Critical Infrastructure Network DDoS Defense, via Cognitive Learning

Todd Booth and Karl Andersson
Research@ToddBooth.Com Karl.Andersson@Ltu.Se
http://OrcId.Org/0000-0003-0593-1253 http://OrcId.Org/0000-0003-0244-3561
Division of Computer Science / Luleå University of Technology / 97187 Luleå, Sweden

***Abstract*—Some public and private services are called part of the Critical Infrastructure (CI), which are considered as the most important services to protect the functioning of a society and the economy. Many CIs provide services via the Internet and thus cyber-attacks can be performed remotely. It is now very simple and free to find and download software, which automates performing cyber-attacks. A recent example is that two teenagers, with close to no security knowledge, created an on-line business. They would run cyber-attacks (online booter service called vDOS, as reported by Brian Krebs) for a small fee. They reportedly earned over 600,000 USD in a short period of time by conducting a large number of automated DDoS cyber-attacks. Then Krebs was retaliated against, and the highest DDoS attack bandwidth ever recorded, 620 Gbps, was launched against Krebs. In this paper we show how cognitive learning can be used to significantly mitigate any effects of DDoS network attacks, against the critical infrastructure.**

1. Introduction

Various acronyms and terms used in this paper, are defined in table 1.

1.1. Research Problem

The scope of this paper is concerning using a cognitive informatics approach, to defend against distributed denial of service (DDoS) attacks, as part of countries' homeland security defenses.

The research problem is that it is extremely easy and inexpensive to initiate a computer network DDoS attack, but it is very difficult and expensive to defend against. One new DDoS trend is that mobile phone BotNets can be used to launch attacks. [1] Further, many countries have developed and are improving warfare grade cyber-attack DDoS capabilities and we should not be surprised if many countries (perhaps North Korea and certainly the USA, Russia and China), now have the capability to perform cyber DDoS attacks, specifically against other countries' critical infrastructures (CI).

The research community has not yet found an easy, inexpensive and general solution to defend against both the server side and the client side, during cyber DDoS CI attacks. There is a lack of adequate research to see if cognitive learning can now be used to provide a better anti cyber-DDoS defense. For example, a SCOPUS search of "TITLE-ABS-KEY (ddos or "denial of service") AND PUBYEAR AFT 2010" found 4,067 hits, but when also adding the "cognitive" search keyword, there were only 72 hits.

However, most of the 72 hits are only concerning DDoS protection of the Cognitive Radio Network (CRN). So the cognitive relevance is only concerning how the radio network works, NOT concerning how the security defenses work. Once we take away the SCOPUS papers which are only concerning the cognitive related to CRN, there are very

Term	Definition
Booters	DDoS attacks as a service (for rent)
CAPTCHA	Completely Automated Public Turing test
CI	Critical Infrastructure
CIA	Confidentiality, integrity and accessibility
CR	Cognitive Radio
DoS	Denial of Service attack
DDoS	Distributed Denial of Service attack
DSR	Design Science Research methodology
IoT	Internet of Things
IT	Information Technology
L3	Layer 4 (network)
L4	Layer 4 (transport)
L7	Layer 7 (application)
L347	IP layer 3, 4 and/or 7 attacks
NAT	IP Network Address Translation
OSI	Open Systems Interconnection ISO 7498
QoS	Quality of Service
PAT	IP Port Address Translation (overload)
PUE	Primary user emulation
SDR	Software defined Radio
TCP	IP L4 protocol, transmision control protocol
UDP	IP L4 protocol, user datagram protocol
VPN	Virtual Private Network

TABLE 1. ACRONYM AND TERM DEFINITION TABLE

few cognitive based anti DDoS papers left. In summary, we find that using a cognitive learning approach, in developing an anti DDoS defense lacks adequate research. Related to this, cognitive cryptography is a new paradigm. [2]

In this paper, we search for a cognitive approach, which can be used in providing an anti DDoS defense. We borrow (or use by analogy) the cognitive meaning used in CRN (adaptive learning) and try to adapt this same meaning, in a different context (anti DDoS defense). Therefore, we perform a review and analysis of existing CRN, so that we can adapt the cognitive related conceptual knowledge, in the our new security context.

1.2. Contributions

Our contributions are 1) An analysis of the cognitive radio networks to understand how to reuse the cognitive concepts in the new security context, and 2) Our proposed solution, which provides a cognitive based anti DDoS solution, which is easy to implement, very inexpensive, and which significantly mitigates computer network based DDoS attacks. Our focus is to greatly mitigate network DDoS attacks which effect authenticated clients or their servers.

