2016 XI International Symposium on Telecommunications (BIHTEL)
October 24-26, 2016, Sarajevo, Bosnia and Herzegovina

Security Issues in Wireless Networks: An Overview

Sabina Baraković
AUBIH
Sarajevo, Bosnia and Herzegovina

Ena Kurtović, Olja Božanović, Anes Mirojević, Selmir Ljevaković, Aleksandar Jokić, Mladen Peranović
AUBIH
Sarajevo, Bosnia and Herzegovina

Jasmina Baraković Husić
Faculty for Electrical Engineering
University of Sarajevo
Sarajevo, Bosnia and Herzegovina

***Abstract*—Wireless mobile communication have grown dramatically in last decades. Due to increased usage of wireless mobile networks and communications in our everyday life, the society has become extremely exposed to cyber security attacks and threats in this environment. In order to provide a basis for further in detail discussion on attacks and security mechanisms in this challenging environment, this paper provides a brief overview of security issues, i.e., attacks, vulnerabilities, and threats in wireless networks. Based on the review, it may be concluded that future steps in this domain should include in detail investigation of security issues in all addressed networks and their categorization in a unified manner, either by the place they occur, network level, type of damage they cause, security breach level, etc., accompanied by the description of proposed classes.**

Keywords—issues, networks, overview, security, wireless

I. Introduction

Throughout the last decades wireless mobile networks and communications have experienced phenomenal growth, going from circuit switched voice and messaging services to Internet Protocol (IP)-based mobile broadband services [1]. By being used for delivery of wide spectrum of services and applications in daily activities, these networks have completely changed the lives of people reflecting in the way they obtain information, communicate, entertain, etc. In other words, wireless mobile networks have realized end users' requirements and expectations to be "always on", i.e., to access a wide variety of services anytime, anywhere, via multiple devices, and variety of networks [2], [3]. According to the latest statistics given by [4], the number of mobile subscribers has reached more than 7 billion worldwide and in December 2015 it counted for 25% [5] of all Internet users. On the other hand, the fact that our data is being more frequently transmitted via wireless mobile networks consequently leads to increased number of wireless mobile users being the victims of illicit cyber-criminal activities which causes many loses, either in data, money, or lives. All this combined with the variable and open nature of wireless mobile networks, reflecting in unstable transmitting medium, limited computation power, battery resources, etc., makes design and implementation of security mechanisms extremely challenging. However, before going into further in detail discussion on applications, technologies, and standards for securing wireless environment, an overview of security challenges in these networks, where each has its own unique characteristics, must be given. Therefore, this paper contributes by providing a brief survey of security issues, i.e., attacks, vulnerabilities, and threats in wireless networks ranging from cellular networks (2G – 5G), over Wireless Local Area Networks (WLANs), Worldwide Interoperability for Microwave Access (WiMAX) networks, Bluetooth networks, Vehicular Ad Hoc Networks (VANETs), Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs), to Radio Frequency Identification (RFID). The paper is organized in a way that each section (II-XII) addresses security issues in one of the aforementioned surveyed networks, while section XIII concludes the review and stresses the future research steps.

II. Security Issues in 2G Networks

The 2nd generation (2G) network provides are terminal mobility, the possibility for users to roam seamlessly, and the separation of the user identity from the terminal phone equipment. Security vulnerabilities in 2G networks include: (i) the obscurity, meaning that none of the security algorithms used by GSM is available to the public, (ii) provision of access security only, (iii) weak and difficult to upgrade cryptographic mechanisms, (iv) mobile subscriber visibility missing, and (v) authentication of user to the network and not vice versa [6]. In addition, there are two classes of security requirements for 2G networks: for mobile user's privacy and data integrity protection.

The most common types of attacks and vulnerability exploits in these types of networks are [6]:

- GSM security flaws - no authentication of the network is provided to the end user; vulnerabilities in the subscriber identity confidentiality mechanism;
- Impersonation attacks - the attacker tends to impersonate a legitimate user for conducting an attack;
- The attack gains anonymity - the attacker gains information on the users habits, calling patterns, etc., which can be used against the end user;
- The attacks against confidentiality - the attacker uses weaknesses in the GSM architecture, flaws in the protocols between the GSM networks and the end user; major attacks of the type are brute force attacks, cryptanalysis based attacks, and non-cryptanalysis attacks;
- Denial of Service (DoS) attacks - the attacker floods the network to disable the end users to access the network either by performing the attack using physical or logical intervention.

