Pulse: Low Bitrate Wireless Magnetic Communication for Smartphones

Weiwei Jiang
Huazhong University of Science and Technology, China
Weiweijiangcn@gmail.com

Denzil Ferreira, Jani Ylioja, Jorge Goncalves, Vassilis Kostakos
Department of Computer Science & Engineering
University of Oulu
{firstname.lastname}@ee.oulu.fi

ABSTRACT
We present *Pulse*, a wireless magnetic communication protocol for smartphones. Pulse is designed for off-the-shelf Android smartphones with magnetometers, and encodes data in magnetic fields. We present the design and evaluation of Pulse in various conditions (e.g., different voltages, number of transfer channels). The system provides security due to its short range (~1 cm), it can reach a speed of up to 44 bits per second, and it is possible to run it on most mobile phones with a magnetometer. We present our evaluation and discuss practical use cases where Pulse can be used today.

Author Keywords
Magnetic field; wireless communication; magnetometer.

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION

We present and evaluate *Pulse*, an alternative to NFC and QRCodes that conceptually shares characteristics with both. We describe how Pulse can be used on smartphones' magnetometers (*i.e.*, magnetic compass) for short-range one-way communications with a bitrate of up to 44 bps (bits per second). Many smartphones today have a magnetometer as it is commonly packaged together with GPS to establish users' direction when navigating. Compared to NFC, Pulse can be used on many more smartphones *today* simply by downloading new software. Compared to QRCodes, Pulse can provide dynamic and streaming data.

Short-range communication technologies such as NFC rely on near-field coupling (up to 20 cm) instead of a discovery mechanism used in other popular wireless standards (*e.g.*, Bluetooth, Wi-Fi). This physically enhances security and overcomes vulnerabilities inherent in discovery-based wireless technologies. Hence the hope of easy, short-lived, short-ranged, and relatively secure data transfers between mobile devices, made NFC a very promising technology. However, this promise has not yet materialised and we are still waiting for NFC to hit the market in big numbers. Current estimates claim that 66% of smartphones will have NFC capability by 2018 [21], but similar claims have been made for years. The slow adoption of NFC, despite its numerous advantages, is due to its focus on payment services, which form a complicated ecosystem. While the market has been trying to figure out how to enable payments over NFC, another "short-range" technology has seen extremely wide adoption on smartphones: Quick Response Codes (QRCodes). This one-way channel has become a widespread alternative, because it is very easy to produce and consume: most smartphones today have a camera and can decode QRCodes by installing an application.

Ubicomp'14, September 13 - 17 2014, Seattle, WA, USA

http://dx.doi.org/10.1145/2632048.2632094

In this paper we present a magnetic near-field communication protocol that offers the best of both NFC and QRCodes: like NFC it is short-range (with and even more tight bounding radius), and like QRCodes it can run on most smartphones today.

RELATED WORK

Near-field magnetic communication is a technique that is not interfered by human bodies, liquids, or metals [3]. Despite its benefits, so far only few commercial products use it (*e.g.*, LibertyLink docker and Freelinc's earpiece [16]), and currently most uses of this technology are research driven: magnetic fields have been used for indoor navigation systems (*e.g.*, [5,7]), as a communication mechanism for underground rescue [18], and to manipulate DNA molecules [23]. Closer related to our work is Won's et al. [22] experiment with magnetic wireless communication between two devices. Their simulations show that magnetic fields allow data transfer in liquid and metal environments with relatively many users, and is energy efficient at ranges below 1 meter. However, their results are mostly theoretical. In our work, we evaluate a real prototype (Pulse) in a laboratory setting by measuring how range, data transfer speed, error rates, and power consumption vary.

More recently, Agbinya [1] investigated the theoretical performance of magnetic communication systems given ideal hardware, identifying optimal configurations for magnetic field communication. However, when it comes to smartphones, many of these decisions are constrained by the actual magnetometer hardware available on the phones. Conceivably, if magnetic communication becomes popular in smartphones, its performance can be greatly increased by improving magnetometers according to their recommendations.

EXPERIMENTAL APPARATUS

Architecture

We built a wireless communication system utilizing magnetic fields to transmit data. The system shown in Figure 1 consists of an Olimex Ltd AVR-MT128 AVR board, which encodes the data and passes it to a DAC0808LCN 8-bit D/A converter chip for modulation. We then use two solenoids, in diameters of 2.5 and 3.5 cm and with 50 loops each, as antennas for the Z and X channels respectively. These two channels are received in the z and x axes of an unmodified

Samsung Galaxy Nexus smartphone's magnetometer accordingly, and are decoded.

