A Self-testing Approach Defending against Rogue Base Station Hijacking of Intelligent Terminal

Dali Zhu, Na Pang and Zheming Fan

Institute of Information Engineering, Chinese Academy of Sciences

Keywords: security; rogue base station; detect; MODEM; handover.

Abstract. The flexibility and convenience offered by mobile communication have made it one of the fastest growing areas of telecommunications, and communication security has become particularly significant and prominent. One of the most challenging security threats is the attack of rogue base station which posing as a radio transceiver station. It uses the same high-power electromagnetic frequencies to occupy the spectrum resources to send large amounts of spam messages. Rogue base station, if undetected, can be an open door to sensitive in-formation. In this paper, we present the process which rogue base station exploits security vulnerabilities to at-tack. Based on the priority handover strategy of channel monitoring in cellular radio system and the SMS which Attention instruction commands MODEM to receive in PDU format, we propose a self-testing approach defending against rogue base station hijacking of intelligent terminal. Extensive experiments have demonstrated the accuracy, effectiveness, and robustness of our approach.

1. Introduction

With the rapid development of Internet and communication technology in public mobile communications network, GSM system becomes one of the most popular digital cellular telecommunications systems in the whole world. When intelligent terminal selects a new Public Land Mobile Network (PLMN) in the cellular mobile communication system, it tries to reside in a cell which decoding downlink reliably and communicating uplink effectively [1]. According to it, the intelligent terminal receives the paging information from PLMN and establishes a call. The BCCH carrier in re-election neighborhood frequency allocation table can be monitored in service cell. Rogue base station sends the BCCH of an adjacent cell of the normal GSM base station. By increasing signal power of the BCCH, the rogue base station can deceive and kidnap the mobile phones which resided the target cell.

Open BTS in [2] can be used to steal the international mobile subscriber identity (IMSI) and disguise as any caller to send any fraud, merchandising any other spam messages. In addition, in the area of hijacking by rogue base station, Open BTS can grab our sending messages and calling. All of them are carried out silently, and the users of mobile phone are extremely hard to detect such a process in [4]. The threat of rogue base station has attracted significant attentions from both industrial and academic researchers.

In this paper, we illustrate the process which rogue base station exploits security vulnerabilities to attack. Based on the priority handover strategy of channel monitoring in cellular radio system and the SMS which Attention instruction commands modem receive in PDU format, we propose a self-testing approach defending against rogue base station hijacking of intelligent terminal which can identify the rogue base station quickly and accurately.

The rest of the paper is organized as follows. In section 2 we describe some of the related works. In section 3 we discuss the model of rogue base station hijacking. In section 4 we propose the self-testing approach. In section 5 we present the experiments and results. We conclude our work and plan the future work in section 6.

2. Related Work

The security threat on rogue base station is taken into account by more and more researchers. In general, the methods are mostly based on IEEE802.16 standard. In paper [5], the authors proposed a new signal fingerprinting approach based on discrete wavelet transformer. Instead of being extracted from the transient part, the signal fingerprint is computed on a part of the signal related to the transmission of a definite sequence of bits.

Jie et al. [6] proposed a set of new authentication protocols for protecting MMR WiMAX networks from rogue base station attacks. They provided centralized authentication by using a trusted authentication server to support mutual authentication. ZHANG Chen in paper [7] presents method of detecting malicious base station. It developed emphasizes that some unique parameters in the system message and signaling information should be extracted and analyzed. In paper [8] a node doesnpsilat block a compromised node when detects it and only send an alert to the base-station. Then the base-station will check transmission buffer of that node and if the base-station concludes that the node is compromised, the rest of the network will be informed, and the appropriate actions will be taken.

Yong et al. [9] proposed a malicious detection algorithm that permits identification of misbehaving wireless stations, and then dispenses punishment by denying an ACK packet which allows transmission by the malicious stations. Gacovski et al. [10] proposed in this paper a new multiple criteria decision-making method in order to solve the location of base station problem under fuzzy environment. Pandit et al. [11] proposed a novel technique to protect the location privacy of the BS against external packet tracer attacks by employing asymmetric power control for the transmissions along the multi hop path between the source and the sink.

Although these methods, to some extent, detect the rogue base station, it would be difficult to configure parameter which is easy to bring false [12] . As for it, the most challenging problem is the time delay.

