논문 2017-12-29

보안 마이크로 웹페이지 기반 전장 스마트 지도

(Security Micro-web Page Based Battlefiled Smart Map)

허 준, 하 선 주, 차 신, 은 성 배*
(Jun Heo, Sunju Ha, Shin Cha, Seongbae Eun)

Abstract : GPS was developed for military purposes. As a result, it is used as a military important means such as guided weapons and strategy / tactics. However, GPS depends on the communication infrastructure and is affected by interference signals. In this paper, we propose a secure micro - web page - based smart map that can enhance security without relying on communication infrastructure on the battlefield.

The proposed system consists of general smartphone, security QR, central server and smart map. Only use the network when downloading the security key and SmartMap before the task starts. During operation, the smartphone transmits and receives data using a secure QR. The security QR inserts the security code to prevent forgery and falsification and confirms whether the data is authentic by checking whether the smart phone is forged or not. As a result of implementation, we solved communication security problem of existing technology by using location based service without relying on communication infrastructure.

Keywords : Battlefield smart map, Security QR, Micro web-page, Smartphone

Ⅰ. 서 론

위치기반 서비스의 기반 기술인 GPS는 병사들이 정확한 목표지점으로 이동하기 위한 군사적 용도로 개발되었다. GPS 위성에서 보내는 시간신호는 군사적으로 유용하게 사용된다.

첨단 유도무기들은 GPS 수신장치를 이용해 정확한 지점에 타격한다. 각지에 흩어진 병사들은 GPS 수신기를 이용해 위치를 확인하고 목표지점과 작전시간을 예측하거나 공유한다.

위성으로부터 보내진 GPS 정보는 중계기를 거쳐 전투무선망에 있는 전술용 단말기로 수신해 작전지시 및 지휘/통제에 이용된다.

그러나 GPS는 네트워크망에 의존하기 때문에 전장의 환경에 크게 좌우된다. 또한 GPS의 기준 신호는 -130dBm으로 주요시설을 방어하기 위한 교란 전파에 취약하다 [1]. 우리나라의 경우 그림 1과 같이 북한의 GPS 전파 교란에 의해 항공센터나 이동통신 기지국이 피해를 입은 사례가 있으며 현재까지 GPS 교란 전파의 간섭신호를 제거하는 방법에 대한 많은 연구가 이루어지고 있다 [2, 3].

본 논문에서는 교란신호에 취약한 GPS 수신 체계의 대안으로 네트워크 연동을 하지 않은 상태의 스마트폰, 마이크로웹페이지와 보안 QR을 이용하는 보안 마이크로웹페이지 기반 전장용 스마트 지도

그림 1. 전파교란에 의한 피해 현황
Fig. 1 Damage due to radio disturbance

*Corresponding Author (sbeun@hnu.kr)
Received: July 10 2017, Revised: July 21 2017, Accepted: July 25 2017.
J. Heo: KCCI Seoul Technical Education Center.
S. Ha, S. Cha, S. Eun: Hannam University
※ 이 논문은 2017년도 한남대학교 학술연구조성비 지원에 의하여 연구되었음

ISSN : 1975-5066
http://dx.doi.org/10.14372/IEMEK.2017.12.4.259

(이하 전장용 보안 스마트 지도) 체계를 제안한다.

선발대와 후발대는 보안키를 작전 수행 전 중앙서버로부터 발급받는다. 선발대는 작전지역 지도와 마커, 텍스트, 보안키로 구성된 스마트지도를 중앙서버에 업로드한다. 후발대는 등록된 스마트지도를 중앙서버로부터 스마트폰에 다운받는다. 선발대는 작전지역을 선행하며 현재 상황과 보안키를 QR코드에 저장한다. 후발대는 작전지역에서 QR코드를 스캔할 때 보안키를 이용하여 QR코드의 위/변조 사실을 전용 앱에서 우선 확인한다. QR코드의 신뢰성을 확인한 뒤 상황을 파악하여 전술에 이용한다.

제안하는 시스템은 네트워크에 의존하지 않고 선발대와 후발대 간 정확한 위치와 전술 내용을 전달할 수 있다. 시스템의 성능을 확인하기 위해 네트워크망에 연결하지 않고 구현한 시스템과 기존 시스템을 비교하여 신뢰성, 환경 영향 등의 항목을 검증한다.