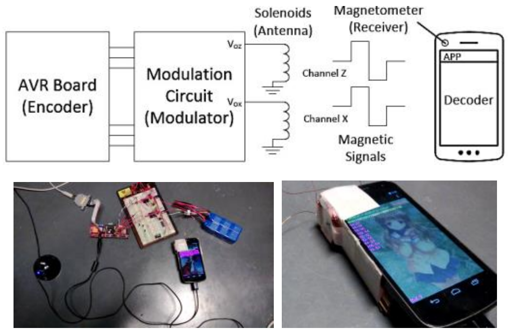

Figure 1. System architecture (top); and prototype (bottom).

Data encoding

A typical smartphone magnetometer with a magnetic sensor can measure magnetic flux on 3 distinct axes simultaneously [20]. Therefore, it is possible to transmit data over these axes in parallel. To maintain a short distance between the device and the magnetic field generator (*i.e.*, solenoid), we use only the z and x axes and ignore the y-axis. To improve the data transmission speed, we use a 4-level amplitude-shift keying (4-ASK) scheme to encode the data. Before transmission, the magnetic signal is briefly calibrated (between 1.6 and 3.2 seconds) to ignore any background magnetic noise. To calibrate, the encoder transmits a series of sequences between 0000 and 1111. The data uses ASCII encoding. Our coding scheme uses a constant period length (t_0 = 80 ms), which is long enough to account for the smartphone's magnetometer limitations. During a period, each of the two channels can transmit 2 bits (given our 4-level ASK coding), and therefore the system can transmit in total 4 bits per period. As a convention, the X channel deals with higher bits, while the Z channel deals with lower bits. Finally, we define data packets to consist of 8 periods (4 bytes) each.

For example, let us assume that we want to transmit the character 'H' whose ASCII representation is 0100 1000. In period 1 we transmit the first 4 bits (0100): the X channel (Figure 2, in blue) transmits 01 while the Z channel (Figure 2, in red) transmits 00 in parallel. This process continues until all bits are transmitted. Figure 2 shows a magnetic signal transmitting the message "Hello world!\n". Since this message requires multiple packets, we use [x] to indicate an empty period (t_0) between two consecutive packets. We acknowledge that our prototype's network protocol does not introduce packet types, sequence numbers, or CRC to minimize the amount of bits transferred.

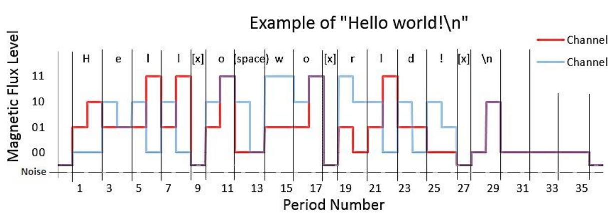

Figure 2. Magnetic transmission of "Hello world!\n".

Magnetic Data Modulation

We designed and built a circuit to modulate digital signals from the AVR board into analog current signals. We used a DAC0808LCN 8-bit Digital to Analog Converter (DAC) chip for this modulation. In our 4-ASK encoding, the signal uses 2 bits (b_1 and b_2) for data, and 1 bit for handling the background noise (b_3). We then used a TL0721P operational amplifier to convert the current signals to voltage signals (V_o). The output voltage from a voltage follower circuit for bits b_1, b_2, and b_3 is $V_O = \frac{R_F}{R_{REF}} \times V_{REF}\left(\frac{b_3}{8} + \frac{b_2}{4} + \frac{b_1}{2}\right)$, where R_F is the feedback resistor of the current-to-voltage converter, R_{REF} the reference resistor of input reference voltage, and V_{REF} the reference voltage. The output voltage signals are then sent through an output resistor (R_O) serially connected to a solenoid. Finally, the solenoid generates magnetic signals with the current intensity $I_O = V_O / R_O$.

