DOI: 10.5604/01.3001.0009.5183

INTRUSION ASCERTAINMENT BY THE ANALYSIS OF SURROUNDING WIRELESS SIGNALS WITH SOFTWARE DEFINED RADIO

Janusz Zawadzki
Opole University of Technology, Faculty of Electrical Engineering, Automatics Control and Informatics

Abstract: *The purpose of this study is the creation of an autonomous system based on software defined radio, with the ability to ascertain and compute wireless signals from the surrounding area. The analysis of previously obscure signals could allow the recognition of the alleged trespassing of the surveilled area.*

Keywords: SDR, software defined radio, wireless networks, signal detection

ANALIZA SYGNAŁÓW BEZPRZEWODOWYCH Z OTOCZENIA A STWIERDZENIE INTRUZJI ZA POMOCĄ SYSTEMU RADIA DEFINIOWANEGO PROGRAMOWO

Streszczenie: *Celem pracy jest utworzenie autonomicznego systemu opartego o układ radia programowalnego, zdolnego wykrywać i przetwarzać sygnały bezprzewodowe z otoczenia. Analiza pojawienia się wcześniej niedostępnych sygnałów ma umożliwić rozpoznanie domniemanego naruszenia przestrzeni objętej obserwacją.*

Słowa kluczowe: SDR, radio definiowane programowo, sieci bezprzewodowe, detekcja sygnałów

Introduction

With increasing miniaturization of integrated circuits a growing number of new possible usages for previously inaccessible or difficult-to-use communication technologies emerges. Given that today's information technology is based largely on wireless transmissions exchange, it is only natural that each one of us carries a device utilizing these forms of communication. The increasing availability of software defined radio systems and their flexibility in reception of radio waves, allows the analysis of signals emitted by such devices [2, 3]. The use of these systems to intercept transmissions may actually not allow to read the data contained in them, however allows the unambiguous determination of actual occurrences of the transmission itself. Fig. 1 shows the general idea behind the fact that an SDR system may be used to detect multiple wireless operating devices. In this work an emphasis has been put on the use of this aspect in order to alert the user about the possibility of unwanted transmissions and thus an intrusion in the area under control of such systems. Due to problems mentioned in the summary, certain aspects remain yet to be clarified, although a large part of the thesis has been put to successful practical implementation. This allows for further, even more sophisticated tests to be conducted in order to obtain more precise readouts and the exclusion of problems encountered.

1. Build system and specifications

The laboratory station for measurements consists of a mobile computer control unit, an IBM X60S notebook, equipped with a dual-core Core Duo U2400 processor and 3GB of DDR2 RAM, an SDR device type Nuand BladeRF x40 equipped with two circular antennas featuring a gain of 5 dBi, mounted on a RP-SMA socket, see Fig. 2. The software includes an UNIX operating system known as Arch Linux with all the newest updates to the day of writing this paper, an application dedicated to capturing radio frequency signals called GNU Radio, also Octave mathematical computing software and the author's scripts in Python and Bash computer language. The whole system operates on an integral basis, it is however possible to change the unit responsible for the software-side to other counterpart's, possibly even embedded systems.Smartphones as well as other common electronic devices were used as the gear introducing desired disturbances.

The scope of the research is to collect measurements of radio-wave frequency in real time and then search for occurrences of the frequency deviation of the curve with respect to background and static noise levels. Fig. 3 shows an occurrence of an induced 433 MHz radio wave transmission. Readings were taken in the laboratory which served as a testing room located one floor underground. In the immediate vicinity there were no known sources of transmission, which could disrupt the control process. Known terrestrial base stations of mobile operators, or radio stations, were intentionally not mentioned.