Ⅱ. 본 론

1. 스마트 지도

위치기반 서비스 중 가장 보편화된 전자지도는 위치정보를 이용해 다양한 서비스를 제공한다 [4]. 그러나 스마트 지도 서비스를 이용하기 위해서는 네트워크망의 연결이 필수적이다. 특정 위치의 정보가 저장된 QR 코드를 다른 사용자에게 전달하여 스마트지도에서 사용할 수 있다. 그러나 QR 코드는 불특정 다수에게 노출되거나 위/변조 될 수 있다 [5].

오프라인 스마트지도는 상대적으로 큐싱(Qshing)이나 개인정보 유출의 위험성이 낮지만 대용량의 지도 전체를 저장한다. 스마트지도의 다양한 기능을 사용할 수 없고 지도를 표시만 할 수 있다.

따라서 작전환경을 예측할 수 없는 환경에서 통신망에 의존하지 않고 접근이 용이한, 적은 용량으로 필요한 정보를 기록할 수 있는 오프라인 스마트지도 체계가 필요하다.

2. 군용 GPS 기술

GPS는 유도무기의 정밀한 폭격 유도와 부대 지휘/통제 등에 사용된다. 군은 GPS 정보를 기반으로 적군의 주요 시설에 대한 집중 포화나 타격을 실행한다 [6]. 각 부대의 지휘/통제관은 전송된 정보를 토대로 전술무선망 안의 아군 부대와 공유한다. 정보를 기반으로 작전의 정밀도와 전투의 능률을 높인다.

GPS는 치명적인 피해를 주거나 받을 수 있는 기술로써 전장에서의 활용도가 높다.

그러나 기준신호의 세기가 -130 dBm 으로 교란 전파에 취약하다 [1]. 이를 위해 GPS 교란 전파의 간섭신호를 제거하는 방법에 대한 다양한 연구가 이루어지고 있다 [2, 3].

3. 마이크로웹페이지 기술

마이크로 웹페이지는 웹을 구성하는 템플릿과 콘텐츠로 구분한다. 스마트단말에 템플릿을 저장하고 QR코드에 콘텐츠를 저장한 뒤 이를 합성하여 경량화 된 웹서비스를 제공한다 [7, 8].

스마트폰의 마이크로웹페이지 앱으로 QR 코드를 스캔하여 컨텐츠 정보를 얻는다. 마이크로웹페이지는 네트워크망에 연결하지 않고 웹 서비스를 할 수 있다.

Ⅲ. 보안 마이크로 웹페이지 기반 전장 스마트 지도

1. 시스템 구성

본 논문에서 제안하는 전장용 보안 스마트 지도는 네트워크망에 의존하지 않고 작전 활동에 활용한다. 그림 2와 같이 전장용 보안 스마트 지도는 전자 지도인 템플릿과 정보를 표시하는 콘텐츠로 구성된다.

템플릿은 작전 지역의 지도와 마커, 화살표, Text들로 구성되며 스마트폰에 저장된다. 콘텐츠는 간단한 텍스트와 식별자 등으로 구성되며 템플릿에 표시하는 구체적인 정보를 저장한다.

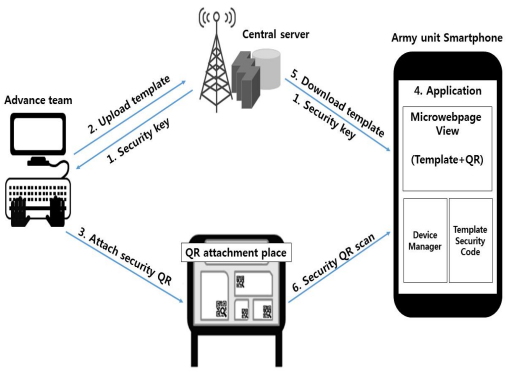

그림 2. 시스템 구성도

Fig. 2 System configuration diagram

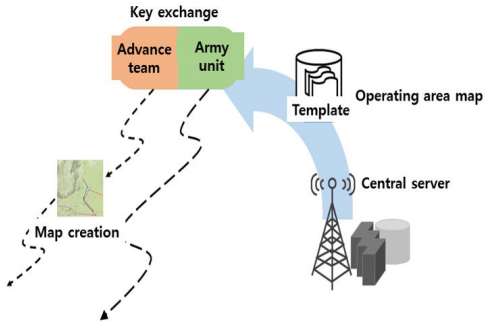

그림 3. 사용자 시나리오
Fig. 3 User scenarios

전장용 보안 스마트 지도의 사용자 시나리오는 그림 3과 같다.

