Intrusion Detection System (IDS) for
Combating Attacks Against Cognitive Radio Networks

Citation:

Zubair Md. Fadlullah, Hiroki Nishiyama, Nei Kato, and Mostafa M. Fouda, "Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks," IEEE Network Magazine, vol. 27, no. 3, pp. 51-56, May-June 2013.

URL:

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6523809

An Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks

Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, Tohoku University
Mostafa M. Fouda, Tohoku University and Benha University

***Abstract*—While cognitive radio networks (CRNs) present a promising solution to solve the scarcity of the radio spectrum, they are still susceptible to security threats. Until now, only a few researchers considered the use of intrusion detection systems (IDSs) to combat these threats against CRNs. In this article, we describe a CRN based on IEEE wireless regional area network (WRAN) and describe some of the security threats against it. For the secondary users in the CRN to quickly detect whether they are being attacked, a simple yet effective IDS is then presented. Our proposal uses non-parametric cumulative sum (cusum) as the change point detection algorithm to discover the abnormal behavior due to attacks. Our proposed IDS adopts an anomaly detection approach and it profiles the CRN system parameters through a learning phase. So, our proposal is also able to detect new types of attacks. As an example, we present the case of detection of a jamming attack, which was not known to the IDS beforehand. The proposed IDS is evaluated through computer based simulations, and the simulation results clearly indicate the effectiveness of our proposal.**

***Index Terms*—Cognitive radio network (CRN), intrusion detection system (IDS), jamming.**

I. Introduction

Recently, the explosive growth of wireless services and applications led to a shortage of radio spectrum. Since the Federal Communication Commission (FCC) approved unlicensed users to access the unused portion of the reserved spectrum (e.g., television channels) for wireless broadband services, various researchers have devoted a lot of effort in designing cognitive radio networks (CRNs) to exploit this feature. CRNs are intelligent networks, which allow unlicensed users to use software radio for making the best use of the available/unused spectrum. While doing so, the unlicensed "cognitive" users should be transparent. In other words, they may not interfere with the primary users (i.e., the users for whom the system was originally designed) in order to share the radio spectrum resource in CRNs such as those based on IEEE 802.22 wireless regional area network (WRAN) technology [1]. This radio spectrum sharing policy among the licensed and unlicensed users, however, opens up the possibility of various security threats. Indeed, a number of attacks have been studied in recent literature that target CRNs. Although some solutions have been presented to detect these attacks, to the best of our knowledge to date, a full-fledged intrusion detection system (IDS) has not yet been designed for combating the attacks against CRNs. The research work presented in [2] pioneered in addressing the need of IDS for CRNs as a second line of intrusion/attack detection in addition to the conventional cryptographic primitives for facilitating authentication and confidentiality. Even though the work in [2] defined some of the essential modules for designing an IDS for CRNs, it did not focus on specifying any lightweight detection algorithm. Having understood the lack of research work on the IDS based defense for CRNs, we are motivated to design an effective IDS for deployment in the cognitive unlicensed users. Our proposed IDS uses cusum based anomaly detection, which is lightweight and is able to discover previously unknown attacks with a significantly low detection latency.

The remainder of the article is organized as follows. First, we survey a number of relevant research works on security threats against CRNs and some possible countermeasures. Then, we describe our considered CRN architecture and major security threats against the CRN. Next, we present our proposed IDS for the cognitive users of a CRN. Then, the performance of the proposed method is evaluated. Finally, the article is concluded.

II. Related Work

An introduction to the first wireless standard based upon CRNs is presented in the work by Cordeiro *et al.* [1] in 2006. The work demonstrated the prospect of CRN based wireless communication by using the IEEE 802.22 WRAN technology. A detailed overview of the WRAN specifications, topology, service requirements, capacity, and applications were presented in the work. Most importantly, it specified the 802.22 system to comprise a fixed point-to-multipoint wireless air interface, in which a base station manages its own cell and all associated consumer premise equipment (CPE). Note that the word "cognitive/secondary users" replaced the term CPE in later literature. While Corderiro *et al.* provided the foundation for using the WRAN technology based on CRN, it was still early days for their work to consider any of the WRAN/CRN security issues.