3. Model of rogue base station hijacking

3.1 Working Background of Rogue Base Station.

The cellular concept was a major breakthrough in solving the problem of spectral congestion and user capacity [13]. It offered very high capacity in a limited spectrum allocation without any major technological change. It is a system level idea which calls for replacing a single, high power transmitter much low power transmitters. The cellular architecture is shown in Fig.1. So it can compose as easy and as the same capacity as local call to communicate. This system is a complete information trans-mission entity, and it includes a Mobile Switching Subsystem (SS), operation and maintenance management subsystem (OMS), the base station subsystem (BSS) and a mobile station (MS).

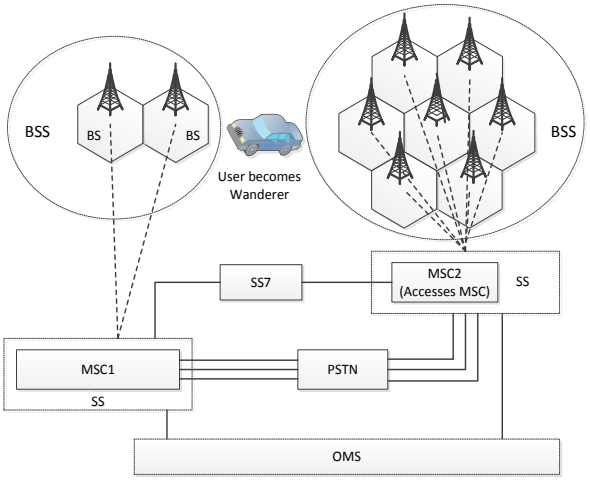

Fig.1: The architecture of cellular mobile communication system

The reason of that rogue base station exploits security vulnerabilities to attack is the one-way authentication mechanism of GSM. As is shown in Fig.2. In the process of communicating base

station with intelligent terminal, network side have the one-way authentication on mobile terminal in GSM, but the terminal cannot detect whether the network identity is legitimated or not [14]). Therefore the intelligent terminal is failed to determine the legitimacy and integrity of received signaling. As for the security vulnerabilities, intelligent terminal can be inhaled by the rogue base station and be forced to disconnect with the public network [15] .

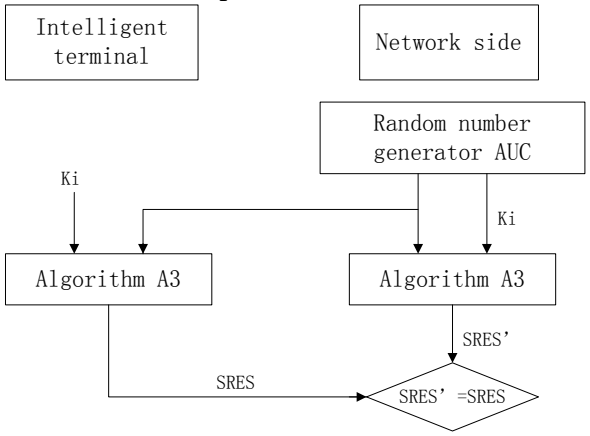

Fig.2: The process of GSM user authentication

3.2 Hijacking of Rogue Base Station.

The BCCH carrier in re-election neighborhood frequency allocation table can be monitored in service cell. Rogue base station sends the BCCH of an adjacent cell of the normal GSM base station. By increasing signal power of the BCCH, the rogue base station can deceive and kidnap the mobile phones which resided the target cell. The hijacking system is shown in Fig.3. It consists of a base station system and a control platform, and the base station system consists of the base unit BSS and the mobile services switching center MSC. It imitates the normal legal base station which providing interface to the intelligent terminal, but it is not connected to the operator network.

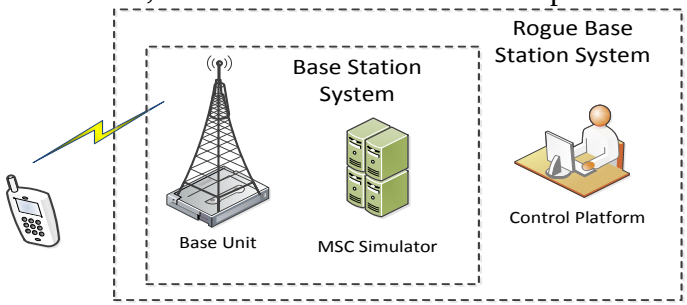

Fig.3: The hijacking system of rogue base station

Open BTS is a low cost alternative to the high end cellular networks that relies on software defined radio. It completely replaces the traditional GSM handover fabric from the baseband transceiver stations. As is shown in Fig.4. It includes the following important processes: transceiver, Open BTS and Asterisk.

