Security Threats Towards Cognitive Radio in 4G LTE-Advanced Network: A Review

Gohar Mumtaz[1], Faisal Nawaz Khan[2], M. Junaid Arshad[3] and Yasir Saleem[4]

[1-4]Department of Computer Science & Engineering, University of Engineering & Technology, Lahore, Pakistan

[1]goharmumtaz@ymail.com, [2]faysalkhaan@live.com, [3]mjunaiduet@gmail.com, [4]ysaleem@gmail.com

***Abstract*— With the rapid growth in the advancement of technology, 4G LTE-Advanced using MIMO and OFDMA techniques, is being capable of providing high data rate and minimum delay but for the better efficiency and usage of wasted spectrum, Cognitive Radio (CR) is novel technology for spectrum regulation and management. In this paper, CR technology with 4G LTE-Advanced is summarized, followed by in depth analysis of security threats and possible counter measures towards the implementation of CR with 4G LTE-Advanced network, to ensure basic security concepts known as CIA triad. Furthermore, Security threats and their counter measures towards CRN, with respect to OSI layers are tabulated for new researchers.**

***Keywords*— 4G LTE-Advanced, MIMO, OFDMA, CR, CIA Triad, and OSI layers**

I. INTRODUCTION

The future concept of the world is a network society with unlimited access and sharing of resources to everyone, everywhere, at any time. For this concept, technology is being improved day by day which will be helpful to accomplish future needs [1].

4G LTE (Long term Evolution) [7] with MIMO [9]-OFDM [11] technique, exceedingly speeds up the network`s capacity with enhanced user `s experience. Moreover, for fully enhance features of 4G system, IMT Advanced introduced by ITU-T, with advance technical specifications like carrier`s aggregation, relaying, multi-point transmission (LTE-Advanced) [2]. It is basically the extension in 3G with some features like minimum delay, High data rate and packet switched network. Technical requirements of LTE Advanced are shown in Table I.

TABLE I
TECHNICAL REQUIREMENTS OF LTE-ADVANCED NETWORK

No.	Technicalities	Requirements of 4G LTE-Advanced
1	Downlink	3 Gbps [5]
2	Uplink	1.5 Gbps [5]
3	Bandwidth	100 MHz
4	Latency	10 ms
5	Access Method	OFDMA
6	Propagation	MIMO

There is no wireless telecommunication without the use of spectrum [3]. With the advancement of 4G, We are being capable of having high data rate minimum delay, but the use of spectrum is inefficient. There is huge popular demand of spectrum but there is unused spectrum as well. To overcome this wastage of spectrum, Cognitive Radio technology is being popular now a days because it is not only radio technology but also has the capability to regulate the spectrum.

In wireless telecommunication, right of spectrum means license [4]. Licensee is primary user (PU), high-priority and licensed. Cognitive Radio user is unlicensed or secondary user (SU). SU first sense the holes or unused spectrum and then employ it, as shown in Fig. 1. SU is intelligent enough that it can sense the spectrum very intelligently. The main objectives of the CR technology are improvement in utilization of Spectrum and to achieve high reliability in wireless telecommunication system. The main advantage of the CR technology is; its aware from environment of surroundings and takes decision on basis of surrounding environment.

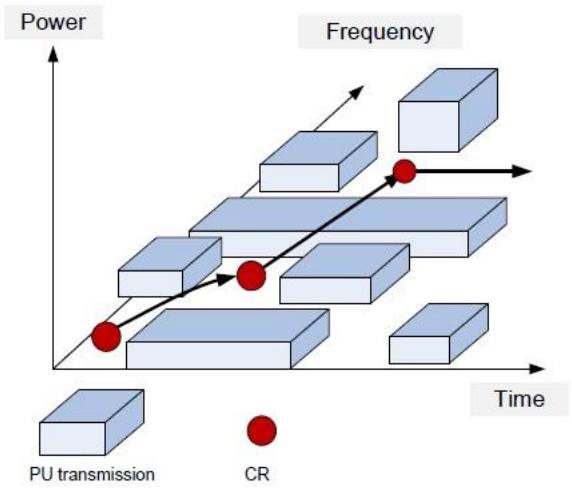

Fig. 1: Cognitive Radio (CR) concept

To use spectrum efficiently, CR is very advanced tool to use with 4G LTE-Advanced. As CR and 4G LTE-Advanced both are wireless technologies, so there is lots of security attacks which needs to be known and resolved. In this review paper, we briefly discuss CR Technology, spectrum sensing

