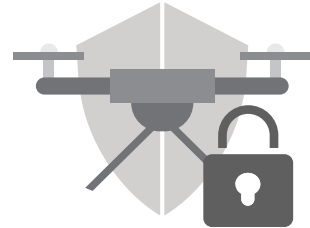


# 드론 기반 서비스를 위한 보안 요구사항



**강유성** 한국전자통신연구원(ETRI) 지능보안연구그룹 책임연구원(PL)  
**김주한** 한국전자통신연구원(ETRI) 지능보안연구그룹 책임연구원  
**김건우** 한국전자통신연구원(ETRI) 지능보안연구그룹 책임연구원

## 1. 머리말

미래학자 토마스 프레이는 미래 드론 시장은 10조 원 이상 규모로 성장하고, 단순 촬영을 넘어 재난감시, 배달, 뉴스제공, 마케팅 등 192개의 비즈니스 도메인에 사용될 것으로 전망하였다[1]. 다양한 예상 서비스 중 재난·재해·환경 무인감시 서비스와 물품수송 무인배달 서비스가 가장 활발하게 연구되어 상용화 단계에 진입하고 있다. 미국 아마존은 자체 제작한 드론을 이용한 30분 이내 무인배달 서비스인 아마존 프라임 에어 서비스를 추진 중이며[2], 독일 DHL은 긴급 구호물품 배달을 위해 Parcelcopter 드론 기반 무인배달 서비스를 추진 중에 있다[3]. 국내에서는 국토교통부의 미래 전략산업 육성 방침에 따라 드론 기반 물품수송, 산림감시, 시설물 안전진단, 국토조사 등의 사업모델 발굴과 시범사업을 추진하고 있다[4].

드론 기반 서비스 사업화 추진은 감시, 조사, 물품수송이라는 고유의 역할에는 충실하지만 디지털 보안 측면에서는 연구가 미흡한 실정이다. 드론은 카메라, 센서, 통신 시스템을 탑재하고 있어서 고의적이든 실수든 보안 취약점 노출 시 해킹과 사생활 침

해 문제 등 심각한 사회 문제를 야기할 수 있다. 드론 해킹 기술로 인해 드론 기반 서비스 시장이 위축될 우려가 있으므로 이를 극복하는 보안 기술에 대한 요구가 커져가고 있다. 따라서, 다양한 드론 기반 서비스 환경에서 신뢰성 확보를 위하여 안전운용 인프라 기술(통신 보안, 네트워크 보안, 보안관제 등)과 역기능(사생활 침해, 테러 등) 예방 기술 개발을 위한 보안 요구사항을 정의하고 이를 기반으로 드론 보안기술을 개발할 필요가 있다.

## 2. 표준의 개요

본 표준[5]의 목적은 드론이 가지는 무인비행이라는 특성과 디지털 디바이스라는 특성을 고려하여 드론 기반 서비스를 위한 보안 요구사항을 정의하는 것이다. 대표적인 무인이동체인 드론은 사람의 개입이 최소화된 환경에서 원격으로 제어되거나 미리 정해진 방식으로 운용되기 때문에 정보유출의 위험이 높다. 특히 드론 기반 다양한 서비스 환경에서 드론이 비행대기 또는 비행 중 여러 디바이스들과 통신을 수행하기 때문에 이에 적합한 보안 요구사항이 필요함에 따라 본 표준에서는 먼저 드론 기반 서비

<표 1> 드론 보안 취약점

분류	보안 취약점
불법 탈취 후 키 해킹	- 비행 중인 드론을 불법 탈취한 후 충분한 시간과 장비로 역공학, 메모리 분석, 부채널 분석 등을 통해 비밀키 해킹 가능 - 드론의 비밀키가 노출될 경우 비행정보, 수집정보, 드론 운영시스템 정보 노출 위험 증가
드론 무력화	- GPS 신호 수신방해, 통신전파 제밍, 자이로 센서 동작 방해 등으로 드론의 비행 또는 통신 무력화 가능 - 공격자는 드론의 비행 자세를 무력화하여 추락시킬 수 있으므로 예상치 못한 충돌로 인한 인명/재산 피해 우려
정보유출	- 저장 정보, 전송 정보, 처리 정보에 대한 보안기술이 없는 경우 무단도청, 비인가 접근을 통해 정보 유출 위험 증가 - 개인정보인 경우 사생활 침해 및 개인정보 오남용 피해로 이어짐
악성코드 감염	- 악성코드 감염에 의한 제어권한 탈취는 드론의 대부분 기능을 오작동시킬 수 있는 위험 존재 - 드론의 비행정보 조작으로 목적지 변경, 공격자에게 수집정보 전달 등의 사이버/물리 공격 가능
불법장치 탐제	- 불법/비인가 드론의 불법장치(예: 총, 폭탄, 생화학무기 등) 탐제를 알아내지 못한다면 사회적 혼란 초래 - 사람/건물에게 직접 공격하므로 인적/경제적/안보적 피해 가능