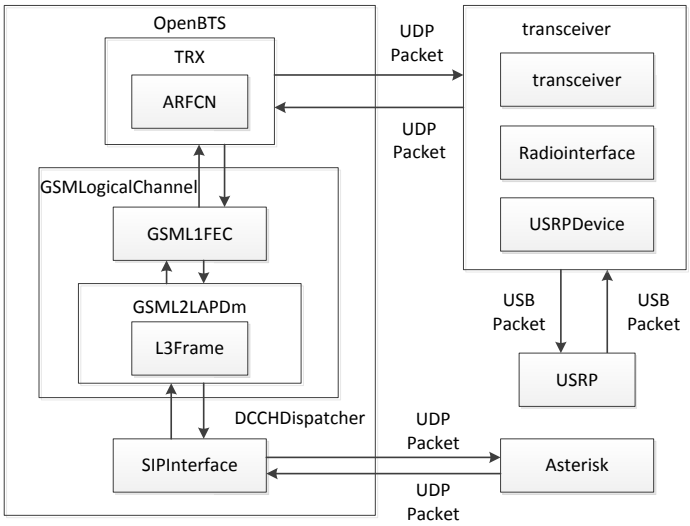

Fig.4: The system architecture of Open BTS

4. Proposed the self-testing approach

4.1 Based on the Priority Handover Strategy of Channel Monitoring.

The basic premise behind cellular system design is frequency reuse, which exploits path loss to reuse the same frequency spectrum at spatially-separated locations. Specifically, the coverage area of a cellular system is divided into no overlapping cells where some set of channels is assigned to each cell. The purpose of inter-cell handover is to maintain the call as the subscriber is moving out of the area covered by the source cell and entering the area of the target cell. For static intelligent terminal, the process on cell selection or reselection can make it get better cell service which resulting in higher quality of communication. For dynamic intelligent terminal, changing the channel or cell is necessary to ensure the communication quality due to the changes on location and environmental factor. The most basic form of handover is when a phone call in progress is redirected from its current cell to a new cell.

The handover event must be indeed very short and not perceptible by user. During a call, one or more parameters of the signal in the channel are monitored and assessed in order to decide when a handover may be necessary. The downlink or uplink directions may be monitored. The handover is requested by the phone or the base station of a neighboring cell. The phone and the base stations of the neighboring cells monitor signals of each other and the best target candidates are selected among the neighboring cells.

Designers must develop the most appropriate signal strength of a start switch. Generally a specific signal strength is designated as the minimum acceptable voice quality for base station receiver (typically between -90dBm to -100dBm). Slightly stronger signal strength can be used as the threshold to start switching. The interval is neither too big nor too small. It is unnecessary to handover which increasing the burden on the MSC if it is set too big. It may be interrupt a call due to weak signal if it is set too small, and leads to not having enough time to complete handover. As is shown in Fig.5.

