4.6

The Application of Advanced IoT in Cyberparks

Jamal Raiyn[1(✉)] and Jugoslav Jokovic[2]

[1] Computer Science Department, Al Qasemi Academic College, Baqa Al Gharbiah, Israel
raiyn@qsm.ac.il
[2] Faculty of Electronic Engineering, University of Nis, Nis, Serbia
jugoslav.jokovic@elfak.ni.ac.rs

Abstract. The diffusion of information and communication technologies (ICT) into public spaces is giving birth to a new type of public space: the cyberpark. ICT and the next generation of internet of things (IoT) impact the evolution of modern cities, changing traditional urban planning processes. The IoT with e-economy, e-government, e-medicine, e-learning, and e-society is believed to make a city more efficient and effective. Both IoT and ICT can be used to incentive people to use public open spaces and to spend more time outdoors. In order to attract people, public open spaces have to be attractive, easily accessible and inclusive. IoT can be used to manage the resources in mediated places, including the street traffic in conjunction with events offered in a particular place at a particular time for different user groups. IoT tools are implemented in public spaces to prevent crime and to increase the safety of users. Security services goes from smart cameras that are being installed in many places, to determining users' position and signal tracking with the support of smart mobile phones, GPS/GNSS, QR codes, web services, and Wi-fi. Furthermore, biometric of all types are considered an enhancement of visual surveillance. Biometric are already being used for identification and verification including fingerprint, face iris, speech, eye, and DNA analysis. Various IoT tools are used to design and to create virtual games based on augmented reality for different target such as, human interaction, information collection, and playing in abnormal condition. This chapter addresses IoT tools used in public places to promote their safer use.

Keywords: IoT · Surveillance · Privacy · Information security · Augmented reality

1 Introduction

The diffusion of information and communication technologies (ICT) into public open spaces is giving birth to a new type of public space: the cyberpark. ICT and the internet of things (IoT) have a strong impact on the evolution of modern cities, changing the traditional urban planning processes. The Internet of Things (IoT), also known as the Internet of Objects, refers to the networked interconnection of everyday objects. Today, the Internet of Things has become a leading path to the smart world of ubiquitous

C. Smaniotto Costa et al. (Eds.): CyberParks, LNCS 11380, pp. 308–321, 2019.
https://doi.org/10.1007/978-3-030-13417-4_24

computing and networking. The IoT is believed to make the e-economy, e-government, e-medicine, e-learning, and e-society of a city more efficient and effective. The major goal is to encourage people to better use the outdoor environment in a safe manner. Advanced IoT aims to promote the movement of people from virtual life to real life in society. In other words, information communication technologies and tools aim to free humans from the prison called virtual life and its predominantly sedentary behaviours. IoT can be used to incentivize people to use public open spaces and to spend more time outdoors. However, in order to engage people, public open spaces have to be attractive, easily accessible and inclusive. IoT can be used to manage the street traffic in cities in conjunction with events offered in a particular place at a particular time for different user groups, namely, the elderly, children and young people.

This chapter is focused on the improvement of human safety in cyberparks by introducing an encryption scheme. Encryption, a method that protects the communications protocol from cyber attacker, uses an algorithm and key to transform data at the source safety. In the secret-key encryption, the sender of the message uses an algorithm and a key to encrypt the message, and the receiver of the message uses the same key to decrypt the message. The receiver and the sender of the message must both agree on the key without any third party knowing, a method called key management. In former encryption schemes, the algorithm and the key were transmitted along with the data at the same time; however, such schemes were considered extremely unsecure. In today's encryption schemes, all communications involve public keys. The public keys for the two parties are published, but the private keys are kept secret. To retain and secure privacy, the biometric data in encryption mechanism are included.

2 IoT Technologies

This section introduces the IoT tools that can be used in cyberparks. Various IoT tools are being already used to monitor public spaces (Hachiya and Bandai 2014), with some of them summarised in Fig. 1.