그림 3의 시나리오를 이용하여 아래와 같은 절차를 가진다.

1) 선발대와 본대는 중앙 서버를 통해 보안 KEY를 나누어 가진다.
2) 선발대는 템플릿에 보안 KEY를 포함하여 중앙 서버에 업로드하며 본대가 사용자 인증 후 접근하여 다운받는다.
3) 선발대는 작전 지역을 선행하며 전용 앱으로 상황에 맞는 QR 코드를 제작하고 약속된 장소에 QR 코드를 설치한다.
4) 본대는 선발대를 쫓으며 약속된 QR 코드 설치 장소에서 QR 코드를 스캔한다.
5) 전용 앱이 보안코드를 해석/비교하여 스캔한 QR 코드의 신뢰성이 확인되면 보안 KEY를 입력한다.
6) 인증 절차가 마무리되면 화면에 작전 지도 데이터가 표시된다.

전장용 보안 스마트 지도는 기존의 QR 코드를 사용하지 않는다. 보안코드가 들어간 QR 코드와 템플릿을 사용하여 QR 코드가 위/변조되었을 때 전용 앱에서 즉시 확인한다. 구성원이 중앙 서버에서 인증 절차를 거쳐 작전 템플릿의 접근 권한을 부여받고 선발대와 후발대가 동일한 보안 KEY를 나누어 가지기 때문에 이중 보안요소를 가진다. 아래 표 1와 같이 제안하는 시스템은 기존 마이크로웹페이지와 GPS의 문제점을 해결할 수 있다.

2. 템플릿

전장용 보안 스마트 지도의 템플릿은 그림 4와

표 1. 기존 문제점 해결
Table 1. Solve existing problems

Network	
Problem	Device is disabled when GPS signal interception or propagation disturbance occurs.
Solution	It is composed of template and contents based on micro web page, so there is no data consumption in actual use, so it is not affected by radio disturbance activity.
QR code	
Problem	Manipulated information confusion during modulated QR code scan.
Solution	QR code is scanned with exclusive application and security code interpretation is determined by modulation.
Template	
Problem	Information leaked in combination with content.
Solution	Designed so that templates and contents are composited only by entering a security key.
Problem	Heavy confusion due to missing information due to randomly created templates.
Solution	Limit creating and modifying templates by specifying access rights on the central server.

같이 특정 지역 지도 이미지가 저장되며 고유 식별번호로 분류한다. 선발대는 중앙 서버를 통해 보안 KEY를 제공받고 이를 템플릿에 포함시켜 서버에 업로드 한다.

중앙 서버에 등록된 템플릿은 설정된 접근권한에 따라 사용자의 접근을 제한한다.

3. QR 데이터

전장용 보안 스마트 지도의 보안 QR 코드는 그림 5와 같이 사용자가 지정한 지점의 좌표 외에 템플릿 고유 식별번호와 목적지/경로 좌표, 보안 KEY가 포함된다. 보안 KEY는 중앙 서버로부터 제공되며 정보유출을 최소화하기 위한 안전장치이다.

