Mobile devices as authentic and trustworthy sources in multi-agent systems

M.Sc. Vedran Vyroubal [*] , Ph.D. Adam Stančić[*], Ph.D. Ivan Grgurević[**]

[*] University of Applied Sciences Karlovac / Engineering Dept., Karlovac, Croatia

[**] University of Zagreb / Faculty of Transport and Traffic Sciences, Zagreb, Croatia

vedran.vyroubal@vuka.hr, adam.stancic@vuka.hr, igrgurevic@fpz.hr

Abstract – Current state of the art of mobile devices enables user to collect measured data of various physical phenomena. Such devices can be viewed as participating agents in a multi-agent system (MAS). By utilizing public key infrastructure (PKI) these devices can be promoted to an authentic and trustworthy source of data which can be used for forensic purposes. Broader picture of circumstances of an event of interest can be achieved by concurrently collecting still images or video files, and sensor measurements from multiple users, who's mobile devices participate as agents in a MAS. Participation of a user is voluntary, conditioned on the close proximity of the user to the event of interest ("*geo-fencing*"). The collected data is processed by cryptographic and steganographic methods, for the purpose of guarantee that the collected data if authentic and trustworthy. By digitally signing, the collected data has legal power and can be used for forensic purposes and in legal proceedings.

I. INTRODUCTION

Moore's law and integration of sensors combined with the development of modern mobile platforms, enables the use of a mobile device for collection and transmission of data regarding various physical phenomena [1]. Data networks with high bandwidth and signal coverage provide the necessary infrastructure for collecting data regarding some incident, in both urban and rural areas [2]. Modern mobile devices are capable of capturing still images and videos in high quality. Combined with measurements from device sensors this data can be delivered to a monitoring system. Capabilities of mobile devices and integrated sensors are constantly being upgraded with each new model to arrive on market [3].

This paper shall present a possible procedure for utilizing users mobile device as device for collecting authentic and trustworthy data, such as road and traffic conditions and environment conditions. Specifically the presented case is about an incident in traffic, where participating user captures still images or video and collects sensor data. After the data has been collected it is digitally signed and sent to the monitoring system. User is thus unable to affect and modify the collected data. Access to the collected data is completely in the monitoring system's domain. Digital signature provides integrity and trustworthiness, thereby giving legal power to the collected data. Such data can later be used in forensic analysis and in legal proceedings. By utilizing the multi-agent paradigm, multiple users can concurrently collect data for a given incident, from various vantage points. Data from various vantage points provides a broader picture regarding the incident in question.

II. CURRENT RESEARCH

Utilizing the mobile device sensors for data collection is not a novel research topic. The device manufacturers primarily assert the possibility of utilizing device sensors for monitoring users health [4, 5]. Current research publications on the topic single out subjects regarding criminal forensics [6], monitoring of human psychosomatic activities [7], effect of the environment of human health [8] and subjects regarding security of data and privacy of users [9]. Published papers take into account issues concerning possible ethical and legal questions, which concern the area of privacy issues and civil rights. Possible privacy issues with the proposed system are the fact that the collected data can include information about a user who happened to be in the vicinity. In some case even the user is not aware that his device is collecting data about his location and communications [6, 9]. Issues regarding the privacy concerns are not in the focus of this paper, but the need for analysis and resolving of such concerns shall be stressed through the discussion.

Research regarding utilizing cameras and sensors of mobile devices for data collection purposes, are focused on vehicle tracking, driver behavior monitoring, control of incident situations and for notification of drivers about traffic conditions (example; danger ahead, speed limit, etc.) [10]. There are publications which give drivers instructions on how to use their mobile devices as a medium for data collection, but also the rules and regulations to which user must abide (example; it is not permissible to covertly record incident situations) [11].

Problems regarding providing the authenticity, integrity and trustworthiness of collected data, are rather poorly represented in current research publications. Mentioned problems are the focus of this paper.

This paper shall present a collaboration procedure of multiple users, in process of collecting, transforming and storing collected data, regarding traffic conditions.