1.3. Research Methodology

We followed the design science research (DSR) methodology [3]. A DSR IT artifact can also be the design guidelines for an IT artifact, as opposed to a physical IT artifact itself. Our high level IT artifact is our proposed cognitive based design guidelines and algorithms, which greatly mitigate any and all OSI layer 3 (network), 4 (transport), and 7 (application) network based DDoS attacks (L347). Via DSR, an IT artifact should be created, then evaluated, and then redesigned with improvements (based on the feedback from the evaluation). This cycle is then repeated several times. These cycles then continue, until an adequate level of new knowledge is acquired and/or a practical solution emerges. This approach has made it easier for the reader to understand our final and total proposed solution.

1.4. Network DDoS Attacks

Direct network attacks and indirect reflection attacks are shown in figure 1.

Via a reflection attack, the amount of attack traffic is amplified, often up to several hundred times as much as the initial traffic. However, our proposed solution covers both scenarios, using the same design guidelines, so we will use the phrase DDoS attacks, to refer to both types of attacks.

1.5. Outline of this Paper

The rest of this paper is organized as follows: In Section 2, we perform the Design Science Research (DSR) methodology and go through several design cycles. This is where we explain the specific research problem issues and our proposed solutions. In Section 3, we analyze related works and include a synthesis of those works. In Section 4, we provide our conclusions and future work suggestions.

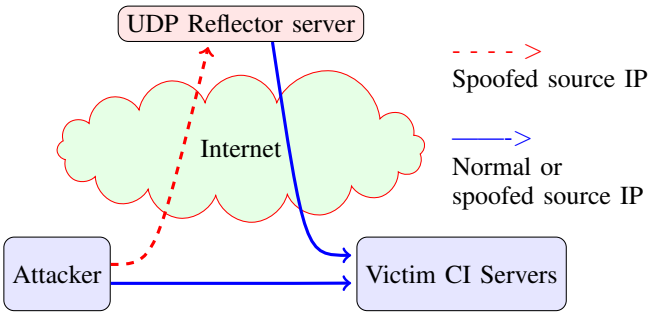

Figure 1. Direct and Reflection Attacks

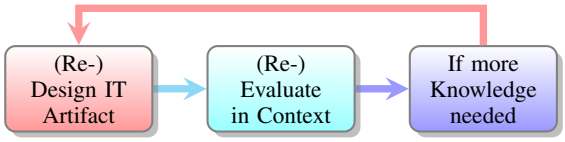

Figure 2. Design Science Research Cycles

2. DSR Methodology - Design Cycles

In this section, we go through the specific steps we took, to develop our proposed solution. In each step, we guide the reader through our incremental solution, and the limitations. At the end, we present the cumulative proposed solution. To give the reader an idea of where the solution is headed, our DSR cycle topics are found in figure 2.

With the exception of our previous three-tier communication strategy [4] and [5], all of the cited academic solutions found, were based on a traffic analysis, where the valid clients could communicate directly to one (or more) servers. There can be thousands of clients accessing the same CI service. Many services allow both authenticated and unauthenticated traffic to be processed via the same CI service IP endpoint.

Using this common strategy, it becomes extremely difficult to have a very efficient and low cost solution to filter malicious DDoS traffic. We have not yet found any academic paper which presents a very efficient and low cost solution to filter malicious DDoS traffic. Even if there was such a solution, based on the numerous reported successful DDoS attacks, we can at least state that the solution is not well known.

For any cognitive learning approach to work well, we need to first find ways to provide the cognitive engine with more information (the more, the better). Then the cognitive engine algorithm must be developed to use the information in a way to solve the given problems. So we start our paper with a quest to find more relevant information, for our cognitive engine.

DSR Cycle 1: Separate authenticated and unauthenticated services

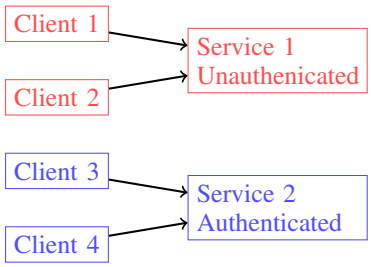

Figure 3. Design guidelines for two server architecture

Our cognitive approach includes the following design guidelines: The organization separates their services onto (at least) two sets of servers. One server set provides services to clients before they are authenticated (un-authenticated clients). The other server set provides services to clients after they are authenticated (authenticated clients). A summary of this high level design, showing that clients 3-4 (but not 1-2) have been redirected after authentication, is shown in figure 3.