4. 전장용 보안 스마트 지도 전용 앱

전장용 보안 스마트 지도 전용 앱은 QR 코드를

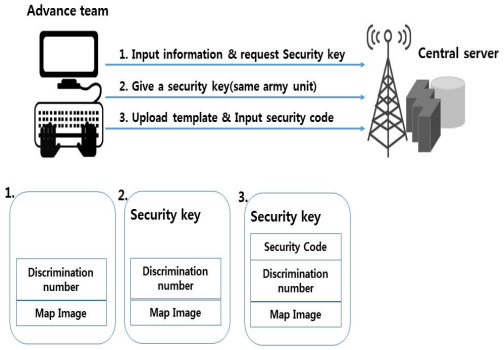

그림 4 템플릿 순서도
Fig. 4. Template Flowchart

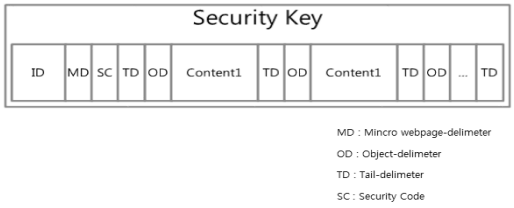

그림 5. 보안 QR코드 데이터
Fig. 5. Security QR Code Data

인식하여 디스플레이에 표시해 주며 로그인 기능을 통해 사용자를 식별하고 서버로부터 각 사용자에 알맞은 접근권한을 부여 받는다. 이는 중앙 서버에 저장된 템플릿을 임의 변경 수정이나 삭제로부터 보호한다. 보안 마이크로 웹페이지 스마트 지도의 보안 QR 코드나 템플릿은 전용 앱을 통해서만 해석이 가능하며 스캔한 보안 QR 코드의 데이터와 보안 코드를 해석하여 템플릿의 보안코드와 비교하여 QR 코드의 위/변조 사실을 판단하고 신뢰성과 보안성을 높인다.

선발대의 경우 QR 코드를 작성하여 습득한 작전 정보를 본대에 알리는 임무를 수행해야 때문에 선발대가 가지고 있는 앱에는 QR 코드 작성 기능이 추가 되어야한다. 전용 앱으로 템플릿을 열어 지도가 표시되면 현 작전 지역에 있는 정보를 지도에 표시한다. 표시할 수 있는 정보는 지형 및 기후 상태와 진행방향, 적군의 병력 구성과 인원, 주요시설 등을 표시할 수 있다. 표시된 정보는 변환되어 QR 코드에 저장된다.

5. 보안코드

보안 코드는 군부대의 매일 바뀌는 암구호의 역할

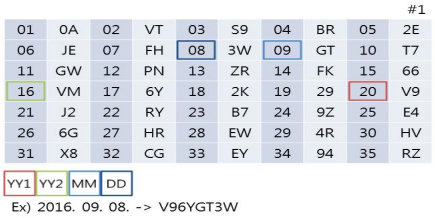

그림 6. 특수상황에서 보안코드 예시
Fig. 6 Security code example
in special situations

표 2. 암호키 사용 유효기간 (NIST 권고안)
Table 2. Cryptographic key validity period
(NIST recommendation)

Key item		Validity	
		Sender	Receiver
Symmetric key	Secret key	Max 2year	Max 5year
Public key	Encryption Public key	Max 2year	
	Decryption Private key	Max 2year	
	Verification Public key	Max 2year	
	Signature Private key	Max 2year	

을 한다. 그러나 작전중의 부대에게 매일 변경되는 보안코드를 전달하는 것은 어렵다. 본 논문에서는 특수 상황에서 정해진 규칙에 따라 보안코드를 구성하기 위하여 그림 6과 같이 복수의 숫자와 문자가 조합된 표를 날짜를 이용해 구하는 방식을 사용하였다.

보안코드를 입력할 때 보안성을 높이기 위해 대칭키 방식의 AES (Advanced Encryption Standard)로 128 비트의 암호화 키를 가지는 방식을 채택하였다. 128 비트의 대칭키 암호 알고리즘을 사용할 경우 최대 30년까지 알고리즘의 안정성이 보장되고, 보안 KEY의 경우 2~5년의 사용 유효기간이 설정된다. 표 2는 NIST의 보안 KEY 관리 권고안을 기반으로 작성한 사용 유효기간이다. 보안 Key는 중앙서버에서 발급하고 군부대에서 수신하기 때문에 전쟁중에도 전달기간에 상관없이 신뢰성 있게 사용할 수 있다.

```
<iframe src = "Daejeon5000.svg" frameborder="
"1" " allowtransparency =" "true" "> </iframe>

Function createMarker1(point){
        var iconBlue = new Gicon(G_DEFAULT_ICON);
            iconBlue.imae = 'Start.png';
            iconBlue.shadowSize = new GSzie(1,1);
            iconBlue.iconSize = new Gsize(23, 26);

                start = new Gmarker(point, iconBlue);

                return start;
}

Map.addOverlay(createMarker1(location));
```