2.1 Smart Video Cameras

Video cameras are being widely used to monitor traffic. Video surveillance systems have also been used in indoor and outdoor environments with the aim of preventing crime (Raiyn 2013). For years video surveillance systems have been used in streets and in public spaces to control, for example, drug-related criminality. Video surveillance is based on features of abnormal behaviour that are represented by energy: the velocity and disorderly features of the moving targets. Energy is a term used to express the relative positions of the moving targets. Current video surveillance systems have many limitations; systems face difficulties in isolating a number of people located at different positions at the same time, and in tracking those people automatically. The number of possibly targeted people is also limited by the extent of user's involvement in manually switching the view from one video camera to another. Furthermore, preserving

personal privacy, the implementation of video surveillance is limited, and the private monitoring of public spaces is restricted. Nonetheless, video surveillance data analysis has proven particularly effective in solving crimes (Raiyn 2015a).

2.2 Mobile Networks

Location based services are offered by various IoT tools (Sekar and Liu 2014). A mobile station is needed to provide users with services related to their location. In some cases, like accidents, a person can call an emergency number but may be not able to give any information about the location of the occurrence. In such cases, the task of the IoT tools is to localize the injured person quickly and accurately (Smit et al. 2012). The user location can be easily determined based on the mobile phone service. In the last decade position determination through wireless network technologies has increased. Mobile and wireless communications systems increasingly offer this service. In a mediated open space (cyberpark), high quality location services can be used to provide more safety and security. A mobile station uses signals, transmitted by antennas to calculate its own position. In other words, the positioning receiver calculates the distance between the mobile station and the base station by signal measurements. Mobile phones mostly use wi-fi networks for internet access, or they use cellular systems to setup audio and video communication (Mok and Retscher 2007).

The cellular concept is a mobile network architecture composed ideally of hexagonal cells. The cells represent geographic areas. Inside the coverage area, the users, called mobile stations (MS) are able to communicate with the network while moving inside the cells. Each cell has a base station (BS), which serves the mobile stations. The coverage zones are however not hexagonal in real radio networks. Interference leads to missed and blocked calls due to errors in digital signalling. Between the transmitter (BS) and the receiver (MS), the channel is modelled by several key parameters. These parameters vary significantly with the environment (urban, rural, mountainous, etc.). The propagation of radio signals on both the uplink and the downlink is affected by the physical channel in several ways. A signal propagating through a wireless channel usually arrives its destination along a number of different paths, referred to as multi-paths. These paths arise from the scattering, reflection, refraction or diffraction of the radiating energy of objects in the environment. The received signal is weaker than the original transmitted signal due to phenomena such as mean propagation loss, slow fading and fast fading. The mean propagation loss comes from square-law spreading, absorption by water and foliage and the effect of ground reflections. Mean propagation loss is range dependent and changes very slowly even for fast mobiles. Slow fading results from a blocking effect by buildings and natural features and is also known as long-term fading, or shadowing. Fast fading results from multi-path scattering in the vicinity of the mobile. It is also known as short-term fading or Rayleigh fading, for reasons explained below. Multipath propagation results in the spreading of the signal in different dimensions (Raiyn 2014).

2.3 Satellite Technologies

There are several self-positioning systems, such as the GPS, GNSS, GLONASS, Galileo (Fernandez-Prades et al. 2011). The global positioning system (GPS) is a worldwide satellite-based radio navigation system (Huang and Pi 2014). It consists of three main segments: a space segment, a control segment and a user segment. There is a basic method for position determination-based cell identification. The cell identification method is based on an approximation of the position of a mobile handset by knowing in which cell the mobile station is located. This method is the basic technique; however, the accuracy of the method is rather low. Satellite navigation system such as the GPS and GNSS are tools well suited for collecting localization data such as a vehicle's speed and the direction of motion at regular time intervals. Satellite navigation systems have been used to manage real-time road traffic information in order to improve route choice decisions. When satellite navigation system data are unavailable, especially in developing countries, or outdoor, travel speeds can be computed on basis of the cellular network data. The GNSS has been used widely for outdoor services.

2.4 Interactive E-Services and Web Services

A cyberpark includes online services across different fields. Interactive e-services enable data collection and processing. Web based collaboration and mobile device applications actualize a user's location. In addition, some information is used to improve location-based e-services.