Since only clients 3-4 were redirected to the Service 2, clients 1-2 do not have the Service 2 destination IP address. Therefore clients 1-2 can't attack Service 2 and can't leak the knowledge of the Service 2 destination IP address. However, one problem with this design is that the authenticated clients all learn the same public IP address of the Service 2. So if Service 2 was attacked, we don't know which specific authenticated client is malicious. We will now limit discussion to this paper's focus, which is on protecting the authenticated clients and the related servers. Therefore, from this point forward, we will now omit the un-authenticated clients and their related servers, from the figures and use the term clients, to refer to clients which have been authenticated.

DSR Cycle 2: Place proxies between clients and servers

To defend against the last vulnerability, we also propose the use a three tier communication strategy. The organizations providing services maintains two sets of what we refer to as a proxy relay. However, the proxy relay can be implemented as a Web proxy, a VPN, Linux iptables rules, etc. The main requirement is that the clients no longer have a direct end to end TCP connection with the Service. The client's TCP connections would terminate at the proxy relay and only the proxy relays would have the end to end connection with the Service.

I.E., there are now two types of TCP connections for each client, TCP connections between the client and their proxy and TCP connections between the client's proxy and servers. This is how we can conceal the servers' public IP address from the clients. Our updated design guideline is shown in figure 4.

The process of clients authenticating and being redirected follows:

1) Clients first surf to one of the pre-authentication proxies, which sits in between the clients and servers
2) Some clients may wish to authenticate, to access additional services
3) After authentication, the server saves the client ID and the client's source IP information (address and port)
4) The Server then refers the client to one of the post-authentication proxies which connects them indirectly to the servers

Figure 4. Design guidelines for three tier architecture

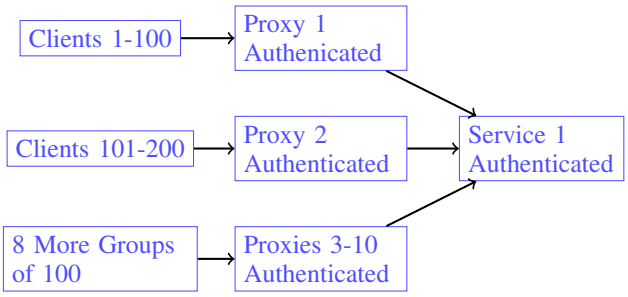

Figure 5. Design guideline example for 1,000 clients (10 proxies with 100 clients each)

Clients can no longer directly attack the servers, via the servers' public IP addresses. However, the client can attack the proxy, which currently is used by all clients. Also, in this figure 4, all clients connect to the same proxy IP address. So they can maliciously share this IP address with others, in order to have a DDoS attack. Under the above, we will not know which specific client shared the proxy's IP address.

DSR Cycle 3: During DDoS attack, perform micro segmentation of clients

To defend against this vulnerability, we also propose to perform a dynamic micro segmentation, of the proxy relays. Let's assume that a service currently has 1,000 active clients and that an attack occurs. We then immediately redirect all 1,000 clients to ten different proxy relays, each of which now has only 100 clients, as shown in figure 5.

Let's suppose that just one of the 1,000 clients is malicious or somehow the client leaked the proxy relays destination IP address. Then only one of the ten proxy relay's IP addresses could be attacked. Previously if the proxy was attacked, we had no idea which of the clients have leaked the proxy relay's IP address. However now, since we gave only 100 clients (not 1,000) the same proxy address, we know that the malicious client is one of 100 clients.