techniques, 4G LTE-Advanced and all security threats and possible counter measures, currently encountered by CR with 4G LTE-Advanced Network, on the basis of OSI layers (Open System Interconnection), from Physical layer to Transport layer [6], to ensure three concepts of Network Security, referred as CIA triad (Confidentiality, Integrity and Availability).

In Section II, we discuss about the 4G LTE-advanced technology with MIMO feature. In Section III, we discuss motivation towards CR threats and importance of this novel technology in the context of LTE-Advanced in wireless telecommunications. In Section IV, we analyse with detail, all latest and vulnerable threats towards CR and also tabulated all threats layer wise with respect to OSI Model. In Section V, we summarize this research including threats and their countermeasures in tabular form. Section VI concludes this research and proposes future work.

II. 4G LTE-ADVANCED

4G LTE-Advanced is Wireless Broadband technology, a totally IP based cellular network communications. LTE-A efficiently reduce latency, uses proper carrier aggregation and 4X4 or higher MIMO configuration technology. LTE-A based upon Rel-10 of ITU provided Low Latency and carrier aggregation help multiple carrier`s transmission [7].

Higher peak of data rates is required by user. Audio/Video streaming, social media, online conferencing are basic necessities of today`s world. Growing need of wireless internet requires more efficient and workable solution of 3G or 3GPP. 4G-LTE (Long Term Evolution) Advance is the solution for wireless broadband service. It has been already introduced in modern world [7]. LTE is the latest standard in wireless technology and is considered as one of core technology that has account for 85 percent of mobile subscribes [8].

A. MIMO (Multiple-Input Multiple-Output) in LTE-A

MIMO Technology plays vital role by supporting multiple antennas on sender and receiver end, achieving 100 Mbps data download and 50 Mbps upload with 20 MHz bandwidth [9], [10]. LTE-Advanced aims to provide downlink up to 15bps/Mz by using MIMO 8X8 and 7bps/Mz uplink using MIMO 4X4 by increasing spectrum efficiency [11]. Previously MIMO used 2X2 antennas for mobile communication. LTE supports 4X4 antennas configuration for upload/download. Enhanced LTE supports up to 8X8 antennas configuration, as shown in Fig. 2, which enhance uplink and downlink throughput.

By using smart MIMO techniques 4X4 antennas configuration with 64 QAM, helps achieving proper upload download throughput as per standard for ITU [7]. Physical Layer in LTE-Advanced earlier suggested 2X1, 2X2 MIMO configuration antennas for better performance using OFDMA (Orthogonal-Frequency-Division-Multiple-Access) and SC-OFDMA (Single-Carrier-Orthogonal-Frequency-Division Multiple-Access) for download. The code provides high data rate without affecting diversity gain is Altamonte code used for 2X2 antennas configuration. MIMO configuration and coding/modulation scheme based on quality of channel as Signal-to-Noise Ratio (SNR) determines improves mobility information [9].

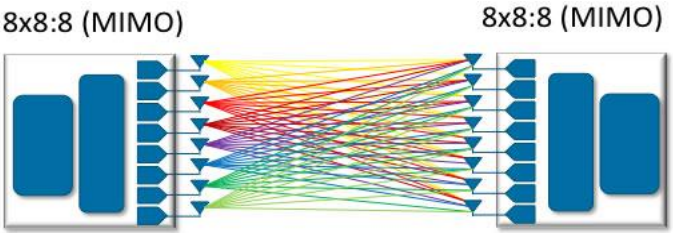

Fig. 2: MIMO System in 8 X 8 configuration [9]

III. MOTIVATION TOWARDS CR THREATS

Cognitive Radio, an approach towards implementation of Dynamic Spectrum Access (DSA) on Software Defined Radio (SDR). CR is an intelligent network consisting of Primary and Secondary users. Primary user (PU) is high-priority and licensed. Secondary user (SU) is unlicensed or also called Cognitive user. CR user first senses the holes or unused radio spectrum and then utilizes it [4]. A cognitive cycle is shown in Fig. 3.