그림 7. iframe과 createMarker
Fig. 7 iframe and createMarker

```
function foundLocation(position){
        latitudex = position.coords.latitude;
        longitudex = position.coords.longitude;
        location = new GLatLng(latitudex, longitudex);

        function createMarker3(point){
                var iconBlue = new GIcon(G_DEFAULT_ICON);
                    iconBlue.image = 'location.png';
                    iconBlue.shadowSize = new GSize(1, 1);
                    iconBlue.iconSize = new GSize(23, 26);

                        hkm = new GMarker(point, iconGreen);

                        return hkm;
        }
        map.addOverlay(createMarker3(location));
}
```

그림 8. GeoLocation
Fig. 8 GeoLocation

Ⅳ. 구현 및 성능 평가

1. 시스템 형상

1.1 템플릿

템플릿에는 SVG형 지도 이미지 파일과 브라우징을 위한 코드가 저장된다. 그림 7과 같이 HTML5의 iframe을 사용하여 지도를 생성한다. QR 코드로부터 받은 좌표는 icon 객체를 생성하여 createMarker 함수로 출발지와 목적지에 마커를 올리고 경로를 그려준다.

JavaScript의 GeoLocation과 Orientation을 이용하여 사용자의 현재위치와 바라보는 방향을 지도에 표시한다. 그림 8과 같이 GeoLocation은 position 메소드를 사용하여 모바일의 위도와 경도를 웹브라우저로 불러온다.

그림 9의 Orientation은 지자기 센서의 값을 읽고 값이 변할 때마다 (이벤트 발생) 각도를 계산하여 사용자의 방향을 나타낸다.

```
var heading=0;

window.ondeviceorientation = changeCompass;

function changeCompass(event){
heading = parseInt(event.alpha)*Math.PI/180;
var pitch = parseInt(event.beta)*Math.PI/180;
var rolling = parseInt(event.gamma)*Math.PI/180;
```

그림 9. Orientation
Fig. 9 Orientation

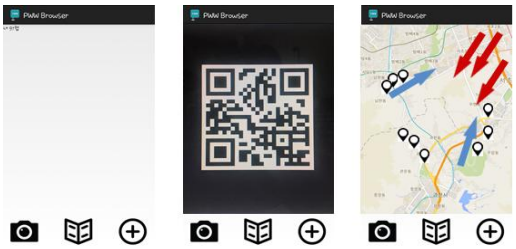

그림 10. 전장 보안 스마트 지도 전용 앱 실행 화면
Fig. 10 Battlefield security smart map exclusive application execution screen

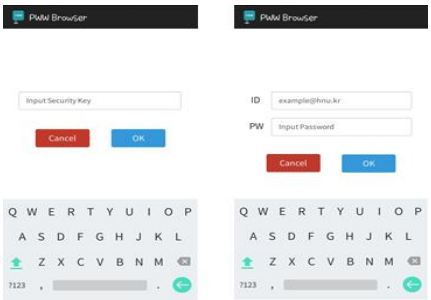

그림 11. 보안 KEY, ID 입력 화면
Fig. 11 Security KEY, ID input screen

1.2 보안 QR 코드

보안 QR 코드는 사용자가 지정한 지역의 좌표 외에 템플릿의 고유 식별번호, 보안 코드, 컨텐츠 위치 및 내용이 저장된다. 보안 코드는 QR 코드 생성 시 계산식에 의해 임의의 문자와 숫자가 조합되며 QR 코드의 위/변조를 탐지하기 위해 사용된다.

1.3 전장용 보안 스마트 지도 전용 앱

전장용 보안 스마트 지도 전용 앱은 그림 10과 같이 보안 QR코드에서 추출한 콘텐츠를 템플릿과 합성하여 스마트폰 화면에 스마트 지도를 표시한다.