So how do we find out which of the 100 clients was the malicious client? For just this group, we can redirect the 100 suspect clients to 10 proxies, each group of which has 10 clients each. Then if any proxy detects another attack,

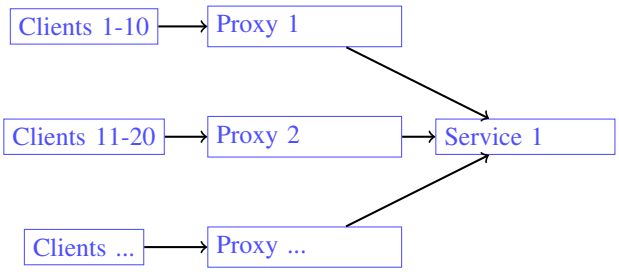

Figure 6. Design guideline example for 10 proxies

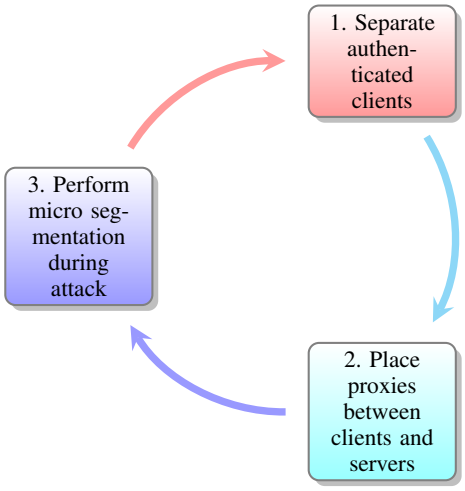

Figure 7. Summary of our DSR Cycles

we will have just 10 suspected clients, as shown in figure 6.

At the same time, we can regroup the other nine groups of 100 into a bigger group of 900 (to conserve IP addresses).

We can then break the group of 10 suspected clients into 10 groups, with just one client connected to each of ten new proxies. If there is another attack, we will know the exact malicious client who is causing the attack or leaking the information (perhaps intentionally or perhaps unintentionally). Either way, we can force this client to perform a CAPCHA, or enter a mobile phone SMS message, etc. Until they properly authenticate, we can isolate this user from causing any DDoS against the authenticated clients since they will be unable to learn the proxies' IP addresses (which are servicing other authenticated clients). We can also keep a log stating that this client was found to be apparently malicious.

Our previous related research [4] and [6] only provided a solution for web clients, but via this proxy relay solution, we have a general solution for protocols other that http/https.

2.1. Our DSR Cycles

A summary of our previous DSR cycles is shown in figure 7. After completing the cycle, we then started over and tried to improve each cycle's results.

3. Related Works and Synthesis

We will now present a few comments, concerning the most relevant works. For the following papers, any of our comments will begin with "**comments:** ".

In [7], Amjad, M.F., et. al. points out that the two-stage spectrum sensing approach presents an opportunity to malicious users where they can launch a smart Denial of Service (DoS) attack by transmitting a very short jamming signal during the fast sensing stage. **comments:** The problem with this approach and how we solve this problem is that once an attack is launched, they do not know who the attacker is.

In [8], Attar, A., et. al. provides a survey concerning known security threats within a cognitive radio network, and provide potential solutions. **comments:** This provides a good background on how the term cognitive applies to dynamic radio networking.

In [9], Baldini, G., et. al. show how Software defined Radio (SDR) and Cognitive Radio (CR) introduce entirely new classes of security threats and challenges. **comments:** SDR allows devices to quickly adapt, in order to work optimally, in changing network environments. By way of analogy, our own DDoS defense is designed to adapt to changing network conditions, as various attacks are discovered.

In [10], Dorbala, S.Y., et. al. provides an approach to defending against DDoS attacks, by using a large scale Apache Hadoop to achieve the required scalability, to perform a deeper analysis of anti DDoS correlation metrics. **comments:** With our solution, after we learn the valid source IP addresses, we can use big data to analyze which various organizations were attacked, using the same source IP addresses.

In [5], Gupta, A., et. al. security of the Internet of Things (IoT) is discussed. They describe the explosion of sensors and the lack of adequate security protection mechanisms to protect CIA (confidentiality, integrity and accessibility). **comments:** This is one of the few papers which uses cognitive computational analysis in an intrusion detection system and proposes a three-tier architecture. Our paper is similar in that we propose a 3-4 tier architecture to defend against DDoS attacks.

In [11], Hao, D., et. al. state that a major attack is the primary user emulation (PUE) attack. **comments:** By analogy, our solution is to defeat attacks such as the PUE attack, by requiring authentication before trusting the node who claims that they are authorized, to communicate.

In [12], Hlavacek, D., et. al. state that in CRN, both old and new security threats are relevant. **comments:** We have the same issue with regard to DDoS attacks, in that they have been well known for years, but there has not yet been a very low cost, pervasive, and easy to implement solution.

