PHY-MAC Detection and Prevention from Distributed Attacks in WiMAX P2P and Infrastructure Networks

Ramis Mlekar and Namik Spanak

***Abstract*—Distributed Denial of Service (DDoS) attacks are especially critical in Wireless Infrastructure Networks, as those network configurations are becoming day by day more and more crowded. In this paper we propose our PHYDETect algorithm based on so called dynamic service primitives (DSP) between MAC and PHY layers in WiMAX 802.16e networks capable to detect the different forms of attack by decoding the OFDM symbols and measuring the guard interval contraction while propagation in the 5 GHz wireless channel. The results show significant improvement of more than 40% in average over standard detection algorithms as Constructive Unified Radio Transmission over Networked Sources (CURToNS) and Estimated Bipartite Inspection over Virtual-Medium Access (EBIoVA), especially in network configurations where Single Carrier (SC-FDE) modulations are used and also in special OFDM modulated configurations using 1024-QAM with 512/223 coding defined in the 802.16e standard.**

***Index Terms*— WiMAX, DDoS, OFDM, SC-FDE, PHYDETect.**

I. Introduction

WiMAX Wireless networks are inseparable part of the fourth generation wireless networks (4G), but it is also considered as one of the key backbone and distribution technologies in the fifth generation (5G) networks where gigabit transfers are expected to reach the data rates of 10 Gbps. However, the lower available bandwidth in this spectral region is experiencing problems to accommodate large number of users in some so called "peak" periods in the day, so offloading procedures are necessary. But one of the most dangerous scenarios which produce significant performance degradation in the overall network is the presence of Distributed Denial of Service DDoS attacks targeting set of networked devices or wireless network segments by producing artificial unusable traffic aimed to overload connection links and produce stack-overflow-like effects to the hosts within the network. Unfortunately in the literature the Physical Layer (PHY) is not well investigated as possible layer where those attacks can be detected so prevention procedures can be applied on link-level manner. Theoretically, the malicious packet detection on the PHY layer can avoid employing of additional upper layer detection procedures so the unnecessary frames can be dropped and physically destroyed in the source where they practically occur. Only few scientific research efforts are conducted on this possibility, resulting in the existence of only two algorithms, to the best of our knowledge [2] [3]. In our previous study [4], we investigated the changes in the channel impulse response in the presence of malicious packets formed by so called and well known State-full Packet Inspection (SPI) algorithm. We conducted these measurements in different percentage loads of the wireless infrastructure, but also P2P WiMAX Wireless Backhaul Devices (WD40 and PP50). The empirically measured data in [4] were confirmed by the simulations implemented in NS-3.56 network simulator and showed significant GI (Guard Interval) contraction and time dilatation of the channel. Fuzzy-Logic procedure based on those parameters can be successfully applied towards decision making i.e. detection of rigid OFDM symbols containing malicious or not well formed WiMAX Data Link Layer Frames (DLL Frames). Separate experiment was realized for SC-FDE (Single Carrier With Frequency Domain Equalization). Here, we were focused on the power consumption of the EQ filter employed (Figure 1) to realize the removing of the channel effect to detect existence of corrupted packet frames. The Equalization is parametric where the N is the number of filter taps and Q is the Q- function where Q=erfc(N-1) for OFDM transmission and Q=erfc((N-1)/|(N-ln(2)|) for single carrier SC-FDE transmission. After applying some basic algebra, the Q function can be approximated to:

$$Q = \frac{\sqrt{2^N}}{2^N - 1} = \frac{1}{2\sinh\left(\frac{\ln(2)}{2}N\right)} \quad (1)$$

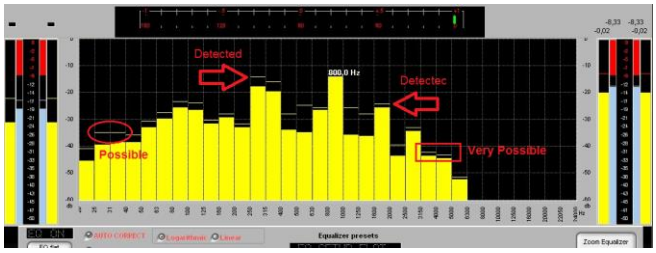

Figure 1. Frequency Response of the OFDM/SC-FDE Channel With Defined Fuzzy-Logic Detection States (Detected, Possible and Very Possible)

On the Figure 1, Fuzzy-Like detection algorithm is presented, where we implement three main Fuzzy levels of detection based on artifacts in the channel impulse responses of 3 dB above or below the main peak of the frequency response component in the WiMAX spectrum at 5 GHz with

Manuscript received April 10, 2015.

