CERTH
CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

Information Technologies Institute

The 8th International Conference on Cyber-Technologies and Cyber Systems CYBER 2023, Porto, Portugal

Presenter: Georgios Rizos

"Challenges in Medical Device Communication: A Review of Security and Privacy Concerns in Bluetooth Low Energy (BLE)"

Paper Authors: Michail Terzidis, Notis Mengidis, Georgios Rizos, Mariana S. Mazi, Konstantina Milousi, Antonis Voulgaridis, Konstantinos Votis

Presentation

by Georgios Rizos

CENTRE FOR RESEARCH & TECHNOLOGY - HELLAS
Information Technologies Institute

Georgios Rizos

Research Associate, ITI
Ph.D. Candidate *field of Cryptography*
M.Sc. Systems Security
B.Sc. Informatics
email: grizos@iti.gr

Acknowledgement

This research has been co-financed by the European Regional Development Fund of the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation, under the call RESEARCH – CREATE - INNOVATE for the Project CyberCare of CERTH Hellas.

Aims of our review

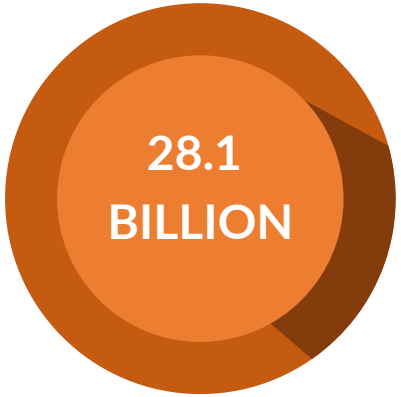
Our review aims to :

- ✓ describe possible attacks against the BLE protocol.
- ✓ assess the security aspects of medical devices, when using BLE.
- ✓ inform about recent vulnerabilities of BLE devices and cyber incidents on medical devices.
- ✓ highlight some mitigation strategies designed specifically for BLE applications.

“The need behind for our review”

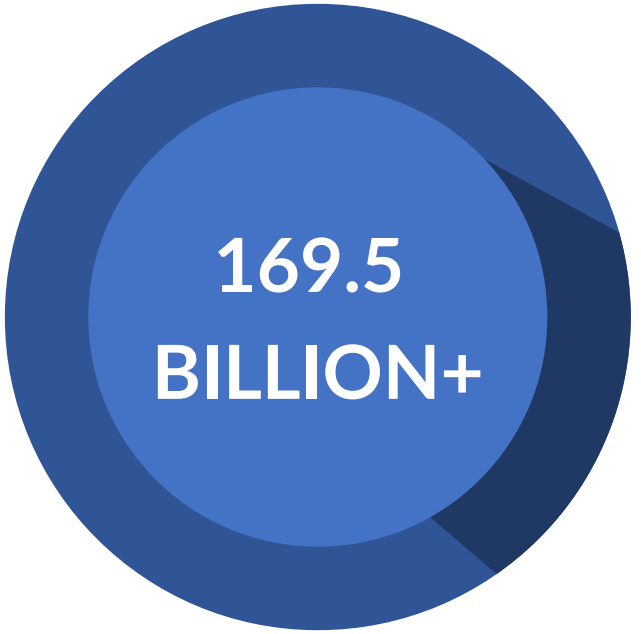
Increasing number of medical IoT devices

The global wearable medical devices market size was estimated at USD 28.15 billion in 2022 and is expected to hit over USD **169.58 billion** by 2030 with a registered Compound Annual Growth Rate (CAGR) of 25.6% from 2022 to 2030



2022

MIoT market size



2030

+603% increased

“The need behind for our review”

on-demand usage of BLE in healthcare devices

The 2020 Bluetooth Market Research report highlights that the healthcare wearable market, encompassing connected blood pressure monitors, continuous glucose monitors, pulse oximeters, and electrocardiogram monitors, witnessed a surge in demand, resulting in 12 million shipments in 2020 alone. This upward trajectory is anticipated to continue, with projected shipments reaching 52 million in 2025.

BLE protocol stack

is divided into three parts

Application Layer

it's responsible for the application logic, user interface and data handling.

