ACTA UNIVERSITATIS AGRICULTURAE ET SILVICULTURAE MENDELIANAE BRUNENSIS

Volume 64 196 Number 5, 2016
http://dx.doi.org/10.11118/actaun201664051785

SYSTEM FOR ANONYMOUS DATA COLLECTION BASED ON GROUP SIGNATURE SCHEME

David Troják[1], Dan Komosný[1]

[1]Department of Telecommunications, Faculty of Electrical Engineering an Communication, Brno University of Technology, Technická 3082/12, 616 00, Brno, Czech Republic

Abstract

TROJÁK DAVID, KOMOSNÝ DAN. 2016. System for Anonymous Data Collection Based on Group Signature Scheme. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis,* 64(5): 1785–1795.

This paper deals with an anonymous data collection in the Internet of Things (IoT). the privacy and anonymity of the data source is important for many IoT applications, such as in agriculture, health, and automotive. the proposed data-collection system provides anonymity for the data sources by applying a cooperation group scheme. the group scheme also provides a low power consumption. the system is built upon the Tor (The Onion Router) anonymous network, which is a part of the Internet darknet. the proposed system was designed for the Android devices on the client side and for Java environment on the server side. We evaluated the anonymous data collection in a real-use scenario that covers selected data acquisition (e.g. signal strength) from smartphones triggered by their geographical location change. the results show that the proposed system provides the sufficient data source anonymity, an effective revocation, a low computational cost and a low overhead.

Keywords: anonymity, data collection, sensors, internet of things, tor, group signature, smartphone.

INTRODUCTION

The current period brings more and more opportunities to us, especially in the field of anonymous data mining. This fact is supported by a huge development of smartphones and also new trend called "The Internet of things". This new field is trying to improve the quality of life. a side effect that significantly enhances the possibilities of using this specific sector is the amount of secondary data which can be obtained for potential usage. This situation is related to a protection of privacy and anonymity of service's users (Cervenka *et al.*, 2014; Mraz *et al.*, 2013).

These days smartphones are equipped with a lot of sensors which provide dynamic data mining of information about their owners, an environment and actually about everything which can be determined, e.g. the quality of surroundings, a traffic, a health condition, a parking availability etc. the sensor, which is able to collect data, can be anything, not only smartphones because of their daily use. For example, the sensor can be used in agriculture by tractor manufacturers to collect anonymous data about usage and fails for a new development, by analytics to detect soil, weather or pesticides to provide new insights and improve decision making process (global population is growing and food production needs to be more effective) etc. (Simek *et al.*, 2012) This comprehensive development is supported by a scientists who create a better platform for development applications and suggest innovative business models based on the incentive mechanism for the capitalization of the scanned data (Moravek *et al.*, 2012).

In recent years, there has been growing interest in privacy and the amount of data which are shared with near surrounding, but also with the broad surrounding. the control of access to information can be divided into two terms:

- the guaranteeing of the required level of information security exchanged between different systems and controlling access to services/ resources,
- the check of the secondary utilize of information.

The contribution of this paper is the proposal of system which is aimed at needs of users in the largest possible degree of privacy while reducing the energy consuming on the user's side. the first prerequisite for high degree of anonymity is a chosen topology which is based on existing topologies, but also

eliminates found security flaws and apply new technologies (Kapadia *et al.*, 2008; De Cristofaro and Soriente, 2013). the biggest disadvantage of existing concepts was evaluated in a large computational complexity. the low power consumption is achieved due to application of group scheme only with simple mathematical operations.

The article consists of a description and an analysis of concepts dealing with the anonymity of personal data. Not only the analysis of concepts is discussed, but also two existing systems for anonymous data collection are analyzed in this article. the new proposal combines advantages of these existing concepts. the section 4 deals with a new topology and description of all elements. the following section focuses on the implementation on Android device and Java server. In conclusion there is a summary of the security audit and time and memory demands of the developed system.

RELATED WORK

In this section, concepts dealing with data anonymity (*K*-anonymity, *L*-diversity, VMDAV and Tor) and current most related anonymous data collecting systems to our proposal (Pepsi and AnonySence) are described.

Truta and Vinay (2006) described concept of *K*-anonymity which creates multiple reports and only one is correct. Collecting application receives the correct report together with additional $k–1$ reports (some attributes must be preserved). the invisibility is achieved by replacing the true values of selected attributes with the general. There is implemented substitution of the sensitive values in Participatory Sensing (PS) applications, particularly in those that deal with location data. Generally, the concept of *K*-anonymity aims to protect users' privacy by using attribute replacement of values that are common to all k records. Even this model adequately protects disclosure of identity (Tang *et al.*, 2006).

Machanavajjhala *et al.* (2007) proposed *L*-diversity. It is another concept designed to enhance users' privacy in an area of multi reports anonymity. the set of reports is a part of this concept if it contains at least l well-represented values for sensitive attributes.

Kapadia *et al.* (2008) proposed tessellation, which is a generalization technique from *K*-anonymity concept. This involves dividing geographic areas into collections of cells and merging neighboring cells into tiles. Users use tiles to conceal their true position. In other words, the tile is taken as the lowest level of recorded position. In real-use implementation, there is the formation of cells that corresponds to locations of Wi-Fi access points.