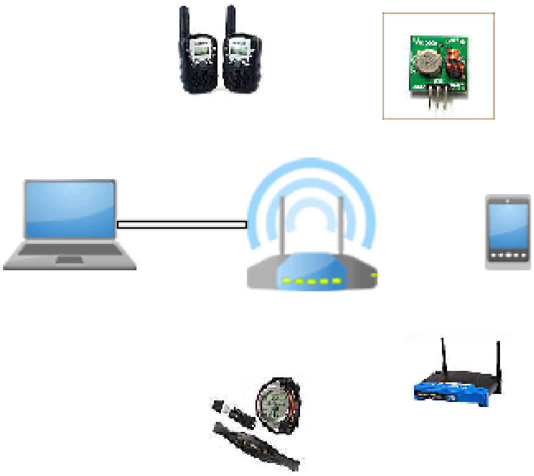


Fig. 1. General system build and the way of its functioning

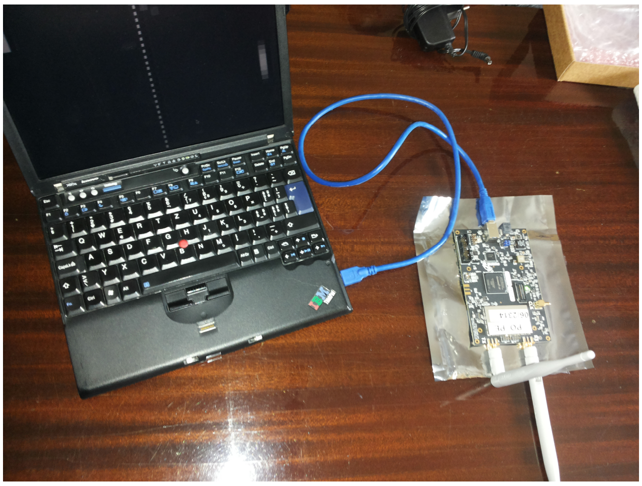


Fig. 2. Measurements equipment

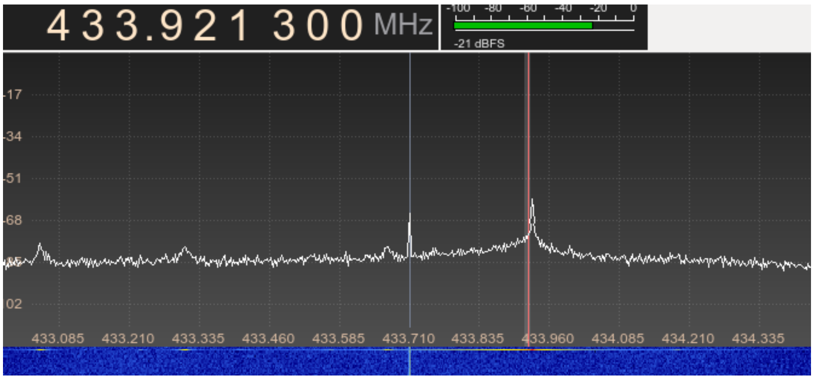


Fig. 3. Graph showing possible occurence of a 433 transmitter

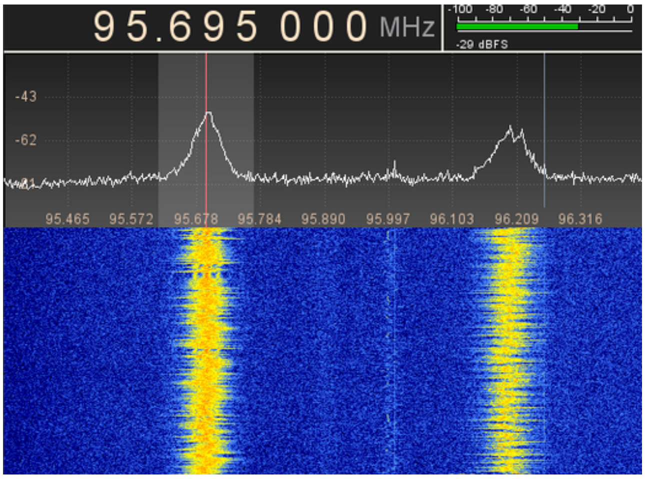


Fig. 4. Waterfall diagram of FM transmissions

Fig 4. shows two frequency broadcasts of known FM radio stations captured just outside the building in which the testing laboratory was located.