스의 구성요소를 정의하고, 각 구성요소별 보안 요구사항, 구성요소 간 인터페이스에서의 보안 요구사항을 정의한다. 또한 드론 기반 서비스 환경을 고려한 키은닉 보안 요구사항을 포함하고 있다. 주요 내용을 살펴보면 다음과 같다.

본 표준에서 정의하는 보안 요구사항은 드론을 디지털 디바이스의 하나로 고려했을 때, 기본적인 디지털 보안 서비스인 기밀성, 무결성, 가용성, 인증, 키 보호 등을 제공하기 위한 보안 요구사항을 정의한다.

특히, 보안 요구사항 정의에 앞서 일반적인 드론 보안 취약점을 설명하고, 대표적인 드론 기반 서비스인 무인감시 서비스와 무인배달 서비스를 고려한 시스템 구성요소를 제안하고 각 구성요소의 주요 역할을 설명하고 있다. 그런 후에 각 구성요소별 보안 요구사항과 구성요소 간 인터페이스 요구사항 및 키은닉 보안 요구사항을 정의한다.

드론은 드론 기반 서비스 제공을 위한 시스템 구성요소 중 하나이며, 드론 자체에 대한 보안 요구사항은 구성요소 보안 요구사항의 하나로 포함된다. 또한 드론과 통신하는 다양한 구성요소들 역시 각 구성요소별 보안 요구사항이 정의되며, 상호 통신이 수행될 때의 인터페이스 보안 요구사항 및 키은닉 보안 요구사항이 정의된다.

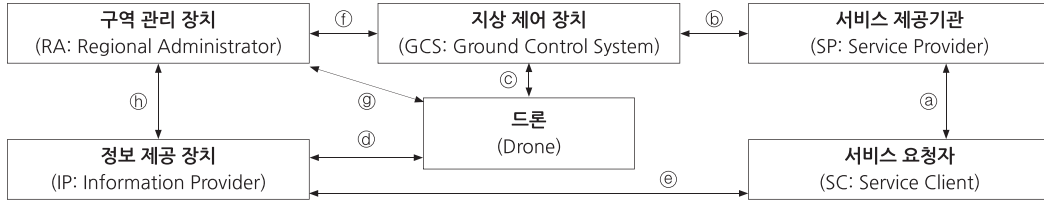
드론은 카메라, 센서 및 별도의 공격물품을 탑재할 수 있기 때문에 사람에 대한 사생활 침해, 개인정보 유출 등의 사이버 피해뿐만 아니라 주요시설 충돌, 공격 등 물리적 피해가 공존한다. 특히 GPS 신호 수신방해, 가짜신호 전송, 악성코드 감염 등을 통한 드론 탈취, 드론 무력화 공격이 가능하고, 무단 도청에 의한 드론의 영상정보, 개인정보 유출 가능성도 매우 크다. 또한 불법/비인가 드론에 의한 주요시설 충돌 및 무기장착 드론에 의한 물적/인적 피해도 우려된다.

<표 1>에 대표적인 드론 보안 취약점을 정리하였다.

### 3. 드론 기반 서비스 보안 요구사항

#### 3.1 시스템 구성요소

드론 기반 서비스 시스템의 구성요소는 [그림 1]과 같이 크게 서비스 요청자, 서비스 제공기관, 지상 제어 장치, 구역 관리 장치, 정보 제공 장치 및 드론 등으로 구성된다. 각 구성요소별 정의 및 주요 역할은 <표 2>와 같다. 서비스 요청자, 서비스 제공기관, 지상 제어 장치, 그리고 드론은 필수(Mandatory) 구성요소이며, 구역 관리 장치와 정보 제공 장치는 선택(Optional) 구성요소이다.



