Journal of Theoretical and Applied Information Technology
20th November 2014. Vol. 69 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ALGORITHMS FOR DATA ANALYSIS AND DETECTION OF CHANGES IN THE SECURITY LEVEL OF DATA TRANSMISSION IN WIRELESS NETWORKS

[1]D.M. MIKHAYLOV, [2]A.V. ZUYKOV, [3]M.I. FROIMSON, [4]A.V. STARIKOVSKIY, [5]S.M. KHARKOV

[1] PhD, Engineering Centre of the National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute), Kashirskoye highway 31, 115409, Moscow, Russian Federation

[2,3,4] PhD candidate, Engineering Centre of the National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute), Moscow, Russian Federation

[5] Graduate student, Engineering Centre of the National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute), Moscow, Russian Federation

E-mail: [1]mr.mdmitry@gmail.com , [2]avzuykov@gmail.com , [3]froimsonm@gmail.com , [4]userandrew@gmail.com , [5]strategys@yandex.ru

ABSTRACT

Personal mobile devices with growing functionality have become an integral part of people`s life influencing complexity of modern mobile networks with increasing number of users and base stations. Mobile phones and networks are not sufficiently protected as conventional systems do not provide an effective means for dealing with existing security problems. This paper addresses the issue of data security transmitted in wireless networks. The main attention is paid to detection of un-trusted base station primarily based on accessible software-defined radio modules. Authors provide the description of data analysis system for wireless networks comprising three modules: wireless cellular connections quality and mobile device condition control module; wireless connection authentication and security control module; wireless Wi-Fi connections authentication module, as well as detection algorithm of untrusted base stations. The article also provides the information about the experiments carried out and points out shortcomings of the current version of the proposed algorithms. The testing experiments and further improvements are underway to increase the system quality. It is planned to pay attention to the eavesdropping issue.

Keywords: *Data Security, Data Analysis, Untrusted Base Station Detection, Base Station, Wireless Network.*

1. INTRODUCTION

Modern smartphones and other mobile devices access the Internet and perform a wide range of functions and, therefore, there is a wide range of possible types of attack by malware or other forms of malicious communications that can be launched against a mobile device. [1-5]

For example, short messages can be sent from the victim's phone to paid numbers (i.e., Short Message Service), the victim can be signed up for a paid service by having an SMS sent from his number, the victim's personal data (i.e., contacts, messages, call logs, etc.) can be obtained and given to spammers, the victim's location can be obtained as well. Additionally, photo and video recording can be performed using the victim's phone as well as private phone talks can be wiretapped. [6-9]

Thus, currently personal mobile devices are not sufficiently protected. Moreover, modern mobile networks have become more complex with increasing number of mobile users and base stations. This can cause several undesirable effects, such as:

- changes in communication quality;
- connections to an unauthorized (un-trusted) base station;
- shortened time of a battery operation of a mobile phone;
- establishing un-trusted (unauthorized) connections (for voice and packet data);

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- mobile network errors and failures; and
- wrong data received from a base station.

Conventional systems do not provide an effective means for dealing with the above listed problems. The conventional mobile networks do not collect and analyze operational statistics for controlling the communications security. The network operators can collect some statistics, but there is no system that aggregates comprehensive data from different operators.

Accordingly, there is a need for effective protection of users of smartphones (or other personal mobile devices) against third-party unlawful acts using fake base stations (BS).

Different papers were devoted to the issue of transmitted data protection. For example Lotvonen et al. propose a method for detecting a rogue base station that interprets a received signaling message by searching for an anomaly comparing signaling parameter of the received message and the default one and alerts the user comparison gives an unequal result [10].

Wolman Alastair and colleagues provide a method of detecting rogue devices coupled to a wired network without generating false negative or false positive alerts [11].

Goldfarb in [12] tells about methods and systems for identifying one or more rogue devices within a wireless communication network over a particular geographic location.