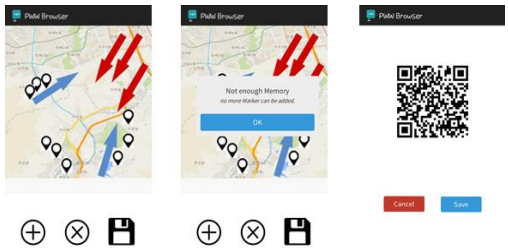

그림 12. QR 코드 생성 UI
Fig. 12 Security QR code generation UI

표 3. 템플릿과 컨텐츠 용량
Table 3. Templates and Content Capacity

Item	Size
Template	17 MB
Contents	700byte

표 4. QR 코드 용량
Table 4. QR code capacity

Category	Conformation	Size
Identification number	12345678 (8count)	8byte
Security code	ABCDEFGH (8count)	8byte
Contents	(contents/location /Separator)	12byte

보안 QR 코드나 템플릿은 전용 앱을 통해서만 해석이 가능하며 스캔한 보안 QR 코드의 데이터는 보안 KEY를 입력해야만 저장된 템플릿에 접근할 수 있다. 본 논문에서는 그림 11과 같이 로그인을 통해 사용자를 식별하여 임의로 조작하지 못하도록 설계하였다.

선발대가 습득한 정보를 QR 코드에 저장하기 위한 QR 코드 작성 기능은 앱을 이용해 저장된 템플릿을 열어 그 위에 병력의 구성과 인원, 진행 방향을 나타내기 위한 화살표, 기후 상태, 지형 지물을 입력하게 되면 그림 12와 같이 컨텐츠의 종류와 위치를 QR 코드 데이터로 변환하여 작성해준다.

2. 성능 평가

스마트폰에 저장되는 템플릿의 크기와 컨텐츠의 크기를 표 3과 같이 측정하였다. 컨텐츠는 QR 코드의 저장 공간과 오류복원레벨을 표준인 “M”을 기준으로 입력 할 수 있는 개수에 제한을 두어 인식률 저하를 방지하여야 한다.

표 5. 템플릿 합성 응답시간
Table 5. Template composite response time

count	1	2	3	4	5	6	7	8
sec.	2.3	3.1	2.7	2.6	2.9	2.9	2.8	2.6
count	9	10	11	12	13	14	15	Aver.
sec.	3.3	3.0	2.8	2.8	2.9	3.1	3.3	2.87

표 6. 기존 방식과의 비교
Table 6. Comparison with existing methods

	Network	Contents Size	Contents Display
Map app	O	-	O
Offline Map	X	Large	X
Military GPS	O	Small	O
Smart Map	X	Small	O

표 4는 QR 코드의 구성과 용량을 나타낸다.

QR 코드의 최대 저장 용량은 약 3KB이며 고유 식별번호와 보안코드 등의 기본 구성요소를 제외한 용량에서 QR 코드의 인식률이 저하되지 않기 위해서는 컨텐츠의 개수를 150개 이하로 제한해야 한다.

표 5은 QR 코드를 스마트폰으로 스캔했을 때, 템플릿과 합성되어 화면에 표시되는 응답시간을 나타낸다.

QR 코드를 스캔하고 나서 템플릿과 합성되어 화면에 표시되기까지 약 3초 정도 걸리는 것을 확인했다. QR 코드 스캔/인식과정 때문에 실제 사용 시 2~3초 정도의 추가시간이 필요함을 알 수 있었다.

다음은 온/오프라인 스마트 지도, 군용 GPS, 보안 마이크로 웹페이지 스마트 지도를 각 항목에 따라 비교한 것이다.

표 6에서 나타난 것과 같이 네트워크 의존성을 제거하고 같은 지역을 저장할 때 저장 공간을 더 적게 차지하는 것을 확인했다. 컨텐츠를 나타내는 것이 가능하여 네트워크가 불안정하거나 GPS 신호의 신뢰성이 떨어지는 환경에서 정확한 정보를 주고받을 수 있어 군사 작전에 큰 효용성을 볼 수 있다.