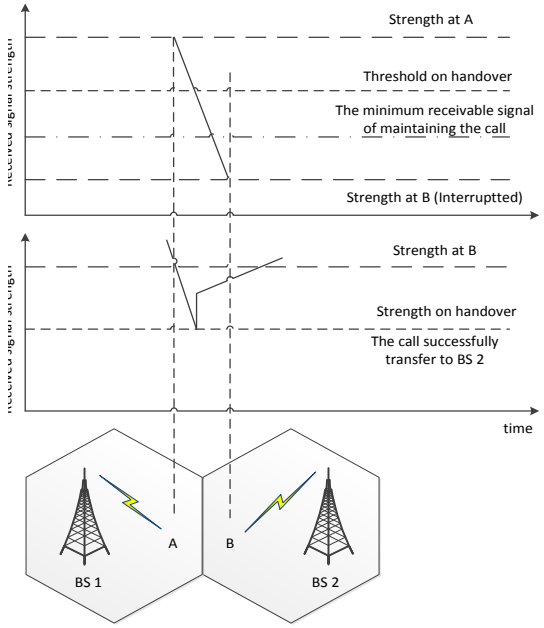

Fig.5: Handover strategy in cell border

Getting the signal strength, Mobile Country Code (MCC), Mobile Network Code (MNC), Location Area Code (LAC), Cell Identity (CI), cell LAT and cell LON in intelligent terminal through the interface provided by android is the first step. When the SIM card is not changed, MCC and MNC will not change. Drawing the change curve of signal strength, LAC, CI, LAT and LON in a certain period of time, if one of these parameters changes greater than a predetermined threshold value per unit time, it will be considered that the intelligent terminal is connected to the rogue base station but not the normal base. Yellow warning will be prompted to user for connecting to the rogue base station, and the sending and receiving about the system messages will be intercepted before disconnecting from it. Extensive experiments have demonstrated the accuracy, effectiveness, and robustness of our approach. The core codes are as follow.

```
/**
* use to acquireInfo of base station, write state to static
* attributes
* @return null
*/
void acquireInfo(){
mTelephonyMgr.listen(MyListener,
PhoneStateListener.LISTEN_SIGNAL_STRENGTHS);
location = (GsmCellLocation) mTelephonyMgr.getCellLocation();
LAC = location.getLac();
MyListener = new MyPhoneStateListener();
if (getAirplaneMode(MonitorService.this)) {return;}
mTelephonyMgr = (TelephonyManager) getSystemService (Context. TELEPHONY_ SERVICE);
mTelephonyMgr. listen (MyListener,
PhoneStateListener.LISTEN_SIGNAL_STRENGTHS);
location = (GsmCellLocation) mTelephonyMgr.getCellLocation();
LAC = location.getLac();
GsmCellLocation location = (GsmCellLocation) mTelephonyMgr
.getCellLocation();
if (location == null)
return;
int detaLAC = LAC - location.getLac();
if ((!(detaLAC < LAC_DETA_RAG && detaLAC > -LAC_DETA_RAG))) {
```

```
_LAC = location.getLac();
count++;} else {
LAC = location.getLac();}}}
```

4.2 AT Instruction Commands Modem to Receive Message.

Modem controls SMS through communication interface. It has three access protocols: Block Mode, Text Mode based on AT instructions and PDU Mode based on AT instructions. PDU mode is the most widely used method to send or receive message which transferred in hexadecimal code. Basically all of the national telephone company provide the message service on supporting PDU Mode, and some do not support Text Mode and Block Mode. It limits the application of these two access protocols which promote that PDU Mode becomes a mainstream trend.

Receiving messages is essentially reading information from the SIM or cache which exploit AT + CMGR and AT + CMGL these two instructions. The wireless modules in response to AT instructions are not the same, so firstly the AT instructions must be confirmed whether it can establish communication with the modem or not. Then AT + CMGF instruction selects data format of message, and completes the process of readout after receipting the correct answer from modem.

Experiment measures the normal information in PDU format of hexadecimal string. It is as follows.

0D71683108370105F004000D81683179133208F1000002608041003380263218 4CF682D95E0 DC2B36D3D170A0243106933D97A0243106933D97A02451068B1983492608

It contains the contents of message, the sender number, number type, message center number, message sending time and so on. Comparing these parameters with the normal values after receiving a message, it will be considered that the intelligent terminal is connected to the rogue base station when one of them is different. Red warning will be prompted to user for connecting to the rogue base station, and the sending and receiving about the system messages will be intercepted before disconnecting from it. The core codes are as follow:

```
/**
* decode pdus of message, get centent message content and so on
* Write info into database. Decode succeed if return true.
* attributes
* @return boolean
*/
void decodeMsg(){
Object[] messages = (Object[]) intent.getSerializableExtra("pdus");
byte[][] pduObjs = new byte[messages.length][];
byte[][] pdus = new byte[pduObjs.length][];
int pduCount = pdus.length;
SmsMessage[] msgs = new SmsMessage[pduCount];
for (int i = 0; i < pduCount; i++) {
pdus[i] = pduObjs[i];
msgs[i] = SmsMessage.createFromPdu(pdus[i]);}
String timeNow = formatter.format(curDate);
for (SmsMessage currentMessage : msgs) {
data = bytesToHexString(currentMessage.getPdu());
String dataSub = new String(hexStringToBytes(data.substring(6, 16)));
msgCenter = currentMessage.getServiceCenterAddress();
body.append(currentMessage.getDisplayMessageBody());}
if ((msgCenter.substring(0, 12)).compareTo(CenterNum) == 0) {return;} else {
msgsDB.insert(msgs[0].getDisplayOriginatingAddress(),body.toString(), msgCenter, timeNow);
abortBroadcast();}
number.append(msgs[0].getDisplayOriginatingAddress());
Return true ;}
```

5. Experiments and results

The self-testing approach defending against rogue base station hijacking of intelligent terminal deploys at the original Android phone nexus4 for testing. Table 1 shows the experimental environment.

