 3차원 상에서의 위치추정 알고리즘[5]

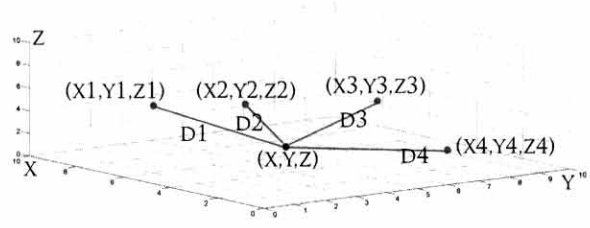
본 장에서는 3차원 상의 위치추정 알고리즘에 대해 알아보게 된다. 차량의 3차원 좌표는 기존의 2차원 좌표에 비해 높이에 해당하는 정보를 더 얻게 된다. 이를 통해 RSU는 차량의 예상되는 위치를 보다 정확하게 알 수 있게 된다. 그림 1의 A는 도시고속도로와 같은 곳에 차량이 가게 될때 도로 위를 달리는 차량과 도로 밑을 달리는 차량이 2차원 평면상에서는 동일하게 나타남을 알 수 있다. 이는 2차원 좌표를 통해서는 표현이 불가능한 부분이다. 또한 그림 1의 B를 보면 차량이 경사진 곳을 오르거나 내려갈 때 차량의 높이 변화를 판단하지 못한다면 속력에 따른 거리를 확인할 수 없으므로 정확한 좌표의 추정이 불가능하다. 따라서 3차원 상의 좌표정보가 필요하게 된다.



(A) (B)

(그림 1) 2차원 상에서 발생하는 오류

다음은 4군데의 장소에서 신호를 전달받아 근원지로 부터의 거리를 알 때 신호의 근원지를 계산하는 알고리즘을 나타낸다.



(그림 2) 3차원 상에서의 위치추정 알고리즘

식(3 ~ 5)는 계산하고자 하는 좌표를 사전에 좌표를 알고 있는 4군데의 점을 통해 계산하는 공식을 나타낸다.

$$2(x_2-x_1)\cdot x+2(y_2-y_1)\cdot y+2(z_2-z_1)\cdot z=\alpha' \quad (3)$$

$$2(x_3-x_1)\cdot x+2(y_3-y_1)\cdot y+2(z_3-z_1)\cdot z=\beta' \quad (4)$$

$$2(x_4-x_1)\cdot x+2(y_4-y_1)\cdot y+2(z_4-z_1)\cdot z=\gamma' \quad (5)$$

식 (6 ~8)에서는 점 간의 거리, 좌표의 관계식을 통해 계산하고자 하는 점의 좌표를 계산하는 공식이다. 여기서 X_j^i는 (x_i-x_j)를 나타내는 것으로써 i와 j간의 거리를 나타낸다.

$$\hat{x}=\hat{f}(d_1,d_2,d_3,d_4)=\frac{\begin{vmatrix}\alpha & 2Y_1^2 & 2Z_1^2\\ \beta & 2Y_1^3 & 2Z_1^3\\ \gamma & 2Y_1^4 & 2Z_1^4\end{vmatrix}}{M} \quad (6)$$

$$\hat{y}=\hat{g}(d_1,d_2,d_3,d_4)=\frac{\begin{vmatrix}2X_1^2 & \alpha & 2Z_1^2\\ 2X_1^3 & \beta & 2Z_1^3\\ 2X_1^4 & \gamma & 2Z_1^4\end{vmatrix}}{M} \quad (7)$$

$$\hat{z}=\hat{h}(d_1,d_2,d_3,d_4)=\frac{\begin{vmatrix}2X_1^2 & 2Y_1^2 & \alpha\\ 2X_1^3 & 2Y_1^3 & \beta\\ 2X_1^4 & 2Y_1^4 & \gamma\end{vmatrix}}{M} \quad (8)$$

식 (6~8)에서 사용되는 M의 값은 식 (9)와 같다.

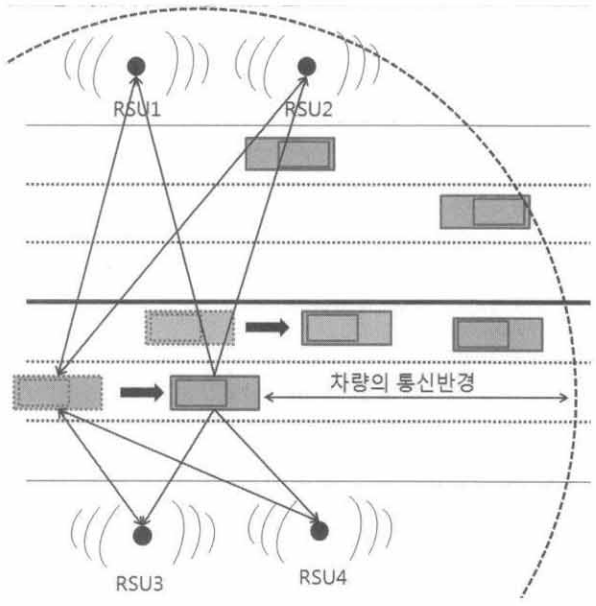
$$M=\begin{vmatrix}2X_1^2 & 2Y_1^2 & 2Z_1^2\\ 2X_1^3 & 2Y_1^3 & 2Z_1^3\\ 2X_1^4 & 2Y_1^4 & 2Z_1^4\end{vmatrix} \quad (9)$$