It's architecture is highly depended on each particular implementation

Host

is composed of several layers

- Generic Access Profile
- Generic Attribute Profile
- Security Manager
- Attribute Protocol
- Logical Link Control and Adaptation Protocol

Controller

Host Controller Interface (HCI) includes the following layers

- Link Layer
- Physical Layer

BLE Attacks

divide into various categories

Next, we will mention basic attacks categories and describe how to implement them against the BLE protocol. Additionally we will present some BLE-specific attacks that exploit distinct BLE vulnerabilities.

ATTACK 01

General Cyber Attacks

operates passive and active eavesdropping attacks, MitM and Replay Attacks

ATTACK 02

Device Cloning Attacks

spoofs MAC address, name and GATT characteristics

ATTACK 03

Cryptographic Attacks

compromises BLE protocol's encryption, weaknesses and key exchange mechanism

ATTACK 04

Denial of Service Attack

targets the master BLE device, acting as common DoS

ATTACK 05

Distortion Attack

exploits the vulnerabilities of BLE protocol services, trying to disrupt the services

ATTACK 06

Surveillance Attack

gather information, cause of lack of proper security enforcement

ATTACK 07

Treacherous Attack

gains full system access, establishing a trusted relation between the devices

General attacks

Passive Eavesdropping

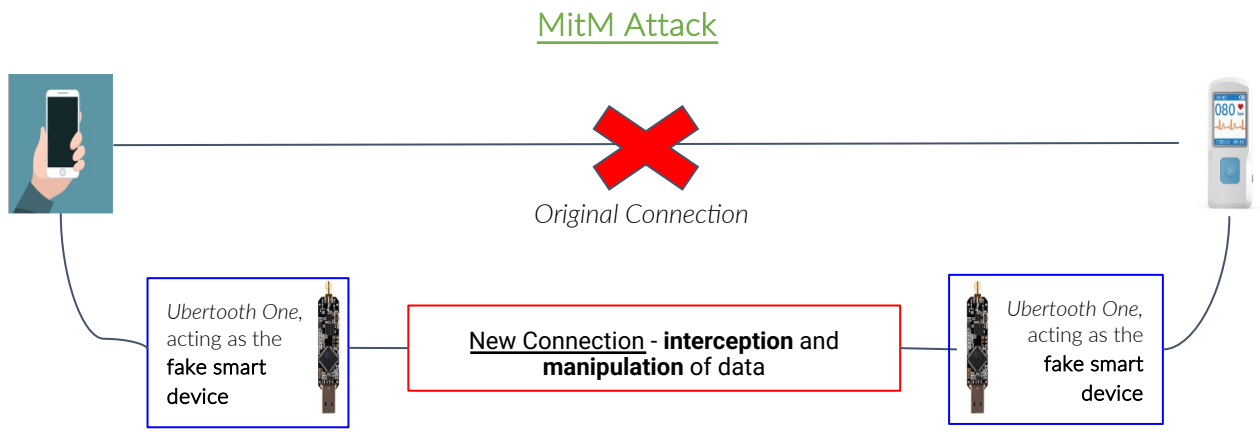
Unauthorized access and monitoring of Bluetooth communications. This form of attack involves the use of specialized software and hardware tools capable of intercepting and analyzing Bluetooth traffic (Ubertooth One).

Man in the Middle (MitM)

BLE MiTM attack necessitates the utilization of two BLE components (ex. Ubertooth One) with the capability to act in unison.

Replay attack

A form of attack for wireless communications where the attacker captures legit communication packets and then re-transmits those packets at a later time.



Denial of Service

Battery Exhaustion

One of BLE's features is its brief wake period. This attack targets this unique feature of BLE by keeping the device awake all the time.

Denial of Sleep

These attacks can reduce the lifespan of the sensing nodes by several orders
of magnitude, rendering the network unusable

Offline PIN cracking *

Can done in many ways, such as using brute force to crack the PIN, or via a dictionary attack. The security vulnerability of BLE is that the length of the Temporary Key (TK) to generate the encryption key might be too short.