Ramiz Mlekar, MSc EE, PhD Student, is with the NGO "Research Center for Computer Science and Electronic Engineering" Bozdogan, Department of Contemporary Sciences. Blvd Temnica, BB, 2000 Pickindol, Republic of Macedonia (e-mail:ramiz.mlekar@gmail.com).

Namik Spanak, MSc CS, PhD Student, is with the NGO "Research Center for Computer Science and Electronic Engineering" Bozdogan, Unit Sector for Experimental Measurements (e-mail:crna.arapina@gmail.com). Blvd Temnica, BB, 2000 Pickindol, Republic of Macedonia (crna.arapina@gmail.com)

frequency offset of 105 kHz, which undoubtedly corresponds to the sub-carrier (subchannel) spacing declared in the 802.16 and 802.16e for OFDM and full bandwidth of 120 MHz in SC-FDE within the same contention period defined by 802.16e MAC specifications. From the Figure 1, we can conclude that for each frequency component after the successfully applied FFT operation on the transmitter side and IFFT in the receiver side for OFDM, and both FFT and IFFT applied one after other for EQ realization at the receiver side of SC-FDE case the frequency domain analysis is the same. At this point we should mention that this does not match the OFDM and SC-FDE aspects implemented in 802.11n or 802.11ac/ad where Wireless Rings are not implemented. We recommend referring to [4] - [7] where the concept of single and multicarrier transmission techniques are well studied.

II. WiMAX and 802.16 Infrastructure Networks

In Metropolitan and Wireless Wide Area Networks, as well as WiMAX, wireless ring topologies are widely deployed almost in all types, topologies and sizes. These radio beacon rings are currently using protocols that are neither optimized nor scalable to the demands of packet networks, including speed of deployment, bandwidth allocation and throughput, resiliency to faults, and reduced equipment and operational costs. At this point we must emphasize the fact the similar algorithms and technologies were applied in very basic infrared and power-line communication and they date almost 20 years ago, but still usable and functional. On Figure 2, the WiMAX frame is depicted. The reader should note that the empty field within the frame is reserved for Wireless Ring Topology Definition (WRTD). Moving from the LSB to the MSB of the frame, and applying ones (1) in big endian and little endian format forming of the complexity of the ring is realized. On the left image in Figure 2 the payload is bigger compared with the right one and it is defined for OFDM. By the standard, in both transmission methods Ring CTL of 16 bits and Direct Access (DA) field is used with length of 48 bits. Exactly this field is highly detectable within the channel impulse response, because the time from modulated symbol to the Cyclic Prefix (CP) field in OFDM mode is contracted during transmission of packets that not correspond to the original requested packets. From the SC-FDE point of view, EXT Ring CTL field is overloaded when the packet within the frame is different than requested packet by the user. Both techniques share the same bandwidth so the spectral frequency domain analyses are possible for both transmission, just with different place of analysis of the packet.

The IEEE 802.16 Infrastructure Wireless Resilient Packet Ring Working Group develops standards to support the development and deployment of Resilient Packet Ring (RPR) networks in Local, Metropolitan, and Wireless Wide Area Networks for resilient and efficient transfer of data packets at rates scalable to many gigabits per second as IEEE 8201.16 based WiMAX can theoretically achieve if the SNR is very close to 0.

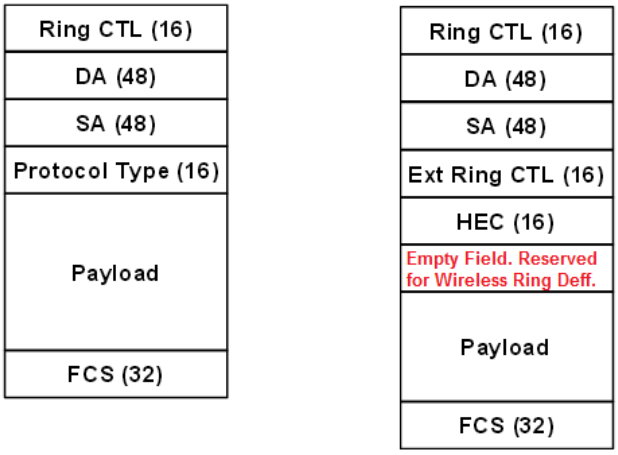

Figure 2. 802.16e Frame Format

These standards build upon existing Physical Layer specifications (PHY), and develop new PHYs where appropriate. IEEE 802.16e is a unit of the IEEE 802 LAN/MAN Standards Committee. Error requests as special form of detecting mechanisms are used to change a standard to correct errors in that standard. Requests (handled via the maintenance request process) are used to correct transmission errors that result in that published standard being different from the approved standard. Interpretation requests are used to clarify the intent of the standard. Maintenance responses are balloted by the IEEE WG (Working Group) and by the sponsor at the time that the standard is next changed as part of the entire document approval process.