[그림 1] 드론 기반 서비스 시스템 구성요소

<표 2> 드론 기반 서비스 시스템 구성요소별 정의 및 주요 역할

[(M)은 필수(Mandatory) 항목, (O)는 선택(Optional) 항목]

구성요소	정의 및 역할
서비스 요청자 (M)	<p>드론 기반 서비스의 요청자(Service Client)</p> <ul style="list-style-type: none"> <li>- (예1. 드론 기반 무인배달 서비스) 물품 구입을 요청하고 물품 값을 결제하는 고객에 해당하며 고객은 PC 또는 스마트폰을 통해 서비스 제공기관과 통신할 수 있음. 최종 물품수령을 확인해 줄 의무가 있으며 판매자로부터 부가서비스를 제공받기 위한 통신을 수행할 수 있음.</li> <li>- (예2. 드론 기반 재난·재해·환경 무인감시 서비스) 특정 지역 또는 특정 사건의 감시 및 정보전달을 요청하는 사용자(예를 들면, 지방자치단체, 소방당국, 경찰, 경비업체 등)에 해당하며 사용자는 드론 또는 드론의 정보 제공 장치([그림 1]의 IP)로부터 합법적 감시 정보를 수집할 수 있어야 함.</li> </ul>
서비스 제공기관 (M)	<p>드론 기반 서비스의 제공자(Service Provider)</p> <ul style="list-style-type: none"> <li>- (예1. 드론 기반 무인배달 서비스) 고객([그림 1]의 SC)으로부터 물품 주문과 물품 값을 받고, 해당 물품 정보를 배달부서 또는 배달전문기관의 지상 제어 장치([그림 1]의 GCS)에게 전달함. 고객의 물품수령 확인이 완료되면 고객과 부가서비스 통신을 수행할 수 있음.</li> <li>- (예2. 드론 기반 재난·재해·환경 무인감시 서비스) 서비스 요청자에게 특정 지역 또는 특정 사건에 대한 감시 정보(영상 정보 또는 센싱 정보)를 제공함.</li> </ul>
지상 제어 장치 (M)	<p>드론에게 명령을 전달하거나 직접 드론을 원격 제어하는 장치(Ground Control System)</p> <ul style="list-style-type: none"> <li>- (예1. 드론 기반 무인배달 서비스) 서비스 제공기관으로부터 배달 요청을 전달받아 드론에 배달 명령을 내림. 실질적으로 드론을 운영하는 기관임. 서비스 제공기관의 배달전담부서 또는 제3의 배달전문회사 가능함.</li> <li>- (예2. 드론 기반 재난·재해·환경 무인감시 서비스) 드론이 감시할 감시 영역을 설정하거나 감시 대상 이벤트 정보를 설정할 수 있음.</li> </ul>
드론 (M)	<p>실질 임무를 수행하는 드론(Drone)</p> <ul style="list-style-type: none"> <li>- (예1. 드론 기반 무인배달 서비스) 드론은 지상 제어 장치의 명령을 받아 물품을 운반하는 무인 배달장치 역할을 수행함.</li> <li>- (예2. 드론 기반 재난·재해·환경 무인감시 서비스) 지상 제어 장치의 명령에 따라 감시 영역으로 감시 정보를 수집/보관/전달함.</li> </ul>
구역 관리 장치 (O)	<p>특정 지역 내에 비행중인 드론을 관리하는 별도의 관리 장치(Regional Administrator)</p> <ul style="list-style-type: none"> <li>- 선택(optional) 구성요소이며, 자신의 통신 범위 내에 있는 드론만 관리함. 통신 상대는 드론, 지상 제어 장치, 정보 제공 장치이며, 드론과 통신하는 통신방식과는 별도의 통신방식을 통해 지상 제어 장치와 통신할 수 있어야 함(예를 들면, 위성통신이 가능한 특수 고성능 드론, 열기구 또는 이동통신망을 사용할 수 있는 별도의 드론 관리용 기지국 등이 구역 관리 장치 역할을 할 수 있음).</li> </ul>
정보 제공 장치 (O)	<p>드론 기반 서비스 관련 정보를 제공해 주는 장치(Information Provider)</p> <ul style="list-style-type: none"> <li>- (예1. 드론 기반 무인배달 서비스) 드론이 운반해 온 물품을 받고 확인해 주는 장치임. 고객([그림 1]의 SC)의 관리하에 있는 장치이며, 고객에게 물품수령을 알려줄 의무가 있음. 디지털화된 택배함이 정보 제공 장치([그림 1]의 IP) 역할을 수행할 수 있음.</li> <li>- (예2. 드론 기반 재난·재해·환경 무인감시 서비스) 감시 영역 내에 있는 센서들이 정보 제공 장치 역할을 하여 센싱 정보를 드론에게 전달하거나 감시 서비스 관련 사항을 확인시켜 줄 수 있음.</li> </ul>