Jamming

By jamming only packets sent by the peripheral to the central device, an attacker can trigger the timeout in the central device and then hijack the BLE connection.

BtleJack: a jamming attack example

This attack was published in 2018 by Damien Cauquil and implemented in the tool BtleJack [1]. Btlejack provides everything you need to sniff, jam and hijack Bluetooth Low Energy devices. It relies on one or more BBC Micro:bit devices running a dedicated firmware.

[1] D. Cauquil, "You'd better secure your BLE devices, or we'll kick your butts!", virtualabs.fr/BtleJack [retrieved: August, 2023]

Cryptographic Vulnerabilities

Device Authentication

This attack is feasible because of a cryptographic weakness of the passkey-based pairing of BLE.

Blue Mirror

During a reflection attack an intruder will collect a message in the authentication protocol, then send it without modification to the original sender.

BLUR attacks

These attacks allow to impersonate, MiTM, and establish unintended sessions with arbitrary devices, by obtaining the Cross-Transport Key Derivation (CTKD).

There are some forms of authentication attacks that crack the shared keys exchanged in the pairing process and they are as follows:

- Guessing Pairing Key : The attacker brute forces the six-digit pin key used for authentication.
- Eavesdropping Encryption Key : The Attacker uses Ubertooth One to read all the key exchange messages and decrypt it. One way to do that is by using Crackle [2].
- Stealing Link Key From the Device: There are many BLE devices in the market whose hardware is not secured enough to protect the stored encryption key

[2] "Crackle : cracks BLE Encryption (AKA Bluetooth Smart)", https://github.com/crackle [retrieved: August, 2023]

BLE Specific

Backdoor

Applying this method, gains the trust of the victim device through the pairing mechanism, while not appearing on the victims list of paired devices. In this way, the attacker can monitor the activities of the victim device.

BlueBump

The attacker gains the trust of the victim, then deletes the link key, then the attacker requests the victim to initiate another link-key, managing to remain concealed in the paired list of the victim device.

MAC Spoofing

The attacker spoofs the MAC address as well as GATT services, with specialized software tools like Gattacker, the attacker effectively replicates the GATT services of the original peripheral device, thereby assuming the role of a counterfeit peripheral entity.

BLE Spoofing Attack, an in practise example of MAC spoofing

These attacks enable an attacker to impersonate a BLE device and to provide spoofed data to another previously-paired device, as described analytically in [3]. Additionally there are other tools to spoof your MAC address

- bdaddr [4], which is most suitable for CSR and Broadcom chip based bluetooth adapters
- gadgets as FlipperZero [5], for which there already exist firmware to change the MAC address.

[3] J. Wu et al., "BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy", 14th USENIX Workshop on Offensive Technologies 2020 BLESA [retrieved: August, 2023]
[4] bdaddr - Utility for changing the Bluetooth device address, bdaddr [retrieved: August, 2023]
[5] Flipper Zero is a portable multi-tool for pen-testers and geeks in a toy-like body. FlliperZero [retrieved: August, 2023]

“Security and privacy for implantable medical devices, who introduced several successful attacks on an **Implantable Cardiac Defibrillator (ICD)**, compromising the confidentiality, integrity, and availability of the device.”

D. HALPERINET et al.

“Hacking medical devices for fun and insulin: Breaking the human SCADA system”, describes a possible **insulin pump** attack scenario.”

J. RADCLIFFE

“Fit and vulnerable: Attacks and defenses for a health monitoring device, by reverse engineering the communication protocol, storage details and operation codes, they identified several vulnerabilities in **Fitbit.**”

M.RAHMAN et al.

Results of cyber attacks in Healthcare

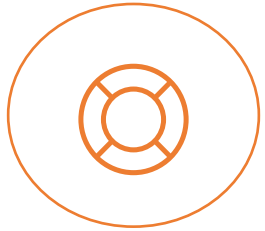
Randy Horton in his research "*What We Can Learn From Bluetooth Medical Device Recalls*", uncovered instances where Bluetooth was the reason for **device recall** in *healthcare*. These recalls highlight important lessons for developing Bluetooth-enabled medical devices. The research mentions :

- Active **implantable** devices, with connectivity issues.
- **Bluetooth-enabled** medical devices, with possible signal interferences.
- Continuous **Glucose Monitor System**, with bugs brought on by OS updates.
- Radiologic Imaging System, with improper **firmware** in the Bluetooth interface.