Tests are conducted in a fixed range of different frequencies, mainly in the precinct of 400 MHz to 950 MHz, 1.4 GHz to 1.6 GHz and 2.3 GHz to 2.5 GHz. The ability of radio reception the SDR device offers is greater, but for the account of optimal operating conditions the available testing devices permit, and also better interpretation of the measurements results, it was decided not to change these parameters. As shown on Fig.5, the quality of reception of a sample GSM transmission induced by a mobile smart phone is quite high. Also worth of noting is the fact that the analysis of any error rates or BER, which is thoroughly described in position [1] of the literature, was of no interest. We take for granted that the actual occurrences of transmission take place in area of up to 5 meters in diameter around the reception antennae. With greater distances it would be unavoidable to loose signal quality or miss the whole RF event altogether. Such topics are outside of the scope of our research, because of its primary goals. The summary adds even more details as of why this is so. Furthermore, as our tests also did not include the need to inspect data we capture in transit, we do not delve into the aspects of the multitude of communication protocols possible to use with our SDR system. The BladeRF is an FPGA capable board, it is possible to upload programs containing entire instruction sets on automating certain aspects of wireless packet analysis. Since our tests were conducted with use of a Laptop PC, this aspect was not utilized. In the hope of obtaining more mobility in future research or tests, it is possible to exchange the controller for an embedded platform. A common example of such use might be the use of a popular Raspberry PI microcomputer board.

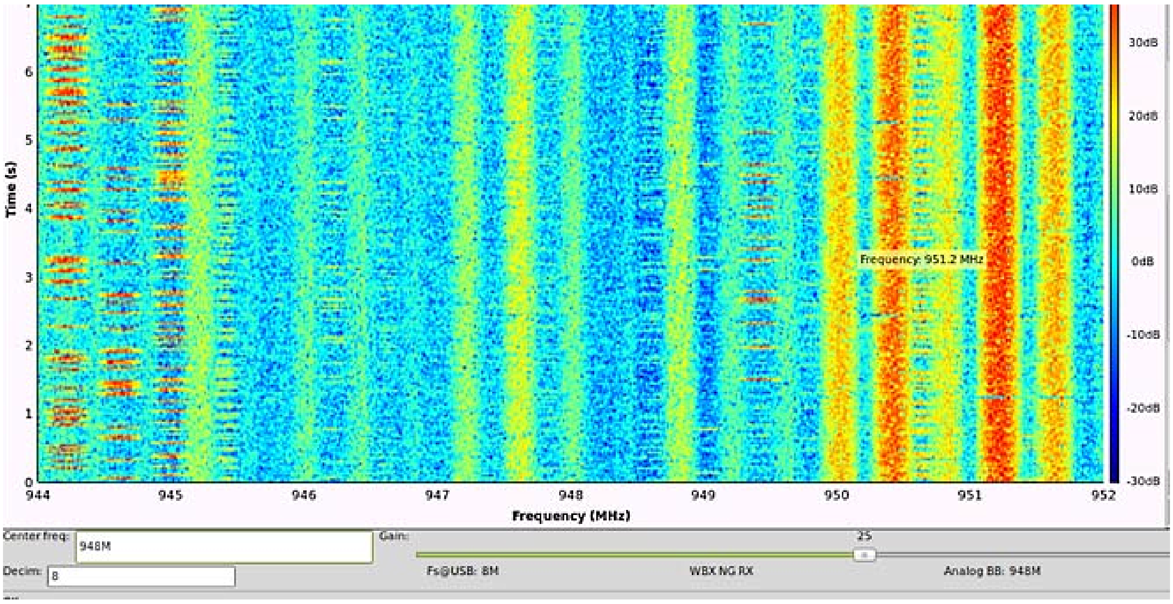
2. Software approach

There is a multiplatform collection of tools for developing communication protocols called GNURadio. Other possible use cases for development are nicely described in reference [4]. In this paper however, full support for our capture device is achieved by using the Osmocom's libbladerf library, and found satisfactory to work with. A block diagram showing an uncomplicated graphical frequency listener used at the beginning of this research work is shown on Fig. 7. During collection, the results are written and compared with the ones stored in the database instance. For the sake of simplicity and performance, we create a MySQL database with one static and two temporary tables. In the first one we hold the defined known frequencies used in the ether, and their descriptions for ease of concatenation. The other two withhold new transmissions found after starting the reception, and the time of last occurrence respectively. If a new spike, like in the waterfall diagram high pinched point representing a possible transmission is spotted, the program calls out a Bash command line function to first compare it with the contents of temporary tables and then informs the user about possible unwanted changes in the vicinity of the application. This is the case if the event was not recorded before. To clarify, a trigger works on the database in case the fortuity ceases to subsist, in which turn it zeroes the time, and writes additional bits to the counter.