The security threats against CRN have been studied by a number of recent researchers. A noteworthy survey on the existing attacks against CRNs was carried out by Olga *et al.* [3] that analyzes the CRN security problems. The work not only classifies attacks and their impact on the CRNs but also identifies novel types of abuses targeting these systems. Furthermore, some security solutions are discussed to mitigate these threats against CRNs. Another comprehensive survey of these threats and their existing countermeasures can be found in the work conducted by El-Hajj *et al.* [4]. The work clearly points out that the successful deployment of CRNs depends on the correct construction and maintenance

TABLE I
ISSUES/REQUIREMENTS OF WIRED AND WIRELESS INTRUSION DETECTION SYSTEMS.

Wired IDS issues	Wireless IDS issues
Wired security defenses are not required to deal with layer 1 and 2 attacks targeting wireless communications, such as reconnaissance, man-in-the-middle attacks, and jamming attacks.	Misconfigured and/or rogue base stations can expose the entire wireless network to layer 2 attacks, which cannot be detected by traditional layer 3 firewalls.
Wired intrusion detection and prevention systems often rely on deep packet inspection.	Wireless intrusion detection systems do not have this luxury as the wireless user usually communicates with the base station over encrypted connections.
Firewalls and network address translation (NAT) can ensure that outsiders cannot directly see the internal end-users connected to the wired network let alone capture their traffic.	Malicious wireless users are free to capture all traffic in the air, and can attempt to directly inject traffic, jam the end-users, and probe their vulnerabilities.

of security measures to thwart attacks. Then, it provides a taxonomy of attacks based on their "layers." Four categories of threats are described, namely physical, link, network, and transport layer attacks. Also, the techniques to mitigate the threats belonging to each of these classes are also discussed in their work. A common point of these surveys is that their covered countermeasures do not indicate recent initiatives on designing appropriate IDSs for combating the security attacks on CRNs.

A pioneering piece of work indicating the need of IDS in a CRN is presented by Olga *et al.* in [2]. This work explains that most of the existing cryptographic primitives (e.g., authentication and encryption techniques) used in other wireless communication systems may be applicable to CRNs as a first line of defense. However, they may not be sufficient. As an additional defensive mechanism, Olga *et al.* proposed a number of modules for designing an IDS for CRNs. However, the work does not offer a full-fledged IDS, especially with a lightweight attack detection technology. This implies that designing an IDS capable of combating attacks against CRNs with a lightweight detection algorithm is, to date, an open research issue. In addition, it is worth mentioning that there are differences between designing IDSs for wired and wireless networks. Table I highlights some of the fundamental issues/requirements of wired and wireless IDSs. From the table, it may be concluded that wired access medium is usually physically secured. So, the traditional wired IDSs do not require monitoring the airspace. On the other hand, wireless communication uses air for data transmission. Air is, however, an uncontrolled and shared medium. So, wireless IDSs confront the challenge of monitoring (and if possible somehow securing) the airspace from which a variety of wireless attacks can be launched.

III. EXISTING CRN ARCHITECTURE AND ATTACK TAXONOMY

In this section, we present one of the existing IEEE 802.22 WRAN based CRN architectures [1], followed by an attack model targeting the considered CRN system.

A. CRN architecture

Our considered CRN system model based on IEEE 802.22 WRAN is depicted in Fig. 1. For simplicity, the figure includes only one television broadcasting tower whereas multiple broadcasting towers may also be present. The television companies have license to broadcast their programs through the reserved band of the 54 to 806 MHz. So, the television companies (along with their subscribers) formulate the "primary users" of the system. On the other hand, the IEEE 802.22 WRAN specification allows a number of "cells", each of which is managed by a base station (BS). The WRAN cells form our considered CRN. The service coverage radius of each of the WRAN cells featuring collocated CRNs varies from 33 to 100km. Each CRN can support a number of "secondary users", who may access the unused spaces of the spectrum, which is usually reserved for the television companies, i.e., the primary users. These unused spaces of the spectrum might occur due to different scenarios, e.g., when the television broadcast is offline/idle. The unused portions of the spectrum are referred to as "white spaces". Each secondary user is equipped with software radio to sense whether the primary users are currently occupying a channel or not. If the channel is occupied, the secondary user has the ability to intelligently adapt his radio to another channel in order to sense the white spaces of that channel. The intelligent adaptation with the external environment is possible as the cognitive engine is able to continuously learn by utilizing online and offline learning policies. The plot in Fig. 1 demonstrates an example of how the secondary users share the spectrum with the primary ones over time. It is worth noting that the plot shows a simple illustration for ease of understanding, and the white spaces are not necessarily contiguous. For detailed overview of the system, interested readers are encouraged to read the work in [1].