In [13] Kulaga and Tikhomirov propose a system and a method for dynamic configuration of the security modules for optimization of execution of security tasks in local network.

In the patents above as well as in our proposed development the methods of un-trusted base stations (UBS) detection are described. However, there is a substantial difference between them. First of all it should be noted that over time new threats, in particular, as described in [12] occur. Cheap ways to intercept traffic like OsmocomBB appear which carry an additional threat with their own specification.

As distinct from analogs during development of algorithms presented in this paper the emphasis was on un-trusted base stations created by hackers. These projects include OpenBTS, SysmoBTS etc. These are base stations implemented in software-defined radio module (SDR) with limited functionality. There are examples of the use of such BS to intercept traffic, IMSI catcher and attacks such as Man-in-the-middle [14]. Such equipment worth about $1,000 and is available to a wide range of people, and openness of the project allows to replicate the existing code. As a consequence, we can assume that the share of "cheap interceptor" in the total number of interceptors will grow, so during the development of the protection system we have focused precisely on un-trusted base stations.

As existing means of fake BS detection are not sufficient and often do not answer the growing threats, this paper deals with the new approaches for data analysis and detection of changes in the security level of data transmission in wireless networks. The main attention is paid to detection of un-trusted base station (virtual cells) primarily based on accessible SDR installed by criminals to perform attacks on mobile devices and data processed and transferred wirelessly.

2. WIRELESS NETWORKS DATA ANALYSIS SYSTEM

Wireless networks data analysis system is designed for any mobile device, equipped with a cellular service module and/or Wi-Fi module, such as mobile phones, tablet computers, notebook computers, devices and modules that make up navigation systems (e.g. , in a car), tracking devices. The system enables to collect and process the data sent/received by such devices, as well as to monitor their condition, such as the battery charge, the power on the communication components, g-meter readings, etc. All this data can be processed and stored in device or transmitted to a remote server.

The collected data provides detailed statistics that can be used later for various studies, e.g., the operator-originated Handover algorithm [15] efficiency study (switching between operator's base station (or base station) without disconnection) or rational battery consumption studies etc. Also it can be used for database and coverage map compilation (e.g., BS and Wi-Fi access points` database with reference to base station or mobile device (MD) location, or mapping signal levels of different operators, or database of network failure causes). The accumulation and processing of such information allows making decisions handling more reliable data for further mobile telecommunications architecture development and planning.

Another aim of the system is real time analysis.

2.1. Real Time Data Analysis

Embedded algorithms on the basis of information

Journal of Theoretical and Applied Information Technology
20th November 2014. Vol. 69 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

on changes of monitored parameters and accumulated data draw conclusions on the possible causes and consequences associated with these changes.

Let's consider examples of such conclusions:

- MD finds in its environment more than one BS with the same identity values. The conclusion in this situation is the fact that one of the base stations is fake, that is, un-trusted BS. An UBS (a virtual base station, for example) can provide a set of services for MD, meaning any device designed to connect to a mobile service provider. Usually, the UBS acts as a base station that does not belong to a trusted mobile service provider (SP). An SP can be a subscriber's home network operator, roaming provider, business intranetwork, or other mobile service provider trusted by the subscriber for use of the network. UBS can act both through direct connection to the MD and without it simply by traffic interception.
- Encryption process between base station and the MD was blocked. Decrease in the level of security of data transfer will be a conclusion in this case; the data transferred can be easily intercepted by a third-party simply by listening to the radio channel.

Further, on the basis of these findings, as well as additional information received from the network preset strategies aimed at reduction of the threat to the MD (MD owner) can be selected. Among such strategies can be notification of the user, prohibition against confidential information transmission, device mode changing. These strategies can be selected by user, or automatically. Here are examples of such strategies:

- MD enters into a zone known not to be covered by mobile provider's services. A possible strategy is to reduce the power / information load supplied to the modem;
- MD connects to an UBS. A possible strategy is to inform the user of the device or the mobile service provider.