Software Decoding

We built an Android application to decode the transmitted magnetic signals, detected by the magnetometer in a Samsung Galaxy Nexus smartphone. Our initial challenge is fto determine the physical position of the sensor, since it varies by handset model, important for positioning the phone in relation to the transmitter. The decoding application first performs a calibration to remove background noise. During calibration, the transmitter will send all values between 0000 and 1111 in sequence. Since the signals between the X and Z channels may interfere with each other, we need to calibrate both channels in parallel. Finally, to decode the data packets we divide each packet into 8 units of 80 ms length each (*i.e.*, data periods). Each unit is then decoded to one of 16 possible values between 0000 and 1111, retrieving the original data.

RESULTS

Physical properties of Pulse

The theoretical magnetic flux density at point X on the axis of a solenoid with a constant current is $B = \frac{\mu_0 n I}{2}(\cos\theta_2 - \cos\theta_1)$ where μ_0 is vacuum permeability (*e.g.*, $4\pi\times10^{-7}$ V s/(A m)), n is the number of loops, I is the current intensity, θ_1 and θ_2 are angles of the axis and connections of point X and the edges of the solenoid. To overcome Earth's magnetism, we need to generate a magnetic field whose flux density is stronger than the Earth's naturally occurring magnetism. Because the flux density of earth's magnetism is 22 µT - 67 µT [14], we have to set the value for I higher than 100 mA for distances of 1 cm between the solenoid and the magnetometer. As an alternative, we could increase the solenoid's radius, but that would require a larger antenna. A larger antenna would create a wider magnetic field, but not without increasing the amount of interference between transmission channels and consequently lower our data signal's stability. For simplicity, when testing our prototype we placed it in a room without potential sources of magnetic noise (e.g., power supplies, electric motors, magnets). In practice, such a device would require a magnetic-proofing enclosure for noise resistance. To keep the shortest distance possible, we varied the solenoid radius (1-3 cm) and distance from the smartphone (0.5-2 cm). The wire's diameter remained constant (0.4 mm) for all tests.

Speed vs. Error

We tested two different ASK schemes to encode the data: 2-ASK and 4-ASK. We conducted experiments for both schemes using different values for the period length (t_0). The relationship between Bit Error Rate (BER) and t_0 is inversely correlated (Pearson r = -0.94, R^2 = 0.89 for 2-ASK; Pearson r = -0.95, R^2 = 0.92 for 4-ASK) (Figure 3).

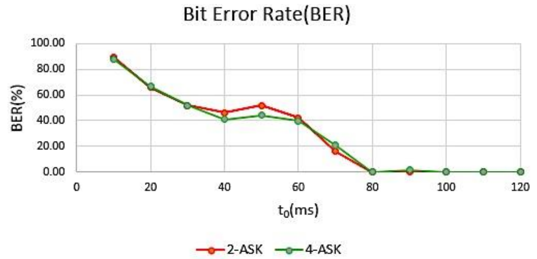

Figure 3. Bit Error Rate (BER) vs data period length (t_0).

To test data transfer errors, we generated 256 random bytes (S_0) and compared those with the smartphone's received bit sequence (S_1). We used Levenshtein Distance (LD) [10] as the number of errors in S_1: the count of the minimal bit changes to turn S_1 into S_0. The BER is then equal to the ratio of bits transmitted to errors in reception. We found that a period length (t_0) of 80ms achieves maximum bandwidth with no errors. Table 1 summarises the BER measured for different reference voltages and thresholds.

Reference voltage (V)	ASK level threshold (µT) 1	2	3	4	5
1.0	35.35	n/a	n/a	n/a	n/a
1.2	5.08	0.00	n/a	n/a	n/a
1.4	36.23	0.24	n/a	n/a	n/a
1.6	36.62	1.81	n/a	n/a	n/a
1.8	35.40	0.00	n/a	n/a	n/a
2.0	33.84	0.00	0.00	n/a	n/a
2.2	26.90	0.00	0.00	0.00	n/a
2.4	35.79	0.00	0.00	0.00	n/a
2.5	26.66	0.00	0.00	0.00	n/a
2.6	28.61	0.00	0.00	0.00	6.49
2.8	35.06	0.00	0.00	0.00	0.00
3.0	11.38	0.00	0.00	0.00	0.00

Table 1. Bit Error Rates (%) observed depending on reference voltage (V_{REF}) and ASK level threshold used (µT).

We find that if the threshold between ASK levels is too low (< 1 µT), the data is indistinguishable from ambient magnetic noise. When the signal threshold is set too high (> 2 µT), we need to increase considerably the reference voltage thus causing higher electromagnetic interference.