3. 제안하는 기법

본 섹션에서는 RSU와 OBU 간의 안전한 통신을 위해 사용되는 VANET scheme을 제안한다. 여기서 RSU와 OBU는 물리적인 공격으로부터 안전하다고 가정한다.

3.1 제안하는 기법

제안하는 기법은 RSU에서 차량의 ID를 RSSI값을 통해 도출된 차량의 좌표를 계산하여 사용하게 된다. (그림 3)은 제안하는 기법의 대칭키 설립과정을 나타낸다. 그림에는 하나의 차량으로부터 신호가 발생하게 되면 도로변에 위치한 RSU에서 해당신호를 수신하여 차량과 RSU간의 거리를 추정하게 된다. 차량은 두 번의 신호를 Broadcast 전송하게 되며 이는 RSU에서 모두 수신가능하다.



(그림 3) 제안하는 기법의 대칭키 설립 및 메시지전송

3.2 대칭키 설립

차량이 RSU의 통신반경 안에 들어오게 되면 차량으로부터 전송되는 메시지의 RSSI값을 이용하여 차량과의 거리를 계산한다. 이와 동시에 차량과 RSU간에는 Diffie-Hellman 키교환 프로토콜이 수행된다[6]. 키교환은 3 Hand shake를 통해 수행되므로 RSU에서는 차량의 RSSI 값을 키교환시 두 번 전송받게 된다. RSSI값은 오차가 발생하므로 2번의 RSSI신호의 세기값을 평균하여 해당 차량과 RSU간의 거리를 계산한다. 차량의 ID값을 생성하기 위해서는 RSSI를 통해 계산된 거리를 통해 차량의 좌표를 계산하고 VANET통신을 통해 암호화되어 전송되는 해당 차량의 속력정보를 종합적으로 판단하여 차량의 위치를 보다 정확하게 판단하는 정보로 사용한다. 해당 좌표는 차량만이 가지는 고유한 정보로써 차량의 ID로 사용된다. 그 이유는 차량이 2차원 상에서는 겹칠수 있지만 3차원 상에서는 차량간에는 고유한 위치정보가 부여되기 때문이다. 이후에 전송되는 메시지에 대해서 RSU는 차량의 RSSI값을 통해 계산된 좌표와 <표 2>의 Key Table을 비교하여 현재 예상되는 좌표로써 가장 적합한 차량을 찾는다. 이때 참조되는 Key Table의 내용은 일정시간동안 갱신되지 않는 경우 RSU의 통신범위를 벗어난 것으로 간주되어 자동으로 삭제된다.

〈표 2〉 Key Table

차량의 좌표	KEY
X_1, Y_1, Z_1	K_1
X_2, Y_2, Z_2	K_2
X_3, Y_3, Z_3	K_3
• • •	• • •
X_k, Y_k, Z_k	K_k

차량의 확인과정은 다음과 같이 진행된다. 메시지가 RSU에게 전송되면 메시지전송 주기를 확인하여 해당 주기에 전송되는 차량에 대한 List를 작성하게 된다. 두 번째로 RSU에서의 RSSI값을 이용하여 현재 차량의 위치를 확인하게 된다. 세 번째로는 차량의 이전 위치와 이전에 전송되어온 속력정보를 종합하여 현재위치를 예측한다. 이는 k-anonimity를 통한 전수조사대신 전송되는 신호의 세기를 이용하여 작성된 ID Table을 통해 보다 효율적으로 차량의 메시지를 판별하는 것이 가능하다.

4. 안전성 및 효율성 분석

안전성에 대한 분석은 RSSI기반 인증기법을 기존 RAISE scheme에 적용한 결과를 토대로 분석하였다.

4.1 안전성

4.1.1 인증

전송되어진 메시지는 해시연산을 통해 계산된 해시체인값의 서명값을 통해 인증과정을 수행한다. 해시체인값은 각각의 메시지들의 서명값을 체인의 형태로써 가짐으로 이를 확인하여 전송된 차량의 각각의 메시지에 따른 정당성을 확인할 수 있다.