III. AIM OF RESEARCH

The aim of the research is the presentation of the feasibility of the system for collection, processing and transmission of data regarding incidents, via mobile devices. By combining data from multiple sources, and users who are participants or witnesses of the situation, it is possible to form a detailed description of the origin, development and epilogue of the observed incident. The authenticity of the collected data will be secured by using public key infrastructure mechanisms and steganographic data integration, with a purpose to ensure the legal grounds and legal power in possible judicial proceedings.

IV. TECHNICAL CHARACTERISTICS OF MOBILE DEVICES

Manufacturers compete for market share with ever more frequent launches of new models of mobile devices, which by every new generation become more computationally powerful and with an increasing number and higher quality of integrated sensors [3], as it is shown in Table 1.

Table 2 shows a comparison of the technical characteristics of mobile devices in 2013 and 2015 based on a review of the technical specifications of major manufacturers [12]. The obvious is the significant increase in processor and memory capacity, image resolution and video format and the presence of fingerprint sensors and atmospheric pressure. It also manifests negative trends: low growth of battery capacity, batteries can no longer be manually replaced, lack of additional memory cards, etc. The use of processors with multiple cores, large screen, large number of sensors and recording in high resolution requires a larger amount of energy that must be provided by the irreplaceable battery.

Table 1: Mobile device features

	CPU	***GPU***	***Memory***	***SD card slot***
2013.	2–4 cores 1,3–1,7 GHz	2-4 cores 1,3–1,7 GHz	16 – 64 GB	Small number of devices
2015.	4–8 cores 1,5–2,0 GHz	Integr. in CPU 192 ALU[1]	16 – 128 GB	Very small number of devices
	Camera resolution	***FPS @ Full HD[2]***	***IP protection***	***Battery capacity***
2013.	4 – 13 MP[3]	24 – 30 FPS[4]	Single manufacturer	1500-2500 mAh
2015.	12 – 21 MP	30 – 60 FPS	Small number of manufacturers	1700-3000 mAh
Integrated sensors				
2013.	accelerometer, gyroscope, proximity detection, magnetometer			
2015.	accelerometer, gyroscope, proximity detection, magnetometer atmospheric pressure			
Access				
WLAN / Bluetooth / GPS / GSM/ HSPA / LTE				

1) ALU: (*Arithmetic/Logic Unit*) – number of arithmetic-logic units
2) Full HD: video resolution @ 1920 x 1080 pixels
3) MP: Million pixels in a still image
4) FPS: Frames Per Second

All this has a direct impact on the use of mobile phone users as a means of data collection during the incident.

The problem may occur during the data collection and recording of image or video if the remaining battery capacity or the free space is insufficient. The above problem can be partially solved by pre-allocation of a certain amount of internal memory (or memory card if present) by the application, and by informing the user about the available battery level. As a measure of saving memory space a reduction of resolution or quality of the video can be used. The minimum resolution of the pictures and quality of the video can define the entity that will receive and analyze the collected data. It should be taken into account the possibility that the user will most likely try to capture a larger number of pictures or videos depicting the incident situation.

The collection and storage of data by the sensor does not require an intervention by the user, as does taking a picture with the camera. The amount of information collected by the integrated sensor can also be significant, and as such can have a direct impact on consumption of memory and battery of mobile devices. Table 2 shows a list of sensors that can be found on the mobile device [3].

From the above mentioned it is clear that mobile devices have powerful hardware capable of collecting and processing large amount of data. Software support has evolved over the years and in today's market there are three mayor mobile platforms: Apple iOS, Google Android and Microsoft Windows Mobile 10 (in previous versions of Windows Phone). Each platform provides development tools and more crucially a market for distributing applications to end-users over the Internet. The largest market share of mobile platform (data for the second quarter of 2015) belongs to Android 82.8%, followed by iOS with 13.9% and Windows Phone with 2.6% of the market [14]. Android devices count over 24 000 different models on the market [3], mainly thanks to openness of the development platform. At this point rest of the mobile platforms are very restrictive and closed. Each of these platforms can be used to develop the suggested data collection system.