The Variable size Maximum Distance to Average Vector is the concept of *K*-anonymity by perturbation. There is a microaggregation which means an alternative approach for realizing *K*-anonymity. This operation involves creating a set of equivalent classes which include members sharing common values of sensitive attributes. Typically, universal values are averages of the given attributes. Equivalent classes relate to the grouping records where members of the class are as much similar as possible. User resemblance is often measured as the relative distance between attribute values, such as the Euclidean distance between the coordinates of the position. the perturbation technique hides sensitive data without generalization, however there are changes based on the application of averaging functions. It was suggested by many algorithms for generating the equivalent of classes with an emphasis on maximum of their consensus. the maximum distance of average vector has been evaluated as the most effective algorithm (Domingo-Ferrer and Mateo-Sanz, 2002; Laszlo and Mukherjee, 2005; Solanas and Martinez-Balleste, 2006).

The onion routing (Tor) is a technique from the field of anonymity communication. It uses routing ensuring to hide source IP address and other factors which could identify the source. It is difficult to track in real-time traces of user activity over the Internet site by utilizing this routing. In other words, all traffic is anonymized on network layer. Nowadays, this technology is implemented only on the software level (Pang *et al.*, 2016).

The model of Tor is client-server and all communication between end users take place through specially designed network. It is composed of a group of routers that act as a server part. the main principle lies in repeatedly encrypted messages including destination IP addresses. a message is sent several times through the virtual circuits comprising the successive random Tor nodes. Each node decrypts one layer of encryption, so it only reveals another node which the message should be sent to. Last node decrypts the innermost layer of encryption and sends the data to its original destination without revealing or even knowing the source IP address. the message recipient thinks the last node in the Tor system was the originator of the communication (Zhang *et al.*, 2015).

The Privacy-Enhanced Participatory Sensing Infrastructure (PEPSI) described by De Cristofaro and Soriente (2013) serves to anonymous data collection from mobile phones. There is a lot of possibilities of gathering information, e.g., temperature, traffic, health data, signal strength, air quality and other entities. the measurements are made directly to mobile phone users. the main advantage of this system is the proven safety of users, low computational demands and almost no side roads. PEPSI consists of five entities: mobile devices, registration authority, access point, providing services and end users. the entities communicate to each other and transmit the necessary data.

The PS architecture used by PEPSI is highly dependent on the number of measuring sensors (mobile devices) registered by registration authority. the system ensures the confidentiality of the identity

of both parties (owner of mobile device and end user who requests data). In other words, end user cannot merge measured data and mobile device. the security is also ensured through discontinuities. It means that none of the users is not able to accurately determine the two reports, which are measured on a single device.

The disadvantage of PEPSI is a discontinuity at the level prior to passing the data to service provider. Records about transiting mobile cells must be removed from the reports.

On the other hand, anonymous data collection system called AnonySense is designed with the use of a wide range of sensors (Kapadia *et al.*, 2008). the concept fully respects the privacy of all registered users. It can be used for environmental measuring e.g., an air quality. the sensors can be placed in a car for scanning traffic density or helping to find a free place to parking. To provide anonymity, the group signature and data of all devices are transported via TLS (Transport Layer Security) protocol with mechanism of authentication.

The service is split into receive task and send reports to end users. In term of anonymity this separation ensures greater security. Integrated group signature appears to be the right to hide the identity of the measuring devices. the potential attacker such as a mobile device or end user will be detected due to usage of certificates. All data are encrypted by group signature to avoid dummy data received by reporting service.

The main difference between PEPSI and the AnonySense is in the structure. the AnonySense uses two services for communication with end users and mobile devices. This action which splits a service into reporting and tasking increases anonymity. When the service does all jobs, it will be easier to attack it from third party. the hacker can modify measured data or edit assigned tasks.

On the other hand, PEPSI system processes received tasks from end users by the provider service. On basis of accepted job, it searches data in available reports and sends a response to the end user.

Tasks in the AnonySense are specified by end users and then the task service processes and creates job which is sent to the mobile device. Mobile devices measure only the desired data. the system is not loaded heavily in case only requested data are measured.

The AnonySense system has extra feature called Mix network. This network provides anonymous communication between a mobile device and reporting service. the mix network hides source IP address and other factors for both sides of communication like Tor project. It is difficult to trace the sender of measured data.

The proposed system in this paper (as well as current concepts) builds anonymity particularly on using group scheme. Among the main benefits of the scheme belongs a lack of a bilinear pairing, which is very computationally intensive. the new topology builds on the advantages of the existing solutions.

OVERVIEW OF GROUP SIGNATURE SCHEMES

In this section we discuss and compare the most commonly used signature schemes in data size, mathematics operations and processing terms.

Among general mathematics operations which are used in signing and verifying belong a bilinear pairing (P), an exponential multiplication (E), a multiplication and division (M/D), an addition and subtraction (A/S) and a hash function (H). Some operations are grouped because computing time is equal. Each mathematics operation (group) can be evaluated by time constant. Tab. II shows these constants which were messured on PC configuration with processor Intel(R)Xeon(R) CPU X3440@2.53GHz, 4GB memory and Windows 7 Professional (Malina *et al.*, 2013).