978-1-5090-2902-0/16/$31.00 ©2016 IEEE

III. Security in 3G Networks

The 3rd generation (3G) proposal for cellular communications aimed at providing global roaming for mobile users, high transmission bandwidths, and protection to sophisticated services such as the global positioning systems and multimedia on the demand of mobile users. There are several classifications of security issues in 3G networks based on different parameters, as given in Table I, which are in detail described in [6], [7].

IV. Security Issues in LTE Networks

The 4th generation (4G) is considered as next generation of wireless technology which brings momentous advances in data rates over the previous wireless technologies. The design relies on expectations to support broadband performance and enable voice/multimedia applications. Due to the fact that the 4G wireless technologies are intended to operate entirely on the IP architecture and suite of protocols, it increases consequences regarding the security issues. Long Term Evolution (LTE) is one of the technologies that are considered to achieve the 4G wireless performance objectives [8], [9]. In this section, security issues in LTE are presented in Table II.

V. Security Issues in 5G Networks

The 5th generation (5G) technology is the newest phase of mobile telecommunication which aims to provide a fully connected mobile society featuring high transmission speeds. Some of the 5G features have been announced and presented,

TABLE I. SECURITY ISSUES IN 3G NETWORKS

Type of issue	Description of the issue
Classification based on the attack type	
Interception	The attacker intercepts information or reads signalling messages, but does not modify or delete them. Such attacks affect the privacy of the subscriber and the network operator.
Fabrication/Replay	The attacker may insert spurious objects into the system that depend on the target means and physical access type (e.g., signalling messages, fake service logic, or fake subscriber data).
Modification of resources	The attacker causes damage by modifying system resources.
DoS attacks	The attacker causes an overload or a disruption in the resources or applications connected to the 3G system, forcing the network to operate in an abnormal manner which reflects in a subscriber not receiving service or the entire network to be disabled.
Interruption	The attacker causes an interruption of operation by destroying resources (e.g., delete signalling messages, subscriber data, stop delivery, etc.).
Classification based on means used to cause the attack	
Data-based attacks	The attacker targets the data stored in the 3G communication system and causes the damage by modifying, inserting, and/or dropping the data stored in the system.
Messages-based attacks	The attacker targets the 3G system by inserting, modifying, replaying, and dropping the signalling messages flowing to and from the network.
Service Logic attacks	The attacker causes important damages by simply attacking the service logic running in the various 3G network entities.
Classification based on the level of physical access the attacker has	
Class I	The attacker obtains access to the air interface using a physical device and use modified mobile stations to broadcast at a high frequency, eavesdrop, and execute man-in-the-middle attacks.
Class II	The attacker obtains access to the cables connecting the 3G network switches and may cause considerable damage by disrupting the normal transmission of signalling messages.
Class III	The attacker has access to some sensitive components of the 3G network and can cause important impairments by editing the service logic or modifying the subscriber data stored in the 3G network entity.
Class IV	The attacker has access to links connecting the Internet to the 3G network and can cause a certain harm by disrupting the transmission of signalling messages flowing between the link and inserting some signalling messages into the link between the two networks.
Class V	The attacker has access to Internet servers or cross network servers providing services to mobile subscribers connected to the 3G network and can cause harmful damage by editing the service logic or modifying subscriber data (profile, security, and services) stored in the cross network servers.
Unauthorized access to sensitive data (violation of confidentiality)	
Eavesdropping	The attacker intercepts messages without detection.
Masquerading	The attacker hoaxes an authorized user into believing that they are the legitimate system to obtain confidential information from the user.
Traffic analysis	The attacker observes the time, rate, length, source, and destination of messages to determine user's location or to learn whether an important business transaction is taking place.
Browsing	The attacker searches data storage for sensitive information.
Leakage	The attacker obtains sensitive information by exploiting processes with legitimate access to the data.
Inference	The attacker observes a reaction from a system by sending a query or signal to the system.
Unauthorized manipulation of sensitive data (violation of integrity)	
Manipulation of messages	Messages may be deliberately modified, inserted, replayed, or deleted by the attacker.
Disturbing or misusing network services (leading to DoS attack or reduced availability)	
Intervention	The attacker may prevent an authorized user from using a service by jamming the user's traffic, signalling, or control data.
Resource exhaustion	The attacker may prevent an authorized user from using a service by overloading the service.
Misuse of privileges	A user or a serving network may exploit their privileges to obtain unauthorized services or information.
Abuse of services	The attacker may abuse some special service or facility to gain an advantage or to cause disruption to the network.
Unauthorized access to services	
Intruders can access services by masquerading as users or network entities.	
Users or network entities can get unauthorized access to services by misusing their access rights.	