Analysis and data structuring of wireless networks allows to track timely changes in the networks within coverage area of which MD is and upon the occurrence of undesirable events to produce notification locally (issue warnings to the user) or remotely (send a notification to the remote server). Undesirable events are understood to be any changes that the MD user or any other user of the system is interested in [16], including, but not limited to the following events:

- degradation of communication quality;
- detecting and / or connection to the UBS;
- encryption algorithms or encryption key length change;
- increase in the rate of battery consumption;
- illegal / unwanted connections making (both voice and packet);
- network errors;
- errors or inconsistencies in the data received from BS.

2.2. Modules of Secured System

Upon detection of any events of interest an algorithm is activated. It can be either preset or dynamically generated in accordance with additional parameters received by the system.

The system protected can be divided into several independent modules:

1. wireless cellular connections quality and MD condition control module;
2. wireless connection authentication and security control module;
3. wireless Wi-Fi connections authentication module.

2.2.1. Quality control module

Quality control module is designed to measure mobile providers' communication quality by monitoring. The module accumulates events that influence communication quality through users' mobile device and special equipment with modems for passive / active connection to the mobile service providers. The data collected includes not only the data received from network, but also MD condition data. These data could then be used, for example, for the following purposes:

- statistic database of BS signal levels creation;
- accurate map of the cellular or Wi-Fi network creation;
- creation of a statistic database of the errors that occur in the network (errors in this case refers to not inappropriate work of the MD with SP network, e.g., failure to finish a call, switch to another base station after finishing a call, failure no switch to a BS with the best signal level, etc);

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- MD performance review and verification of correctness of its algorithms.

2.2.2. Authentication and cellular connection security module

Authentication and cellular connection security module is designed to testing and statistics data accumulation on the facts of the BS substitution and / or data (packet / text / voice) transfer security-related malfunctions. UBS detection is one of the objectives of this module. There are both explicit and implicit indicators to detect an UBS.

Explicit indicators include:

- inconsistency of BS identity information (MCC (Mobile Country Code), MNC (Mobile Network Code), LAC (Local Area Code), CellID);
- existence of more than one base station with the same MCC, MNC, LAC and CellID within MD signal reception range;
- inconsistency of data received from the BS (MCC, MNC, LAC, CellID) and base station and / or MD location.

TC location and its identity information can be detected in several ways:

- by a query to the SP about BS location-based data and subsequent comparison with the current base station or MD location-based data;
- by a query to the BS database about BS location-based data and subsequent comparison with the current base station or MD location-based data;
- by a query to the BS statistic database about BS location-based data and subsequent comparison with the current base station or MD location-based data.

BS databases can be either local or stored in the MD or remote and stored on servers in inter- or intranet networks.

Implicit indicators include:

- lack of encryption between MD and BS;
- lack of response or failure of USSD (Unstructured Supplementary Service Data) query;
- inability to use the SP geo-location services on MD;
- lack of packet connection;
- failure to switch to another BS when location is changed;
- presence of only one base station within MD signal reception range;
- presence of connections between MD and BS hidden for the user;
- lack of ability to connect to a remote server;
- TMSI (Temporary Mobile Subscriber Identity) super long lifetime; etc.

Implicit indicators do not give an absolute proff that the MD is connected to the UBS, but used in combination with each other and further indicators can significantly increase the level of confidence.

Another objective of the module is to determine the level of data transfer security. Despite the fact that this objective involves the problem of determining UBSs, there are several additional features. This module determines the type of established connection, if data is encrypted and, if possible, encryption key length. Data transfer is considered insecure if there is no encryption or encryption is weak.

2.2.3. Wireless Wi-Fi connection authentication module

Wireless Wi-Fi connection authentication module is designed to secure the system (system user) from fake. The basic principle is to monitor Wi-Fi connection parameters with respect to unauthorized / unwanted changes. This monitoring is performed by checking periodically Wi-Fi access points parameters and recording them in a database (DB) for future comparison.