Table 2: Mobile device sensors

Sensors present in modern mobile devices		
Accelerometer	Atmospheric pressure	Bluetooth
Camera (CCD[1])	Telecomm. network	Rotation
Orientation	GPS[2]	Gravity
Gyroscope	Air humidity	IR[3]
Brightness	Magnetometer	Microphone
NFC[4]	Step counter	Proximity
Motion	Thermometer	WiFi[5]

1) CCD (*Charge-Coupled Device*)
2) GPS (*Global Positioning System*)
3) IR (*Infra-Red*)
4) NFC (*Near Field Communication*)
5) WiFi (IEEE 802.11 standard)

V. Collecting data on incident

Application of user mobile device collects two kinds of information regarding the incident: analytical sensor readings and a snapshot of the location taken by the mobile phone's camera. The collected data provide further insight into the conditions at the site of an incident, and into the transport environment. The collected data can be subsequently compared with data from other data sources (e.g. roadway control system) as a method of verification.

The collected data can be stored in a structured text file to facilitate export into a database for further analysis and comparison with other relevant data. For simplicity's sake proposed structure and file format for storage is JSON (“*JavaScript Object Notation”*). The advantages of the above mentioned format is that it is independent of programming languages and platforms, and that its simple syntax enables rapid data processing [15]. The file contains data that clearly defines the sources of data, the time of collection, location and value of the sensor readings. Before sending the collected data to the control center, a process of digital signing of files is performed by leveraging public key infrastructure.

The collected videos or photos of an incident are stored on the mobile device in a pre-defined directory. Also data regarding location, time of the recording and on the parameters of the camera, is automatically stored in the structure of the picture file itself (EXIF, *Exchangeable Image File Format*). The application performs the digital signing of the records (images or videos). Even though the sensor data and image recordings are temporally correlated a steganographic mechanism can be used to further establish the link between the diverse collected data files. A hash value (SHA-1, or similar) of the JSON file, containing sensor readings, is integrated within each of the images, by use of the steganography mechanisms. For added security, it is possible to password protect the process of steganographic data integration.

In addition to the aforementioned analytical and visual data regarding the incident, it is possible to use additional control data, e.g. adding the identification information of the user, device, sessions and the like, for faster and easier control, search and processing of collected data. The company that manages the roadway can also publicly transmit data on the current state of the roads. Optionally collected data on traffic signs and signals, state of road and environment, visibility, current load and all other relevant traffic data, can further improve the process of analysis of the incident.

Data protection is performed on different levels and in every stage of processing: integration of control data, use of a password on methods of data compression and with steganographic integration of hash value of analytical data, and also by using cryptographic mechanisms and digital signature. The proposed system increases the ability to detect manipulation of the content of files in order to provide a basic condition for successful analysis of an incident situation - authentic and trustworthy collected data.

VI. Proposed system for data collection on incident

Concerning the heterogeneity of mobile devices with regard to their abilities and available mobile platforms, it presents a challenge to consider using such devices in a distributed data submission system. Even if we limit ourselves on only one mobile platform, the problem persist because of different capabilities of different models of mobile devices, especially if the devices are of different generation. The problem is particularly clear on the Android platform while slightly less on iOS platform, due to smaller number of device models available on the market. This research was limited on Android platform, due to its market share and platform openness.

System for submission of collected incident data, which we propose here, is both distributed and asynchronous. The system consists of a central node for the receiving data collected by the user and of a variable number of users mobile devices, that are logged into the system. Due to the nature of distributed systems, parameters that must be taken into account are delay, throughput and robustness of the data network.

The submission system presumes that the user must voluntarily install the appropriate software on their own mobile device, thereby confirming their intention to participate in such a system.