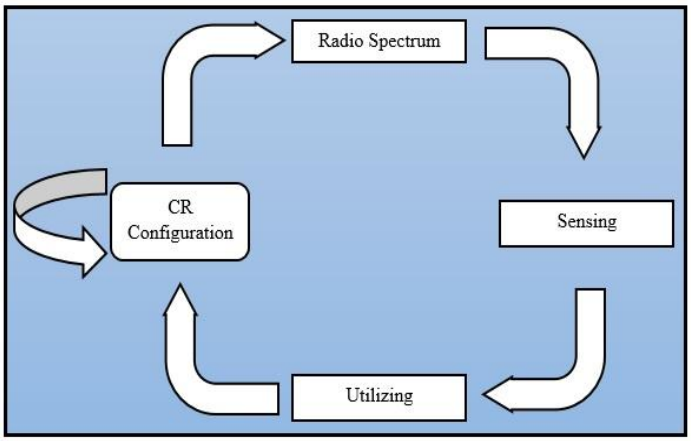

Fig. 3: Cognitive Cycle

Scare Radio Spectrum is precious resource that is being used with current fixed spectrum licensing policies. A secondary system is need a part from primary mobile communication that can Sense scare spectrum and dynamically use radio resources to meet mobile communications is known as Cognitive Radio Networks. Interference management of scare spectrum is essential for coexistence of primary and Cognitive Networks. System design involves spectrum sensing, spectrum management, resource management, MAC level signal processing (Interference Cancellation Techniques) [3].

Spectrum Licenses are controlled by Federal Communication Organizations, and provide right to use licensed wireless spectrum for different services to Primary

Users (PU). The licensed spectrums are being filling up by service providers and left very narrow bands unlicensed. Recent studies have concluded that 90% of the time large slots of licensed spectrum bands remain idle or unused. The need emerged to entertain Secondary Users (SU) without affecting PU and Licensed Spectrum, Cognitive Radio Technology emerged. Cognitive Radio – wireless devices by configuring hardware and software level (transmission parameters and protocol) – will be capable to deliver services to Secondary Users (SU). Careful sense technique for Primary Users (PU) presence and adapting their transmission to guarantee a specific performance, cognitive devices could improve spectral performance. Along this newfound flexibility come with challenge to understand limits, protocol design and transmission scheme to fully exploit cognitive capabilities [4].

As most of Mobile service providers already introduced and deployed LTE, LTE-A as their Next-Generation mobile system, the mobile traffic will keep increasing in foreseeable future. The Cognitive Radio (CR) will open the possibilities for reusing under-utilized spectrum resources [2].

A. *Functions of Cognitive Radio Networks*

1) CR Spectrum Sensing: Spectrum Sensing is fundamental objective of Cognitive Radio Network in LTE-A. CR Spectrum Sensing determines unused portions of the licensed spectrum availability and presence of licensed user. Spectrum Sensing Techniques are mentioned in below Figure 4. We discuss each Technique briefly.

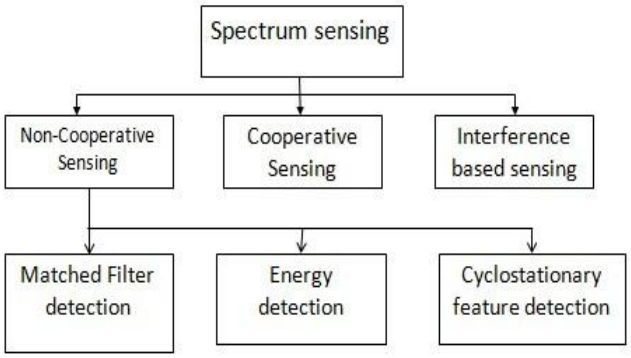

Fig. 4: Spectrum Sensing Techniques

- ***Non-cooperative or Transmitter Sensing:*** Non-Cooperative or Transmitter Sensing Techniques used on Receiver end to determine whether a signal generating from Primary Transmitter to be occur locally in available allotted spectrum. Some approaches are used for Transmitter Detection.

  i. Matched Filter Detection

  Matched Filter is type of linear filtration used for maximizing output SNR (signal to noise Ratio) for given signal(s). It's applied when priori knowledge of Primary User is known.

  ii. Energy filter Detection

  Energy Detection methods as name explains, based on sensed energy. Prior knowledge is not required for this sensing technique.

  iii. Cyclostationary Feature Detection

  Communication Signals like BPSK, QPSK, AM, OFDM, etc. have cyclostationary behaviour. The algorithms used to sense such signal patterns transmitted by Primary users.