Maximum Range

Using a reference voltage of 2.5V, 4-ASK coding, and considering exclusively the z-axis (*i.e.*, to measure the distance between our prototype and the smartphone), we found the optimal distance between the solenoid and the mobile's magnetometer (*i.e.*, without data transfer errors) to be between 0-0.6 cm (Figure 4). Earth's magnetic background noise is approximately 29.0 µT on the z-axis at 65 degrees north latitude as we detected, and can be up to 61.0 µT at higher latitude areas [14]. Thus, to recognize a substantial change in magnetic pulses we must set the signal threshold at least 1 µT above the Earth's (*i.e.*, absolute value > 30 µT in our study) for accurate readings. A different threshold calibration might be required at Earth's higher latitude areas. Given this setup, errors occurred farther than 0.6 cm. The maximum data transfer rate achieved is 44 bps (V_{REF}=2.5V, t_0 = 80ms), using both x and z axes and 4-ASK encoding.

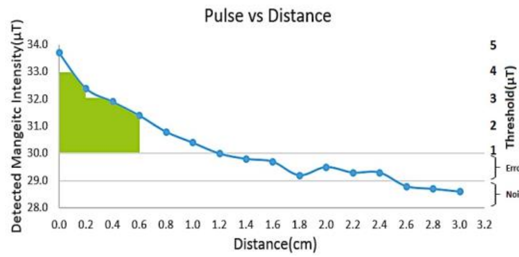

Figure 4. Given the communication distance (x-axis) and magnetic flux generated by Pulse (y-axis), the green area shows the conditions under which communication is possible.

DISCUSSION

Magnetic data bandwidth

Our prototype's magnetic data transfer is slow in comparison to Wi-Fi or Bluetooth at a mere 44 bps link speed. Note that the effective transmission speed would be slower if we had implemented packet types, sequence numbers or CRC in the protocol due to the bit overhead. The bitrate is limited due to three factors: the sample rate of the magnetometer hall sensor, the number of levels in our ASK data encoding, and the channels' capacitance. The magnetometer sensor in smartphones is unable to detect higher frequency magnetic signals, and the Android OS restricts the sampling rate of sensors for power efficiency.

There are three strategies to overcome these limitations. First, we could use faster magnetometers that can sense magnetic flux more rapidly. Second, we could modify Android's kernel to increase the sampling rate, but that would mean that our software would not work with off-the-shelf smartphones. Third, we could add the y-axis (in addition to the x and z axes) to increase the bits per period, but that would affect the distance between the antenna and smartphone.

ASK encoding schemes can use multiple levels, increasing bandwidth proportionally. This can be achieved by using more input bits in our Digital-to-Analog Converter (DAC). However, since the sensing frequency of the magnetometer sensor is limited, higher ASK levels would divide the signal into smaller pieces, decreasing the signal recognition threshold. This would increase Pulse's susceptibility to background noise, including Earth's (Table 1). Moreover, using higher ASK levels also leads to an increase in electromagnetic interference between the channels due to higher power requirements when adding ASK levels.

From the Shannon-Hartley's theorem, the maximum transmission rate R must be lower than channel capacitance C (R<C), and $C = B\ log_2(1 + SNR)$. B is the bandwidth of the channel, which equals to the sampling rate of the magnetometer sensor; and SNR is the signal-to-noise ratio between 1-4 and is proportional to the chosen threshold. An increased sampling rate and threshold would increase the channels' capacitance: a higher threshold induces a larger magnetic signal scale per ASK level, but only a limited amount of ASK levels are available due to the smartphone's magnetometer sensor sampling limitations.

Energy consumption

We estimated the energy consumption of the magnetometer [2], NFC transceiver [17] and camera [6] found in our device (Table 2). Pulse's energy consumption is higher than NFC and QRCode, but we expect a substantial reduction if bespoke hardware is used for Pulse.

Parameter	Pulse	NFC	QRCodes
Bitrate	44 bps	~ 424 kbps	2953 B p/shot
Processing	1.6-3.2 s	~ 0.1 s [4]	1-3.5 s [12]
Energy (J/bit)	$\sim 1.9 \times 10^{-5}$	$\sim 6.9 \times 10^{-7}$	$\sim 8.1 \times 10^{-6}$

Table 2. Energy consumption comparison

Multichannel communication

In wireless communications research, the concept of Multiple Input Multiple Output (MIMO) has recently been used in "smart antenna" technology to overcome many of the shortcomings of Single Input Single Output (SISO) communication [19]. MIMO entails the use of multiple antennas at the transmission point, and multiple receivers at the receiving point. MIMO is used in standards such as 802.11n, 4G, and LTE, and offers a number of benefits: higher capacity and higher resilience.