TABLE II. SECURITY ISSUES IN LTE

Type of issue	Description of the issue
Physical Layer Issues	
Interference	The attacker deliberately inserts man-made interference onto a medium that causes communication system to stop functioning due to the high signal to noise ratio.
Scrambling	The form of interference which is activated for short time intervals. It is targeted at the specific frame od parts of frames, i.e., management or control information in order to disrupt a service. This attack is very difficult to launch successfully.
Media Access Layer (MAC) Layer Issues	
Location tracking	The attacker tracks the presence of user equipment in a particular cell or across multiple cells, and although it does not represent a direct security threat, it definitely is a security breach in the network which can be viewed as potential threat.
Bandwidth stealing	The attacker achieves the attack by inserting messages during the Discontinuous Reception (DRX) period or by utilizing fake buffer status reports.
Security issues due to open architecture	Due to the fact that LTE networks are IP networks with a large number of devices with highly mobile and dynamic activities, diversity in these devices and open architecture of an IP-based LTE is resulting in increasing number of security threats.
DoS attacks	Carried out against specific user equipment, where malicious radio listener can use the resource scheduling to send an uplink control signal at the scheduled time, causing some conflicts and service problems or achieved by utilizing DRX period, and thereby creating security hole and injecting packets and causing DoS attacks.
Security Issues at Higher Layers	
The departure from proprietary operating systems for handheld devices to open and standardized operating systems and the open nature of the network architecture and protocols results in increasing number of potential security threats to the LTE wireless network and makes it vulnerable to a wide range of security attacks including malwares, Trojans, and viruses.	

but the security threats and vulnerabilities will also arise with this technology. However, current security concerns regarding 5G are as follows [10]:

- 5G drivers - drivers for mobile networks, mainly used to improve the latency and throughput; in 5G are almost the same, but there are key factors which will be introduced with the 5G that may affect security;
- User identity and confidentiality - the security mechanisms in 5G have pretty much stayed the same as in 4G: they protect the user against passive attacks, but not the active ones;
- New trust models - 5G should as should be introducing new trust models for authentication, accountability and non-repudiation for capturing evolved usage scenarios;
- Security for new service delivery models - 5G will be using clouds computing and virtualization in order to optimize the service, thereby rising a new level of security concerns; when providers host 3rd party applications in their clouds, executing on the same hardware as their services, there will be increased demands on virtualization with strong security;
- Evolved threat landscape - the threat landscape will evolve as more technologies link; there already are some increased privacy concerns of mass surveillance that users speculate about; the damage may be even more severe and could affect even public safety;
- 5G radio network security - the bigger threat space and new low-cost technology leads to more attacks to the radio network; LTE provides a decent cryptography mechanism for protection against eavesdropping attacks, but there is no protection against modifying or injecting user traffic;
- Cloud security and virtualization - cloud security is extremely important and could be resolved by developing network virtualization with high level of isolation and building a useful ecosystem that should provide more effective alternatives for cloud encryption; 5G should consider a more flexible security in regard to the virtualization as well.

VI. Security Issues in WLAN

The WLAN is one of the most frequently used wireless technologies nowadays which offers many advantages and features to be exploited. However, it is very vulnerable to different kinds of attacks which can result in different consequences. Some of the most known attacks include: DoS and man-in-the-middle attacks, message modification and injection, packet sniffing, etc., and may be categorized as given in Table III [6], [11]. Although WLANs may have different infrastructure and support different applications, and as any other wireless network, each require the following when it comes to security: (i) confidentiality, (ii) authentication, (iii) access control, (iv) integrity, and (v) intrusion detection and prevention.