### 3.2 구성요소 보안 요구사항

<표 3>은 각 구성요소의 보안 요구사항을 정의하고 있다. 구역 관리 장치와 정보 제공 장치와 관련된 요구사항은 해당 장치가 사용될 경우를 가정한 요구사항이다.

### 3.3 인터페이스 보안 요구사항

<표 4>는 구성요소간 인터페이스의 보안 요구사항을 정의하고 있다. 구역 관리 장치와 정보 제공 장치와 관련된 요구사항은 해당 장치가 사용될 경우를 가정한 요구사항이다.

<표 3> 구성요소 보안 요구사항

구성요소	보안 요구사항
서비스 요청자 (M)	<ul style="list-style-type: none"> <li>- 서비스 제공기관([그림 1]의 SP)에게 정당한 사용자임을 증명해야 한다(M).</li> <li>- 안전한 통신 채널을 통해 서비스 제공기관에게 드론 기반 서비스를 요청해야 한다(M).</li> <li>- 정보 제공 장치([그림 1]의 IP)가 정당한 장치임을 검증해야 한다(M).</li> <li>- 안전한 통신 채널을 통해 정보 제공 장치의 최신 이벤트를 확보할 수 있다(O).</li> </ul>
서비스 제공기관 (M)	<ul style="list-style-type: none"> <li>- 서비스 요청자([그림 1]의 SC)가 정당한 사용자임을 검증해야 한다(M).</li> <li>- 지상 제어 장치([그림 1]의 GCS)에게 정당한 사용자임을 증명해야 한다(M).</li> <li>- 안전한 통신 채널을 통해 지상 제어 장치에게 드론 기반 서비스를 명령해야 한다(M).</li> </ul>
지상 제어 장치 (M)	<ul style="list-style-type: none"> <li>- 서비스 제공기관([그림 1]의 SP)가 정당한 사용자임을 검증해야 한다(M).</li> <li>- 드론([그림 1]의 Drone)에게 정당한 사용자임을 증명해야 한다(M).</li> <li>- 안전한 통신 채널을 통해 드론을 제어하고 통신해야 한다(M).</li> <li>- 구역 관리 장치([그림 1]의 RA)와 상호 정당한 사용자임을 증명해야 한다(M).</li> <li>- 안전한 통신 채널을 통해 구역 관리 장치와 통신해야 한다(M).</li> <li>- 드론 또는 구역 관리 장치로부터 수신한 정보를 안전한 통신 채널을 통해 서비스 제공기관에게 전달해야 한다(M).</li> </ul>
드론 (M)	<ul style="list-style-type: none"> <li>- 정당한 통신 상대방에게 자신이 정당한 드론임을 증명해야 한다(M).</li> <li>- 키는 안전하게 생성해야 한다(M).</li> <li>- 드론에서 구동되는 프로그램의 무결성을 보장해야 한다(M).</li> <li>- 실시간으로 악성코드를 탐지할 수 있어야 한다(M).</li> <li>- 드론 수집 정보의 무결성을 보장해야 한다(M).</li> <li>- 키 사용 기간을 제한할 수 있어야 한다(M).</li> <li>- 키 사용 시점을 관리하는 타임스탬프 기능이 있어야 한다(M).</li> <li>- 배터리 소모를 야기하는 비정상 메시지를 감지하고 대응할 수 있어야 한다(M).</li> <li>- GPS 방해전파를 탐지하고 회피할 수 있다(O).</li> <li>- 무선통신 방해 재밍신호를 탐지하고 우회 통신채널을 확보할 수 있다(O).</li> <li>- 자이로 센서 방해전파를 탐지하고 회피할 수 있다(O).</li> </ul>
구역 관리 장치 (O)	<ul style="list-style-type: none"> <li>- 정당한 통신 상대방에게 자신이 정당한 구역 관리 장치임을 증명해야 한다(M).</li> <li>- 불법/비인가 비행 드론을 감지하고 추적해야 한다(M).</li> <li>- 드론 모니터링 정보를 지상 제어 장치에게 전달해야 한다(M).</li> <li>- 드론 형태의 구역 관리 장치는 드론의 보안 요구사항을 준수해야 한다(M).</li> <li>- 비행 중인 드론에게 직접 명령을 전달할 수 있어야 한다(O).</li> <li>- 정보 제공 장치로부터 서비스 관련 정보를 안전하게 수신할 수 있다(O).</li> </ul>
정보 제공 장치 (O)	<ul style="list-style-type: none"> <li>- 서비스 요청자([그림 1]의 SC)에게 정당한 통신장치임을 증명해야 한다(M).</li> <li>- 드론([그림 1]의 Drone)로부터 서비스 정보를 안전하게 수신해야 한다(M).</li> <li>- 서비스 요청자에게 서비스 관련 정보를 안전하게 전달해야 한다(M).</li> <li>- 서비스 요청자가 정보 제공 장치의 관리자 역할을 수행해야 한다(M).</li> <li>- 드론에게 서비스 완료 메시지를 안전하게 전달할 수 있다(O).</li> </ul>