The protocol we have described also makes use of a MIMO design. In telecommunications engineering the multiple transmitted signals are de-multiplexed using statistically driven algorithms. However, in our case MIMO is decoded using the physical properties of magnetism and the geometric positioning of the antennas. In this paper we have used MIMO to double the bandwidth of Pulse, but of course MIMO can also be used to increase the resilience of communication. Using our two channels we can transmit redundant information, so that the receiver has a higher likelihood of decoding the message in adverse environmental conditions. In addition, the MIMO capability can be used to increase the compatibility of Pulse with a wider range of handsets. Although magnetometers are extremely popular in handsets today [8], their specifications may vary. Specifically, it is possible that the update frequency may vary between magnetometers. For our purposes we have limited the frequency of Pulse to 12.5Hz, but it may be possible to push this a bit higher as new smartphones hit the market. Therefore, Pulse could use Channel X to transmit data at this frequency, and use Channel Y to transmit data at a higher frequency. This would likely make the protocol more resilient, and compatible with a wider range of smartphones.

Near-Field Security

The visual complexity of QRCodes makes it hard for a human to detect malicious operations beforehand (*e.g.*, SQL injections, redirect to malicious websites, prompt the device to install malware) [9]. On the other hand, QRCodes can be used as user-generated or randomly generated input, useful as a pre-shared password mechanism [11]. A limitation of QRCodes is that, unless they are digital (*e.g.*, on a phone's screen), they are static and therefore limited in the dynamic security features they can offer, such as a rotating key.

To overcome some of these limitations, NFC offers 3 data exchange approaches [13]: *reader/writer* (R/W) mode, where the NFC smartphone can read and alter data on a passive NFC transponder; *card emulation*, where the NFC smartphone acts as a read-only (e.g., ticketing card); and *peer-to-peer* (P2P) mode. They do not specify how encryption or security is handled for NFC communication. The developer must implement this in the application layer. We speculate that the lack of a standardized NFC security mechanism could explain its slow market adoption, fomented with the users' fear of exposing their data without being aware (as you can read NFC data from afar) [15]. At the same time, QRCodes have been adopted quite rapidly because most smartphones come with a camera.

Pulse uses a magnetic "bubble" of approximately 1 cm, immune from radio frequency interference. An eavesdropper would have to be within the magnetic bubble (< 1 cm) to intercept magnetic transmissions to and from the coupled devices. A larger antenna and more power would increase the size of the "bubble." For practicality, we used a small antenna for transmission. Therefore, in our prototype, there is no security mechanism besides the magnetic and physical restrictions of the prototype itself. It is possible to further integrate encryption algorithms in the application layer but that is beyond the scope of our work.

Applications & Limitations

Pulse is unidirectional: we can transmit data from the prototype to the smartphone, but not the other way around since we are unable to produce a magnetic field with off-the-shelf smartphones. The limited speed and bandwidth also constrain Pulse's applications. Pulse is not a replacement for NFC or QRCodes, but can be used as a complimentary, widely available protocol – given the availability of devices with magnetometers. Pulse is ideal for short-lived and extremely short distance data transfers. In payment scenarios, a short code can be transmitted via Pulse near a payment terminal to confirm or verify payment using a smartphone, by transferring a 64bit or 128bit authentication key, passcode or other token to bootstrap a higher bandwidth communications channel. At a cash machine, Pulse can be used to transmit voucher information and balance information to the user's smartphone. Finally, low-bit streaming data can be transmitted using Pulse to enable the personalisation of services and applications. As a demo, we developed a music application that can transmit MIDI-like standard music for reproduction on the smartphone. The authors have provided as supplementary material a video of streaming music via Pulse.

Furthermore, Pulse can be used to complement QRCodes by providing up-to-date information from digital signage, with no need for Internet access. A QRCode can only provide a limited amount of data per snapshot, while Pulse can stream data within one single transmission event. This could reduce incurring data roaming fees for tourists, as Pulse could be used to provide, for example, bus schedules at bus stops without requiring visitors to access the Internet. Considering a city-scale deployment, Pulse installed on lampposts could be used to provide text-based street names to the visually impaired. We leave to the community to design and implement future use-cases.