Developing web-based applications and services is assumed to make smart cities more efficient for citizens, such as e-services for hospitals, education, banking, events, transportation, tourism, security, to name a few. Similarly, Web services support social interactivity and cyberpark events.

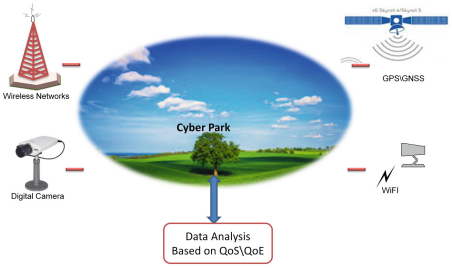

Fig. 1. IoT technologies that can be used in a mediated public space

3 Surveillance in Cyberpark

People tend to use public spaces that are inviting, attractive, accessible, and above all safe. Crime in public places reflects a societal problem. It is a very complex issue with several aspects, and it cannot be solved by urban planning alone. Crimes consist of assaults, and threats and offenses against personal property. Various IoT tools and other

techniques may help to create a safer environment. The use of IoT tools in public place is not new, cameras have been installed in many places around the world. However, their application in public open spaces and other natural settings is more recent, and therefore limited. IoT tools are increasingly being implemented in public spaces with the intention to prevent crime and to increase the safety of outdoor activities. Security services include position determination and signal tracking with the support of smart digital, mobile phones, GPS/GNSS, QR cod, web services, and wi-fi as listed in Table 1.

User location can be determined by these services (Patil et al. 2014). When a user requests information about a place from the location-based server, the server needs to know the location of the user, and a location information is normally requested. Furthermore, biometrics of all types are considered an enhancement of visual surveillance; biometrics are already being used for identification and verification including fingerprint, face iris, speech, eye, and DNA analysis.

Table 1. IoT-based services

IoT	Services\tasks	Feature	Reliability	
			Static	Dynamic
Digital camera	Monitor\surveillance	Image detection	√	
Mobile phone	Information	Signal		√
GPS\GNSS	Positioning, tracking	Altitude, longitude		√
WiFi	Internet connection	IP		√
QR code\web service	Information providing	IP/signal	√	
Interactive digital map	Visitor guide			√
Screen	Media playing		√	
Multimedia place	Calling, music, games		√	

To improve the safety in open spaces, an agent has been introduced (a cyberpark-agent) into the wireless video surveillance system, and a cyberpark agent based, multi-node, collaborative, wireless video monitoring scheme is proposed. The cyberpark agent is designed for target tracking, it can move among network nodes a designated path or on an independently selected path based on network conditions and cumulated information. The target will pass through multiple monitoring regions of nodes. Although aimed at the same target, each device obtains different target moving information, e.g., the target trajectory. Different cyberpark agents created for each target can be used to achieve continuous tracking. While the target switches between different monitoring regions, the cyberpark agent moves between different nodes, records target motion information, and accordingly reaches the goal of multi-node collaborative tracking. Videos, sensors and cellular networks are not sufficient for collecting data because of their limited coverage and expensive costs for installation and maintenance. To overcome the limitations of the tools mentioned above, GNSS can be introduced, as its application to monitor travel time has proven to be accurate. Its data are being used, for example, to monitor indoor areas and traffic congestions. GNSS products provide worldwide and real-time services using precise timing information, and positioning technologies (Bhuvana and Jiang 2014).

3.1 Privacy in IoT Technology

Information about users that is collected and stored should be kept secure. There are various algorithms for protecting information from possible cyber-attacks (Raiyn 2014). In general, cyber-attacks are actions that attempt to bypass the security mechanisms of computer systems. Cyber threats detection has been defined as "the problem of identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are abusing their privileges" (Bhuvana and Jiang 2014). To this definition the identification of attempts to use a computer system without authorization or to abuse existing privileges should be added (Karthikeyan and Indra 2010).