- ***Cooperative Sensing:*** Cooperative Sensing Techniques are used when multiple CR Secondary users cooperates in sensing channel then we need higher sensitivity requirements.
  i. Centralized Coordinated
  ii. Decentralized Coordinated
  iii. Decentralized Uncoordinated
- ***Interference Based Sensing:*** Interference is typically regulated in a transmitter-centric way, because of this interference is controlled at the transmitter thru the radiated power, the out of band emission and location of individual transmitter. However, interference usually takes place at the receiver`s end.

2) CR Spectrum Decision: Cognitive Radio Network requires the functionality to pick the first-class channel in available spectral band according to QoS requirement and its application. Spectrum Decision mainly depends upon statistical characteristics of Primary network and observation of CR users. Some challenges are there for decision like: Decision Models, Reconfiguration of CR transmission parameters and Heterogeneous Spectrum band decision [12].

3) Spectrum sharing: Cognitive Radio Network shares its coordination with primary users and CR users. Spectrum sharing includes MAC Protocol functionality. Spectrum sharing in CR aims to address some challenges like: architecture, spectrum allocation pattern, access techniques, and its scope.

4) Spectrum Mobility: CR also maintains spectrum mobility of primary user on selected channel if its operating band is changed. Spectrum handoff – if CR user change its operating frequency, the network protocol should modify its operating parameters as well. Spectrum mobility in Cognitive Radio Network ensure smooth transition with affecting performance during spectral handoff. CR Network uses different layer protocols to adopt channel parameters of operating frequency band. Some challenges are there in CR network regarding spectrum mobility like: Spectrum mobility in space (location) and in time domain.

IV. THREATS TOWARDS COGNITIVE RADIO

Implementation of CR with 4G LTE-Advanced network is very vulnerable because of security threats towards CR. In CR network, there are some rules and some kind of agreement between PU and SU. Attackers or malicious users break their trust and also some users are not able to be relied as honest. So, for successful deployment of CR with LTE-Advanced

needs to be secure [13]. Fig. 5 shows different types of security threats which we discuss here one by one.

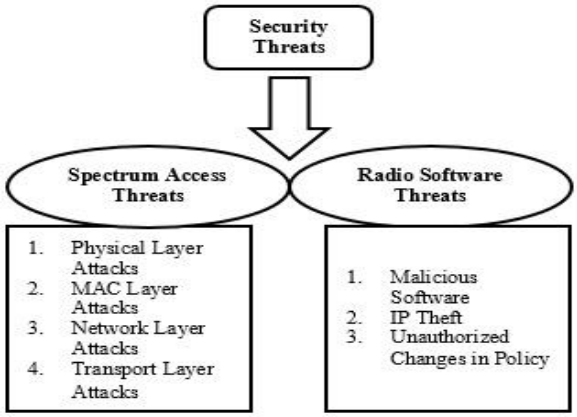

Fig. 5: Types of Security Threats

Spectrum Access Threats are characterized by different layers. Some attacks are physical layer attacks like PU (Primary User) Emulation (PUE), Function Objective, Jamming and so on. Spectrum-Sensing-Data-Falsification (SSDF), Control Channel-Saturation-DoS (CCSD) and Selfish-Channel-Negotiation (SCN) are MAC layer`s attacks. Similarly different types of Attacks are distributed layer wise in Table II.