Table 1: Experimental environment

phone		
Hardware Configuration	Model	LG E960 (Nexus4)
	CPU	Snapdragon APQ8064
	RAM	2GB RAM&8 GROM
Software Configuration	Android Version	4.2.2
	Kernel	3.4.0-perf-g7cellcd
	Baseband version	M9615A-CEFWMAZM-2.0.1700.84

Based on the priority handover strategy of channel monitoring in cellular radio system, the changes of signal strength are in Fig.6. Compared of the two curves changes, the signal strength changes greater than a predetermined threshold value instantaneously, and this state maintains about 8-10 seconds. Then it returns to normal. These two curves represent the intensity of the normal base station and the intensity of the rogue base station.

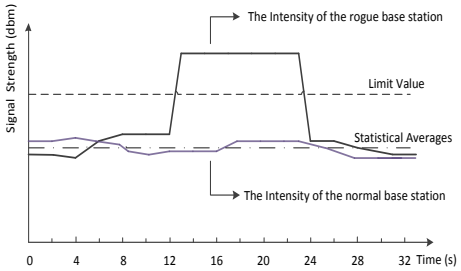

Fig.6: Changes of signal strength

Based on the priority handover strategy of channel monitoring in cellular radio system, the changes of the number of LAC are in Fig.7. It would not be a big fluctuation under normal circumstances. The statistical maximum fluctuation is shown in Fig.7. Fluctuations exceed this value will be seen connect to rogue base station. It is shown by the dashed box.

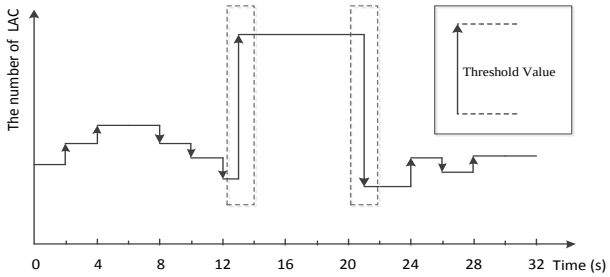

Fig.7: Changes of LAC value

Based on the SMS which Attention instruction commands MODEM to receive in PDU format, message center number, the sender number, message sending time and content can be get according to parsing the PDU messages. As is shown in Table 2. Three sets of data are tested. Receiving content for "Testing" message from normal base station in PDU format is:

0891683108100005f0240d91687190000107f900005110813152152307f4f29c9e769f01.

Receiving content for “hello world" message from normal base station in PDU format is:

0891683108100005f0240d91685106625106f700005110813193102 30be8329bfd06dddf723619.

Receiving content for “Please visit http://hsxzuk.com to accept the award. The code is 2384. “Message from rogue base station in PDU format is:

0883357629853981902 40d8387992875427249000051108141509323455076393c2f83ece9799a0e42d3e970ddeb859ee3f5f5b56bfc6e83e86f50783c2ec3e9203aba0c0adfc372b20b44459741e337b90c4acf41b2198ee602.

Table 2: Receiving content in PDU format

SMS content	message center number	sender number	message sending time	content	results
Testing	6831081 00005f	68719000 0107f	511081315 21523	f4f29c9e 769f01	Normal BS
hello world	6831081 00005f	68510662 5106f	511081319 31023	e8329bfd0 6dddf…	Normal BS
Please visit http:// hsxzuk.com to accept the award. The code is 2384	3576298 539819	87992875 42724	5110814150 9323	5076393 c2f83ec…	Rogue BS

From table 2, passing through the low nibble transposition processing of hex bytes, the message center number of the third one is 5367925893189, and sender number is 7899825724274. They are not legitimate obviously. They do not match the information to the normal operators. It can be seen connected with the rogue base station.

Comprehensive judgment in these areas is shown in Fig.8. The condition around can be detected real-time. Once the phone is connected to the rogue base stations, it will be in yellow or red warning to user. Before the phone is not connected with rogue base station, it will intercept the sending and receiving of messages.