The main scientific challenge is to develop a multi-agent that detects, and tracks suspected cyber attackers (Maskat et al. 2011; Raiyn 2015b). Cyber security should be considered a top priority issue in the digital era since digital technology advancements seem to increase the incidence of criminal and terrorist acts. Moreover, we note that specific communities, like the Israeli society for example, suffers from frequent cyber-attacks. Since the inception of the internet the society and human life have become divided between the real and the virtual worlds. Large number of people spend their lives in the virtual world, many of them have misused internet. Criminal and cyber-attacks are increasing exponentially. To save people's life, we suggest setting ethical rules for the virtual world based on those of the real world. Furthermore, new security measures are required to protect privacy in the virtual world. Cyber-attacks attempt to bypass the security mechanisms of computer systems. According to Jerry Durlak (Smit et al. 2012), privacy is a human value consisting of elements he calls rights: the right to be alone without disturbances, the right to have no public personal identity, the right not to be monitored, the right to control one's personal information including the methods of dissemination of that information.

3.2 Information Security

In general, security can be considered a mean to prevent unauthorized access to information. It includes the integrity, confidentiality, privacy, availability, authentication, and authorisation of information stored and disseminated in servers, including information in files and databases and in transition between servers, and between clients and servers. The security of information can be ensured in a different number of ways. The most common are cryptography for information transmission and authentication. Cryptography, the science of writing and reading coded messages, forms the basis for all secure transmission. This is done through three functions: symmetric and asymmetric encryption, and hash functions.

4 Cyberpark's IoT Design Proposal

A mediated public space (cyberpark) can be designed in line with IoT services and what follows is our proposal to develop a safer open space. The cyberpark users have at hand several IoT tools to determine a user's location, as illustrated in Fig. 2. Users

could also select and reserve social events a priori. The information received from the IoT tools is stored and the data obtained are organized in databases according to the type of IoT tool that is involved, and a cyberpark agent manages the data. Furthermore, to keep user information secure, the cyberpark (CP) agent protects the information from cyber-attacks. To manage the various IoT e-services resources in the cyberpark, a cyberpark agent that considers quality of service (QoS) and quality of experience (QoE) is put in place.

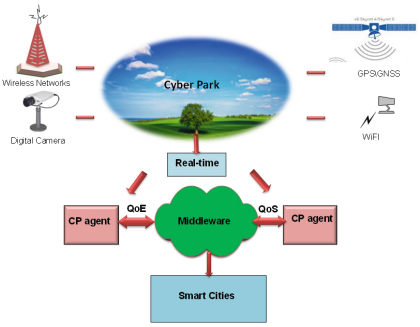

Fig. 2. The proposal for a cyberpark design

4.1 Cyberpark Agent

The cyberpark agent plays an important role in mediated places. It collects information about the activities of the cyberparks, updates the local information constantly, and takes the proper decision in terms of how to perform safely the selected activity. A cyberpark aims to increase the number of the users by applying the cyberpark agent. The cyberpark agent should have autonomy to work, in order to manage negotiation and take decisions (Fig. 3). Figure 2 depicts the decision-making process.

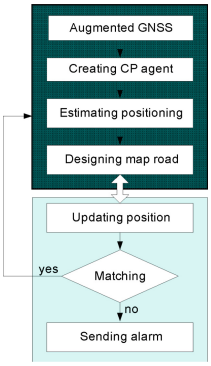

Fig. 3. Cyberpark agent strategy

4.2 Cyberpark Agent Communication

In this phase, the cyberpark agent collects information about the activities by using messaging exchange. The message exchange is secured based on biometric data. After that, the cyberpark agent sends request message to acquire an activity (Fig. 4).

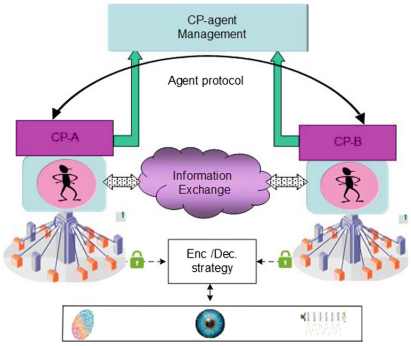

Fig. 4. Communication protocol

4.3 Information Collection

A new user who wishes to make use of cyberpark activities, is requested to register; a cyberpark agent is created to serve the user. According to the received information, a cyberpark agent offers activities suitable for the user's requirements and preferences. Furthermore, the cyberpark agent performs data analysis to improve the services based on quality of experience (Fig. 5).