While considering what parameters must be taken into account for the submission system, in addition to the parameters stemming from the characteristics of the data network, it is also necessary to take into account inherent limitations of mobile devices. Also additional parameters can be custom data submission rules that may be prescribed by the central data receiving node. The rules can define what should be the quality of still images or video files, what sensors should be read and with what frequency or, for example, whether the users data is relevant to situation at hand. Factors that primarily influence the relevance of the collected data are physical proximity of the user to the incident (“*geo-fencing*”) and a time-stamp. These rules can be dynamic in their nature and can be subject to change within a relatively short time intervals.

Because of all the aforementioned limitations and design parameters a suggested model for the submission system is based on multi-agent paradigm. Multi-agent systems (MAS) have in practice proved themselves to be a good paradigm for the development of complex systems whose components require a high degree of autonomy and flexibility [16]. One of the most important areas of application of multi-agent systems is in data management [17, 18].

VII. System architecture

The proposed system is based on JADE-LEAP agent platform, which is developed in Java, primarily due to the fact that a version for the Android operating system is available. JADE-LEAP platform allows creation of any number of agent containers within which agents are executed. Architecture of JADE-LEAP platform is implemented in accordance with *FIPA Abstract Architecture standard* [19]. Running agents communicate

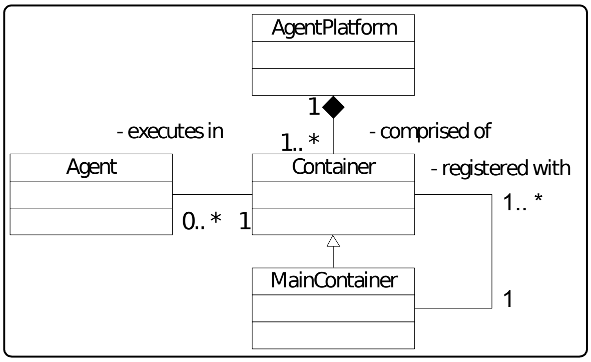

Figure 1: JADE-LEAP UML class diagram

with the other agents, within the same or different containers, by exchanging FIPA ACL messages [20]. Key components of the agent platform are messaging system (*Agent Communication Channel*, ACC), directory service (*Directory facilitator*, DF), and system management agents (*Agent Management System*, AMS). AMS and DF are also agents that run on agent platform and communicate with other agents by exchange FIPA ACL messages.

Each instance of the agent platform consists of at least one container, which is also called the "*main container*", whose main tasks are execution of AMS and DF agents, maintaining a list of other possible containers which are components of a single instance of an agent platform and maintaining a global list of agents that are executed within the current running instance the agent platform (Figure 1).

All containers of an agent platform can be run on the same physical computer or can be distributed across multiple nodes in the network, which by definition makes the agent platform a distributed system. JADE-LEAP provides two modes of operation for the container: a "*stand-alone container"* and "*split container"*. In first mode the container is running on the same physical device that is running JADE-LEAP execution environment. In a second mode an agent container is divided into a "*front*" and "*rear*" part. "*Rear*" part of the container can be executed on another device in the network.

Split mode containers are recommended for use on devices with very limited resources and volatile network connectivity. Split container requires substantially less memory than the full container, and therefore runs faster. Also significant feature is the fact that the communication between the front and rear parts of the container is optimized, which results in lower bandwidth requirements. The rear of the container takes care of communication with the rest of the agent platform. In a case of interruption in network link between the front and back part of the container, the back part of the container receives messages intended for the agent that runs in the front part of the container and stores them in a message queue for the respective agent. After the re-establishment of the link between the front and rear parts of the container all messages are forwarded to the agent. These features of the JADE-LEAP platform allows for the robustness of the proposed solution.