B. Major security threats against CRN

Since CRNs are basically wireless networks, they inherit most of the well known security threats of wireless systems. The attack taxonomy presented in the work [4] classifies these threats based on the layer in which they are carried out. The transport layer threats usually disrupt the transport control protocol (TCP). "Lion" attack is an example of this. The network layer attacks against CRN include sinkhole and HELLO flood attacks. The link layer attacks comprise spectrum sensing data falsification (which is a type of Byzantine attack similar to that studied in ad hoc networks) and a denial of service (DoS) attack by saturating the control channel of the CRN. On the other hand, the physical layer attacks against CRNs consist of primary user emulation (PUE) attack, objective function attack, and the jamming attack. Since physical layer attacks

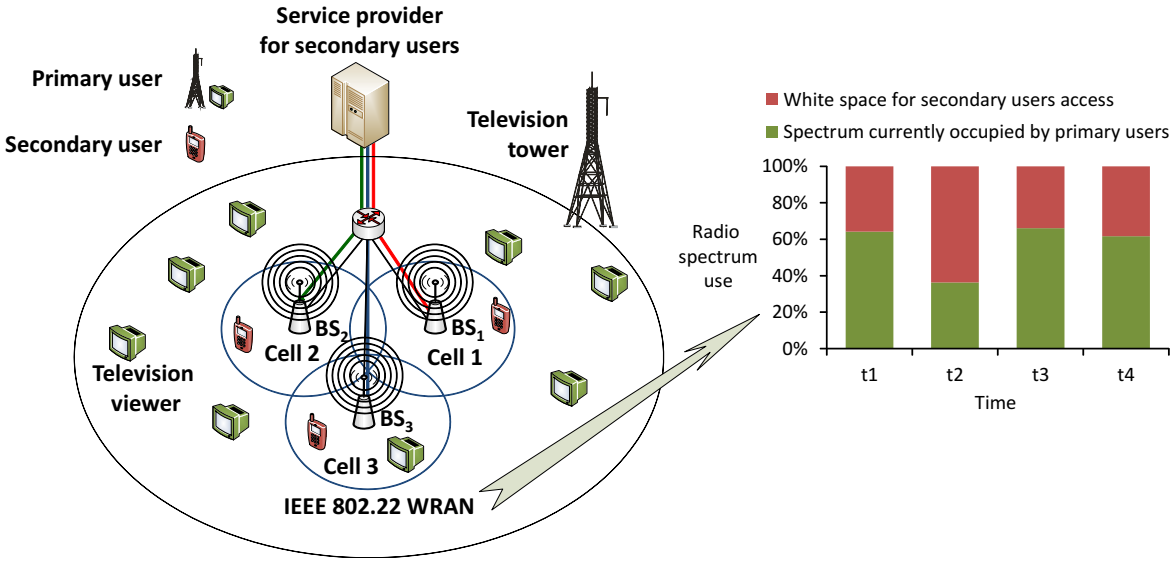


Fig. 1. Considered CRN architecture illustrating how the licensed band with white spaces can be shared by the secondary users.

are more challenging to deal with, we present a brief overview of these threats as follows [4].