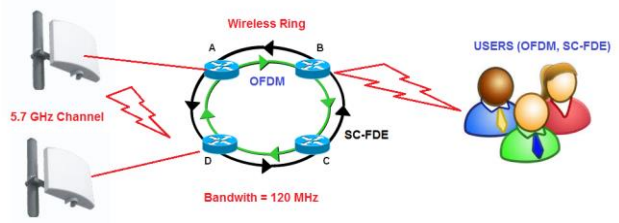

Figure 3. WiMAX Wireless Ring Infrastructure Topology

III. WiMAX P2P Wireless Access Networks

The 802.16e standard doesn't specifically define a "bridge" so we fall back on the industry-accepted definition of a bridges as a device that connects two portions of the same network using the same, or different Data Link Layer protocol (i.e.: 802.11 Wi-Fi, 802.16, 802.23, and 802.3 Ethernet). In the realm of bridging as a general technology the term "learning bridge" refers to a bridge that keeps track of where frames came from so it knows how to intelligently forward frames back only onto the port out which the intended destination can be reached. In the case of most wireless WiMAX MAN bridging, and always in the case of the Wireless Distribution System in WiMAX, there is no learning [7][10]. All packets received on by the wireless bridge are forwarded to either one destination or to a group of destinations or they can be dropped. In our case we will drop the attacking and malicious packets at this stage by specially designed service primitive that will be initiated by the MAC layer to the lower physical layer so the SA and DA fields will be modified or rearranged to avoid the execution of the

malicious code which is contained by the frame. In every case, however, the destination is the same for all packets forwarded by the wireless MAN ring topology bridge. This, of course, is not a limitation of any kind when viewed in the context of the most common implementation of WDS in WiMAX - the point-to-point token ring wireless topology between two peers in the network.

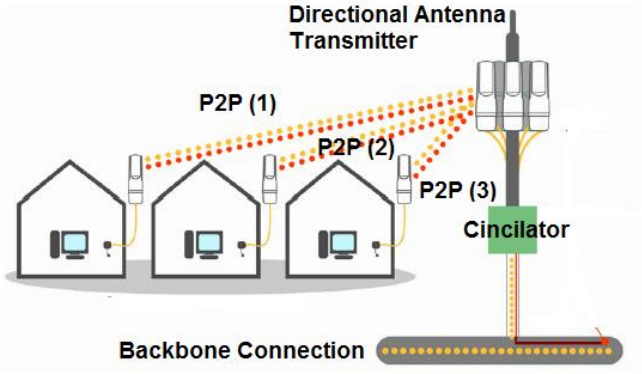

Figure 4. P2P WiMAX Wireless Access Network Architecture

IV. PROPOSED PHYDETECT ALGORITHM

Suppose we have burst series of received packets corresponding and fulfilling the Equation 1 where N in Equation 1 is the number of filter taps corresponding to the number of OFDM subcarriers, or in this case number of active peers sharing the bandwidth of the channel and accommodating 1/N part of the spectrum [8][9]:

$$\sum_{n=0}^{\infty} a_n = \lim_{N\to\infty} S_N = \lim_{N\to\infty} \sum_{n=0}^{N} a_n \qquad (2)$$

where, a_n is the current packed size in bytes, N is the number of peers within the networks, S_N is the number of pairs of receiving/transmitting antennas (within the cell) and n is the number of possible links in one wireless ring segment. Then for sure the number of successful accessed link per time is the sum limited by the sum of the active links when the number of peers tends to go to the infinity which corresponds to the real big number of peers. In the real-life WiMAX wireless network ring topology it can go up to 1000, as in most of the cases 1000 is the limit per antenna segment within the cell, also defined in the 802.16e and also corresponding to the equipment used in our measurements WD40 and PP50 backhaul and repeater infrastructure WiMAX devices. Suppose we have Sk number of peer pairs and let's define L as the potential malicious number of packet per peer. Then, by the Equation 2, L will be limited to S_k when k is tending to reach the number of N. Therefore:

$$L = \sum_{n=0}^{\infty} a_n \Leftrightarrow L = \lim_{k\to\infty} S_k \qquad (3)$$