4.1.2 메시지 무결성

메시지는 서명값을 포함하므로 수신자는 메시지의 무결성 확인이 가능하다. 또한 RSU에 저장된 키 Table이 공격자에게 노출되지 않는다면 차량과 RSU의 메시지는 안전하게 보호된다.

4.1.3 가용성

위치기반 ID기법을 사용하면 차량은 자신의 고유한 정보인 좌표정보를 가짐으로써 언제 어디서나 RSU와의 통신이 가능한 지점에서는 안전한 인증을 거친 이후 메시지 전송이 가능하다.

4.1.4 익명성

본 알고리즘에서는 RSSI기반 위치, 속도 그리고 가속도 개념을 이용하여 차량을 정확하고 빠르게 확인한다. 이는 ID값이 메시지에 포함되지 않으므로 공격자로 하여금 메시지의 송신지를 확인하는 것이 불가능하게 한다.

4.2 효율성

4.2.1 계산량

제안된 스킴의 계산량은 해시연산을 통해 메시지 인증을 수행하므로 Pairing연산을 통해 서명값을 생성하는 Chang. et. al에 비해 수행속도가 빠르다. 또한 k-anonymity를 사용하지 않으므로 RAISE스킴에서 사용하는 차량확인을 위한 해쉬연산의 전수 조사가 필요하지 않다. 대신 RSSI를 통한

〈표 3〉 기존 기법과 제안된 기법의 계산량비교

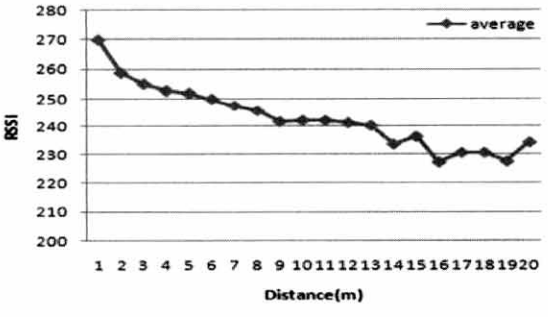
	Chang. et. al[2]	RAISE[3]	제안된기법
해쉬 통합 (RSU)	해쉬통합없음 $H\times n$을 통한 메시지 서명계산	$H\times k\times n$ $H\times n$, HAggt의 서명 계산	$R\times n$ $H\times n$, HAggt의 서명 계산
검증 (V)	메시지의 수에 관계없이 $3\times P$	HAggt의 서명, 검증, H	HAggt의 서명, 검증, H

P : Pairing 연산
H : 해쉬함수
n : 메시지의 개수
k : 키 테이블에 등록된 개수
R : RSSI를 통한 좌표 계산

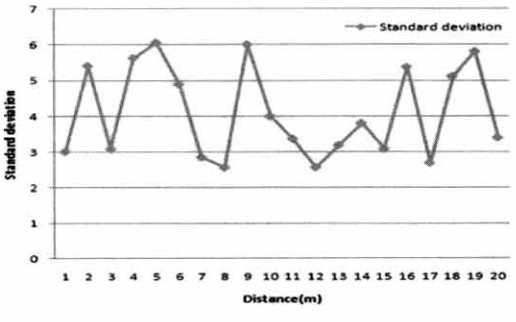
거리계산을 통해 좌표를 생성하고 이를 ID로 사용할 수 있다. RSSI를 통한 거리 계산은 수식(1~9)에 나타난 공식을 통해 계산가능하다. 이는 3차원 행렬연산으로써 k-anonymity에 따른 해시전수조사에 비해 연산 부하가 작다.

4.2.2 정확도

RSSI기반 좌표 계산 알고리즘의 정확도를 검증하기 위해 거리에 따른 RSSI값을 1000회씩 측정하여 신호의 정확도를 확인하였다. 결과값은 (그림 4)와 같으며 RSSI값이 거리에 따라 선형적으로 감소한다는 것을 알 수 있다. 여기서 RSSI값은 255가 넘어서는 경우에 modular연산이 되어 작



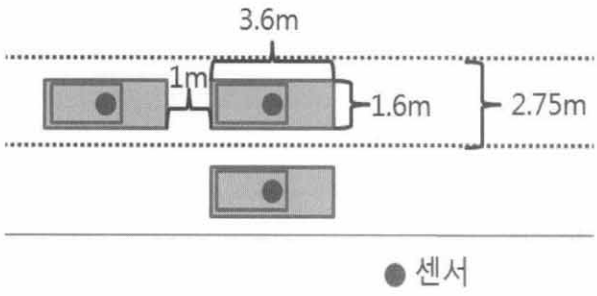
(그림 4) 거리에 따른 RSSI



(그림 5) 거리에 따른 표준편차

은 값이 나오게 되는 데 해당 값에 255씩 더해서 그래프에 나타내었다. (그림 5)는 측정된 RSSI값에 따른 표준편차값을 나타내며 이를 통해 측정된 RSSI값의 오차범위를 확인할 수 있다.