However, if they were present beforehand, the timings are compared to validate the 'if and when' the case was registered.

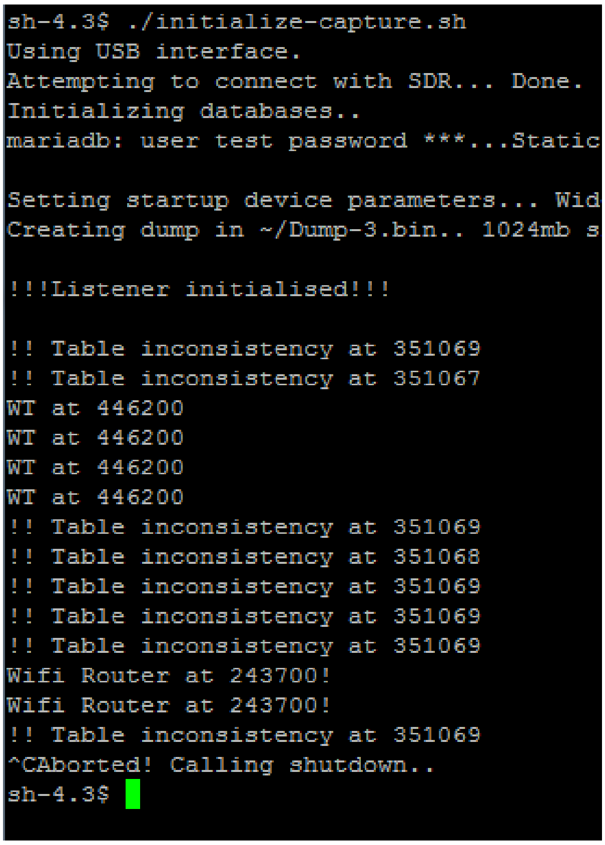
Then, in order to become acquainted with the cause of the information occurrence, a verbose message is displayed on the command line with data regarding the approximate frequency. Then the comparison with the built-in base of known requests takes place, showing the type of the detected objects and their possible designation. If the static database does not contain such information, the event is considered an obvious intrusion. In order to receive even more useful information regarding the detection of unwanted presence occurrences in close environment transmissions, it is possible to manually extend the database to hold more records of known devices, or extend the original script to run an initial learning mode each time the program is restarted. Such approach was acknowledged, however due to the nature of this research, it was found as not essential. Another desirable function could be a further expansion in programming to include an array of changes for the transmitted signal strength. This could in turn significantly increase the comfort of handling and the ease of sorting out real threat occurrences. Research has shown, that the charts show many unidentified signals that may be either harmonic waves or other unknown electromagnetic emanations, despite a separated and controlled environment in which the research was conducted.

The tests resulted in a successful detection of the wireless networks broadcast using a smartphone and two different WiFi routers as well as the mere presence of modern mobile phones, two transmitters operating on frequencies of 433 MHz, a Sigma digital heart rate monitor with built-in transmitter, a bluetooth ad-hoc station, standard walkie-talkie tunable broadcast device, a low power FM transmitter and a RF operated car key.



Center freq: 948M
Decim: 8
Gain: 25
Fs@USB: 8M
WBX NG RX
Analog BB: 948M

Fig. 5. Waterfall diagram of GSM broadcasts



```
sh-4.3$ ./initialize-capture.sh
Using USB interface.
Attempting to connect with SDR... Done.
Initializing databases..
mariadb: user test password ***...Static

Setting startup device parameters... Wid
Creating dump in ~/Dump-3.bin.. 1024mb s

!!!Listener initialised!!!

!! Table inconsistency at 351069
!! Table inconsistency at 351067
WT at 446200
WT at 446200
WT at 446200
WT at 446200
!! Table inconsistency at 351069
!! Table inconsistency at 351068
!! Table inconsistency at 351069
!! Table inconsistency at 351069
!! Table inconsistency at 351069
Wifi Router at 243700!
Wifi Router at 243700!
!! Table inconsistency at 351069
^CAborted! Calling shutdown..
sh-4.3$ 
```