Keeping in mind that we will make the soft decisions based on the power consumed by the EQ filter with N weighting coefficients, than naturally one question occur: How we relate the channel dilatation time and GI contraction in the length during the propagation with the content of the SA and DA fields in the 802.16e frame format. The answer of the question is quite simple and it is based on analytical and experimenatal analyses and traffic logging of real WiMAX TCP/IP environment. Namely, when the SPI algorithm detects source of unwanted packets, which means that packets arrive in the network but nobody requested, then the contention period of the MAC and LLC sub-layers is practically unmodulated from the transmitter side, but only arriving at the receiver side. DA frame is affected in a way that neither little or big endian form of the bit sequence is detectable in the frame. This is only one processing function that must be provided by the upper layers in our algorithm and approach. This function can be easily implemented within the firmware of any device in only combinatorial logic without employing storage elements as registers or SRAM blocks, but directly from the truth table in Sum of Products (SoP) form, pure digital logic. After that simple service primitive is sent to the PHY layer, stating the the packet of corresponding source n in the Equation 1 can be blocked in a way that it will not take a part in the channel access contention period anymore, as long as some part of the internal network does not required communication with corresponding source. If activity is recorded in the channel impulse response corresponding to the frequency region where previously detected malicious source and possible source of DDoS attack, then the equalizer tap corresponding to that frequency (in the frequency domain after the FFT) is attenuated to zero realizing function as practically nulling that frequency component. At this point we can mention that the algorithm will function if the node is directly included in the DDoS or other type of malicious intentions, as much as indirectly, realizing the function of so called "zombie" where without awareness the node is trying to access some network segment within the wireless ring infrastructure. The same algorithm is applied to the P2P Wireless WiMAX based access network infrastructures. The only one difference is that we are limiting the transmission mode to only SC-FDE (also defined by the standard). In this case TDMA (Time Division Multiple Access) is used by the WiMAX specifications leading to apply the algorithm on the full bandwidth channel instead of only subcarrier used by the detected node.

V. RESULTS

We realize both P2P and WiMAX Infrastructure Wireless Ring Network with same network traffic load strongly defined by exact number of PPDU frames and SA and DA length corresponding to the PHY-MAC specifications of 802.16e and applied also in WiMAX wireless standard. It is interesting to note that for the same channel impulse response in OFDM and SC-FDE transmission mode our algorithm PHYDect and both EBIoVA [1][5] and CURToNS [2][6] have the same initiation time response, reacting within the occurrence of the main peak in the channel impulse response (CIR). Considering that all of the three different algorithms have different processing time, they all finish within the complete delay of the channel dilatation. However, right after the attenuation of the main peak of the CIR CURToNS and EBIoVa showed greater successfully detected DDoS attacks belonging in one of the three main Fuzzy defined states: Possible, Very Possible and Sure Detected. By our analysis,

almost 90% of the Possible Detected packets were containing the artificially injected random malicious code detectable by the CIR characteristics. Fuzzy logic processing, however has less exponentially lower processing time [10] comparing to the sequential execution of the other two algorithms, so within the complete decay of the channel right after the second replica of the multipath propagation, it start to exponentially over-performing the both other algorithms. In the infrastructure scenario, after 15 ns, we can experience much more significant exponential growth, comparing to the P2P access network scenario and this is quite normal and can be explained by the following fact: Namely, if we consider that P2P is SC-FDE based, the reconfiguration of the weight factors of the EQ filter, which in the both cases serve as formal detector and then preventer, is taking longer time as it is acting over the full bandwidth of the channel. The other two algorithms from that point have almost steeper linear behavior and by the end of the time they enter into saturation, while PHYDect is still performing until new CIR occur, when it is stopped by simple service primitive from the MAC layer, stating that the symbol sequence is finished and new transmission should occur. This behavior is depicted on Figure 5.

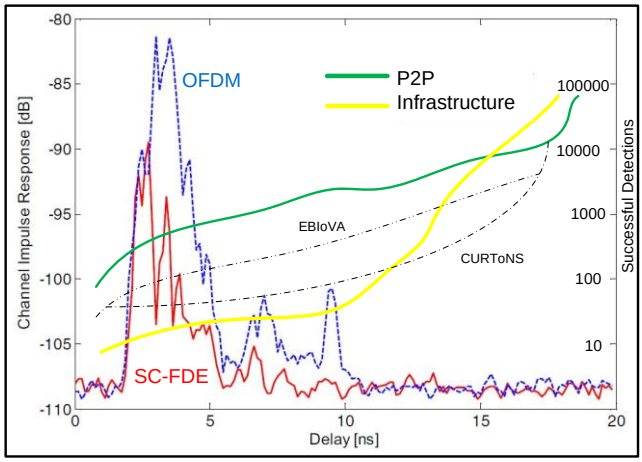

Figure 5. Results: Comparison of the execution time and number of detected packets/frames in all scenarios and three algorithms