- PUE attack: In this attack, an adversary secondary user aims at preventing legitimate secondary users from using the white spaces in the spectrum. For example, the adversary may exploit the "quiet periods" of the CRN during which no secondary user should transmit in order to facilitate spectrum sensing. If the adversary transmits during the quiet period, then the other legitimate users will back off by considering that a primary user (i.e., the adversary in this case) is accessing the spectrum. There are a number of other techniques by which the adversary may pretend as a primary user and trick the legitimate secondary users.
- Objective function attack: Cognitive radio is an intelligent radio, which is capable of sensing the spectral environment, learning from previous history, and making smart decisions for adjusting its transmission parameters depending on the current environmental conditions. These parameters are computed by the cognitive engine by solving objective functions. Assume a simple objective function to find the radio parameters, which balance the data rate and security. Consider the impact when a knowledgeable malicious attacker performs jamming attack every time a legitimate secondary user attempts to transmit data with high security. This makes the legitimate secondary user's cognitive engine to experience that the network conditions are unfavorable for secure transmission. As a consequence, the legitimate user drops his security level and transmits data with low/no security. Thus, the malicious attacker forces the victim radio to use a low security level, which can be eavesdropped or hacked.
- Jamming attack: Like other wireless communication systems, jamming attack is one of the most difficult threats in CRNs. A jamming attacker may transmit continuous packets to force a legitimate secondary user to never sense an idle channel. This leads to a DoS type attack whereby the legitimate user is unable to access any white space.

In order to detect the above mentioned attacks, there have been many scattered proposals, which have been surveyed in [3], [4]. However, IDS based attack detection strategy has not yet been studied extensively. In fact, it is important to have a common IDS with a general detection policy to fit (i.e., thwart) most, if not all the threats. In the next section, we present our proposed IDS to deal with this issue.

IV. Proposed IDS

The conventional IDSs usually follow either mis-use or anomaly based attack detection methods. The mis-use based detection method uses signatures of already known attacks. However, the mis-use based approach cannot discover new types of attacks effectively. On the other hand, as its name implies, the anomaly based detection methodology relies on finding the "anomaly", which represents an abnormal mode of operation in the system. By designing an appropriate anomaly based intrusion/attack detection system, it may be possible to detect new (i.e., not known beforehand) attacks, which generate some abnormal change in the targeted CRN. This is the reason why it is better to use the anomaly based intrusion detection technique in the IDS for identifying attacks in CRNs. It is worth mentioning that some of our earlier works employed a variety of statistical detection techniques for different types of wireless networks [5] [6]. However, many of the existing statistical detection techniques may not be adequate for designing an IDS for CRN as it presents a unique challenge. Specifically in CRN, a centralized IDS may not be able to detect a malicious attack and notify the secondary users quick enough, and therefore, it is important to facilitate lightweight yet effective IDSs in the secondary users themselves. Toward this end, in the following, we present our anomaly based IDS, which utilizes time-series cumulative sum

(cusum) hypothesis testing [7]. The reason behind choosing cusum for our proposed detection engine is due to its low complexity and overhead. As a consequence, the IDS can be lightweight and deployed in the individual secondary users. Note that such IDS deployment does not conflict with the regulation of the FCC that prohibits changing primary user systems [4].

As mentioned earlier, each secondary user is assumed to have an IDS. The IDS operates in two steps, namely learning or profiling phase and detection phase. In the remainder of this section, we describe these two phases in detail.

A. Learning phase

To effectively detect anomalies due to various types of attacks, the IDS needs to be designed in such a fashion that it may learn the normal behavior of protocol operation, traffic flow, primary user access time, packet delivery ratio (PDR), signal strength (SS), and so forth. The IDS may learn these information by constructing a statistical profile during normal CRN conditions or with acceptable (i.e., low) level of suspicious activities.

To make it clear to the readers, an example of a physical layer attack, i.e., the jamming attack, is considered for our study. In order to identify the jamming attack, let us consider a simple observation made by a secondary user involving its PDR and SS. The PDR of a user indicates the ratio of the number of packets received by the user to that of the packets sent to him. Note that while this is an example case of the IDS learning phase (which arises from a specific jamming attack against the CRN), our IDS is not limited to learning this feature only. In fact, if the IDS is appropriately designed by taking into consideration the CRN system specifications, wireless protocol behavior, and so forth, it can learn various modes of operation of the CRN. The acquired information can facilitate the detection phase of the IDS to discover unknown intrusions or attacks against the targeted CRN.