<표 4> 인터페이스 보안 요구사항

인터페이스	보안 요구사항
서비스 요청자 - 서비스 제공기관 [그림 1]의 ㉔	- 상호 인증이 되어야 한다(M). - 전송 메시지의 기밀성, 무결성, 부인방지 기능이 제공되어야 한다(M).
서비스 제공기관 - 지상 제어 장치 [그림 1]의 ㉕	- 상호 인증이 되어야 한다(M). - 전송 메시지의 기밀성, 무결성, 부인방지 기능이 제공되어야 한다(M).
지상 제어 장치 - 드론 [그림 1]의 ㉖	- 키 해킹 방지기법에 기반하여 실시간 세션키 생성을 지원하는 프로토콜이 동작해야 한다(M). - 상호 인증이 되어야 한다(M). - 전송 메시지의 기밀성, 무결성, 부인방지 기능이 제공되어야 한다(M). - 전송 데이터 암호화/복호화 세션키를 저장하지 않는 보안 채널을 제공할 수 있다(O). - 비인가 메시지를 감지할 수 있다(O).
드론 - 정보 제공 장치 [그림 1]의 ㉗	- 키 해킹 방지기법에 기반하여 실시간 세션키 생성을 지원하는 프로토콜이 동작해야 한다(M). - 상호 인증이 되어야 한다(M). - 전송 메시지의 기밀성, 무결성, 부인방지 기능이 제공되어야 한다(M). - 전송 데이터 암호화/복호화 세션키를 저장하지 않는 보안 채널을 제공할 수 있다(O). - 비인가 메시지를 감지할 수 있다(O).
정보 제공 장치 - 서비스 요청자 [그림 1]의 ㉘	- 상호 인증이 되어야 한다(M). - 전송 메시지의 기밀성, 무결성, 부인방지 기능이 제공되어야 한다(M). - 서비스 요청자는 정보 제공 장치의 관리자 권한으로 접속 가능하여야 한다(M).
구역 관리 장치 - 지상 제어 장치 [그림 1]의 ㉙	- 상호 인증이 되어야 한다(M). - 전송 메시지의 기밀성, 무결성, 부인방지 기능이 제공되어야 한다(M).
구역 관리 장치 - 드론 [그림 1]의 ㉚	- 키 해킹 방지기법에 기반하여 실시간 세션키 생성을 지원하는 프로토콜이 동작해야 한다(M). - 상호 인증이 되어야 한다(M). - 전송 메시지의 기밀성, 무결성, 부인방지 기능이 제공되어야 한다(M). - 전송 데이터 암호화/복호화 세션키를 저장하지 않는 보안 채널을 제공할 수 있다(O). - 비인가 메시지를 감지할 수 있다(O).
구역 관리 장치 - 정보 제공 장치 [그림 1]의 ㉛	- 상호 인증이 되어야 한다(M). - 전송 메시지의 기밀성, 무결성, 부인방지 기능이 제공되어야 한다(M).