In [13], Hu, N., et. al. proposes a countermeasure strategy, with a coordinated concealment strategy, to counter the attack. **comments:** By analogy, our anti DDoS solution is based on this same exact high level conceptual design (concealment), however, we apply the defense in an entirely different context. I.E., we are taking Hu's solution, and generalizing it to a completely different domain knowledge

research area. So we kindly give great credit to Hu, et. al. (that allowed us to build upon this great, but somewhat specific work).

In [14], Karumanchi, S., et. al. introduce a proxy based solution, to protect Web services. **comments:** However, they have clients directly access the services, and it is the service which sends the workflow to the proxy. In our solution, the proxy hides or shields the service IP address from the client.

In [15], Kärkkäinen, A. propose a cognitive service configuration model for tactical military networks and propose that user and other services are established and maintained dynamically by adapting the service configuration continuously. **comments:** We are using the same exact approach, and also providing secrets so that any and all malicious sources can be immediately detected.

In [16], Lent, R., et. al. discuss how active flows can be driven by the users' choice of a quality of service (QoS) goal. **comments:** We thank Lent and adopt their specific approach in our solution. So we propose that during normal status (when there is no attack), that our proposed solution is not used (bypassed), which provides the users with an optimal QoS. We recommend that only during an actual ongoing attack, that the protocols are changed, in order to use our proposed solution as an anti DDoS defense.

In [17], Li, J., et. al. state that there exist enormous challenges for the open and random access environment of CRNs, where the unlicensed secondary users can use the channels that are not currently used by the licensed primary users. **comments:** We believe that our approach, to require senders to first authenticate, before being trusted, is both a partial solution to the anti DDoS attacks, as wells as the attacks against the SDR and CR.

In [18], Liang, S. state that IP tracking based on packet marking and attacking package recognition technology is one of the main means for effective against distributed denial of service attacks, and propose a tracking solution. **comments:** We believe that our tracking solution is much better, since we provide authenticated clients with a unique secret, and if there is an attack based on a unique secret, we know exactly which customer has leaked the secret.

In [19], Lo, B.F., et. al., they introduce a jamming resilient control channel (JRCC). **comments:** We thank Lo for this contribution. In our solution, we adapt Lo's strategy, and we also provide a control channel, however in a much different way. With a secret concealed control channel, if we lose our primary communication, we can instantly refer to the control channel, to obtain the new destination IP address or proxy information.

In [20], Nayeem, M.T., et. al. describes Human Interactive Proofs (HIP), which are easy for humans to solve but difficult for computers to solve. They improve HIP by making use of human cognitive processing abilities through emoticons focusing mainly on users. **comments:** With our anti DDoS solution, we too use HIP such as CAPTCHA, but only after the user is identified as suspicious.

In [21], Sorrells, C., et. al. specifies an approach to very quickly detect cognitive radio attacks. Specifically, they propose a non-parametric version of the Pages cumulative sum (CUSUM) algorithm to minimize the detection delay so that a network manager may react to the event as soon as possible. **comments:** Our solution also provides an extremely quick detection of any DDoS attack. By having various clients indirectly access the service via different proxies, we can much more easily detect a higher than normal traffic bandwidth, for a given user. This allows us to easily detect attacks, in just a few seconds.

In [22], Tan, Y., et. al., they analyze DDoS attacks, as a cooperative game among the malicious nodes. **comments:** We were inspired by this work and we also analyze DDoS attacks via a game model. However, we analyze the DDoS attacks, via a game played by the valid (non-malicious) organizations offering their services.

In [23], Wang, W., et. al. proposes a cooperative defense strategy among participates. **comments:** Our work also proposed a cooperative defense strategy among on-line service organizations. However, we don't consider these services as trusted parties.

4. Conclusion and Future Work

For this Workshop on Security and Cognitive Informatics for Homeland Defense, our anti DDoS strategy is to provide the cognitive engine with much more information on which specific authenticated clients are suspects. We then quickly and repeatedly break the suspects into much smaller groups, until the group size is just one client. This allows the cognitive engine to quickly determine exactly which client is the specific malicious client. We then remove the malicious client from the trusted list, so that that client can do absolutely no damage to the servers (which are servicing authenticated clients). We also performed research as to what is the most prevalent cognitive networking topic, which turned out to be cognitive radio networks. We analyzed the relevant DDoS cognitive papers and showed how our solutions could generalize some of the cognitive radio research towards our cognitive anti-DDoS research.

References

[1] A. Kitana, I. Traore, and I. Woungang, "Impact study of a mobile botnet over lte networks," *Journal of Internet Services and Information Security (JISIS)*, vol. 6, no. 2, pp. 1–22, May 2016.