Mitigation Techniques

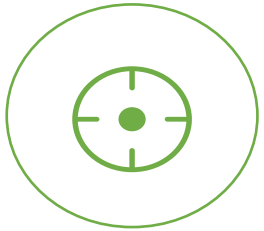
S. Shrestha

"A Systematic Literature Review of Bluetooth Security Threats and Mitigation Measures", present various **sets of rules** for users to help them perform actions safely, thereby minimizing the susceptibility to potential attacks.



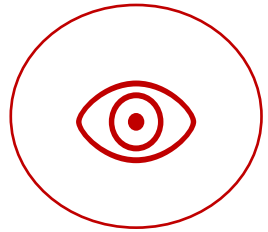
A. Ray

"Bluetooth Low Energy Devices Security Testing Framework", present a **framework**, which encompasses various software components designed to **carry out attacks**, in order to assess the security of BLE networks.



M. Yaseen

"A Novel **Framework** for Detecting MiTM Attacks in **eHealthcare BLE** Systems", introduces an innovative framework, known as MARC, which is specifically tailored to identify MiTM attacks in HealthCare BLE systems.



S. Shrestha

"Automated Security Assessment Framework for **Wearable BLE-enabled** Health Monitoring Devices", present an automated security assessment 4-stage framework designed specifically for Wearable BLE-enabled Health Monitoring Devices.

Conclusion

1. In our review we presented many ***cyber attacks***, both general type of attacks but also some BLE specific attack, due to BLE vulnerabilities.

2. We showed that, these types of ***vulnerabilities*** can raise a lot of concerns in many IoT fields and specifically in healthcare.

3. Software increasingly embedded into medical devices, provides a larger ***surface of attacks*** to malicious attacks.

4. It is critical to take the necessary measures and ***mitigate the damage*** in healthcare IoT applications, because the results of cyber attacks could be detrimental.

Future Work

PERFORMANCE

enhance the performance of BLE, like the improvement and design of the physical layer in BLE v5.x.

AVOID INTERFERENCE

research on the coexistence of BLE with other wireless technologies, as well as adaptive frequency hopping techniques to avoid interference.

BLOCKCHAIN

researchers may start looking into employing distributed type Blockchain technology to safeguard linked IoT devices.

Thank You!

Ευχαριστούμε :)