CONCLUSION

Pulse is a magnetic communication protocol for short-range communication. The applications and scenarios we have presented for Pulse are not new: most proximity-based technologies provide similar motivations. However, Pulse has a key advantage: it can run on millions of smartphones today simply by installing software, not hardware.

ACKNOWLEDGEMENTS

Funded by the Academy of Finland project 137736, TEKES project 2932/31/2009, and EU grant agreement PCIG11-GA-2012-322138. We thank Chen Yu for his insightful comments.

REFERENCES

1. Agbinya, J.I. Performance of Magnetic Induction Communication Systems Using Induction Factors. *Wireless Personal Communications 70*, 2 (2013), 945-968.
2. AK8963 | Product | AKM - Asahi Kasei Microdevices. http://www.akm.com/akm/en/product/datasheet1/?partno=AK8963.
3. Bansal, R. Near-field magnetic communication. *Antennas and Propagation Magazine 46*, 2 (2004), 114-115.
4. Coskun, V., Ozdenizci, B. and Ok, K. A Survey on Near Field Communication (NFC) Technology. *Wireless Personal Communications 71*, 3 (2013), 2259-2294.
5. European Satellite Navigation Competition 2014. http://www.galileo-masters.eu/index.php?anzeige=overall12.html.
6. Image Sensors - MT9P031I12STC - Aptina Imaging. http://www.aptina.com/products/image_sensors/mt9p031i12stc/, retrieved 14/05/2014.
7. IndoorAtlas. https://www.indooratlas.com/index.html.
8. Jones, W.D. A compass in every smartphone. *IEEE Spectrum 47*, 2 (2010), 12-13.
9. Kieseberg, P., Leithner, M., Mulazzani, M., Munroe, L., et al. QR Code Security. *MoMM'10*, ACM (2010), 430-435.
10. Levenshtein, V.I. Binary Codes Capable of Correcting Deletions, Insertions and Reversals. *Soviet Physics Doklady 10*, (1966), 707.
11. Liao, K.-C., Lee, W.-H., Sung, M.-H. and Lin, T.-C. A One-Time Password Scheme with QR-Code Based on Mobile Phone. *NCM*, IEEE (2009), 2069-2071.
12. Liu, Y., Yang, J. and Liu, M. Recognition of QR Code with mobile phones. *IEEE Xplore* (2008), 203-206.
13. Madlmayr, G., Langer, J., Kantner, C. and Scharinger, J. NFC Devices: Security and Privacy. *ARES*, IEEE (2008), 642-647.
14. McLean, S., Macmillan, S., Maus, S., Lesur, V., et al. *The US/UK World Magnetic Model for 2005-2010. NOAA Technical Report NESDIS/NGDC-1*. 2004.
15. Mulliner, C. Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones. *ARES*, IEEE (2009), 695-700.
16. Near Field Magnetic Induction Communication. http://www.freelinc.com/technology/aboutnfmi.php.
17. NFC / RFID - NFC / RFID ICs - TRF7970A - TI.com. http://www.ti.com/product/trf7970A.
18. Radio-Style System of Communication Via Magnetic Waves Demonstrated in Deep Mines | Popular Science. http://www.popsci.com/technology/article/2010-08/lockheed-develops-magnetic-communication-mine-safety.
19. Raleigh, G.C. and Cioffi, J.M. Spatio-temporal coding for wireless communication. *Communications, IEEE Transactions on 46*, 3 (1998), 357-366.
20. Sensors Overview | Android Developers. http://developer.android.com/guide/topics/sensors/sensors_overview.html.
21. Two in three phones to come with NFC in 2018 • NFC World. http://www.nfcworld.com/2014/02/12/327790/two-three-phones-come-nfc-2018/.
22. Won, Y.-J., Kang, S.-J., Kim, S.-H., Choi, D. and Lim, S.-O. A communication system using magnetic fields. *Wireless ViTAE*, IEEE (2009), 265-269.
23. Yan, J., Skoko, D. and Marko, J.F. Near-field-magnetic-tweezer manipulation of single DNA molecules. *Physical Review E 70*, (2004).