The bilinear pairing can be considered as the most energetically expensive computing operation and have a huge effect to total result which is related to time.

In Tab. III, there are shown signature schemes with an enumeration of their mathematics operations and expected recalculated time values. the signing and verifying entries are important for the proposed system as well as the length of the signature.

The signature column in Tab. IV is the most significant because every report must be linked with the signature. In other words, the length of the report will be increased by the length of the signature. the evaluation of comparison's result is in subsection 5.5 which is devoted to a description of implementation of the group signature scheme.

I: *Comparison of PEPSI and AnonySense*

	PEPSI		**The AnonySense**
+	Group signature	+	Group signature
	No side roads		Division of services
	Lower computational demands		Reports on requests
			The Mix network
–	Simple attack to report manager	–	Computationally demanding – bilinear pairing
	Constantly reports		

II: *Mathematics operations with time constants.*

Operation	P	E	M/D	A/S	H
Time [ms]	40,64	5.37	0.028	0.005	0.016

III: *Comparison of group signature schemes I.*

Scheme	Signing		Verifying	
	Operations	Time [ms]	Operations	Time [ms]
Camenish, Standler [17]	3P + 14E + 10M/D	197.38	4E + 4M/D	21.592
Ateniese, Camenisch, Joye, Tsudik [18]	14E + 11M/D + 8A/S + 1H	75.544	11E + 6M/D + 5A/S + 1H	59.279
Boneh, Boyen, Shacham [19]	3P + 12E + 10M/D + 8A/S + 1H	186.696	5P + 12E + 8M/D + 2A/S + 1H	267.89
Nguyen, Safavi-Naini [20]	3E + 32M/D + 14A/S + 1H	17.092	3P + 2E + 14M/D + 8A/S + 1H	133.108
Hajny, Malina [10]	9E + 14M/D + 4A/S + 1H	48.758	14E + 9M/D	75.432

IV: *Comparison of group signature schemes II.*

Scheme	Signature [b]	Public Group Key [b]	User Group Key
Camenish, Standler [17]	11,200	–	600b modulus + hash
Ateniese, Camenisch, Joye, Tsudik [18]	8,696	8,144	2,960b
Boneh, Boyen, Shacham [19]	1,533	1,026	160b curve G1
Nguyen, Safavi-Naini [20]	4,776	–	160b curve G1
Hajny, Malina [10]	5,383	4,435	562b

PROPOSED SYSTEM FOR ANONYMOUS DATA COLLECTION

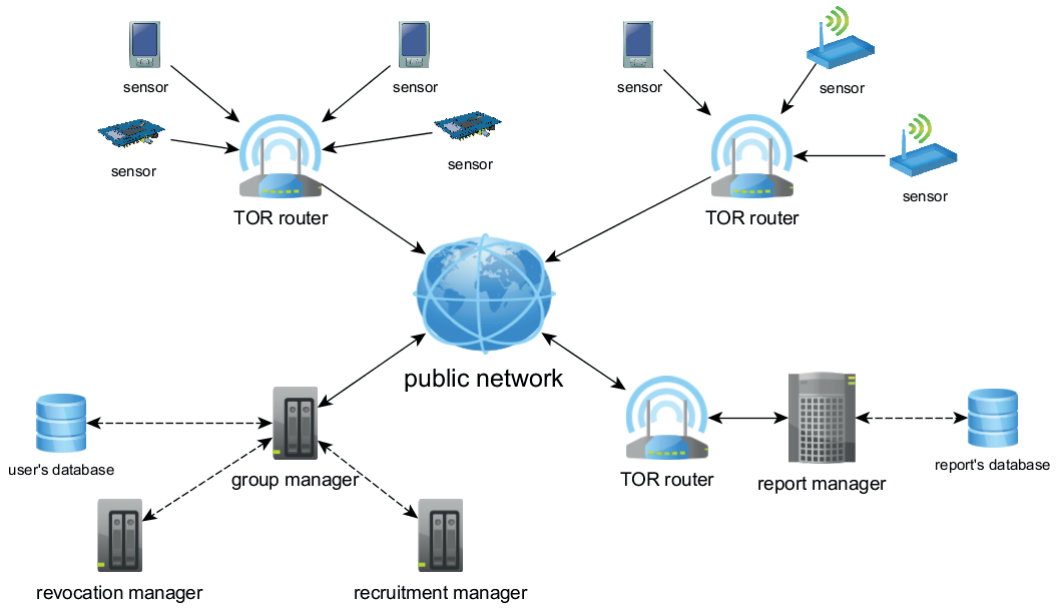
The standard authentication protocol for screening security has to combine the above mentioned principles. It should be simple and expressive enough to contain the following safety requirements:

- **Openness** – policy and privacy practices should be transparent.
- **Individual management** – users should be able to specify who can see what kind of information is displayed and when it is done.
- **Collecting limits** – parts that collect personal data for the purposes of the transaction should not acquire more data than the actual transaction exactly needs.
- **Purpose specification** – those who collect and disseminate personal data have to specify a purpose for which the data is used. It means personal data was collected because of particular purpose and cannot be used in any other cases.
- **Consent** – users should be able to give their explicit and informed consent how their personal data is used.
- **Data quality** – those who collect and disseminate personal data must maintain accurate information. Therefore, users should have access to their personal data and they could change it anytime.
- **Safety** – an adequate security mechanism for data protection is necessity. It depends on the sensitivity of collected personal data.