CONTACT US

ITI.GR

GREECE

57001, 6th km Harilaou -
Thermis, Thermi
Thessaloniki

References

[1] R. Horton, "What We Can Learn From Bluetooth Medical Device Recalls" [retrieved: August, 2023]
[2] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," Med Devices (Auckl), vol 8, pp. 305—316, 20 Jul 2015. Doi: https://doi.org/10.2147/MDER.S50048
[3] "Medical devices market". [retrieved: August, 2023]
[4] "How bluetooth technology is enabling safe return strategies in a COVID-19 era". [retrieved: August, 2023]
[5] K. Zetter, "It is insanely easy to hack hospital equipment". [retrieved: August, 2023]
[6] M. Kijewski, "Medical devices most vulnerable to hackers". [retrieved: August, 2023]
[7] P. Paganini, Smartwatch Hacked, "How to access data exchanged with smartphone". [retrieved: August, 2023]
[8] T. Melamed, (2018). "An active man-in-the-middle attack on bluetooth smart devices". International Journal of Safety and Security Engineering, vol. 8, pp. 200-211, 2018. Doi: https://doi.org/10.2495/SAFE-V8-N2-200-211
[9] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, "Security vulnerabilities in bluetooth technology as used in IoT," J. Sens Actuator Netw, 2018. Doi: https://doi.org/10.3390/jsan7030028
[10] "Bluetooth Low Energy A Complete Guide". [retrieved: August, 2023]
[11] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain, "Security and privacy threats for bluetooth low energy in IoT and wearable devices: a comprehensive survey," in IEEE Open Journal of the Communications Society, pp. 251-281, 2022. Doi: 10.1109/OJCOMS.2022.3149732
[12] W. Saltzstein, "Bluetooth wireless technology cybersecurity and diabetes technology devices," Journal of Diabetes Science and Technology, vol 14, no. 6, pp. 1111-1115, 2020. Doi: 10.1177/1932296819864416
[13] M. C¨asar, T. Pawelke, J. Steffan, and G. Terhorst, "A survey on bluetooth low energy security and privacy," Computer Networks, vol 205, p. 108712, 2022. Doi: https://doi.org/10.1016/j.comnet.2021.108712
[14] P. Cope, J. Campbell, and T. Hayajneh, "An investigation of bluetooth security vulnerabilities," IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, pp. 1-7, 2017. Doi: 10.1109/CCWC.2017.7868416
[15] F. Rigan, M. and A. Nasr, "Eavesdropping in bluetooth networks," International Journal of Current Engineering and Technology. [retrieved: August, 2023]
[16] S. Jasek, "GATTacking bluetooth smart devices," Tech. rep., SecuRing, p. 15. [retrieved: August, 2023]
[17] Gattacker, "A Node.js package for BLE (Bluetooth Low Energy) Man-in-the-Middle & more". [retrieved: August,2023]
[18] G. Kwon, J. Kim, J. Noh, and S. Cho, "Bluetooth low energy security vulnerability and improvement method," IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), Seoul, Korea (South), pp. 1-4, 2016. Doi: 10.1109/ICCE-Asia.2016.7804832
[19] Rosa, "Bypassing passkey authentication in Bluetooth low energy", 2013. [retrieved: August, 2023]
[20] C. Gomez, J. Oller, and J. Paradells, "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology Sensors," Sensors 12, no. 9, pp. 11734-11753, 2012 Doi: https://doi.org/10.3390/s120911734
[21] T. Martin, M. Hsiao, Dong Ha, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," Second IEEE Annual Conference on Pervasive Computing and Communications, pp. 309-318, 2004. Doi: 10.1109/PERCOM.2004.1276868
[22] J. Uher, R. G. Mennecke and B. S. Farroha, "Denial of Sleep attacks in Bluetooth Low Energy wireless sensor networks," MILCOM IEEE Military Communications Conference, Baltimore, MD, USA, pp. 1231-1236, 2016, Doi: 10.1109/MILCOM.2016.7795499
[23] D. Cauquil, "You'd better secure your BLE devices, or we'll kick your butts!". [retrieved: August, 2023]
[24] A. Ray, V. Raj, M. Oriol, A. Monot and S. Obermeier, "Bluetooth Low Energy Devices Security Testing Framework," IEEE 11th International Conference on Software Testing, Verification and Validation (ICST), V¨aster˚as, Sweden, pp. 384-393, 2018. doi: 10.1109/ICST.2018.00045