VII. Security Issues in WiMAX

The WiMAX is a Wireless Metropolitan Area Network (WMAN) communication technology using the IEEE 802.16 standard. The connection security in WiMAX is accomplished by complying with the Privacy Key Management Protocol (PKM), which ensures the correct application of authentication algorithms and encryption. As any other wireless technology, WiMAX introduced several security risks, and one of the most common attacks, the Message Replay attack, which is targeting the authentication and key formation protocols [12]:

- If messages exchanged within an authentication protocol do not have updated identifiers, an attacker can replay messages copied from a legitimate authentication session. Due to the short 2-bit Transport Encryption Key (TEK), which repeats every four rekey cycles, an attacker can easily become authenticated.
- Man-in-the-middle attacks are associated with the PKMv1 protocol, where mutual authentication was missing.

TABLE III. SECURITY ISSUES IN WLANs

Type of issue	Description of the issue
Deauthentication	The attacker attempts to defeat the authorization mechanism in WLANs and thereby steal legitimate wireless users' identities, or authorized wireless access points' deployment rights, or deploy rogue access points without going through security process and review. Attacks that fall into this category are: (i) MAC spoofing – the attacker bypasses the MAC filtering policies by modifying the MAC address of a wireless client; (ii) IP spoofing – the attacker can evade IP address based authentication and present itself as legitimate user by modifying the source IP address of the one; (iii) rogue access points – the attacker can gain open access to WLAN by deploying unauthorized access points.
Eavesdropping and interception	The attacker may eavesdrop or intercept legitimate wireless traffic by compromising legitimate users' wireless communication channel, thereby accessing to all information sent by the user. Attacks that fall into this category are: (i) Traffic eavesdropping – the attacker utilizes the network sniffer to eavesdrop the traffic in whole WLAN; (ii) Man-in-the-middle – the attacker obtains, intercepts, modify, and impersonate the communication between sender and receiver who believe to have secure channel by sitting in the middle of the two-way communicating parties; (iii) Network injection – the attacker injects bogus network traffic into legitimate traffic and achieves malicious goals; (iv) Session hijacking – the attacker steals a legitimate authenticated conversation session ID and controls the session.
Traffic jamming	The attacker heavily consumes the bandwidth of the WLAN to overwhelm the legitimate traffic by flooding the messages or high radio frequency signals. Attacks that fall into this category are: (i) DoS attacks – the attacker disrupts legitimate traffic to reach the destination by flooding the high frequency radio signals or messages; (ii) Spam attacks – the attacker launches spam attacks by flooding spam messages over the wireless channels.
Brute force attacks against access point passwords	The attacker brute forces dictionary attacks to compromise the single shared password of an access point by testing every possible password.
Attacks agains security protocols	The attacker compromises the vulnerabilities of Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) security protocols.
Misconfiguration	The attacker exploits limited security knowledge of the WLAN administrator, human misconfigurations, or improper operations to the access point.

Some other attacks occur due to the IEEE 802.16 protocol stack organization. Since the physical layer resides just below the privacy sub-layer, in which most of the WiMAX's security mechanisms are implemented, WiMAX is vulnerable to the physical layer attacks such as [13]:

- Jamming - presenting a strong Radio Frequency (RF) noise source to significantly reduce channel bandwidth, resulting in DoS;
- Scrambling - requires more precise RF injections in short time periods during the transmission of specific messages;
- Water torture - an attacker sends series of frames to drain the receiver's battery.

Impersonation attacks are also a threat in WiMAX [14]:

- Identity theft - reprogramming a device by replacing its hardware address with a stolen legitimate one that may be intercepted in management messages. Management messages are unencrypted in WiMAX;
- Rogue Base Station (BS) attack - A rogue BS transmits signals at the same time the real BS does, but with more power. When a Mobile Station (MS) attempts to get service, it can be tricked into sending confidential information to the Rogue Station, which results in eavesdropping, replay, or scrambling attacks.

Other known attacks include: (i) parallel session, (ii) DoS, (iii) reflection, (iv) interleaving attacks, (v) attacks due to type flaw, (vi) name omission attacks, and (vii) attacks due to misuse of cryptographic services.