TABLE II
DISTRIBUTION OF ATTACKS IN OSI LAYER

Attack Type	OSI Layer Distribution			
	Physical	MAC	Network	Transport
Primary User Emulation (PUE)	✓	×	×	×
Objective Function (OF)	✓	×	×	×
Jamming	✓	✓	×	×
Spectrum Sensing Data Falsification (SSDF)	×	✓	×	×
Control Channel Saturation DoS (CCSD)	×	✓	×	×
Selfish Channel Negotiation (SCN)	×	✓	×	×
HELLO Flood	×	×	✓	×
Sinkhole	×	×	✓	×
Ripple Effect	×	×	✓	×
Lion	×	×	×	✓
Key Duplication	×	×	×	✓
Jelly Fish	×	×	×	✓

A. Primary User Emulation (PUE) attack

The basic principle of cognitive radio is; SU uses the free band of spectrum until PU occupies it. When SU sense that PU needs the channel, SU must change the channel immediately. But if SU detects another SU then both of them share the same channel equitably using some kind of algorithm [6].

PUE attack occurs when some malicious user acts as masquerade and pretends as PU. SU detects it as PU and leave the channel for malicious user. So, PUE attacks is likewise known as masquerading assault. It is categorized in to two types, Selfish-PUE (SPUE) and Malicious-PUE (MPUE).

- ***Selfish PUE attack:*** The basic purpose of this attack is to maximize its share in the band of spectrum. Further it is carried by two attackers simultaneously and they make a dedicated link between each other.
- ***Malicious PUE attack:*** This attack works as DoS attack because it stops legitimate SU to use free spectrum.

1) PUE detection approach:

- ***Wireless Sensor Network (WSN) technique:*** By mapping of Received Signal Strength (RSS) on large number of sensors Network, larger peaks confirms the availability of CR user.
- ***Cryptographic technique:*** Using this technique, a helping node which acts as relay, enables SU to authenticate PU. Impulse response function is used for comparing amplitude ratios.
- ***Signal Activity Pattern (SAP) technique:*** SAP of transmitter is compared with the actual SAP of PU. If it is matched, then transmitter is legitimate user otherwise it is attacker.
- ***Deck lock technique:*** Radio metrics, a part of radio signal, act as finger print. Deck lock technique is novel technique which enables radio metrics to act as finger print. It is also used to differentiate between PU and attacker.

2) PUE defensive approach:

- ***Advanced Encryption Standard (AES) technique:*** AES can be used at transmitter end, then can be decrypted at receiver end. Using this technique, we can detect licensed PU and also malicious attack.
- ***Location Verifiers technique:*** Location verifiers are used to detect licensed PU and can be enabled with GPS based network. There are two types of test. In Distance Ratio Test (DRT), ratio of received signal strength at different location verifiers, is measured as signal strength varies with the distance. If both ratios are similar then PU is legitimate otherwise not. In Distance Difference Test (DDT), difference between phases of received signal is compared at different location verifiers. Similar results show the PU is licensed or legitimate otherwise not [13], [14].
- ***Probability Density Function (PDF) technique:*** This technique is also used to detect PU legitimacy.

B. Objective Function (OF) attack

Cognitive radio is basically a radio who sense the surrounding environment, analyse it and take intelligent

decision. Intelligent decision includes changing in transmission parameters to meet some technical requirements such as high security, high data rate and low power consumption. Transmission parameters are frequency, encryption type, frame size etc. To calculate these parameters, cognitive radio uses objective function [15].

Objective function attacks occurs when cognitive radio try to find parameters but at the same time, the attackers attacks to change the transmission parameters. For example, Cognitive radio using objective function, calculates parameters for high level security. But attacker changes the parameters and provide back door for hackers.

1) OF defensive approach: Prevention from this attack is a very critical and difficult task but some techniques can be implemented. Threshold values can be used, also Intrusion Detection System (IDS) technique is supposed to be helpful.

C. Jamming attack

Jamming attack is physical layer attack and also MAC layer attack. In jamming attack, jammers (Attackers) maliciously sends packets and create interference in the communication between primary and secondary user. Primary and Secondary users receive these packets as junks and channel seems to them as busy.

There also are four kinds of jammers. Random Jammer, Reactive Jammer, Constant Jammer and Deceptive Jammer. Random Jammer acts as Constant Jammer or Deceptive Jammer. Constant jammer continuous sends packets and don't care about idleness of the channel. Deceptive jammer deceives users and make them capable of receiving packets until jammer sends packets. Reactive jammer first sense the communication in channel and then sends packets. It does not sends packets when the channel is idle [13].