A second, often external, database is used for conducting a "black list" or "list accepted". This database contains a list of wireless access point`s parameters including location and required additional information.

General verification algorithm will be as follows (Fig. 1).

For authentication a table which shows the correspondence between the MAC (Media Access Contro) addresses of access points and SSID (Service Set IDentifier) is filled in. If the MAC address changed without changing the SSID, it means that connection between different devices has occurred.

Journal of Theoretical and Applied Information Technology
20th November 2014. Vol. 69 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 1: Wi-Fi connection verification algorithm.

3. UNTRUSTED BASE STATION DETECTION ALGORITHM

An "Untrusted" means a third-party base station, while a subscriber suggests being connected to the authorized service provider. UBS is aimed at listening to voice calls and text messages, subscriber's disorienting, damaging MD software, getting MD and SIM-card IDs [16], [17]. UBS equipment can be operated in an active, semi-active (semi-passive) and passive modes.

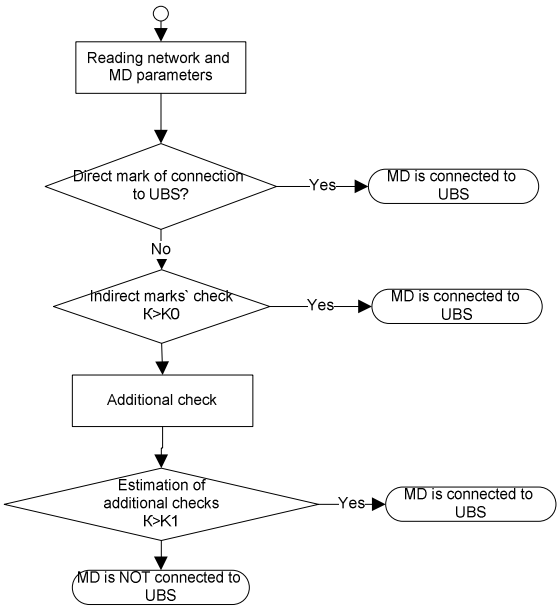

Figure 2: General algorithm for UBS identification.

Untrusted base station detection algorithm consists of several independent conditions of testing, which can be implemented at any MD if there is necessary software.

At the beginning of the algorithm (Fig. 2) network settings are read. The following data is collected:

- MNC (mobile network code combined with MCC is a unique identifier of the mobile service provider);
- MCC (mobile country code combined with MNC is a unique identifier of the mobile service provider);
- CellID (a parameter that is assigned by provider to each base station sector and serves to identify it);
- LAC (local area code, local area is a set of base stations served by a particular base station controller) for the current (the one currently connected to the MD) and surrounding base stations;
- signal level;
- encryption used;
- TMSI data (Temporary MD Identity), etc.

Once some or all data is received, verification for any explicit indicators of connection to a UBS according to the Scheme 1 algorithm starts. If at least one of the explicit indicators is found, it is concluded that there is connection to an UBS, otherwise verification continues.

During the second step search for implicit attributes of connection to UBS begins (Scheme 2). The result of this step is a certain degree of confidence that the current BS is an UBS. If this confidence degree exceeds a certain value K0 – a factor that in a global sense can be changed (for example, set by the user in profile settings) – it is concluded that MD is connected to an UBS. If the factor K (the confidence degree after verification of implicit attributes of connection to an UBS) does not exceed the threshold value K0, algorithm proceeds with verifications.

In general the number of additional verifications can be changeable, which allows to adjust quantity of time and resources spent to perform them. Verification algorithms are outlined in Schemes 3 and 4. According to the results of each verification the value of the confidence degree K is changed. After completing planned verifications value of K reaches the preset threshold value K1 which concludes that the established connection is secure.