B. Detection phase

The proposed IDS detection phase relies on finding the point of change in the CRN operation as quickly as possible under an attack.

First, let us present a physical layer jamming attack as follows. When a malicious user jams a secondary user's connection, the following observations can be made. While the SS measured at that secondary user remains high, his PDR usually drops [2], [8], [9]. This happens because the secondary user never receives some/all of the packets sent to him. Our point of interest is how to detect the change point in the PDR behavior of a secondary user (targeted by a jamming attacker). In other words, how can the IDS find when the PDR of the secondary user is dropping significantly enough to reflect the impact of a jamming attack? In the following, our proposed IDS with cusum based anomaly detection is presented to deal with this issue.

Assume that the IDS operates over equal time-rounds, Δ_n (where $n = 1, 2, 3, ...$). Let the mean of F_n during the profiling period (i.e., no or low jamming attack scenario) be represented by m. The idea is that the IDS continues to monitor a significant change in the value of m that can be considered as the influence of the jamming attack. m remains close to one until an anomaly occurs (which is later shown in Fig. 2(a) in Section V). However, an assumption of the non-parametric cusum algorithm suggests that the mean value of the random sequence should be negative during the normal conditions and becomes positive upon a change. Therefore, a new sequence $G_n = \beta - F_n$ is obtained where β is the average of the minimum/negative peak values of F_n during the profiling period (as shown in Fig. 2(b)).

During a jamming attack, the increase in the mean of G_n can be lower bounded by $h = (2\beta)$. Then, the cusum sequence Y_n is expressed as follows.

$$Y_n = (Y_{n-1} + G_n)^+; \quad Y_0 = 0 \tag{1}$$

where $x^+ = x$ if $x > 0$; otherwise, $x^+ = 0$.

A large value of Y_n strongly implies an anomaly (i.e., the effect of jamming attack in this case). The detection threshold, θ is computed as follows [10].

$$\theta = (m - \beta)t_{des} \tag{2}$$

where t_{des} denotes the desired detection time, which should be set to a small value for quickly detecting an anomaly.

At the detection phase, the IDS computes Y_n over time. Y_n remains close to zero as long as normal conditions prevail in the CRN. Upon a jamming attack, Y_n starts to increase. When Y_n exceeds θ and as long as the SS measured at the secondary user is high, the IDS generates an alert of a possible attack (i.e., jamming in this case). An example of this is illustrated in Fig. 2(c).

V. Performance Evaluation

In order to evaluate the performance of the proposed IDS at the secondary user level, we consider IEEE 802.22 WRAN topology [1]. For interested readers, the details pertaining to the WRAN model are presented in Table II. Note that there may be up to 68 channels and each channel may support a maximum of 12 simultaneous secondary users in the WRAN CRN model. Because our proposed IDS is deployed at each of these secondary users, it is sufficient to demonstrate how the IDS effectively operates at any secondary user under the influence of the jamming attack. We construct computer simulation by using MATLAB [11] to demonstrate this point as follows.

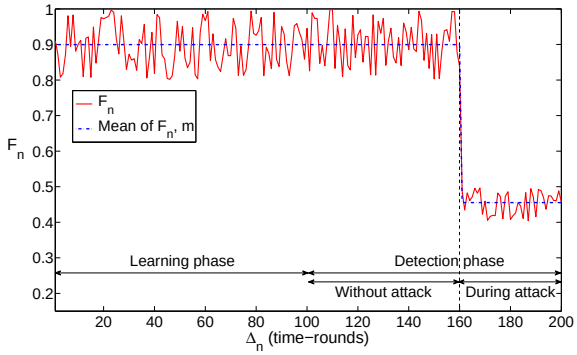
In our experiment, a jamming attack is simulated which interferes with the PDR of the secondary users. The strength of the jamming attack against a victim (i.e., influenced or overwhelmed by the attack) secondary user is defined to be proportional to the decrease in PDR of the victim. In other words, if the attack strength (in terms of percent of the transmitter's SS) is denoted by μ and the normal PDR is n (note that the value of n is assumed to be from 80% to 100% under normal conditions), then the victim experiences a drop in PDR by $(100 - \mu)\%$ of $n\%$. By using this definition, the jamming attack strength is varied from a significantly small value of 2% to an overwhelming 100%. The performance of

TABLE II
IEEE 802.22 WRAN BASED COGNITIVE RADIO NETWORK SYSTEM PARAMETERS.