1) Jamming detection approach: Carrier Sense Multiple Access (CSMA) is a technique in which user sense the medium until it is free. Even then, User will wait for some time and then transmit data. In case of jammer attack, medium will not be free and hence it is DoS attack for the user. Comparison between Signal Strength (SS) and Packet Delivery Ratio (PDR), is also a technique for detecting Jamming attacks. Location consistency check is also a technique, in which locations of neighbours is checked by Global Positioning System (GPS).

2) Jamming defensive approach: There are two defensive techniques. One is Frequency Hopping or Channel Surfing. Second technique is Spatial Retreat. The common in both techniques is; user changes the channels or region while remains in range of communication.

D. Spectrum Sensing Data Falsification (SSDF) attack

SSDF, also called Byzantine Attack, in which an Attacker sends wrong sensing results to the receiver. Receiver takes decision based on wrong information. Distributed as well as Centralized both CRNs are affected by this attack [14].

1) SSDF defensive approach: A decision fusion technique, where all received results is summed. If the resultant accumulated sum is more than a particular threshold cost, then that channel flagged as "busy", otherwise it's "free". A technique known as Weighted Sequential Ratio Test (WSRT), consists of two steps; reputation maintenance step and hypothesis test step. This is trust based scheme and works on the principle of Sequential Probability Ratio Test (SPRT).

Another technique which is based on WSRT and "pre-filtering". This scheme focus on pre-filtering the results to nullify malicious users. This scheme works good in all conditions, all other have some limitations.

E. Control Channel Saturation DoS (CCSD) attack

This works only for multi-hop CRNs, because in centralized environment, MAC frames are authenticated by Base Station. In multi-hop CRN, communication between CRs is only possible after channel negotiation. During negotiation, MAC frames are exchanged to book the channel. In case of concurrent transmission, communication becomes impossible. Attacker uses this fact and generate bogus MAC frame to saturate the channel. It is called DoS because CRN reaches to near-zero throughput [15].

Based on trust, a detection mechanism, known as Sequential Probability Ratio Test can be utilized for defending against CCSD attack.

F. Selfish Channel Negotiation (SCN) attack

Again in multi-hop CRN, if the CR does not allow other host to send his data, this is called Selfish Channel Negotiation. This attack decrease the node to node throughput of the whole CRN.

Based on trust, a detection mechanism, known as Sequential Probability Ratio Test can be utilized for defending against SCN attack.

G. HELLO Flood attack

This is basically routing attack and occurs when attacker broadcast a message and claims itself as a good neighbour, having high quality link and more power to forward their packets. When other nodes starts sending packets, they become aware of no neighbour, because original neighbours are busy in forwarding packets.

1) Hello flood defensive approach: Symmetric key cryptography is the defensive mechanism. Symmetric key is shared with Base Station, which acts as Trusted Third Party as in Kerberos [6], helps in generating session keys for the nodes in the network. Session keys used by nodes are for their identity as well as their authentication. In order to prevent this system from attacker, number of shared keys should must be limited. Identification protocol may also be used for identification of nodes.

H. Sinkhole attack

When nodes try to sends their packets, Attacker declares itself the better route to move their packets towards destination. Attacker changes packets or discard, known as selective forwarding. This attack mostly occurs in mesh and infrastructure architecture based networks [13].

1) Sinkhole defensive approach: Geographic Routing Protocol (GRP) is the defensive mechanism for sinkhole

attack, which relies on geographic position information. Using this approach, each node gets its own location. Sender sends packets directly to location of the destined node, without having knowledge about preliminary route discovery.

I. Ripple Effect attack

This attack occurs due to false information regarding spectrum assignment. This is alike PUE attack and SSDF attack. Attacker shares false information in the network regarding free nodes. The possible countermeasure is to keep going on continuous trust on cognitive users [16] [17].

J. Lion attack

This attack is inter connected with PUE attack. This attack occurs due to PUE attack. When PUE attack occurs, hand off becomes necessary for Secondary Users, without the acknowledgement of TCP. So, TCP keeps creating logical channels and sending packets. When TCP does not receive acknowledgements of sending packets, timeout value increases and hence delay and packet loss increases [17].