The proposed solution consists of one instance of the agent platform, and a single agent container for each physical user of the submission system (Figure 2). Within each of the users containers one agent is created and started. This agent represents a physical person. Inside the main container one or more *Inbox* agents is created and started, whose primary task is to store received collected data in the database. The proposed system

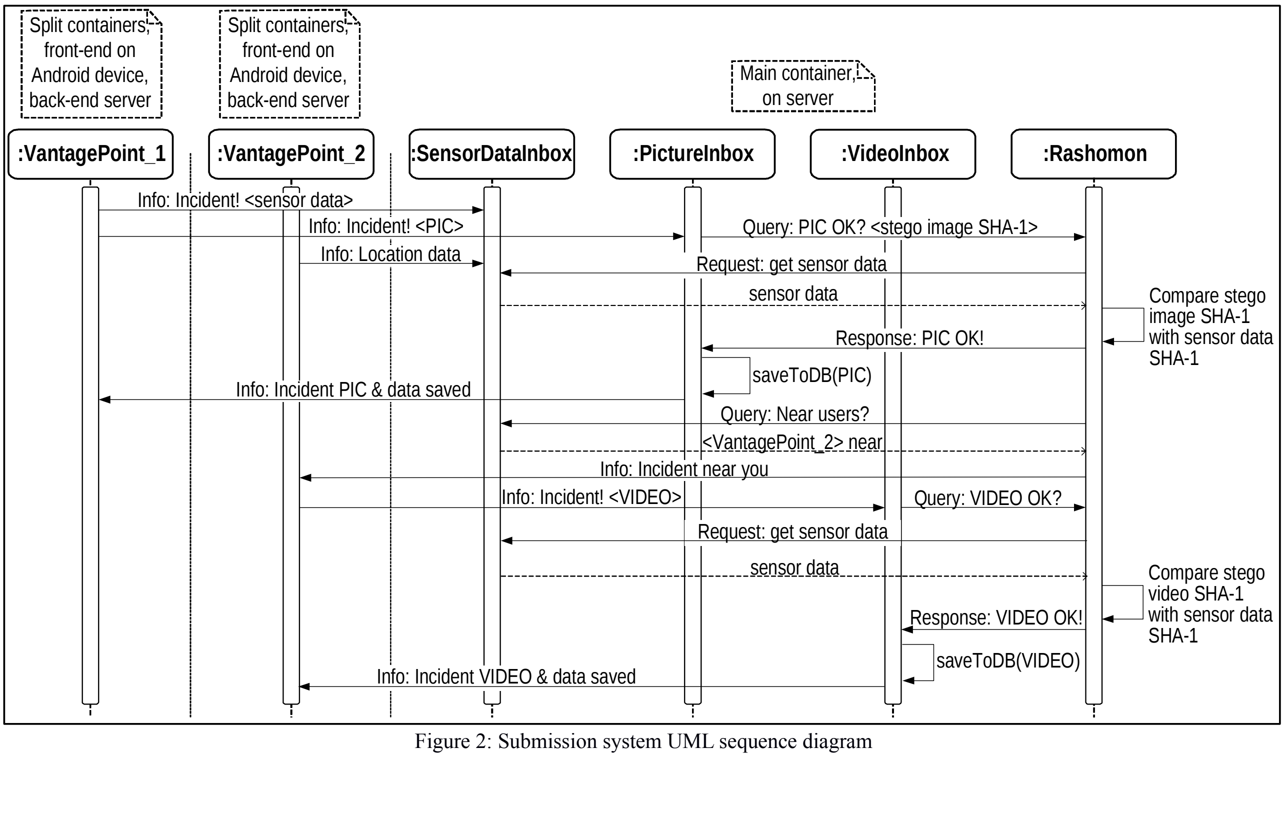
Split containers, front-end on Android device, back-end server
Split containers, front-end on Android device, back-end server
Main container, on server
:VantagePoint_1
:VantagePoint_2
:SensorDataInbox
:PictureInbox
:VideoInbox
:Rashomon
Info: Incident! <sensor data>
Info: Incident! <PIC>
Query: PIC OK? <stego image SHA-1>
Info: Location data
Request: get sensor data
sensor data
Compare stego image SHA-1 with sensor data SHA-1
Response: PIC OK!
saveToDB(PIC)
Info: Incident PIC & data saved
Query: Near users?
<VantagePoint_2> near
Info: Incident near you
Info: Incident! <VIDEO>
Query: VIDEO OK?
Request: get sensor data
sensor data
Compare stego video SHA-1 with sensor data SHA-1
Response: VIDEO OK!
saveToDB(VIDEO)
Info: Incident VIDEO & data saved