VIII. Security Issues in Bluetooth Networks

Bluetooth is a wireless technology that uses ad hoc architecture and allows the creation and usage of temporary networks and, just like any other wireless technology, it has its security flaws as well [11], [14]. Old versions of Bluetooth had a flaw which included the Unit Key which could be reused to become public. This way a hacker could perform an eavesdropping. All versions before 1.2 were vulnerable, but later, for the versions up to 2.1 the Personal Identification Number (PIN) was the vulnerability. Vulnerabilities of later Bluetooth versions include: (i) keys (keys were not saved as properly, shared master key, only 256 different keys), (ii) authentication (no user authentication except in apps, (iii) cryptography (weak cipher algorithm), (iv) privacy (user data may be compromised), and (v) security services (no end to end security, no audit). Some of the most common attacks are described further:

- Bluejacking - happens because of misusing and bypassing the device pairing procedure due to which the attacker can send a message to any device in the range;
- Bluesnarfing - the attacker exploits a victim by using a firmware flaw initiating a connection without an alert, and thereby gains access to the phone data, directories, phone number, etc.;
- Bluebugging - the attacker gains full access to the device, including data, call logs, and other services;
- Car Whisperer - a software that allows the attacker to transmit audio to the car speakers, as well as receive audio from the microphone;
- DoS attacks - the attacker can initiate sending a large number of unsolicited messages in order to make the freeze or to drain device's battery.

IX. Security Issues in VANETs

Vehicles Access Network

The VANETs are specific type of wireless networks in constant growth. The major specification of these types of short range wireless networks is that they are directly involved in protecting human lives through the safety applications and services implemented which leads to the fact that they have to be extra safe for the end users. Based on the types of attacks in VANETs, we can divide issues into classes presented in Table IV [15], [16].

TABLE IV. SECURITY ISSUES IN VANETS

Type of issue	Description of the issue
Class I (the ones on the network)	
Sybil attack	The attacker sends multiple messages to other vehicles and each message contains different fabricated source identity (ID).
Node impersonation attack	Each vehicle has a unique identifier in VANET and it is used to verify the message whenever an accident happens by sending wrong messages to other vehicles.
Class II (the ones attacking the applications that are running on the network)	
Traffic application attacks	The attackers change the content of the actual message and send wrong or fake messages to other vehicles which in the end cause an accident.
Bogus information attack	The attacker sends wrong information to the network and these wrong messages directly affect the behaviour of users on the road.
The NON-safety applications	These applications are concerned with the comfort of the passenger, rather than providing vital security information.
The third class of issues	
Time attacks	The main goal of this class of attacks is to create a delay in the message you receive as a regular user of the VANET.
The fourth class of attacks	
Social attacks	An attacker in these types of attacks impersonates one of the users while sending an offensive message to any other user.
The fifth class of attacks	
Monitoring or sniffing attacks	Very similar to classic sniffing attacks, the attacker listens to the communication on a VANET. The information gathered is used for malicious intentions.

X. SECURITY ISSUES IN WMN

Wireless machine networks

The WMN is an emerging technology which in a past few years has significantly developed. WMN's main characteristic is that there are only one or several nodes which are connected to the infrastructure network as the gateway, while other nodes are connected through relay of the neighbouring nodes, and afterwards to the Internet. Due to its wireless and multi-hop nature, the security vulnerabilities have become a major problem. Following text discusses some of the most common and most relevant vulnerabilities represented in WMN [14].

For example, the risk in WMN can be the absence of physical protection of the mesh stations which leads to **compromised mesh stations** (battlefield, army). Such event may trigger consequences, such as: (i) leakage of top secrets, keys or any other information in transit, (ii) disappearance of mesh point from the network, (iii) the attacker can reroute the mesh point, or (iv) the mesh point could be a subject of cloning so it can be used for future attacks.

Threats and attacks related to routing are present in WMNs given that these networks rely on multi-hop routing. The routing has to be made vigorous and secure, while routing information should be exchanged with an efficient protection. Received routing messages need to be authenticated and validated to be sure that they come from a trusted mesh point. Their integrity also needs to be checked to make sure that they are not modified during the transmission. In addition, **DoS attacks** performed at different layers (e.g., jamming at physical layer) are another vulnerability of WMNs. Further on, **wormholes, grey, and black holes** are vulnerabilities performed with intention to re-direct network traffic to attacker's mesh nodes. The most damaging attack out of these three is the wormhole attack where the attacker can modify the routing settings in order to initiate a number of DoS attacks later on [14].