1) Lion defensive approach: Mechanisms based on Cross layer detection, are good for defending against this attack. In this scenario, Transport layer will be privy to what is occurring at the Physical layer. So, TCP might be aware about frequency hopping at physical layer and forestalls sending packets.

K. Key Duplication attack

Also known as Key Depletion attack; a transport layer attack occurs when attacker breaks the cypher system. Basically, Transport layer is responsible for generation of cryptographic keys for each session. In the context of wide variety of keys, there is a chance of repetition and hence breaking of cypher system. For countermeasure, proper investigation of protocol activity is required for each session. Also needs to make protocols more secure with robust key distribution management process [17].

L. Jelly Fish attack

This is similar to Lion attack in the sense that both attacks on TCP. Re-ordering of the packets received by the attacker, is basically Jelly Fish attack. In a result, congestion in the network increases and it badly affects the throughput of the network [17]. For countermeasure, trust based mechanism can be implemented on each node for the verification of packet losses.

V. THREATS VS COUNTERMEASURES

Implementation of CR with 4G LTE-Advanced network is very vulnerable because of security threats towards CR. In our evaluation, we summarized all countermeasures and the best one countermeasure according to our assessment and research, as shown in Table III.

TABLE IIII
THREATS AND COUNTERMEASURES SUMMARY

Threat	Existing Countermeasures	Best One Countermeasure	Limitations
Primary User Emulation (PUE) [6]	Authentication using Cryptography, Distance Ratio Test (DRT), Distance Difference Test (DDT), Finger printing	Finger Printing is considered the best [6].	There exists issues like increased storage requirement, and sensing time because of overheads of additional signal processing performance [13], [14].
Objective Function (OF) [15]	Threshold Value, Intrusion Detection System (IDS)	Threshold Value is a good solution [15].	The major limitation is fixed thresholds [15].
Jamming [6] [13]	Comparison between Signal Strength (SS) and Packet Delivery Ratio (PDR), Location Consistency Check, Frequency Hopping, Spatial Retreat	Frequency Hopping is best [6].	Good technique to mitigate Jamming [6].
Spectrum Sensing Data Falsification (SSDF) [14]	Decision fusion technique, Weighted Sequential Ratio Test (WSRT), Weight based fusion scheme	Weight based fusion scheme uses trust approach and pre-filtering techniques [14].	This gives effective results [14].
Control Channel Saturation DoS (CCSD) [15]	Sequential Probability Ratio Test	This is trust based mechanism which is the best [15].	Effective one [15].
Selfish Channel Negotiation (SCN) [15]	Sequential Probability Ratio Test	This is trust based mechanism which is the best [15].	Effective one [15].
HELLO Flood [6]	Symmetric key cryptography	Symmetric key based mechanism is a good solution [6].	Gives effective results [6].
Sinkhole	Geographic Routing Protocol (GRP)	A good solution for Sinkhole attacks [13].	There is no limitation because base stations will be located physically [13].
Ripple Effect [16] [17]	Persistent trust on Cognitive users	A good approach for Ripple Effect attacks. [16]	It gives effective results. [16]
Lion [17]	Algorithms based on cross layer detection	Good solution [17]	It is a good solution [17].
Key Duplication [17]	Proper investigation of protocol activity is required for each session. Also needs to make protocols more secure with robust key distribution management process	A good solution proposed for key depletion [17].	It is a good solution [17].
Jelly Fish [17]	Trust based mechanism can be implemented on each node for the verification of packet losses.	Good solution	Good one [17].

This can be concluded from Table III, that Physical Layer attacks can be defended in CRN by unifying frequency hopping, fingerprinting and thresholding. Similarly, a trust based CRN architecture and Weighted Sequential Ratio Test can defend against Link Layer attacks. Also Network and Transport layer attacks can be defended using suggested countermeasures.

To ensure basic security concepts known as CIA triad (Confidentiality, Integrity and Authentication) in CRN, all these vindication techniques require to be implemented in the CRN.