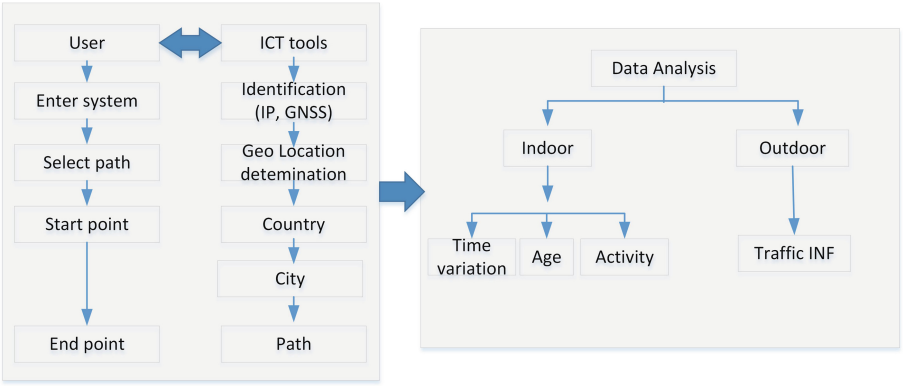

Fig. 5. The pathway of gathering information

5 Cyber Security with GNSS

This section addresses the currently available Global Navigation Satellite System (GNSS). The main task of GNSS is to provide localization and time synchronization services, for this it counts on three basic elements: the set of satellites, ground augmentation systems, and user equipment. Four main satellite technologies have gone live in recent years: Global Positioning System (GPS), GLONASS, Galileo, and BeiDou/Compass (Fernandez-Prades et al. 2011; Mok and Retscher 2007; Quddus et al. 2003). Among these technologies the GPS is the most commonly-used, especially for vehicle navigation and localization (Bernstein and Kornhauser 1996). The GPS data is transmitted via the Coarse/Acquisition (C/A) code, which is the unencrypted navigation data. The encrypted (military) signal is called the Precision-code, also broadcasted by every satellite. It has its own PRN codes, in the order of 1012 bits long. When locked onto the signal, the receiver will get the Y code, which is the encrypted signal with an unspecified W code. Only authorized users can decipher this information. Newly GPS satellites can perform further features.

To get a better estimation of a location, there are several methods of augmenting GNSS data. Three of these methods are: satellite-based augmentation systems (SBASs), assisted-GPS and differential-GPS (Greenfeld 2002). SBASs are commonly used in airplanes, especially for critical issues such as the landing phase. SBASs consist of few satellites and many ground stations, a SBAS covers only a certain GNSS for a specific area. For every GNSS, the accuracy is greatly dependent on and influenced by external factors, as propagation errors and "space weather" conditions (Langley 2000). These factors affect not only to GNSS applications, but all other wireless transmission applications. As the satellites are orbiting earth at a height of approximate 20.000 km, signals can be affected in many ways. According to Langley (2000), 'space weather' is greatly influenced by the sun, and this affects satellite signals too. GNSS requires however exact timing in the order of nanoseconds to determine a position. Furthermore, when the satellite signal reaches earth, it can be reflected on buildings and other objects, causing an increase in travel time. These factors have impact on the measurements. In order to overcome these issues and to increase the estimation of users' position outdoors, we combine augmented GNSS with biometric data, as Fig. 6 illustrates.

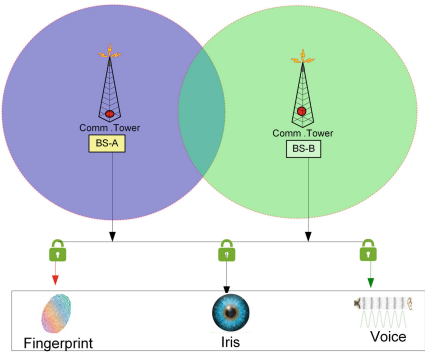

Fig. 6. Biometric data

6 Implementation

IoT tools can be a mean to invite and engage people in public spaces even seven days per week. When using public spaces, people consider the weather conditions and the time available. In this chapter, we introduce an application for interactive digital mapping based on the GNSS. Figure 7 illustrates the management of various resources in this application. Some resources, like e-services, are allocated in public spaces according to the date and time.