Let us examine the algorithms of explicit and implicit indicators detection.

Journal of Theoretical and Applied Information Technology
20th November 2014. Vol. 69 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 Scheme 1. Identification of Explicit Marks of UBS

To run the algorithm (Fig. 3) it is necessary to collect data on the BS to which the MD is currently connected. The next step is to verify the authenticity and validity of the data received. The following characteristics are verified:

- MCC of the current BS compliance with and MD location country code;
- MNC code compliance with the code of SP;
- LAC is unchanged when CellID is unchanged;
- wrong format of a BS identifier;
- BS identifier compliance with the value in the table of correspondences.

Any discrepancy of the characteristics above can be interpreted as a UBS explicit indicator.

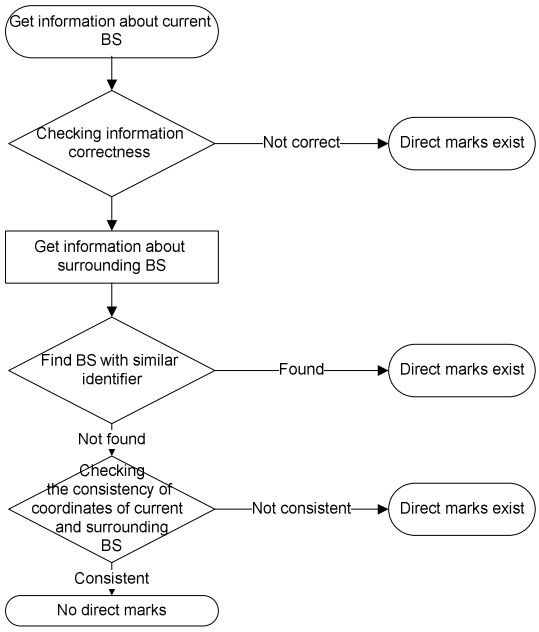

Figure 3: UBS explicit indicators detection.

The next step of the algorithm is to provide the missing information for the subsequent verifications. Once all the necessary information is obtained, the current and nearby BSs' identification data correspondence analysis and search for conflicts of intersection starts. Conflicts of intersection mean that some of the base stations have any impossible intersection of identification numbers (CellID, a variety of LAC or MCC, a complete coincidence of all the parameters, etc.).

If no inconsistencies were found and all the data corresponds, verification of location of the current and surrounding BSs, as well as the location of the MD, takes place. It is a sign of connection to a UBS if any inconsistencies are detected.

3.2 Scheme 2. Identification of Implicit Marks of UBS

Certain values of the parameters considered to detect the implicit indicators of connection to a UBS do not always mean such connection, while such connection does not always cause such displays (Fig. 4).

One of the important parameters of security is proper encryption of the communication channel between the MD and the BS. Encryption is enabled by the command from the BS to the MD, which specifies the encryption algorithm. Encryption can be disabled both by the base station and the MD (for example, if the MD does not support encryption at all). However, as UBS has no information about the secret key stored on the SIM-card it will fail to establish encryption.

Lack of encryption leads to the possibility of passive listening when the third-party interception of the traffic does not manifest itself.

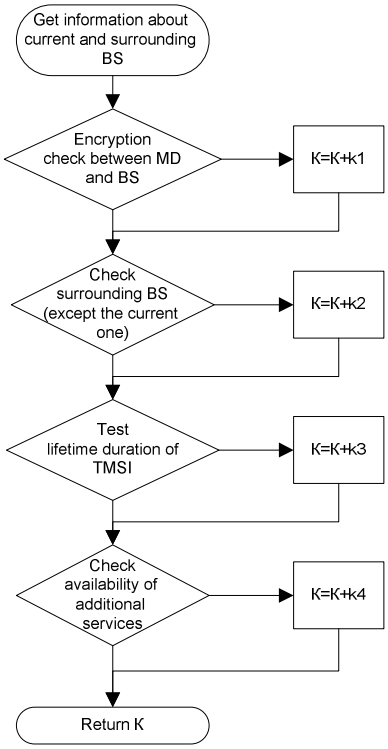

Figure 4: UBS implicit indicators detection.