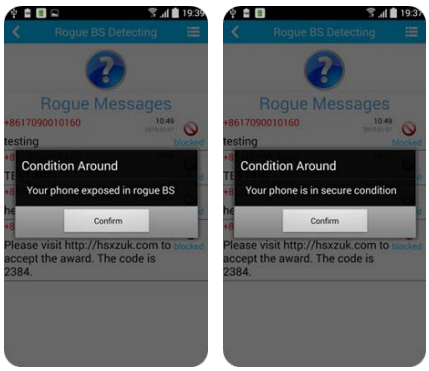

Fig.8: The results of detection

6. Concluding remarks

Communication security has become increasingly prominent today. The thing that intelligent terminals are hijacked by the rogue base station occurs frequently. Researching the process of hijacking and detecting has great significance. Based on the priority handover strategy of channel monitoring in cellular radio system and the SMS which Attention instruction commands MODEM to receive in PDU format, we propose a self-testing approach defending against rogue base station hijacking of intelligent terminal and provide the yellow or red warning to users. This program is convenient without increasing the burden on the interface or signaling of core network with the base station. It is unnecessary to change the hardware configuration of intelligent terminal and the existing communication protocols. The flexibility and scalability make it easily to resolve the deceptive issues. Future work will address the characterization of the best sequence in order to better locate the rogue base station and attack it.

References

[1] Alipour, H.; Gholami, M.; Vahdani, A 2008. A base-station oriented anomaly detection for wireless sensor networks. Internet, 2008. ICI 2008. 4th IEEE/IFIP International Conference on, Page(s): 1-7.
[2] Cameron, T.; Poulin, D.; Sychaleun, D.; Beaudin, S.; Kung, W. 1999; Nisbet, J. A multi-chip receiver module for PCS1900 and DCS1800 GSM basestations. Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE, Page(s): 732 - 736 vol.2.
[3] Chouchane, A.; Rekhis, Slim; Boudriga, N, 2009. Defending against rogue base station attacks usingwavelet based fingerprinting. Com-puter Systems and Applications, IEEE/ACS International Conference on, Page(s): 523-530.
[4] Dudoyer, S.; Deniau, V.; Adriano, R.R.; Slimen, M.N.B.;Rioult, J.; Meyniel, B.; Berbineau, M 2012. Study of the Susceptibility of the GSM-R Communications Face to the Electromagnetic Interferences of the Rail Environment. Electromagnetic Compatibility, IEEE Transactions on, Page(s): 667 - 676.
[5] Gacovski, Z.; Cvetanoski, I 2006. Fuzzy decision-making for selection of mo-bile basestation location. Information Technology Interfaces, 2006. 28th International Conference on, Page(s): 401-406.
[6] Haverinen, H.; Asokan, N.; Maattanen, T 2001. Authentication and key generation for mobile IP using GSM authentication and roaming. Communications, 2001. ICC 2001. IEEE Interna-tional Conference on, Page(s): 2453-2457.
[7] Hillebrand, F. 2013. The creation of standards for global mobilecommunication. GSM and UMTS standardization from 1982 to 2000. Wireless Communications, IEEE, Page(s): 24-33.
[8] Huang Jie; Huang Chin-Tser 2011. Secure Mutual Authentication Protocols for Mobile Multi-Hop Relay WiMAX Networks against Rogue Base/Relay Stations. Communications (ICC), 2011 IEEE International Conference on, Page(s): 1-5.
[9] Lo ChiChun; Chen YuJen 1999. Secure communication mechanisms for GSM networks. Con-sumer Electronics, IEEE Transactions on, Page(s): 1074-1080.
[10] Malone, D.; Kavanagh, D.F.; Murphy, N.R 2013. Rogue femtocell owners: How mallory can monitor my devices. Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on, Page(s): 429-434.
[11] Pandit, V.; Hailong Li; Gottumukkala, V.; Agrawal, D 2012. APCAPT: Asymmetric power control against packet tracer attacks for base station location anonymity. Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on, Page(s): 1-6.
[12] Pace, P.; Loscri, V, 2012. OpenBTS: A Step Forward in the Cognitive Direction. Computer Communications and Networks (ICCCN), 2012 21st International Conference on, Page(s): 1-6.
[13] Prasannan, N.; Xavier, G.; Manikkoth, A.; Gandhiraj, R.; Peter, R.; Soman, K.P 2013. OpenBTS based microtelecom model: A socio-economic boon to rural communities. Au-tomation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on, Page(s): 856-861.
[14] Yong Woon Ahn; Jinsuk Baek; Cheng, A.M.K.; Fisher, P.S. 2011; Minho Jo. A Fair Trans-mission Opportunity by Detecting and Punishing the Malicious Wireless Stations in IEEE 802.11e EDCA Network. Systems Journal, IEEE, Page(s): 486-494.
[15] Zhang Chen 2014. Malicious base station and detecting malicious basestation signal. Communi-cations, China, Page(s): 59-64.