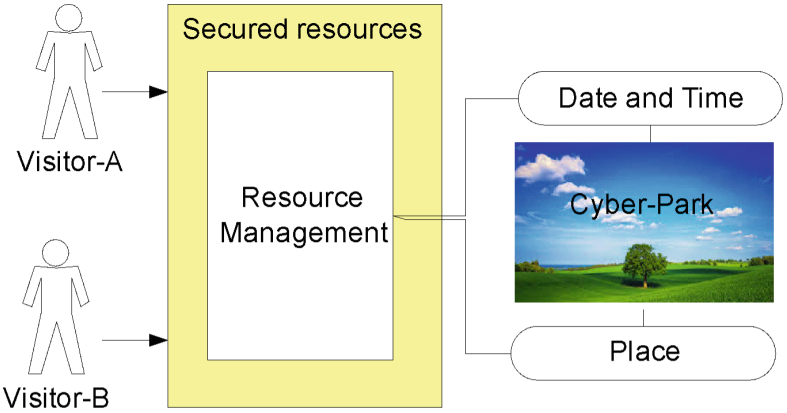

Fig. 7. E-services management

To use IoT tools outdoors, in a cyberpark, the user should log on the system as illustrated in Fig. 8. The system is protected by password authentication, also in data communication, authentication is used to ensure to the digital message recipient the identity of the sender and the integrity of the message. The authentication mechanism is based on cryptography use, either with secret-key or public-key schemes and mostly done via digital signatures based on biometric data, while the message exchange between users is secured with protocol supported with biometrics data, as shown in Fig. 9.