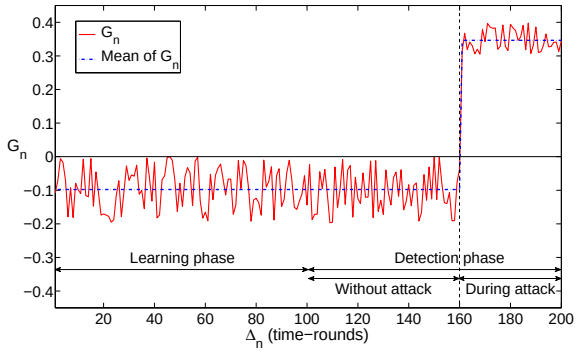
WRAN parameter	Value
Wireless bandwidth	54 to 806 MHz
Number of channels	68
Individual channel bandwidth	6 MHz
Band ranges	54 to 72 MHz, 76 to 88 MHz, 174 to 216 MHz, and 470 to 806 MHz
Maximum number of simultaneous secondary users	12
Minimum peak downlink rate per secondary user	1.5 Mbps
Minimum peak uplink rate per secondary user	384 Kbps
Cell coverage	33 to 100 km
Spectral efficiency	3 bits/s/Hz
Total physical data rate per channel	18 Mbps
Packet size (MTU)	1518 bytes
Minimum frames per second (received per secondary user)	129.51

the IDS is investigated under these attacks of various attack strengths.

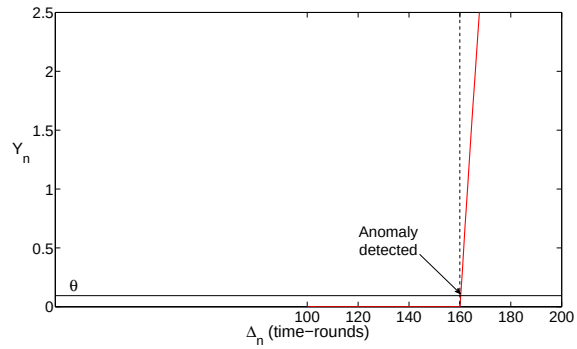
In the graphs presented in Fig. 2, we demonstrate how the proposed cusum based detection algorithm operates at the IDS of a secondary user under the influence of a jamming attack with μ=50%, which represents a medium strength attack in our simulations. The monitoring time-round length is set to 1s. The learning phase of this user is considered to run for 100 time-rounds. The detection phase also comprises 100 time-rounds. For ease of understanding, we show both normal (i.e., without attack) and jamming attack scenarios during the detection phase. The attack commences during the 160th time-round, and continues up to the end of the conducted simulation. Fig. 2(a) exhibits the F_n sequence monitored by the IDS of the secondary user during learning and detection phases. As shown in the figure, F_n remains close to one during the learning phase and also during the attack-less segment of the detection phase. Observe how sharply F_n drops at the advent of the attack with $\mu = 50\%$ and continues to exhibit this trend for the remaining course of the simulation. In other words, the mean of F_n remains close to 0.9 when there was no attack, and drops substantially to 0.45 as the secondary user is jammed. Fig. 2(b) demonstrates the G_n plot over time that was obtained by subtracting F_n from the transformation parameter β. In the simulation, β is set to the minimum F_n value found (i.e., 0.8019) during the observation period. As a consequence, G_n becomes negative during the normal learning phase. Then, by using eq. (2), the attack threshold θ is computed to be 0.0941. This is used in computing the Y_n values in the detection phase of the IDS as demonstrated in Fig. 2(c). As evident from the result, Y_n remains zero from 100 to 160 time-rounds. After the beginning of the jamming attack at the 160^{th} time-round, Y_n exceeds θ just in the following time-round. This reflects an anomalous event with respect to the normal profile constructed during the learning phase. Therefore, the IDS issues an alert to the victim secondary user about a possible attack (i.e., jamming attack in this case). If the anomalous condition persists for a long time, the IDS may instruct the victim to move to a different channel of the CRN, or even change its location.