Another indicator pointing to the fact that MD is connected to an UBS is the absence of any other BSs except for the one connected. This may mean

Journal of Theoretical and Applied Information Technology
20th November 2014. Vol. 69 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

that other base stations are blocked out. To prove this assumption noise pollution level in other channels must be checked. If it exceeds a certain threshold value (mdb), it means that special means of suppressing the signal are used.

Some of the BSs have special standards to regulate the frequency of changing the temporary identifier TMSI, which presumably will not be observed by UBS. It may be an indicator of a UBS if these standards are not met.

Following the assumption that not every UBS is designed using expensive, fully-functional equipment some (or all) of the additional services such as, for example, GPRS, USSD, network service messages, etc. are checked. Test verifies not only availability of the selected services, but also content of the responses. For example, for GPRS an IP inappropriate for this provider, special server wrong answers may be such indicators, for SMS it may be missing or invalid data in delivery reports.

All of the above tests return "0" if the attribute is not revealed and "1" if the signs were found. The result of each test is multiplied by the corresponding multiplier ki, and then the results are added. The final value of K is the all implicit attributes tests' result.

The multipliers are introduced by the developer of the program and can be changeable according to the performance statistics analysis.

3.3 Scheme 3. Additional Verification # 1

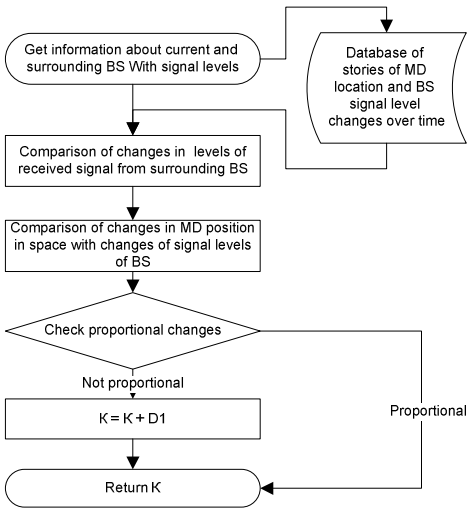

Figure 5: Additional Verification Number 1.

D1 is a multiplier that shows how much each attribute is more or less important than the others (Fig. 5).

More effective testing requires a certain "history" of events. Events are stored by this module as well as any other part of the system or a third-party system. This verification is aimed at detecting moving BSs. Since absolute majority of base stations worldwide are stationary, a moving BS is likely to be a UBS.

To detect the movement two parameters are checked: corresponding changes of signal level between the base station in question and the nearest ones to it and the difference between the location changing without having to switch to another BS. If at least one of the indicators returns a positive take, verification returns "1" multiplied by a factor corresponding to this test.

3.4 Scheme 4. Additional Verification # 2

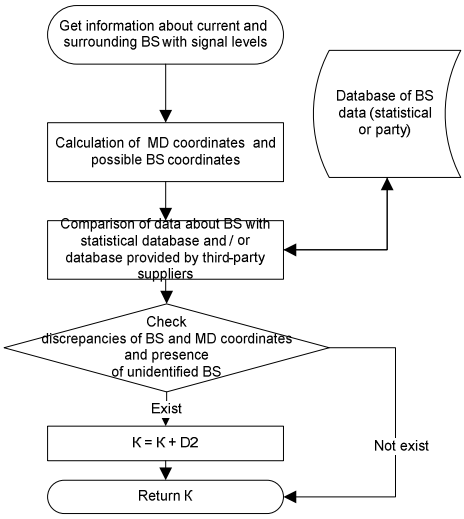

Figure 6: Additional Verification Number 2.