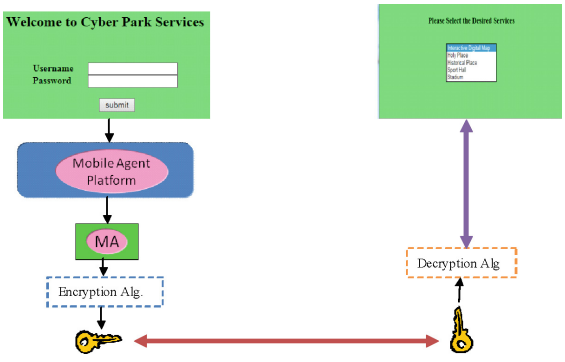

Fig. 8. The secured logon system

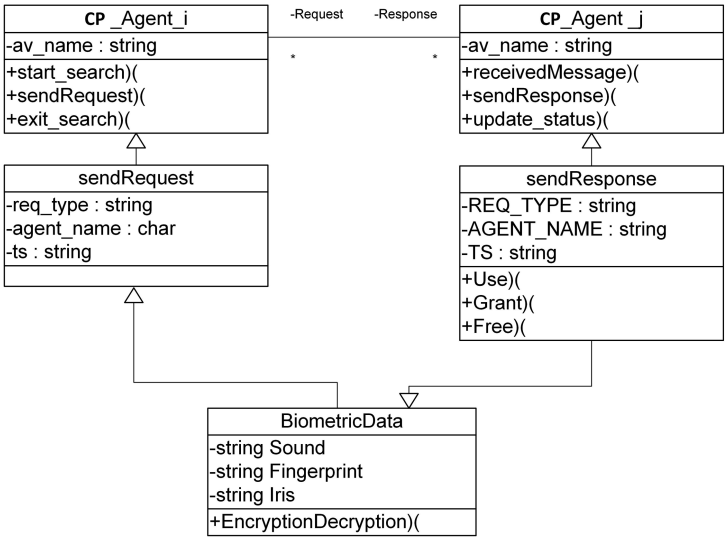

Fig. 9. Secured message exchange

7 Interactive Digital Map

In order to offer an enhanced service for users of a mediated public space, an interactive digital map can be installed as a station, or map can be displayed on a touch screen for people who do not carry mobile devices, or for those who have difficulties in using modern IoT devices. In this station users select a starting point and a destination for the trip and the cyberpark agent calculates the longitude and the altitude of the path as illustrates Table 2. Users have to provide some information in order to use IoT tools. Users start the trip by selecting a path, the system delineates the path, and tracks the users, as shown in Fig. 10. The tracking process can accomplish via various IoT tools. In this application, GNSS has been used to draw the trip path (Fig. 11).

Table 2. Location of nodes

Positioning	Longitude	Latitude	Velocity [km/h]
A	32.875902	35.187868	35.53
B	32.876271	35.191891	45.53
C	32.876866	35.197041	40.37
D	32.874280	35.197020	40.41
E	32.869117	35.200281	31.42
F	32.879540	35.203779	39.00
G	32.869838	35.207169	Final destination

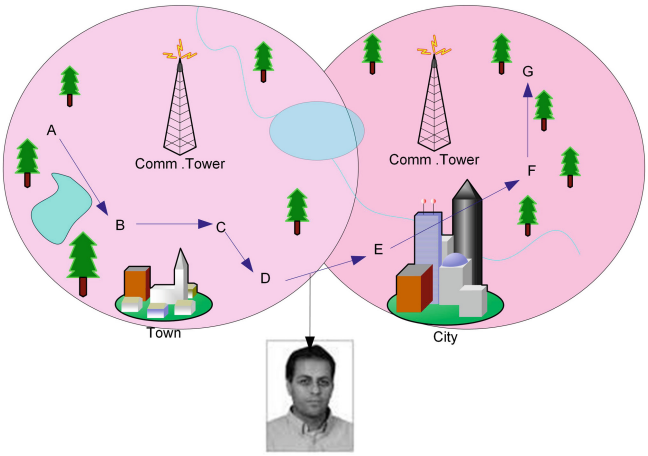

Fig. 10. Position tracking

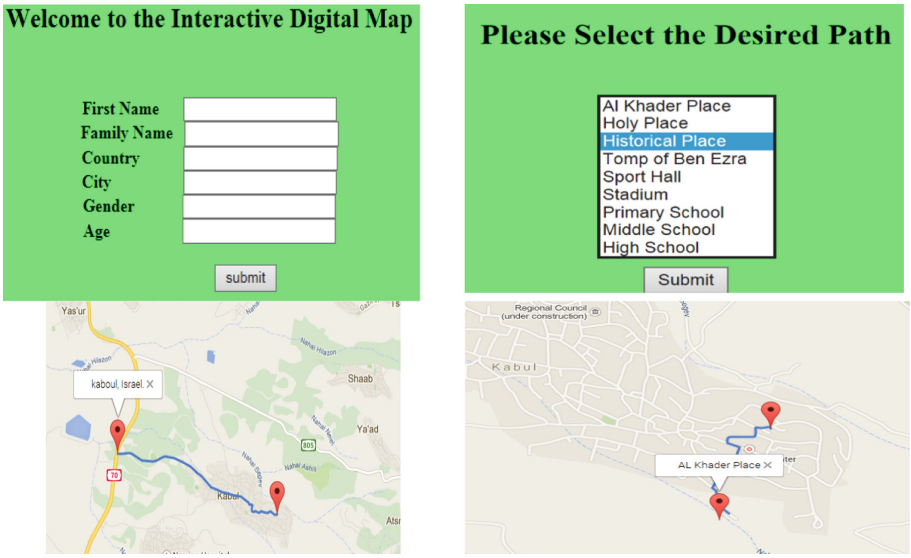

Fig. 11. Interactive digital map showing a fictive trip path

8 Conclusion

In this chapter some significant IoT tools were described and analysed. This analysis contributes to a broader understanding towards our primarily interest: developing a new scheme for securing the privacy of users in a mediated public space. Most cyber-attack detection schemes are fixed on use of authenticity strategies with session key