Fig. 6. Example command-line output of the created listener program

3. Measurements

Fig. 6 shows an example dry run of the main intrusion detection program. The output states that it successfully recognized the pushes of the transmission button located on the walkie-talkie enclosure. Just a moment later out test wifi-router was powered up and started broadcasting its signal. Unknown radio emissions were classified as inconsistencies. The recognition of known devices this instance allows, is achievable only by correct definition of variables in the static database table. In theory all other devices of similar attributes will also be detected, as long as their transmitter parameters are within the reception abilities of the SDR platform. However, it might not be possible to distinguish similar devices from one another, like manufacturer or model of various wireless routers, because of the kind of approach used. Other approaches are beyond of the scope of this research. A brief summary of different devices used for testing is shown in Table 1.

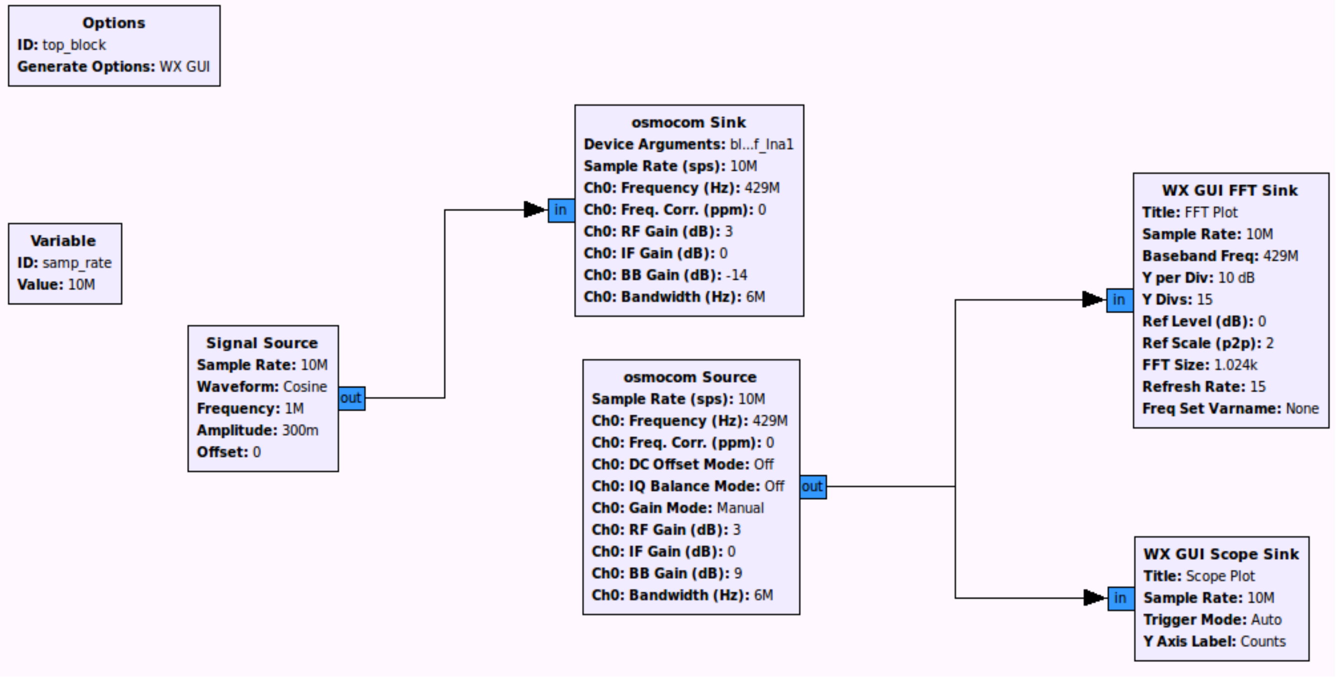
Table 1. Devices used

Device	Frequency [MHz]
Walkie-talkie	450
Transponder	433
FM transmitter	95
Bluetooth dongle	2455
Wifi router	2412