보다 현실적인 적용을 위해 경차에 해당 알고리즘을 적용하여 정확도에 대한 분석을 해보도록 하겠다. 경차는 길이 3.6m, 너비 1.6m, 높이 2.0m 이하인 차량을 의미하며 차량 도로의 폭은 최소 2.75m이상을 유지해야 한다. 이를 그림으로 나타내면 (그림 6)와 같다.



(그림 6) 센서간의 거리

또한 차량 간의 안전거리는 도로교통안전수칙에 명시된 공식(10)을 사용하면 10km/h로 주행 시 1m의 안전거리를 유지해야 한다. 여기서는 차량이 밀집된 환경에서의 계산을 위해 10km/h로 차량이 운행한다고 가정하도록 하겠다. 만약 차량의 순환이 잘되어 80km/h로 달린다면 차량 간의 안전거리가 증가하며 차량의 밀집도가 줄어들어 거리측정의 오류에 대한 영향을 적게 받게 된다.

$$\text{안전거리} = \text{속력}^2 \div 100 \qquad (10)$$

차량의 기준을 고려해 볼 때 차량들에 설치된 센서간의 거리는 도로의 폭으로는 2.75m, 차량의 길이와 폭으로는 각각 3.6m, 1.6m이상을 유지하게 된다. (그림 4), (그림 5)와 같이 표준편차의 평균은 4.1이며 RSSI를 이용한 거리계산에서 센서간의 거리가 2m일 경우 RSSI값의 차이가 4.2이다. 따라서 VANET환경에서의 RSSI값을 이용한 거리계산은 오류가 발생할 확률이 낮다. 만약 해당 차량 ID를 RSSI를 통해 얻지 못한 경우에는 k-anonymity의 특성을 이용하여 해당 차량의 ID를 확인해 낸다.

5. 결 론

본 논문에서는 차량이 밀집된 지역에서의 VANET 통신에 적합하게 설계된 RAISE스킴의 문제점인 k-anonymity를 RSSI를 통한 위치기반 ID기법으로 대체하여 알고리즘을 보다 효율적으로 수행할 수 있도록 하였다. 이는 전수조사를 통한 차량인증과정의 문제점을 적은 연산으로 해결함과 동시에 보안 요구사항인 무결성, 기밀성, 사용자 인증 그리고 익명성을 만족한다. 이를통해 차량 간에는 보다 안전하고 효율적인 통신이 가능하게 된다.

앞으로의 연구방향은 센서의 거리를 추정하는 다양한 알고리즘 (TDOA, TOA, AOA)과 결합하여 RSSI를 통해 발생할 수 있는 거리추정의 문제점을 개선해야 한다는 점이다. 3차원 상에서의 거리 계산 시 RSSI를 통해 발생하는 오차는 차량의 좌표선정 결과의 신뢰성을 떨어트리기 때문이다.

참 고 문 헌

[1] 조영준, 이현승, 박남제, 최두호, 원동호, 김승주, "VANET에서의 보안 기술동향", 한국정보보호학회, 제19권 제1호, pp.134-142, Feb., 2009.

[2] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, ""An efficient identity based batch verification scheme for vehicular sensor networks,"" in Processings of the IEEE International Conference on Computer Communications (INFOCOM'08), Phoenix, Arizona, 2008.

[3] C. Zhang, X. Ling, and P-H. Ho, "RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks," in Proc. IEEE ICC 2008, Beijing, China, pp.1451-1457, May, 2008.

[4] Erin-Ee-Lin Lau, Wan-Young Chung, ""Enhanced RSSI based Real-time User Location Tracking System for Indoor and Outdoor Environments"", 2007 International Conference on Convergence Information Technology, IEEE, 2007

[5] Q. Shi, T. F. H. Huo, and D. Li, ""A 3d node localization scheme for wireless sensor networks, Vol.6, No.3,"" IEICE Electron. Express, pp.167-172, 2009.

[6] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol.22, No.6, pp.644-654, Nov., 1976.

서 화 정

e-mail : hwajeong@pusan.ac.kr

2010년 2월 부산대학교 정보컴퓨터공학과 (공학사)

2010년 2월~현 재 부산대학교 컴퓨터공학부 석사과정

관심분야 : 정보보안, RFID/USN, 암호이론, VLSI 설계

김 호 원

e-mail : howonkim@pusan.ac.kr

1993년 2월 경북대학교 전자공학과(공학사)

1995년 2월 포항공과대학교 전자전기공학과 (공학석사)

1999년 2월 포항공과대학교 전자전기공학과 (공학박사)

2008년 2월 한국전자통신연구원(ETRI) 정보보호연구단 선임연구원 / 팀장

2008년 3월~현 재 부산대학교 정보컴퓨터공학부 조교수

관심분야 : 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안