For the scheme, it is necessary to satisfy certain criteria for the use in the proposed application. Also, it must ensure discontinuity – two signatures cannot have link to each other. It means that no one can see that two reports were created by one member of the group. There is another condition for the scheme – the adding members to a group requires dynamism. the keys are not dependent on the number of users (Bellare *et al.*, 2003).

The scheme with lower computational complexity in signing and verifying was preferred for proper functionality of the application on the mobile device. a smaller size of signature was relevant property, too.

The proposed system implements the group signature to a collection of anonymous data from sensor. a smartphone can be considered a scanning and reporting device. the signal strength of the mobile operator with time and location properties is used like sensitive measured data. the sensor creates a report under predetermined conditions from the measured values. If the connection to the Internet network is available, the device will sign and submit report to server. When the respond from report manager is successful, the report is marked as delivered. the user can see all reports with delivery status in the application. There is a possibility to send manually all undelivered reports. In setting of the sensor, the user can find an option to enable massive sending which will try to deliver all potential reports to the manager when a connectivity is



1: *Architecture of anonymous data collection system*

available. Sent data contain measured values and digital signature.

The system consists of three parts shown in Fig. 1: a group manager, a report manager and already mentioned sensor (the mobile device). Each manager represents a standalone application which runs on different server. the sensor, in contrast, has two applications. the first, which is the output of this work, takes care of measurement required values and creating reports. the second one created from a third party provides an administrative control over the Tor network. the sensor is able to send the expected report with cooperation of both applications.

Group manager

The application which serves as group signature takes care of generation of initialization data. There are parameters group scheme needs to create a group. They are public and reachable for everyone. the manager has to allow modification or reconfiguration of these parameters.

It also ensures the entire agenda with users. the users belonging to the group are able to obtain their private key via a protected channel.

The application representing the group manager includes a recruitment and revocation manager, but the structure inside the application is designed to allow these authorities to simply separate each other to increase security level. the recruitment manager generates and stores the necessary data of group signature including all keys. the revocation manager ensures the disclosure of the identity of the sensor when the received report is evaluated as unsuitable.

Report manager

The report manager receives the data which is verified using by a group public key obtained from the group manager. the connection between the group and report manager must be created via secure channel to prevent security. the public key is distributed through the channel as well as revocation keys. These revocation keys are used for the detection of adverse reports. the application also cares about the overall management of received reports.

Sensor

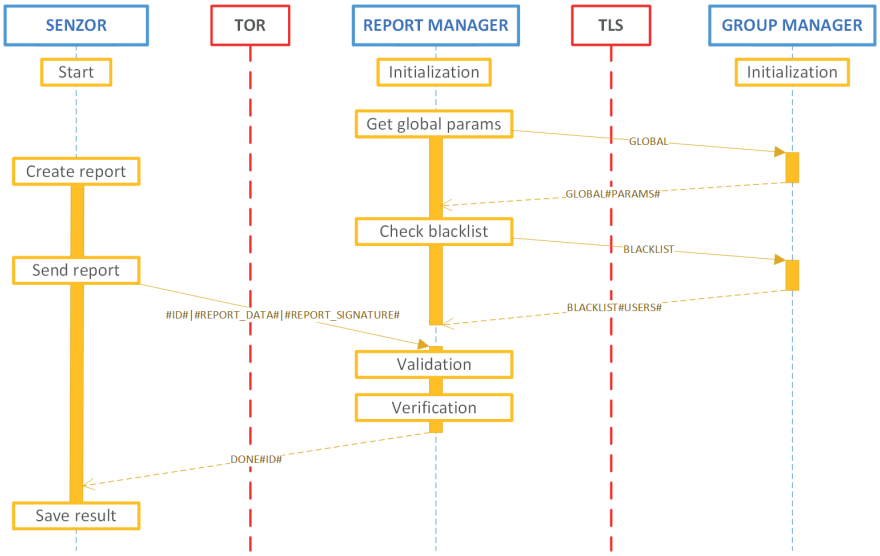
In this case, the sensor is a mobile device that uses the operating system called Android. Two applications are running at the sensor:

- *reporting application*, which processes the data from the sensor and sends them to the appropriate server,
- *communication application*, which uses Tor technology to provide anonymity communication from sensor to server.

The sensor needs the group key and IP address of server to work properly. This key signs the reports which cannot be sent without the digital signature. the connection to the Internet network is not necessary to be available all time. All of the reports are flagged by a delivery property.

The reasons for undelivered report can be:

- **Internet** – when the report was taken the Internet network was unavailable,
- **inaccessibility of server** – finding the server by IP address was unsuccessful or the service was turned off,



2: *Communication between applications*

- **error in data** – violation of the integrity of the data during sending data to the server (the server send to the sensor an error message),
- **blacklist** – the sensor received rejection from the server (user who created report occurs in the list of undesirable).