References

[25] R. Nasim, "Security threats analysis in bluetooth-enabled mobile devices". arXiv:1206.1482
[26] C. Zuo, H. Wen, Z. Lin, and Y. Zhang, "Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps," in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 1469–1483, 2019. Doi: https://doi.org/10.1145/3319535.3354240
[27] C. Herfurt, C. Martin and C. Mulliner, "Remote Device Identification based on Bluetooth Fingerprinting Techniques". [retrieved: August, 2023]
[28] P. Lloyd, "Blue Tracking". [retrieved: August, 2023]
[29] T. Claverie and J. L. Esteves, "BlueMirror: Reflections on Bluetooth Pairing and Provisioning Protocols," 2021 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2021, pp. 339-351, Doi: 10.1109/SPW53761.2021.00054
[30] BLURtooth: "Exploiting cross-transport key derivation in Bluetooth Classic and Bluetooth Low Energy", arXiv:2009.11776
[31] Swentooth, Unleashing Mayhem over Bluetooth Low Energy. [retrieved: August, 2023]
[32] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," in IEEE Pervasive Computing, vol. 7, no. 1, pp. 30-39, 2008. Doi : 10.1109/MPRV.2008.16
[33] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human SCADA system," in Black Hat Conference Presentation Slides. [retrieved: August, 2023]
[34] M. Rahman, B. Carbunar, and M. Banik, "Fit and vulnerable: Attacks and defenses for a health monitoring device," in Proceedings of the 6th Workshop on Hot Topics in Privacy Enhancing Technologies. arXiv 2013, arXiv:1304.5672
[35] Y. Park, Y. Son, H. Shin, D. Kim, and Y. Kim, "This ain't your dose: Sensor spoofing attack on medical infusion pump," in Proceedings of the 10th USENIX Workshop on Offensive Technologies. [retrieved: August, 2023]
[36] S. S. Hassan, S. D. Bibon, M. S. Hossain, and M. Atiquzzaman, "Security threats in bluetooth technology," Comput. Secur. pp. 308–322, 2018. Doi: 10.1016/j.cose.2017.03.008
[37] S. Shrestha, E. Irby, R. Thapa, and S. Das, "A Systematic Literature Review of Bluetooth Security Threats and Mitigation Measures," in Computer and Information Science, vol 1403, pp. 108–127, 2022. Doi: https://doi.org/10.1007/978-3-030-93956-4 7
[38] M. Yaseen et al. "A Novel Framework for Detecting MiTM Attacks in eHealthcare BLE Systems," Journal of Medical Systems vol 43, p. 324, 2019. Doi: https://doi.org/10.1007/s10916-019-1440-0
[39] G. A. Zendehdel, R. Kaur, I. Chopra, N. Stakhanova, and E. Scheme, "Automated Security Assessment Framework for Wearable BLE-enabled Health Monitoring Devices," ACM Trans. Internet Technol, vol 22, no. 14, pp. 1-31, 2021. Doi: https://doi.org/10.1145/3448649
[40] W. Zhou and S. Piramuthu, "Security/privacy of wearable fitness tracking IoT devices," Proc. 9th Iberian Conf. Inf. Syst. Technol. (CISTI), pp. 1-5, 2014. Doi: 10.1109/CISTI.2014.6877073
[41] M. Rahman, B. Carbunar and M. Banik, "Fit and vulnerable: Attacks and defenses for a health monitoring device," Proc. IEEE Symp. Security Privacy, pp. 447-459, 2013. arXiv:1304.5672v1
[42] O. Arias, J. Wurm, K. Hoang and Y. Jin, "Privacy and security in Internet of Things and wearable devices," IEEE Trans. Multi-Scale Comput. Syst., vol. 1, no. 2, pp. 99-109, 2015. Doi: 10.1109/TMSCS.2015.2498605
[43] H. Wang, T. T.-T. Lai and R. R. Choudhury, "MoLe: Motion leaks through smartwatch sensors," Proc. 21st Annu. Int. Conf. Mobile Comput. Netw., pp. 155-166, 2015. Doi: https://doi.org/10.1145/2789168.2790121
[44] M. Kijewski, "The Medical Devices Most Vulnerable to Hackers". [retrieved: August, 2023]
[45] J. Seo, K. Cho, W. Cho, G. Park, and K. Han, "A discovery scheme based on carrier sensing in self-organizing Bluetooth Low Energy networks," Journal of Network and Computer Applications, vol 65, pp. 72-83, 2016. Doi: https://doi.org/10.1016/j.jnca.2015.09.015
[46] J. Yang, C. Poellabauer, P. Mitra, and C. Neubecker, "Emerging applications and challenges of BLE," vol 97, 2020. Doi: https://doi.org/10.1016/j.adhoc.2019.102015
[47] "PoC hack on data sent between phones and smartwatches". [retrieved: August, 2023]
[48] "BlueBump Attack". [retrieved:August, 2023]
[49] E. Park, M. S. Lee, H. S. Kim, and S. Bahk, "AdaptaBLE: Adaptive control of data rate, transmission power, and connection interval in bluetooth low energy," Computer Networks, vol 181, 2020. Doi: https://doi.org/10.1016/j.comnet.2020.107520