4. Conclusions

The study shows another approach to the vast number of possible different implementations of nowadays SDR systems which reflects their versatility. Although the concept to use radio frequencies for wave monitoring is not new, it is the angle at which it was achieved that makes it so robust. With a small but capable enough device you may start to mind a specific area for unknown signal occurrences, or possibly even reverse engineer applications in search for weaknesses and additional hidden functionalities. During the research it was concluded possible to achieve the main expectations set before this project, but it also has come to the notice that a number of problems related to the effective use of transmission events classification in the control area are to be considered. The problem of distinguishing ordinary occasional interference from a real world event is subject to further investigation. In addition, the inability to establish a complete database of all foreseeable frequencies for events makes it difficult to inform the user about what he or she may have to deal with, when communicating such instances. It is also worth noting that the distinction between devices was not possible due to the lack of metadata gathering and analysis.

Another obstruction is the ability to anticipate the area from which the transmission takes place. The main problem lies within the very own nature of transmitted waves, there may be a local source from which they originate from close distance, with small amount of transmitted power, then again we can expect the inherence of high power broadcasts made over very long distances. Without some way of triangulating the signals, like by using multiple reception modules, or using beam aerials in an established scheme outside of the perimeter, we are unable to determine their origin. During the study it was conceived that this area remains dormant until further research.



Options
ID: top_block
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 10M

Signal Source
Sample Rate: 10M
Waveform: Cosine
Frequency: 1M
Amplitude: 300m
Offset: 0

osmocom Sink
Device Arguments: bl...f_lna1
Sample Rate (sps): 10M
Ch0: Frequency (Hz): 429M
Ch0: Freq. Corr. (ppm): 0
Ch0: RF Gain (dB): 3
Ch0: IF Gain (dB): 0
Ch0: BB Gain (dB): -14
Ch0: Bandwidth (Hz): 6M

osmocom Source
Sample Rate (sps): 10M
Ch0: Frequency (Hz): 429M
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 3
Ch0: IF Gain (dB): 0
Ch0: BB Gain (dB): 9
Ch0: Bandwidth (Hz): 6M

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 10M
Baseband Freq: 429M
Y per Div: 10 dB
Y Divs: 15
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 10M
Trigger Mode: Auto
Y Axis Label: Counts

Fig. 7. Graphical listener diagram written in GNU Radio Companion

The study was conducted in a laboratory environment which makes it difficult to verdict the efficiency of this approach in terms of real life scenarios. A large number of changing wireless transmitters that can be found in residential or office buildings may adversely affect the test results. However, there is a good chance to eliminate most of the problems associated with distinguishing between the desired and intermittent events through the implementation of an advanced learning and decision-making algorithm. Due to time constraints the author of the study could not delve further into this subject. However, the research concluded the undeniable fact of creating a unique, comprehensive system for the detection of close proximity wireless events. This opens the opportunity to further study the implementation of computer controlled software defined radio systems in regards of both an application and purely hardware side.

References

[1] Martinek R., Zidek J., Tomala K.: Pomiary BER w systemie radia programowalnego. *Przegląd Elektrotechniczny,* 2b/2013, 205–210.

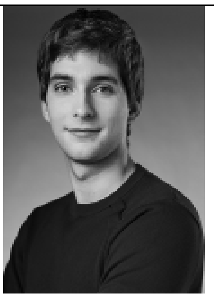
[2] Sklivanitis G., Gannon A., Batalama S. N., Pados D. A.: Addressing next-generation wireless challenges with commercial software-defined radio platforms. *IEEE Communications Magazine,* 54(1)/2016, 59–67.

[3] Ulversoy T.: Software Defined Radio: Challenges and Opportunities. *IEEE Communications Surveys & Tutorials,* 12(4)/2010, 531–550.

[4] Vilches T., Dujovne D.: GNUradio and 802.11: performance evaluation and limitations. *IEEE Network,* 28(5)/2014, 27–31.

M.Sc. Janusz Zawadzki
E-mail: janusz.zawadzki@doktorant.po.edu.pl

First year doctoral student at the Opole University of Technology, Faculty of Electrical Engineering, Automatics Control and Informatics, Department of Electrical Power and Renewable Energy. His science interests include the topics of EM emanations, embedded devices, security and modern computer technology.



otrzymano/received: 22.04.2016 *przyjęto do druku/accepted: 30.10.2016*