V. 결 론

본 논문에서는 군용 GPS 체계의 문제점에 대한

대안을 제시하였다. 기존의 GPS 체계는 네트워크망에 의존적이기 때문에 인프라가 없거나 정상적인 동작을 하지 않는 환경에서 사용할 수 없다. 이를 마이크로 웹페이지를 기반으로 하는 스마트 지도를 설계함으로써 해결하였다. 사용자는 중앙서버로부터 경량화된 템플릿을 미리 다운로드 받아 스마트폰에 저장하여 QR 코드를 스캔 하는 행동만으로 스마트 지도를 사용할 수 있다. 다음으로 QR 코드를 이용한 접근방법의 보안성 문제는 보안 KEY와 보안코드를 통해 QR 코드의 위/변조를 막고 접근을 제한함으로써 접근 방법에 따른 보안 위협을 제거하였다. 또한 중앙서버에서 이뤄지는 사용자 인증 절차를 통해 템플릿의 무단 수정, 변경과 삭제를 미연에 방지 하였다. 네트워크를 사용하지 않고 위치기반 서비스를 사용할 수 있고 보안성을 위협하는 요소를 제거하였다.

향후 전장에서 실제 선발대가 전술적으로 사용할 수 있도록 QR코드의 설치 및 훼손방지 방법에 대한 연구와 스마트폰과 실제 군 전용 단말기간의 호환성, QR코드와 스마트폰간 응답시간 단축, 스마트 지도를 경량화 하는 등의 기능 개선을 통해 실제 전장에서 적용할 수 있도록 하는 후속 연구가 필요하다.

References

[1] J.J Spilker, “GPS Signal Structure and Performance Characteristics.” Navigation, Vol. 25, No. 2, pp. 121-146, 1978.

[2] E.R Jeong, H.H Won, S.W Cho, B.S Ahn, “An Active Interference Cancellation Technique for Removing Jamming Signals in Array Antenna GPS Receivers,” Journal of the Korea Institute of Information and Communication Engineering, Vol. 19, No. 7, pp. 1539-1545, 2015 (in Korean).

[3] I.S Lee, S.J Oh, J.H Han, “Narrow-Band Jamming Signal Cancellation Algorithm for GPS,” The Journal of Korean Institute of Communications and Information Sciences, Vol. 41, No. 8, pp. 859-867, 2016 (in Korean).

[4] http://mashable.com/2010/04/06/location-history-infographic/#St2ZJFY0GkqD, The History of Location Technology [INFOGRAPHIC], Mashable.

[5] H.K Yang, “A Study of Security Weaknesses of QR Codes and Its Countermeasures,” The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 12, No. 1, 2012 (in Korean).

[6] E. Kaplan, C. Hegarty, “Understanding GPS: Principles and Applications. Artech house,” 2005.

[7] S. Ha, S. Eun, S.S. So, Y.S Yun, J. Jung, “Design and Implementation of μ-Webpage Based on QR Code,” Journal of Computing Science and Engineering, Vol. 21, No. 3, 2015 (in Korean).

[8] J. Lee, J. Heo, J. Jung, S. Eun, N.S. Kwak, S.S So, “Smart Maps Based on μ-Webpages in the Infrastructure-less Communications,” Korea Information Science Society 2015 Korea Computer Engineering Conference, pp. 2091-2093, 2015 (in Korean).

Jun Heo (허 준)

2016, Master In information and communication engineering Dept. Hannam University.

2017~ Teacher, KCCI Seoul Technical Education Center .

Email: magicarrow98@naver.com

Sunju Ha (하 선 주)

Ha Sunju received her master's degree and Ph.D. in information and communication engineering from Hannam University in 2011 and 2016. Her research interests are image processing, IoT, embedded systems.

Email: police0729@naver.com

Shin Cha (차 신)

1995 Dept. of Computer Science, KAIST (Ph.D)

1986~2000 Chief Engineer, Innovation Center, LG Electronics

2000~2013 Executive Managing Director, Multimedia Communication Division, IA

2013~2015 Executive Managing Director, Reliable Software V&V Center, Suresofttech

2016~Professor, Dept. of Computer, Communications and Unmanned Technology, Hannam University

Email: scha@hnu.kr

Seongbae Eun (은 성 배)

1995, Ph. D In Computer Science Dept. KAIST.

1995~ , Professor in Hannam University.

Main Research Field: Embedded System, Wireless Sensor Networks, Embedded Deep Learning, etc.

Email: sbeun@hnu.kr