(a) Computing F_n and mean of F_n.



(b) Computing G_n and mean of G_n.



(c) Computing cusum sequence, Y_n.

Fig. 2. Illustrating the functionality of cusum based attack detection. In this example, an attack with μ = 50% is considered that started from the 160^{th} time-round.

Next, we investigate the detection latency experienced by the proposed IDS for different attack strengths as shown in the plot in Fig. 3. For this purpose, the simulations are conducted 100 times, and the average values are used as results. Note that the detection latencies for the jamming attack with μ = 2% to 6% are not shown in the plot. This is because this particular attack is too weak and cannot be detected within the considered detection period. However, these attacks with relatively low attack strength cannot have a substantial impact on the victim, i.e., they cannot decrease the victim's PDR dramatically. On the other hand, for the attack with μ = 8%, 10%, 12%, 14%, 16%, and 18%, the corresponding

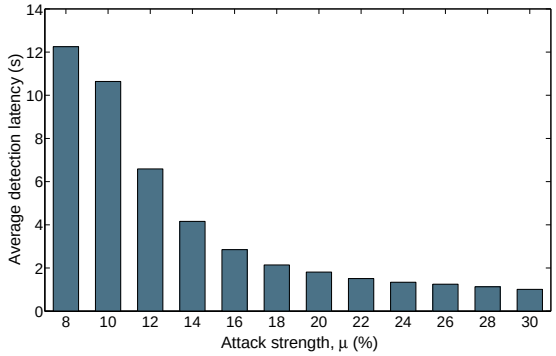


Fig. 3. The detection latencies for different attack rates.

detection latencies are 12.25s, 10.64s, 6.59s, 4.16s, 2.85s, and 2.14s, respectively. It is worth mentioning that in an individual simulation run, the detection latency should be an integer value as the time-round length is set to 1s in the conducted simulations. However, due to the fact that we used the average of the detection latencies obtained from multiple simulation runs, the corresponding detection latencies are computed to be non-integer values. The time to detect the attack decreases further for the attacks with $\mu \geq 20\%$, and is found to be ranging from 2s to 1s since the commencement of the attack. Note that μ values exceeding 30% are not shown in the plot in Fig. 3 as they also exhibit the same detection latency of 1s. In summary, these results indicate that our proposed IDS at the victim secondary user can effectively detect the influence of the considered attack with substantially low detection latency.

VI. Conclusion

In this article, we highlighted the importance on designing appropriate intrusion detection systems to combat attacks against cognitive radio networks. Also, we proposed a simple yet effective IDS, which can be easily implemented in the secondary users' cognitive radio software. Our proposed IDS uses non-parametric cusum algorithm, which offers anomaly detection. By learning the normal mode of operations and system parameters of a CRN, the proposed IDS is able to detect suspicious (i.e., anomalous or abnormal) behavior arising from an attack. In particular, we presented an example of a jamming attack against a CRN secondary user, and demonstrated how our proposed IDS is able to detect the attack with low detection latency. In future, our work will perform further investigations on how to enhance the detection sensitivity of the IDS.

References

[1] C. Cordeiro, K. Challapali, and D. Birru, "IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios," Journal of Communications, vol. 1, no. 1, pp. 38-47, Apr. 2006.

[2] O. Leon, R. Roman, and J. H. Serrano, "Towards a Cooperative Intrusion Detection System for Cognitive Radio Networks", in Proc. Workshop on Wireless Cooperative Network Security (WCNS'11), Valencia, Spain, May 2011.

[3] O. Leon, J. Hernandez-Serrano, and M. Soriano, "Securing cognitive radio networks", in International Journal of Communication Systems, vol. 23, no. 5, pp. 633-652, May 2010.

[4] W. El-Hajj, H. Safa, and M. Guizani, "Survey of Security Issues in Cognitive Radio Networks," Journal of Internet Technology (JIT), vol. 12, no. 2, pp.181-198, Mar. 2011.