Communication

All sensors are able to communicate just with the report manager. Fig. 2 shows that both packets (request and response) between the sensor and report manager travel through Tor network. Managers own certificates which are used to transfer the data with TLS protocol. Necessary parameters need to be distributed by another communication channel for sensor to participate in group. the initialization process takes place at both managers. the group manager either reloads or generates parameters for group and opens a socket to listening for incoming connections. the report manager creates request to the group manager to get global parameters and blacklist in the initialization phase. the manager is ready and opens a socket for incoming reports after that process.

The sensor which is running as a background application periodically requests system to provide new data for report. When the attempt is successful, the report gains a unique identifier (within the device) and the application checks connectivity to Tor network. If it is possible, the sensor sends collected data to the report manager. There are two processes when the report arrives on the server side. the first process is called validation and its task is to control received data. the second process controls a blacklist and the correction of the signature. the final result is sent back to the sensor and the proper report is saved on the server.

IMPLEMENTATION OF PROPOSED SYSTEM

In this section, we discussed the implementation of individual blocks of the proposed system in detail. the language applied in programming is Java. the applications designed for the sensor are written for devices with the operating system Android.

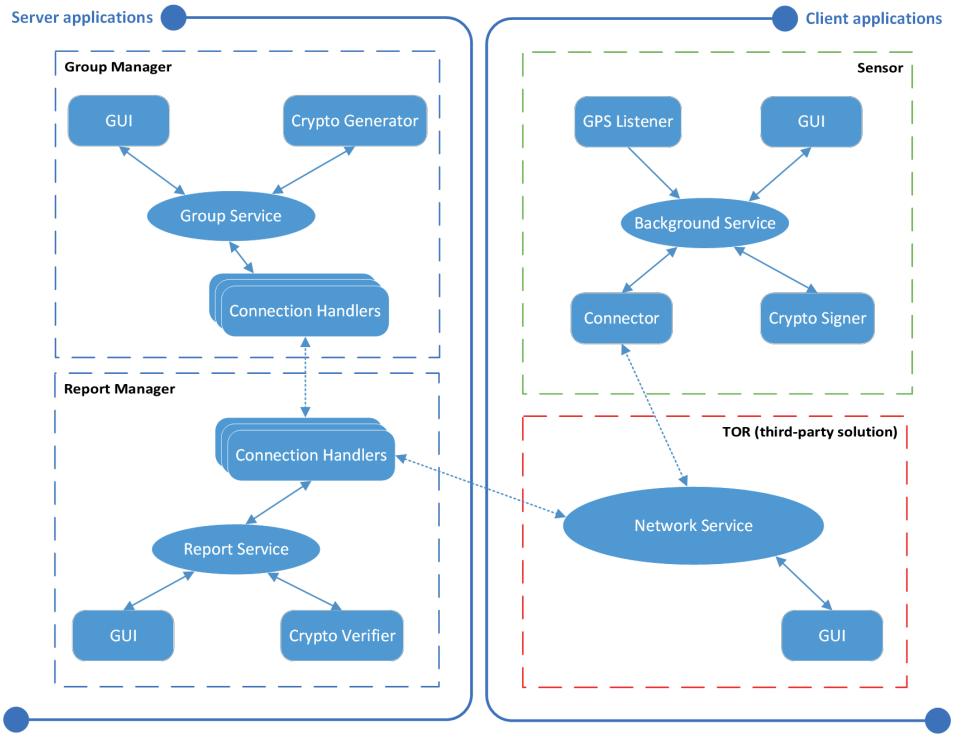
Fig. 3 illustrates classes of proposed applications and links between them and third-party application. Each application has private setting which is modifiable through Graphical User Interface (GUI). Detailed descriptions of each block are depicted in subsections below.

Implementation of group manager

The group manager encompasses all classes for managing the group signature, for communication with the report manager and for GUI. the kernel of the application is service called Group Service which runs when the application starts. the main tasks are controlling all traffic and transferring events to individual entities. Communication takes place at three ports. the first port with number 60 000 is used for servicing the requirements of blacklist. the second port 60 006 is able to return the global parameters. the last port has number 60 066 and may be used to revoke a user. On the other hand, there is entity which is linked with communication and which is used to send the blacklist or global parameters to a specified address. Both sides of communication have to own trusted certificate. This fact is declared by use of TLS protocol. the main cryptography entity is Crypto Generator which possesses all necessary information about participants and group parameters.

Implementation of report manager

The second proposed application, which is on the server side, is the report manager. Its main task



3: *Class diagram of applications*

is to receive reports from sensors and subsequently verify it.

The main thread of the application is a service named Report Service. It contains sockets, the blacklist and global parameters for the group. the first socket with port number 50 000 is used for receiving reports and the second one has number 55 000 which is used to communicate with the group manager. For receiving reports from the sensor, there is entity called Report Handler which serves for basic processing of received data and then authenticates report by calling entity Crypto Verifier. Then the algorithm saves the report or discards it. This action is based on the result of the verification. Because data storage is not a subject of this research, the reports are stored only by process of serialization of report's classes. the database solution offers better performance when amount of reports grows.

For cases where the reporting service needs to get the blacklist or global group parameters, there is a class called Connect Thread Pull which sends a request to a specific port and address.