D2 is a multiplier that shows how much each indicator is more or less important than the others (Fig. 6).

This test uses the data on base stations' locations obtained from third-party sources or statistic database. If the list of base stations for the current location of the MD is known in advance, the emergence of a new one (BS with other location data or "out of place" base station or even BS completely absent in the database) can be a sign of the UBS.

There are some requirements for completeness and timeliness of the databases used in this algorithm. However, depending on the location and nature of data, quality of the algorithm can be

Journal of Theoretical and Applied Information Technology
20th November 2014. Vol. 69 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

improved by introducing the multiplier for the signal level and distance. If a mismatch of current surrounding BS and the database is detected, the algorithm returns "1" multiplied by the appropriate factor, otherwise – "0".

4. TESTING

The described algorithms have been implemented on the mobile operating system Android 4.0 as it is the most flexible allowing access to many system parameters. It is noteworthy that despite the flexibility of the system not all of the features listed in the article could be tested: access to such parameters as, for example, the presence of the encryption is not provided with API standard.

In order to test the implemented algorithms in conditions close to the real, the OpenBTS system with the hardware platform USRP [18] was used, allowing to emulate the network of GSM standard. It should be noted that OpenBTS is not a complete virtual base station, and only emulates the basic functionality of the network such as voice calls and SMS exchange between subscribers connected to the network as well as GPRS traffic.

By choosing different identifying options and modeling different situations occurring in the network the testing of algorithms` implementation was carried out. In particular the switching on OpenBTS was performed by temporarily suppression of signals from surrounding base stations. As identifying parameters (MCC, MNC, LAC, CelID) parameters of neighboring base stations, parameters of not existing base stations as well as parameters of base stations from other regions were taken.

The most difficult situation for the algorithms, as it was expected, was the situation when the virtual base station introduced itself as a located nearest base station, but the signal from it was not received by the mobile device. Since checking the database is not the only means of identification, the virtual base station was detected in this case.

The results of the experiments have led to the following conclusions:

- for efficient operation of algorithms it is required a valid selection of coefficients for verification of implicit parameters that was achieved experimentally;
- lack of possibility in modern mobile operating systems to check the encryption in the network leads to a grate decrease in the overall security and security of active and passive signal interception. In addition to the functions of determining the presence/absence of encryption it is also necessary to check the key bit size and encryption algorithm type. Otherwise, decoding of transmitted data will become too simple [19];
- filling databases with information about network base stations is essential and strongly affects the quality of recognition of the fact of connection to the virtual base station.

The question that remains unsolved is the universality of selected coefficients for different countries as well as the ways to filter false operation.

Figure 7: The Interface Of The Software Using Proposed Algorithms.

5. CONCLUSION

The algorithms described above are aimed at using to protect the user's mobile phone or tablet from the possible negative effects caused by addressing to an un-trusted base station. The authors provide information about wireless networks data analysis system comprising real time data analysis and modules of secured system. Moreover, the paper deals with UBS detection providing algorithms of explicit and implicit indicators of fake cells.

The system can be used with any mobile devices having a network module or a Wi-Fi module, such as mobile phones, tablets, notebooks, navigation systems, monitoring devices, etc. The system processes data sent and received by the mobile devices and detects connections to unauthorized base station.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

It is planned to enhance the system wherein the system is configured to survey MD microphone for its availability and, if the microphone is not available, to check an MD user interface for messages indicating microphone related issues. If the microphone is not available, the system determines that a hidden call is taking place. Also the control module is going to be configured to notify a mobile subscriber of changes of mobile communication standards

The testing experiments and further algorithms` improvements are underway to increase the quality of data analysis and detection of changes in the security level of data transmission in wireless networks.

REFRENCES:

[1] Boudriga, N. Security of Mobile Communications. *IEEE International Conference on Signal Processing and Communications*, 2007. ICSPC 2007. Pages: li – lii.