agreement. However, traditional cyber-attack detection schemes do not satisfy current security requirements; and there are limitations in order to increase the threat defenses. The main limitation of misuse detection-based IDSs is that these schemes can accurately detect only known attack procedures; they are unable to notice unknown or novel attacks. Moreover, predefined attack specifications have to be provided to the IDS to enable misuse detection, which requires human security experts to manually analyse attack's related data and formulate attack specifications. However, attack specifications can be generated automatically by applying various automated techniques. In future work we will consider a novel cyber-attack detection scheme that is based on a cognitive security system. This system should act autonomously, analysing user behaviours, managing vertical handoff to track suspected cyber-attacks, moving over networks, considering anomaly detection, and handling cyber-attacks in real-time.

References

Bernstein, D., Kornhauser, A.: An introduction to map matching for personal navigation assistants. Technical report, New Jersey TIDE Center (1996)

Bhuvana, S., Jiang, B.L.: Location based mobile apps development on Android platform. In: IEEE 9th Conference on Industrial Electronics and Applications (ICIEA), pp. 2148–2153 (2014)

Fernandez-Prades, C., Presti, L., Falletti, E.: Satellite radio localization from GPS to GNSS and beyond: novel technologies and applications for civil mass market. Proc. IEEE **99**(11), 1882–1904 (2011)

Greenfeld, J.S.: Matching GPS observations to locations on a digital map. In: Proceedings of the 81st Annual Meeting of the Transportation Research Board (2002)

Hachiya, T., Bandai, M.: SmartLocService: place identification method using space dependent information for indoor location-based services. In: 28th International Conference on Advanced Information Networking and Applications Workshops, pp. 578–581 (2014)

Huang, P., Pi, Y.: An improved location service scheme in urban environments with the combination of GPS and mobile stations. Wirel. Commun. Mob. Comput. **14**, 1287–1301 (2014)

Karthikeyan, K.R., Indra, A.: Intrusion detection tools and techniques – a survey. Int. J. Comput. Theory Eng. **2**(6), 1793–8201 (2010)

Langley, R.B.: GPS, the Ionosphere, and the Solar Maximum. In: GPS World (2000). http://gauss.gge.unb.ca/gpsworld/gpsworld.july00.pdf (cit. on p. 19)

Maskat, K., Afizi, M., Khairuddin, M.A., Isa, M.R.M.: Mobile agents in intrusion detection system: review and analysis. Mod. Appl. Sci. **6**(5), 218–231 (2011)

Mok, E., Retscher, G.: Location determination using WiFi fingerprinting versus WiFi trilateration. J. Locat. Based Serv. **1**, 145–159 (2007)

Quddus, M.A., Ochieng, W.Y., Zhao, L., Noland, R.B.: A general map matching algorithm for transport telematics applications. GPS Solut. **7**, 157–167 (2003)

Patil, D.S., Gavali, A.B., Gavali, S.B.: Review on indexing methods in location based services. In: IEEE International Advance Computing Conference (IACC), pp. 930–936 (2014)

Raiyn, J.: Detection of objects in motion - a survey of video surveillance. Adv. Internet Things **3**, 73–78 (2013)

Raiyn, J.: A survey of cyber attack detection strategies. Int. J. Secur. Appl. **8**(1), 247–256 (2014). https://doi.org/10.14257/ijsia.2014.8.1.23

Raiyn, J.: Introduction to big data management based on evolution agent in cyberparks. J. Multi. Eng. Sci. Technol. 2(9), pp. 2432–2437 (2015a)
Raiyn, J.: Information security and safety in cyber parks. Global J. Adv. Eng. Technol. Sci. 2(8), pp. 33–38 (2015b)
Sekar, B., Liu, J.B.: Location based mobile apps development on android platform. In: IEEE 9th Conference on Industrial Electronics and Applications (ICIEA), pp. 2148–2153 (2014)
Smit, L., Stander, A., Ophoff, J.: An analysis of base station location accuracy within mobile-cellular networks. Int. J. Cyber Secur. Digit. Forensics (IJCSDF) **1**(4), 272–279 (2012)