Module sensor implementation

The proposed application includes Background Service and GUI which guides the service. This service periodically records information about a location, time, signal strength and network operator. This record starts a short timer and call to GPS listener for geographic coordinates. There are possibilities to set the timing and accuracy of measurement in the GUI. If generating of report is successful, the application writes a measurement data to memory and checks the availability of the public network. If it is possible, the service attempts to send data to the report manager. the connector class tries to open TCP connection to the server. the structure of a packet is shown in Tab. V. Data consists of blocks which are formed by the variable name and value with delimiter between them, such as Operator-Vodafone CZ. Individual blocks are separated by a special character. the last block represents the real signature that incorporates parameters separate from each other in same way like data. the principle and implementation HM12 signature scheme is discussed below.

Implementation of Tor technology

There are two options for using Tor project: own implementation of library Orchid or freely available application called Orbot. the application provides the same functionality like the aforementioned

V: *Structure of data report.*

Packet											
	Data										
Packet header	ID	Latitude	Lopngtitude	Altitude	Time	FixTime	Speed	Operator	Signal	Accuracy	Sign

VI: *Parameters of group signature scheme HM12.*

parameter	N	R	s	w1	w2	S1	S2	S3Inv	Ks	hash	error
length [b]	1024	350	324	160	80	243	160	80	160	160	80

library but it is separated from the proposed application. Also it can be used by other applications on the mobile device. the most significant advantage of Orbot is ability to provide complete communication through the anonymity network. This type of connection is followed by low delay in every interaction with server. This fact is acceptable because of very small traffic between a client and server.

Implementation of group signature scheme HM12

The designed system implements a group signature scheme based on the HM12 that best meets the requirements imposed (Hajny and Malina, 2013). the scheme, in contrast to other schemes, uses only primitive mathematical operations which leads to lower computing time.

This is illustrated in Tab. III. the overall choice had three important criterions. the first criterion in choosing of best suitable scheme was signing time. There are two fastest schemes: NS04 and HM12 in Tab. III. Second criterion is verifying time which has better result scheme HM12. Last criterion is the length of the signature (in Tab. IV). the smallest signature has BBS04 (failed in time performance) but also NS04 and HM12 schemes have not much bigger signature.

We have to specify the initialization parameters before using the scheme. Tab. VI shows the individual parameters of the scheme and its values (length). Higher security can be achieved by increasing these values. However, this process is not linear.

RESULTS

This section deals with the control of the security features of the proposed system and results achieved in time and data demands.

Privacy analysis

The effort of this analysis is to achieve maximum appreciation of security from different perspectives, possibility of attack by a third-party and the evaluation to ensure anonymity sensors.

Get information for creating signatures

In production the system should have a web service which will provide GUI to register sensors. the user fills in his personal data which will be sent to the group manager. Then the manager based on received data generates the necessary data that the user downloads via web services. After successful registration, users have the option to download the application, which contains necessary data of the group for a given sensor. the web service is not a part of an independent system and it is used only for data transfer.

Ensuring anonymity

Revealing the identity of user is allowed only by the group manager upon request from the report manager. a link between the report and identity of the sensor can be detected only by the report manager. No other entity is able to connect the sensor to the received report.

Ensuring discontinuities

The report manager is not able to detect two reports coming from one sensor. This fact is declared by the group signature scheme.

Proving signature

The signed report is associated with the sensor. This fact is declared by a hash chain which arises during signing process consisting of data and calculated value of the signature. This hash is used to create the signature parameter e. the sensor cannot deny that the report had not signed its private key.

Control of sending the report from the sensor

The report manager sends back an acknowledgment that received the report. There is no possibility to receive the duplicate report in case of sending reports manually.

Secure communication between managers

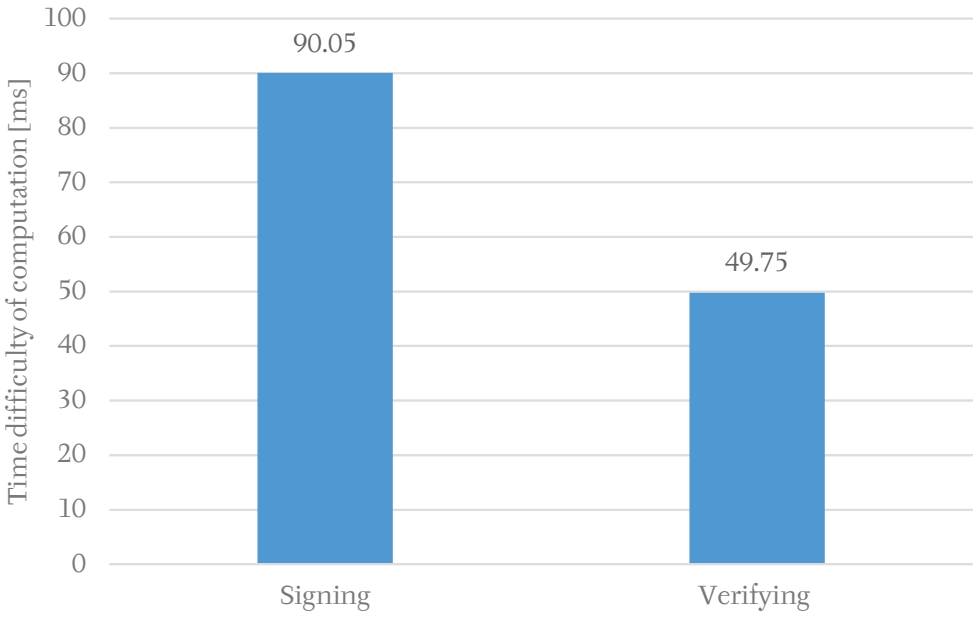
The channel is encrypted using TLS to ensure higher security of communication between managers. Everyone has to provide certificate to authentication before starting communication.