[5] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, Vol. 5, No. 3, pp. 338-346, Nov. 2007.

[6] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communications, vol. 14, no. 5, 85-91, Oct. 2007.

[7] Z. M. Fadlullah, T. Taleb, A. Vasilakos, M. Guizani, and N. Kato, "DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis," IEEE/ACM Transactions on Networking, vol. 18, no. 4, pp. 1234-1247, Aug. 2010.

[8] K. Ju and K. Chung, "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks," International Journal of Security and Its Applications, vol. 6, no. 2, pp. 149-154, Apr. 2012.

[9] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in Proc. ACM international symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'05), Urbana-Champaign, Illinois, USA, May 2005.

[10] H. Wang, D. Zhang, and K. G. Shin, "Change-Point Monitoring for Detection of DoS Attacks," IEEE Trans. on Dependable and Secure Computing, vol. 1, no. 4, pp. 193-208, Oct. 2004.

[11] MATLAB, available online at http://www.mathworks.com

Biographies

Zubair Md. Fadlullah [M'11] (zubair@it.ecei.tohoku.ac.jp) received B.Sc. degree with Honors in computer sciences from the Islamic University of Technology (IUT), Bangladesh, in 2003, and M.S. and Ph.D. degrees from the Graduate School of Information Sciences (GSIS), Tohoku University, Japan, in 2008 and 2011, respectively. Currently, he is serving as an Assistant Professor at GSIS. His research interests are in the areas of smart grid, network security, intrusion detection, game theory, and quality of security service provisioning mechanisms. He was a recipient of the prestigious Dean's and President's awards from Tohoku University in March 2011 for his outstanding research contributions.

Mostafa M. Fouda [M'11] (mfouda@it.ecei.tohoku.ac.jp) received his Ph.D. degree in Information Sciences in 2011 from Graduate School of Information Sciences, Tohoku University, Japan. He received B.Sc. degree with honors in Electrical Engineering (Electronics & Telecommunications) in 2002, and M.Sc. degree in Electrical Communications in 2007, both from Faculty of Engineering at Shoubra, Benha University, Egypt. He is currently serving as an Assistant Professor at Tohoku University and holds a Lecturer position at Benha University. He has served as a Technical Program Committee (TPC) member in several international conferences. He also serves as a reviewer of a number of renowned journals such as IEEE COMST, TPDS, TWC, TSG, etc.

Hiroki Nishiyama [SM'13] (bigtree@it.ecei.tohoku.ac.jp) is an Associate Professor at the Graduate School of Information Sciences (GSIS) at Tohoku University, Japan. He was acclaimed with the best paper awards in many international conferences including the IEEE WCNC 2012 and the IEEE GLOBECOM 2010. He was also a recipient of the IEICE Communications Society Academic Encouragement Award in 2011, and the 2009 FUNAI Foundation's Research Incentive Award for Information Technology.

Nei Kato [M'03, SM'05, F'13] (kato@it.ecei.tohoku.ac.jp) has been a full professor at GSIS, Tohoku University, since 2003. He has been engaged in research on satellite communications, computer networking, wireless mobile communications, smart grid, image processing, and pattern recognition. He has published more than 300 papers in peer-reviewed journals and conference proceedings. He is a distinguished lecturer of IEEE ComSoc, and a Fellow of IEICE. He currently serves as the Vice Chair of the IEEE Ad Hoc & Sensor Networks Technical Committee. His awards include Minoru Ishida Foundation Research Encouragement Prize (2003), Distinguished Contributions to Satellite Communications Award from the IEEE Communications Society, Satellite and Space Communications Technical Committee (2005), the FUNAI Information Science Award (2007), the TELCOM System Technology Award from Foundation for Electrical Communications Diffusion (2008), the IEICE Network System Research Award (2009), the IEICE Satellite Communications Research Award (2011), the KDDI Foundation Excellent Research Award (2012), IEICE Communications Society Distinguished Service Award (2012), IEEE GLOBECOM Best Paper Award (twice), IEEE WCNC Best Paper Award, and IEICE Communications Society Best Paper Award (2012).