Figure 2: Submission system UML sequence diagram

consists of *PictureInbox*, *VideoInbox*, *SensorDataInbox* and *Rashomon* agents, and for each physical user one *VantagePoint* agent. All agents publish their capabilities to DF agent. The system can be expanded with additional functionalities by adding agents who specialize in a particular purpose. *VantagePoint* agent is executed within split container of any physical user. Its task is to collect data from mobile device sensors and camera and depending on the data context, send the data encapsulated in a FIPA ACL message to one of the above mentioned *PictureInbox*, *VideoInbox* or *SensorDataInbox* agents. These agents then query the *Rashmon* agent about relevance of the received data to the current incident. The decision whether the received data is relevant is based on several parameters; validity of digital signature, geo-location of the user, or if hash value of received sensor data matches the hash value steganographically embedded in the received image or video file.

If the received collected data is deemed relevant and trustworthy it is stored into the database by the *Rashomon* agent, for the purpose of forensic analysis later.

A typical scenario for an incident situation is a traffic accident. In such case external forces are acting on a user and his mobile device. *VantagePoint* agent polls the accelerometer of the mobile device. In accordance with pre-defined rules, the agent then concludes that it is necessary to initiate the process of data collection. After the corresponding *Inbox* agents receive sensor data, images and video via FIPA ACL messages, the *Rashomon* agent may deduce that other users are in the proximity of the incident. It is then possible to send a FIPA ACL message to agent running on those users mobile device, with a request for participation in data collection.

VIII. Privacy protection

The presented work is primarily focused on the process of collecting, processing and transfer of data collected on the incident to the submission system. Since the present method of data collection can involve other users, it is necessary to give an overview on the subject of privacy. According to the provisions of the Croatian Criminal Code in part which refers to criminal offenses against privacy, presented is an Article 144 which deals with procedures of unauthorized image recording [21]. The text explicitly states that the image recording in an apartment or in an enclosed space protected from view is criminal, while image recording in public areas is not mentioned explicitly or implicitly. It is inevitable that the user of the submission system, as well as potential participants in an incident shall have to provide certain personal information to the competent authorities. The question is whether the privacy of all participants and witnesses of an accident is violated, especially in the case of recorded image or video.

An image of the vehicle, or a person, who accidentally passed by the incident may compromise person's safety or be a cause of inconvenience in the area of private and professional life. It should be noted that the video surveillance systems are an integral part of modern transport infrastructure and that each user and vehicle on the road can be monitored and under surveillance in accordance with the purpose of such system, which further diminishes privacy rights.

IX. Conclusion

The proposed method is to be regarded as an aid in the process of analyzing the traffic incidents and road conditions. The degree of technological development does not prevent the implementation of the described solution in any way. Proposed system has various methods of confirming that the collected data is both authentic and trustworthy. If the data is manipulated in any way it can be detected. Utilizing the public key infrastructure the submission system becomes a reliable source of legally verifiable information with legal power. The larger amount of collected data relevant to the incident can aid forensic examinations and analysis, which in turn can be faster, more detailed and precise. It should be emphasized that is necessary to ensure privacy of all participants in the incident, during the collection, processing, analysis and especially in the presentation phase of the data collection process. In the development of the submission system a multi-agent paradigm was used.

The advantages of the presented system are ease of use, portability, scalability, utilization of the existing infrastructure for data transmission and the minimal additional investment in development and user training. Disadvantages are the heterogeneity of the system in terms of technical characteristics of equipment, varying number of samples collected and their quality.

Limitations of mobile devices and the ability of devices and users to react and trigger the process of data collection can represent a problem. In the event of an incident with potential damage to mobile device, presented data collection method's usefulness can be limited.