VI. CONCLUSION & FUTURE WORK

In this paper, we narrated 4G LTE-Advanced, CR and focused on the most latest and vulnerable threats targeting towards Cognitive Radio Networks. We tabulated these attacks with respect to OSI Layers and briefly described them. Also discussed and tabulated existing countermeasures and the best one according to our research. Although, these proposed countermeasures are not supported by any simulation results, but we keep this for our future work.

ACKNOWLEDGEMENT

Thanks to Almighty Allah with His blessings, our Teachers and our Parent's supportive behaviour. Their love and encouragement always empower us and help us in going on. This research work is funded by Directorate of Research Centre, University of Engineering and Technology, Lahore, Pakistan.

REFERENCES

[1] Akhil Gupta and Rakesh Kumar Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," IEEE ACCESS, vol. 3, Aug. 2015.

[2] Wei Jiang, Hanwen Cao, Trung Thang Nguyen, Asim Burak Guven, Yue Wang, Yuan Gao, Ammar Kabbani, Michael Wiemeler, Theo Kreul, Feng Zheng and Thomas Kaiser, "Key Issues towards Beyond LTE-Advanced systems with cognitive radio," in IEEE 14th Workshop on SPAWC, June 2013.

[3] Maninder Jeet Kaur, Moin Uddin and Harsh K Verma, "Role of Cognitive Radio on 4G Communications A Review," Journal of Emerging Trends in Computing and Information Sciences, vol. 3, No. 2, Feb. 2012.

[4] Ayubi Preet and Amandeep Kaur, "Review paper on Cognitive Radio Networking and Communications," (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5 (4), 2014.

[5] Jeanette Wannstrom, for 3GPP, on LTE-Advanced [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced.

[6] Wassim El-Hajj, Haidar Safa and Mohsen Guizani, "Survey of Security Issues in Cognitive Radio Networks," Journal of Internet Technology, vol. 12, No. 2, 2011.

[7] Muhammed Mustaqim, Khalid Khan, Muhammed Usman, "LTE-Advanced: Requirements and Technical Challenges for 4G Cellular Network," Journal of Emerging Trends in Computing and Information Sciences, vol. 3, No. 5, May 2012.

[8] Anastasios Bikos and Nicolas Sklavos, "LTE/SAE security issues on 4G wireless networks," IEEE Security and Privacy Magazine, March 2013.

[9] Juho Lee, Jin-Kyu Han, and Jianzhong (Charlie) Zhang, "MIMO technologies in 3GPP LTE and LTE-advanced," EURASIP Journal on Wireless Communications and Networking, vol. 2009, Jan. 2009.

[10] Tommaso Beniero, Simone Redana, Jyri Hamalainen, and Bernhard Raaf, "Effects of Relaying on Coverage in 3GPP LTE-Advanced," in Vehicular Technology Conference, 2009, VTC Spring 2009, IEEE 69th, pp. 1-5.

[11] S. Parkvall, A. Furuskar, E. Dahlman, "Next Generation LTE, LTE-Advanced," Ericsson review 2010, pp. 22-28.

[12] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty, "A Survey on Spectrum Management in Cognitive Radio Networks," IEEE Communications Magazine, April 2008.

[13] Elangovan K. and Subashini S., "A Survey of Security Issues in Cognitive Radio Network," ARPN Journal of Engineering and Applied Sciences, vol. 11, No. 17, Sep. 2016.

[14] R. Chen, J.M. Park, J.H. Reed. "Defense against primary user emulation attacks," IEEE Journal on Selected Areas in Communications, vol. 26, Issue: 1, Jan. 2008, pp. 25-37.

[15] Yuan Zhang, Gaochao Xu and Xiaozhong Geng, "Security Threats in Cognitive Radio Networks," 10th IEEE International Conference on High Performance Computing and Communications (HPCC 2008), Dalian, China, September, 2008, pp.1036-1041.

[16] Yenumula B. Reddy, "Security Issues and Threats in Cognitive Radio Networks," AICT 2013: The Ninth Advanced International Conference on Telecommunications, 2013.

[17] Shriraghavan Madbushi, Rajeshree Raut and M.S.S. Rukmini, " Security Issues in Cognitive Radio: A Review," In book: Microelectronics, Electromagnetics and Telecommunications, January 2016, pp.131-133.