XI. SECURITY ISSUES IN WSN

Wireless sense network

The WSN is defined as a wireless network that consists of spatially distributed autonomous devices that are using sensors in order to monitor physical or environmental conditions. Providing security in WSN is defined as a great challenge due to the factors, such as: large scale deployment, extremely limited resources of sensor nodes, dynamic network topology, lack of global identification, etc. Since WSN represents a special type of a network, while still sharing some similarities with an ad hoc network, it can be deduced that the requirements of WSN obtain the typical network requirements and the unique ones that are suited for wireless sensor networks, such as [6]: (i) data confidentiality, (ii) data integrity, (iii) data freshness, (iv) availability, (v) self-organization, (vi) authentication, (vii) social attacks, (viii) key distribution, (ix) time synchronization, and (x) secure localization. The security issues in WSN can be classified by different layers and are presented below in the Table V [14], [17], [18], [19].

TABLE V. SECURITY ISSUES IN WSNS

Type of issue	Description of the issue
Physical Layer Attacks	
Jamming	Emission of radio signals with the aim of disturbing the transceivers operation.
Tampering	The attacker can temper with node physically and compromise them.
Link Layer Attacks	
Collision	The attacker can cause a lot of disruptions to the network operations.
Unfairness	The attacker can cause a lot of disruptions to the network operations.
Exhaustion	This represents the active type of an attack and it can culminate in nearby nodes when the battery resources were exhausted.
Network and Routing Layer Attacks	
Selective forwarding	This attack leads to disruption of an existing connection between two end points, where attacker can forge the messages between end points, causing the end points to request retransmission of missed frames.
Sybil attack	Malicious nodes are faking multiple legal node IDs, while behaving like legitimate one and providing such an environment where it can modify, selectively discard or forge packets or even eavesdrop on passing data flow.
Sinkhole attack	The attackers aim to mislead all the traffic from the particular area through a compromised node, metaphorically creating a sinkhole with the adversary at the centre.
Wormhole attack	Two malicious nodes are connected with a link (wormhole link) which provides to attacker ability to capture data transmissions on one node and send them through the wormhole link to the other node.
HELLO Flooding	Malicious nodes broadcast HELLO packets to the neighbouring nodes by luring them to establish routes passing them.
Transport Layer Attacks	
Flooding	The attacker sends many connection establishment requests and in such a way, in order to maintain the state for each connection, he forces the victim to allocate memory.
Desynchro-nization	This attack leads to disruption of an existing connection between two end points, where attacker can forge the messages between end points, causing the end points to request retransmission of missed frames.

XII. Security Issues in RFID

The beginnings of RFID networks go back to the period just after the World War II in context of development of spying devices that are powered by outer energy source. RFID architecture is composed of three elements: RFID tags, readers and backend servers. This technology is frequently used today and is very important to assess it in regards to the security issues. Following bulletins address security attacks in RFID [14]:

- Unauthorized access - to prevent it, security engineers must address two attack patterns: (i) by design, RFID tag will respond to every query, and (ii) attacker's sniffing over the air communication with the radio equipment;
- Illicit tracking - represents data and object privacy issue in which it is not questioned if the answer from the tag is valued for the attacker, but if the tag can be tracked in time and space;
- Skimming - in RFID terms means capturing legitimate information stored on the tag and then replaying the information back to the reader; it can also be considered as multi-layered attack since the collection data (form tag) can occur by multiple means;
- Mafia fraud - a man-in-the-middle attack where the genuine reader interacts with a rogue card that manages to fool the reader into thinking that it is directly communicating with the genuine card [11];
- Grouping proofs - the challenge related to advanced tag operations;
- RFID malware - RFID tag can observe as an input interface to the backend computer systems that have applications and databases, deliver malware to the system and cause problems to whole organization;
- DoS attacks - the attack can be performed on the RFID system on various ways, but although the complexity of attack is easy and consequences serious the like hood of happening is low.