VI. Conclusion

We presented novel PHY-MAC based algorithm for detection of malicious behavior - PHYDect, based on analysis of the CIR behavior and implementing prevention on the EQ filter, attenuating the frequency components belonging to the dangerous and malicious potential DDoS nodes in both SC-FDE and OFDM transmission nodes. Detection is Fuzzy Logic based, which release from additional firmware processing of exact digital values, and categorized in three states which can still be detected with great accuracy. Considering those facts, our algorithm out-performed it's counterparts within the time actually needed for complete decay of the CIR, even it showed less performance right after the occurrence of the CIR peak. However, the frame processing is going to take place to the final CIR complete decay, so there is still time where our algorithm showed exponential out-perform comparing to the other two in all of scenarios regarding the transmission modes and topology. Future work on this algorithm should improve the reaction time, so it can be implemented within the wireless technologies with drastically greater bandwidth and symbol rates, where the CIR time delay spread is several tens time smaller. Applying the Fuzzy Logic with greater number of states, theoretically makes the reaction time capable to be improved and implemented within the Wireless Ring Network Topologies in the spectrum around 30 GHz, 60 GHz and 72 GHz, where in those unlicensed bands the available bandwidth is around 10 GHz and data rate expectations are close to 20 Gbps.

Acknowledgment

This work was fully supported by the Bozdogan NGO Research Funds. The authors would like to thank to the professors Mitar Miric, Dzej Ramadanovski, Era Ojdanic and Meho Puzic for their valuable comments and constructive recommendations during this work.

References

[1] A. Twain, K. Cobain "Frame Processing at Physical Layer: Perspectives for Implementation in Broadband Wireless Networks", IEEE Trans. Sig. Processing. vol. 12, pp. 22-41, Jun. 2014

[2] K. Cobain, "Infrared navigation—Part I: An assessment of feasibility," *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34-39, Jan. 2013.

[3] A. Bloom, I. and M. Miller, "Wireless Coding Evaluations," *IEEE Comm. Mag*, vol. 47, no. 1, pp. 47-58, Nov. 2014.

[4] R. Mlekar, M. Shutovski, "Possibility for Signal Separation and MAC-PHY interface in Broadband Networks", AICIT AISS Journal, vol. 23, pp. 12-27, Oct. 2014

[5] G. Proakis, Digital Communications, 5th Edition, Wiley, 2005, New York

[6] V. Podgorec, Beloto Cigance, 3th Edition, Detska Radost, 1978

[7] http://wimax-wireless/ithotn/aspx (accessed April, 2015)

[8] R. Mlekar, M. Supelkov, Wireless Network Engineering and Applications, Detska Radost, 2012

[9] A. Sor, K. Sekira "Frame Processing at Physical Layer: Perspectives for Implementation in Broadband Wireless Networks", IEEE Trans. Sig. Processing. vol. 11, pp. 122-141, Jun. 2012

[10] O. Sakato, A. Kurosava, "Processing at MAC Layer: Ethernet Wireless Ring Toplologies", ACM Letters of Wireless Communication. vol. 11, pp. 122-141, Feb. 2014

Ramis Mlekar, received B.Sc. E.E, M.Sc. E.E from Mile Kitic Institute of Technology in 1994 and 2002 respectively. From 2001 to 2006, he was with the Faculty of Agriculture and Technology, "Vesna Zmijanac" in Bogovinje, Macedonia, and from 2006-2009 with the Institute of Technology and Science of Pickindol, Macedonia. Currently he is preparing his PhD Dissertation under supervision of professor K. Krajkur from the Institute of Advances Studies and Technology in Kurbinovo, Macedonia.

Namik Spanak, received B.Sc. E.E, M.Sc. C.S from Mile Kitic Institute of Technology, Macedonia in 1996 and 2005 respectively. From 2004 to 2006, he was with the Faculty of Agriculture and Technology, "Vesna Zmijanac" in Bogovinje, Macedonia, and from 2006-present, with the Institute of Technology and Science of Pickindol, Macedonia. Currently he is preparing his PhD Dissertation under supervision of professor K. Krajkur from the Institute of Advances Studies and Technology in Kurbinovo, Macedonia. In 2008 he was awarded with the "Seljak na godinata" award, considered as highly appreciated award for exceptional achievements of young researchers in Novi Pazar, Serbia.