Communication through Tor

Procuring greater anonymity of the sensor can be achieved by using Tor network. the data from the sensor traveling over the network have hidden source IP address. No one is able to track back source of data.

Performance evaluation

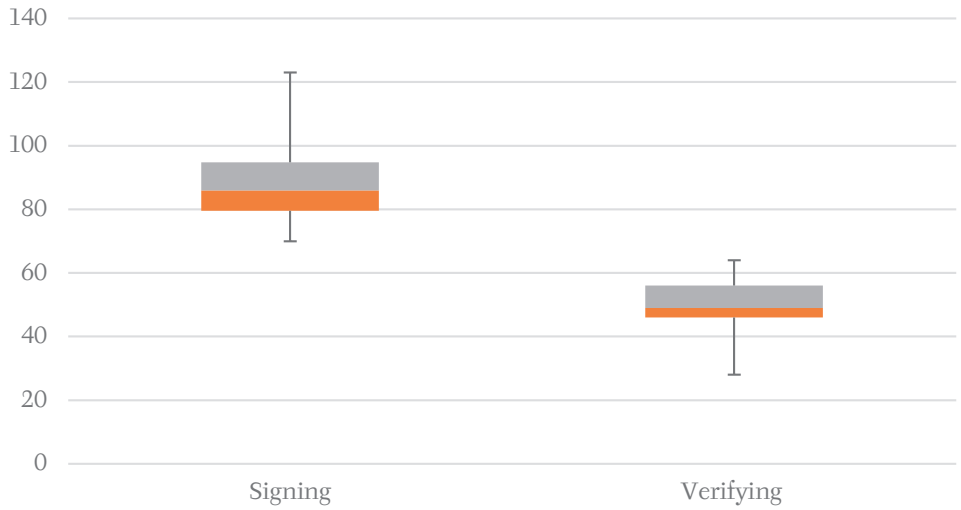
Time difficulty of computation of the group signature HM12 was monitored on both sides (the verification operation on the server and the signing operation on the sensor). For the evaluation of the results the measurement was carried out only on the mobile device, LG Optimus 2X with processor Nvidia Tegra2 250, RAM 512 MB and running on CyanogenMod 10 (Android 4.1.2). the average values of 100 measurements are plotted in Fig. 4. the operation of verification had a time around 50 ms and was the fastest but more important is the signing operation as it is performed on a mobile



4: *The computational demands of operations with HM12 on the tested device I.*

device in the real system. the signed message with size approx 163 bytes busies a processor of the selected device about 90 ms. the size of real signature of message is about 1637 bytes and size of total message transmitted through the network to the report manager is about 1799 bytes. the byte size of the group signature is dependent on the settings of the group scheme that was described above.

There is a diagram (Fig. 5) where statistical analyses are introduced. the left side of diagram contains data related to signing operation. the second and third quartiles of values range from 79,5 ms to 94,75 ms and whole data set correspond with interval of 70 ms to 123 ms. the median is situated in 86 ms (interface between red and green box). Similarly, the quartiles of verifying start from 46 ms to 56 ms with border in 49 ms. Marginal values of data set are 28 ms and 64 ms.



5: *The computational demands of operations with HM12 on the tested device II.*

CONCLUSION

Based on analysis of related works, we proposed a new anonymous data collection system that uses cryptographic primitives.

The proposed system is built by using the signature scheme HM12 that best fits criteria which were required. the proposal seeks to ensure the highest possible privacy of users. the described system was implemented to verify its functionality. It allows to collect data about the position of sensor (a mobile device) related to a world map and ensures a higher degree of privacy. the privacy is achieved by providing anonymity on the application layer where individual reports are signed by the group signature, and on the network layer where the data is transmitted by the Tor technology. In other words, the anonymity of the user who generated the report is ensured. Because of to the effective revocation, it is possible to immediately remove a user from the group.

The whole system consists of four applications. They can be divided into two groups. the first group is designed to run on the server side and the other one on sensor side. Two applications run on the server which are represented by the group manager and report manager. the group manager adds users and serves blacklist above all. the report manager performs the overhead of all reports. the users' applications are running on Android consists of a third-party application realizing the connection through Tor network and own application generating reports and signing it on behalf of the group.

Deployment of the proposed system into real-use scenario produced results in field of time and data demands. the signing operation on testing device took approximately 90 ms in average and the median of measurement was 86 ms. Evaluated values have insignificant difference which refers to computing stability of operation. the size of the signature message had about 1637 bytes. the security audit mentioned above highlights the advantages obtained by the application of anonymous methods and technology.