<표 5> 키은닉 보안 요구사항


분류	보안 요구사항
키 노출 방지	- 통신 개체들은 데이터 암호화/복호화 동작을 수행하되, 암호화/복호화 키가 공격자에게 노출되지 않아야 한다.
키 정보 노출 방지	- 드론이 탈취되더라도 암호화/복호화 키와 관련된 어떠한 정보도 노출되지 않아야 한다.

### 3.4 키은닉 보안 요구사항

드론은 비행하는 과정에서 불법 포획될 위험이 있으며, 이러한 경우에 공격자는 충분한 시간과 장비를 가지고 메모리에 저장된 비밀키를 읽는 메모리 공격 또는 전력소모/전자기파를 이용하여 비밀키를

찾아내는 부채널 공격 등을 시도할 수 있다. 이러한 비밀키 노출의 위험을 방어하기 위하여 드론 기반 서비스에서는 키은닉 기법의 활용이 필요하다. 다음 <표 5>는 키은닉 보안 요구사항을 정의하고 있다.

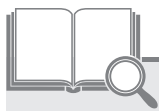
#### 4. 맺음말

드론 기반 서비스의 상용화 모델이나 시기에 대해서는 국내외 전문가들 사이에서도 다양한 의견이 존재한다. 그러나 국내외 선도적 기업과 정부 차원의 준비가 진행되고 있고, 무인감시 서비스와 무인배달 서비스를 중심으로 상용화에 박차를 가하고 있으므로 조만간 드론 기반 서비스가 등장할 가능성이 커지고 있다. 머지않은 미래에 드론 기반 서비스를 상용화하고자 하는 기업·기관에서는 필수적으로 보안 기술을 적용해야 하며, 본 표준에서 정의하는 보안 요구사항을 만족시키는 방향으로 보안 기술 개발을 진행해야 할 것이다. 본 ‘드론 기반 서비스 보안 요구사항’ 표준은 안전하고 표준화된 드론 기반 서비스 제공을 지원하기 때문에 드론 기반 서비스 산업 생태계에서 준용하는 기업·기관의 글로벌 경쟁력 강화에 기여할 수 있을 것으로 기대된다. 

※ 본 연구는 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2016-0-00399, 사물인터넷 디바이스 안전한 키온닉 기술 연구[KeyHAS 프로젝트]).

#### [참고문헌]

- [1] <http://www.futuristspeaker.com/2014/09/192-future-uses-for-flying-drones/>
- [2] <http://www.amazon.com/b?node=8037720011>
- [3] [http://www.dhl.com/en/press/releases/releases\\_2014/group/dhl\\_parcelcopter\\_launches\\_initial\\_operations\\_for\\_research\\_purposes.html](http://www.dhl.com/en/press/releases/releases_2014/group/dhl_parcelcopter_launches_initial_operations_for_research_purposes.html)
- [4] [http://www.molit.go.kr/7works/content/sub\\_0201.jsp](http://www.molit.go.kr/7works/content/sub_0201.jsp)
- [5] TTAK.KO-12.0317, 드론 기반 서비스를 위한 보안 요구사항, TTA 표준, 2016.12.



정보통신 용어 사전

<http://terms.tta.or.kr>

#### ✓ 감정 그림 문자 Emoji

감정을 표현하는 유니코드의 그림 문자 처리 기술.

일본어 ‘그림(絵, 에[え])’과 ‘문자(文字, 모지[もじ])’의 합성어이다. 이모티콘(emoji)은 텍스트(아스키 문자)의 조합으로 감정을 나타내지만, 감정 그림 문자(이모지)는 이미지로 감정을 표현한다. 1999년 일본의 이동통신사 NTT 도코모(NTT DoCoMo)가 이미지로 된 문자인 이모지를 처음 도입하였다. 모바일 운영 체제를 개발하던 구글(Google)과 애플(Apple)의 제안으로 2007년 유니코드 기술 위원회(Unicode Technical Committee)에서 유니코드 이모지 기술 표준이 제정되었다. 이로써 일본뿐만 아니라 전 세계적으로 인기를 얻게 되었다. 광대역 이동통신으로 데이터 전송 속도가 빨라져 애니메이션 형태의 이모지인 스티커(sticker)도 등장하였다.