Future research should focus its attention on privacy issues of all participants in the incident. It should also be useful to consider the possibility of integration of existing sensors in the vehicles into the data collection system.

References

[1] C. Bonnington, In Less Than Two Years, a Smartphone Could Be Your Only Computer, URL: http://www.wired.com/2015/02/smartphone-only-computer/ (22.01.2016.)

[2] Hrvatski Telekom, 4G najbrži mobilni Internet, URL: https://www.hrvatskitelekom.hr/4g (22.01.2016.)

[3] Mobile Sensors Database, URL: https://opensignal.com/sensors/library (22.01.2016.)

[4] Apple Inc., An innovative new way to use your health and fitness information, URL: http://www.apple.com/ios/health/ (22.01.2016.)

[5] E.J. Topol, The Future of Medicine Is in Your Smartphone, URL: http://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632 (22.01.2016.)

[6] A. Mylonas, V. Meletiadis, L. Mitrou and D. Gritzalis, „Smartphone Sensor Data as Digital Evidence“, Computers & Security, Cybercrime in the Digital Economy, Volume 38, pp. 51–75, October 2013

[7] G. Chettya, M. White and F. Akthera, „Smart Phone Based Data Mining for Human Activity Recognition“, Procedia Computer Science, Proceedings of the International Conference on

Information and Communication Technologies, Volume 46, 2015, pp. 1181–1187, December 2014

[8] V. Patel, M. Nowostawski, G. Thomson, N. Wilson and H. Medlin, „Developing a free open-source smartphone application for studying tobacco use in the field (observing smoking in vehicles)“, Report for the Asthma and Respiratory Foundation of New Zealand, February 2012

[9] T. Jeske, „Floating car data from smartphones: What Google and Waze know about you and how hackers can control traffic“ Proceedings of the BlackHat Europe, March 2013

[10] L. Hannawald, M. Marschner and H. Liers, „The usage of smartphones for recording accidents and incidents from the critical situation up to the post-crash phase“, Verkehrsunfallforschung an der TU Dresden, Paper Number 13-0293, URL: http://www-nrd.nhtsa.dot.gov/pdf/esv/esv23/23ESV-000293.PDF (22.01.2016)

[11] Anderson, Hemmat & McQuinn LLC: How to Use Your Smartphone as Your Singular Tool for On-Scene Information Gathering, URL: http://www.andersonhemmat.com (22.01.2016)

[12] Technical speciation's: All mobile phone brands, URL: http://www.gsmarena.com/makers.php3 (22.01.2016)

[13] IDC Worldwide Smartphone OS Market Share, URL: http://www.idc.com/prodserv/smartphone-os-market-share.jsp (22.01.2016)

[14] Android Fragmentation Visualized (August 2015), URL: https://opensignal.com/reports/2015/08/android-fragmentation/ (22.01.2016)

[15] RFC 7159: The JavaScript Object Notation (JSON) Data Interchange Format, URL: https://tools.ietf.org/html/rfc7159 (22.01.2016)

[16] Nicholas R Jennings. 2000. On agent-based software engineering. Artificial intelligence 117, 2 (2000), pp. 277–296., 2000

[17] K. Decker and K. Sycara, Intelligent Adaptive Information Agents. Journal of Intelligent Information Systems, 9(3): pp. 239–260, 1997.

[18] N. Jennings, and M. Wooldridge, Applications of Intelligent Agents. In Agent Technology: Foundations, Applications, and Markets, pp. 3–28, Secaucus, NJ, Springer-Verlag, Berlin, 1998.

[19] FIPA:Abstract Architecture Specification, doc. SC00001, URL: http://www.fipa.org/specs/fipa00001/index.html (22.01.2016)

[20] FIPA: ACL Message Structure Specification, doc. SC00061, URL: http://www.fipa.org/specs/fipa00061/index.html (22.01.2016)

[21] Kazneni zakon RH: Kaznena djela protiv privatnosti,(NN 125/2011) URL: http://narodne-novine.nn.hr (22.01.2016)