XIII. Conclusion and Future Work

The contribution of this paper is the brief addressing of security issues, i.e., attacks, threats, and vulnerabilities in wireless mobile networks, thereby covering cellular networks, WLANs, WMANs, WMNs, VANETs, Bluetooth, WSNs, and RFID networks and communications. After surveying this challenging and contemporary topic, which, for the importance of its effects on our daily lives and future, requires more in detail and comprehensive approach, conclusion is that the subject wireless networks share susceptibility to the several same types of attacks, threats, or vulnerabilities, such as: DoS, eavesdropping, interception, etc., and at the same time are subjected to security issues characteristic for them only due to their specific nature (e.g., WSN, VANETs, etc.). Also, although each of them has its own characteristics in terms of architecture and security issues (besides common ones, e.g., wireless medium, DoS attacks, etc.), they typically have the same set of security needs reflecting in requests for mutual authentication, integrity, and confidentiality. However, a variety of unique characteristics and specific applications of addressed wireless networks make design and implementation of unique security algorithms, mechanisms, and protocols extremely challenging and difficult. This causes having multiple and different security mechanisms in these networks, which in the end causes other security problems in emerging "all-connected" and "always-on" environment. The few first steps in future work towards resolving these issues and easing the work on unique and effective security mechanisms in wireless environment, should include in detail investigation of security issues in all addressed networks and their categorization in a unified manner, either by the place they occur, network level, type of damage they cause, security breach level, etc., accompanied by the description of proposed classes. This would provide a useful input for research community and industry dealing with security mechanisms.

References

[1] S. Baraković and L. Skorin-Kapov, "Survey and Challenges of QoE Management Issues in Wireless Networks," Journal of Computer Networks and Communications, Article ID 165146, 2013.

[2] S. Baraković and L. Skorin-Kapov, "Multidimensional Modelling of Quality of Experience for Mobile Web Browsing," Computers in Human Behaviour, vol. 50, pp. 314-332, 2015.

[3] S. Baraković and J. Baraković Husić, ""We Have Problems for Solutions": The State of Cybersecurity in Bosnia and Herzegovina," Information&Security: An International Journal, vol. 32, pp. 131-154, 2015.

[4] ITU, "The World in 2015: ICT Facts and Figures," 2015.

[5] Netmarketshare, "Browsing by Device Category Trend," 2015.

[6] N. Boudriga, Security of Mobile Communications. Taylor and Frances Group, 2010.

[7] ETSI TS 121 133 V3.1.0, "Universal Mobile Telecommunications System (UMTS); 3G Security; Security Threats and Requirements," 2000.

[8] S.K. Mohapatra, et al. "Comprehensive Survey of Possible Security Issues on 4G Networks," International Journal of Network Security & Its Applications (IJNSA), vol. 7, no. 2, 2015.

[9] N. Seddigh, et al., "Security Advances and Challenges in 4G Wireless Networks," 8th Annual International Conference on Privacy, Security and Trust, 2010.

[10] Ericsson, "5G Security Scenarios and Solutions," Whitepaper, 2015.

[11] H. Chaouchi and M. Laurent-Maknavicius, Wireless and Mobile Network Security. Wiley, 2007.

[12] M. Ginley, et al., "Efficient and Secure Multicast in Wireless MAN," 2nd International Syposium on Wireless Pervasive Computing, ISWPC'07, 2007.

[13] S.Y. Tang, P. Muller, and H.R. Sharif, "WiMAX Security Defined in 802.16 Standards," WiMAY Security and Quality of Service: An End-to-End Perspective. John Wiley & Sons, 2010.

[14] L. Chen, J. Ji, and Z. Zhang, Wireless Network Security: Theories and Applications. Springer, 2013.

[15] I.A. Sumra, et. al. "Classes of attacks in VANETs," Saudi International Electronics, Communications and Photonics Conference, SIECPC, 2011.

[16] W: Liang, et al., "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends," International Journal of Distributed Sensor Networks, Article ID 745303, 2015.

[17] S. Mohammadi and H. Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks," International journal on applications of graph theory in wireless ad hoc networks and sensor networks, GRAPH-HOC, vol. 3, no. 1, pp. 35-56, 2011.

[18] H. Soleman, et al., "Detection Collision Attacks in Wireless Sensor Network Usingrule-Based Packet Flow Rate," International Journal of Engineering Research and Applications, IJERA, vol. 3, no. 4, pp. 261-268, 2013.

[19] P. Sharma, M. Saluja, and K. Kumar Saluja, "A Review of Selective Forwarding Attacks in Wireless Sensor Networks," International Journal of Advanced Smart Sensor Network Systems, IJASSN, vol. 2, no. 3, 2012.