[2] L. Ogiela and M. R. Ogiela, "Towards cognitive cryptography," *Journal of Internet Services and Information Security (JISIS)*, vol. 4, no. 1, pp. 58–63, February 2014.

[3] A. Hevner, S. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly: Management Information Systems*, vol. 28, no. 1, pp. 75–105, 2004.

[4] T. Booth and K. Andersson, "Network Security of Internet Services: Eliminate DDoS Reflection Amplification Attacks," *Journal of Internet Services and Information Security (JISIS)*, vol. 5, no. 3, pp. 58–79, 2015.

[5] A. Gupta, O. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A. Ingle, "Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks," 2013, dOI: 10.1109/ICCIC.2013.6724156.

[6] T. Booth and K. Andersson, "Network DDoS Layer 3/4/7 Mitigation via Dynamic Web Redirection," in *Future Network Systems and Security*, ser. Communications in Computer and Information Science. Springer International Publishing, no. 670. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-319-48021-3_8

[7] M. Amjad, B. Aslam, and C. Zou, "DS3: A dynamic and smart spectrum sensing technique for cognitive radio networks under denial of service attack," 2013, pp. 1149–1154, dOI: 10.1109/GLOCOM.2013.6831229.

[8] A. Attar, H. Tang, A. Vasilakos, F. Yu, and V. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proceedings of the IEEE*, vol. 100, no. 12, pp. 3172–3186, 2012.

[9] G. Baldini, T. Sturman, A. Biswas, R. Leschhorn, G. Gódor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 355–379, 2012.

[10] S. Dorbala, R. Kishore, and N. Hubballi, "An experience report on scalable implementation of DDoS attack detection," *Lecture Notes in Business Information Processing*, vol. 215, pp. 518–529, 2015.

[11] D. Hao and K. Sakurai, "A differential game approach to mitigating primary user emulation attacks in cognitive radio networks," 2012, pp. 495–502, dOI: 10.1109/AINA.2012.84.

[12] D. Hlavacek and J. Chang, "A layered approach to cognitive radio network security: A survey," *Computer Networks*, no. PartA, pp. 414–436, 2014.

[13] N. Hu, Y.-D. Yao, and J. Mitola, "Most active band (MAB) attack and countermeasures in a cognitive radio network," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 898–902, 2012.

[14] S. Karumanchi and A. Squicciarini, "A Large Scale Study of Web Service Vulnerabilities," *Journal of Internet Services and Information Security (JISIS)*, vol. 5, no. 1, pp. 53–69, February 2015.

[15] A. Kärkkäinen, "Improving cyber defence of tactical networks by using cognitive service configuration," 2013, pp. 135–143.

[16] R. Lent, G. Sakellari, and G. Loukas, "Strengthening the security of cognitive packet networks," *International Journal of Advanced Intelligence Paradigms*, vol. 6, no. 1, pp. 14–27, 2014.

[17] J. Li, Z. Feng, Z. Feng, and P. Zhang, "A survey of security issues in Cognitive Radio Networks," *China Communications*, vol. 12, no. 3, pp. 132–150, 2015.

[18] S. Liang, "The new method of DDOS defense," *Advances in Intelligent and Soft Computing*, vol. 128, pp. 145–151, 2011.

[19] B. Lo and I. Akyildiz, "Multiagent jamming-resilient control channel game for cognitive radio ad hoc networks," 2012, pp. 1821–1826, dOI: 10.1109/ICC.2012.6364117.

[20] M. Nayeem, M. Mukta, S. Ahmed, and M. Rahman, "Use of human cognition in HIP design via emoticons to defend BOT attacks," 2012, pp. 178–185, dOI: 10.1109/ICCSE.2012.33.

[21] C. Sorrells, L. Qian, and H. Li, "Quickest detection of denial-of-service attacks in cognitive wireless networks," 2012, pp. 580–584, dOI: 10.1109/THS.2012.6459913.

[22] Y. Tan, S. Sengupta, and K. Subbalakshmi, "Analysis of coordinated denial-of-service attacks in IEEE 802.22 networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 890–902, 2011.

[23] W. Wang, M. Chatterjee, and K. Kwiat, "Collaborative jamming and collaborative defense in cognitive radio networks," 2011, dOI: 10.1109/WoWMoM.2011.5986172.