There are several possibilities of the use of the proposed system, since the development of IoT has a huge expansion. Small sensors are connected to the Internet network and send the measured data. There is a big demand for systems that can efficiently collect measured data and keep the privacy, e.g., in agriculture: manufacturers need to collect data about usage and fail to improve weak parts of their machines; climatologists or analytics need data about forecasts or pesticides for more efficient decision in selection of crops or seeds.

REFERENCES

CERVENKA, V., MRAZ, L. and KOMOSNY, D. 2014. Comprehensive Performance Analysis of Lightweight Mesh and Its Comparison with ZigBee Pro Technology. *Wireless Personal Communications*, 78(2): 1527–1538.

MRAZ, L., CERVENKA, V., KOMOSNY, D. et al. 2013. Comprehensive Performance Analysis of ZigBee Technology Based on Real Measurements. *Wireless personal communications*, 71(4): 2783–2803.

DE CRISTOFARO, E. and SORIENTE, C. 2013. Extended capabilities for a privacy-enhanced participatory sensing infrastructure (PEPSI). *IEEE Transactions on Information Forensics and Security*, 8(12): 2021–2033.

DOMINGO-FERRER, J. and MATEO-SANZ, J. M. 2002. Practical data-oriented microaggregation for statistical disclosure control. *IEEE Transactions on Knowledge and Data Engineering*, 14(1): 189–201.

LASZLO, M. and MUKHERJEE, S. 2005. Minimum spanning tree partitioning algorithm for microaggregation. *IEEE Transactions on Knowledge and Data Engineering*, 17(7): 902–911.

SOLANAS, A. and MARTÍNEZ-BALLESTÉ, A. 2006. V-MDAV: A Multivariate Microaggregation with Variable Group Size. In: *17th COMPSTAT Symposium of the IASC*.

TRUTA, T. M. and VINAY, B. 2006. Privacy protection: P-sensitive k-anonymity property. In: *22nd International Conference on Data Engineering Workshops (ICDEW'06), 94*.

MACHANAVAJJHALA, A., KIFER, D., GEHRKE, J. et al. 2007. L-diversity. *ACM Transactions on Knowledge Discovery from Data*, 1(1): 3–es.

KAPADIA, A., TRIANDOPOULOS, N., CORNELIUS, C. et al. 2008. AnonySense: Opportunistic and privacy-preserving context collection. In: *Lecture Notes in Computer Science.* Springer Science + Business Media, 280–297.

HAJNY, J. and MALINA, L. 2013. Unlinkable attribute-based credentials with practical revocation on smart-cards. In: *Smart Card Research and Advanced Applications*. Springer Science + Business Media, 62–76.

PANG, S., KOMOSNY, D., ZHU, L., et al. 2016. Malicious Events Grouping via Behavior Based Darknet Traffic Flow Analysis. *Wireless Personal Communications,* in print.

ZHANG, R., ZHU, L., LI, X. et al. 2015. Behavior Based Darknet Traffic Decomposition for Malicious Events Identification. In: *Lecture Notes in Computer Science.* Springer Science + Business Media, 251–260.

SIMEK, M., MORAVEK, P., KOMOSNY, D. et al. 2012. Distributed Recognition of Reference Nodes for Wireless Sensor Network Localization. In: *Radioengineering*, 21(1): 89–98.

MORAVEK, P., KOMOSNY, D. and SIMEK, M. 2012. Multilateration and Flip Ambiguity Mitigation in

Ad-hoc Networks. In: *Przeglad Elektrotechniczny*, 2012(05b): 222–229.

TANG, K.P., KEYANI, P., FOGARTY, J. et al. 2006. Putting people in their place. In: *Proceedings of the SIGCHI conference on Human Factors in computing systems – CHI '06.* 93102.

BELLARE, M., MICCIANCIO, D. and WARINSCHI, B. 2003. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In: *Advances in Cryptology – EUROCRYPT 2003*. Springer Science + Business Media, 614–629.

CHAUM, D. and HEYST, E. V. 1991. Group Signatures. In: *Advances in Cryptology – EUROCRYPT 91. Lecture Notes in Computer Science.* 257–265.

ATENIESE, G., CAMENISCH, J., JOYE, M. et al, G. 2000. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In: *Advances in Cryptology – CRYPTO 00. Lecture Notes in Computer Science.* 255–270.

BONEH, D., BOYEN, X. and SHACHAM, H. 2004. Short Group Signatures. In: *Advances in Cryptology – CRYPTO 04. Lecture Notes in Computer Science.* 41–55.

NGUYEN, L. and SAFAVI-NAINI, R. 2004. Efficient and Provably Secure Trapdoor-Free Group Signature Schemes from Bilinear Pairings. In: *Advances in Cryptology – ASIACRYPT 04. Lecture Notes in Computer Science.* 372–386.

MALINA, L., HAJNY, J. and ZEMAN, V. 2013. Trade-off between signature aggregation and batch verification. In: *Telecommunications and Signal Processing. 36th International Conference on. IEEE.*

Contact information

Ing. David Troják: david.trojak@phd.feec.vutbr.cz
doc. Ing. Dan Komosný Ph.D.: komosny@feec.vutbr.cz