[2] La Polla M., Martinelli F., Sgandurra D. A Survey on Security for Mobile Devices. *Communications Surveys & Tutorials, IEEE* (Volume: 15, Issue: 1), 2013. Pages 446 – 471.

[3] Ghallali M., Ouahidi B.E. Security of mobile phones: Prevention methods for the spread of malware. *2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT).* Pages: 648 – 651.

[4] Spaulding J., Krauss A., Srinivasan A. Exploring an open WiFi detection vulnerability as a malware attack vector on iOS devices. *2012 7th International Conference on Malicious and Unwanted Software (MALWARE).* Pages: 87 – 93.

[5] Sandhu, R. Good-enough security. *IEEE Internet Computing*, Volume: 7, Issue: 1. Jan/Feb 2003. Pages: 66 – 68.

[6] Zhukov Igor, Mikhaylov Dmitry, Starikovskiy Andrey, Dmitry Kuznetsov, Tolstaya Anastasia, Zuykov Alexander. Security Software Green Head for Mobile Devices Providing Comprehensive Protection from Malware and Illegal Activities of Cyber Criminals. *International Journal of Computer Network and Information Security,* Vol. 5, No. 5, April 2013. Pages 1-8.

[7] Mikhaylov Dmitry, Zhukov Igor, Starikovskiy Andrey, Kharkov Sergey, Tolstaya Anastasia, Zuykov Alexander. Review of Malicious Mobile Applications, Phone Bugs and other Cyber Threats to Mobile Devices. *Proceedings of 2013 5th IEEE International Conference on Broadband Network & Multimedia Technology (5th IEEE IC-BNMT 2013),* November 17-19th 2013 Guilin, China. Pages: 302-305.

[8] Kurushin V.D., Minaev V.A. Computer crimes and information security. Moscow, *New Lawyer*, 1998.

[9] Weinmann, Ralf-Philipp: Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks. *6th USENIX Workshop on Offensive Technologies*, August 6-7, 2012, Bellevue, WA, USA, Proceedings, USENIX, 2012, pp. 12-21.

[10] Jukka Lotvonen, Juha Kumpula, Markus Ahokangas, Janne Pauna. Man-in-the-middle detector and a method using it. *US patent 20090104889 A1*. 2009.

[11] Wolman, Alastair; Zill, Brian D.; Padhye, Jitendra D.; Chandra, Ranveer; Bahl, Paramvir; Singh, Manpreet; Sivalingam, Lenin Ravindranath. Detection and management of rogue wireless network connections. *United States Patent 8000698*. 08/16/2011.

[12] Goldfarb, Eithan. Systems and methods for identifying rogue base stations. *United States Patent Application 20130344844*. 2013.

[13] Kulaga, Andrey and Tikhomirov, Anton. System and method for optimization of execution of security tasks in local network. *United States Patent Application 20120173609*. 07/05/2012.

[14] Adam Kostrzewa. Development of a man in the middle attack on the GSM Um-Interface. Master Thesis, Technische Universität Berlin. April 15, 2011.

[15] Handover. Cellular communication. URL: http://celnet.ru/HO.php.

[16] D.M. Mikhaylov, I.Yu. Zhukov. *Protection of mobile phones from attacks.* ed. By A.M. Iwashko. Moscow. Foylis, 2011. - 192 p.: Ill.

[17] A.G. Beltov, I.Yu. Zhukov, D.M. Mikhaylov, A.V. Staricovskiy. *Mobile technology: services. Easy, briefly, quickly.* Moscow: INFRA-M, 2012. - 206.

[18] Abul Azad. Open BTS Implementation With Universal Software Radio Peripheral. URL: http://mathinstitution.com/ECE/SDR/sdr_openBTS_aazad.pdf.

[19] Elad Barkan, Eli Biham, Nathan Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication Advances in Cryptology - *CRYPTO 2003 Lecture Notes in Computer Science Volume 2729, 2003*, pp 600-616.