Application Layer DDoS Attack Defense Framework for Smart City using SDN

Conference Paper · May 2016

CITATIONS
6

READS
1,173

2 authors:

Narmeen Bawany
Jinnah University for Women
24 PUBLICATIONS **192** CITATIONS
SEE PROFILE

Jawwad Shamsi
National University of Computer and Emerging Sciences, Karchi, Pakistan
65 PUBLICATIONS **475** CITATIONS
SEE PROFILE

Application Layer DDoS Attack Defense Framework for Smart City using SDN

Narmeen Zakaria Bawany and Jawwad A. Shamsi
nshawoo@gmail.com and jawwad.shamsi@nu.edu.pk
Systems Research Laboratory
FAST-National University of Computer and Emerging Sciences, Karachi, Pakistan

ABSTRACT

Smart city brings enormous opportunities and exciting challenges. In a smart city, operations and services such as traffic, transport, electric power, and water distribution are monitored, operated, and controlled through ICT based infrastructure, smartly. This allows efficient management of resources and facilitates smooth access to services. However, it also induces stringent requirements and challenges for uninterrupted operation and execution of ICT-based monitoring and controlled infrastructure. Cybersecurity is one of the foremost challenge in a smart city network. That is, protecting the smart city application services from cyber-attacks and ensuring continuity of services is utmost desirable. As smart city services typically comprised of web based applications, application level distributed denial of service (AL-DDoS) attack is a major cybersecurity threat that can have catastrophic impact on an extremely critical smart city network. This paper presents an efficient framework for AL-DDoS attack detection and mitigation for a smart city network. The proposed framework utilizes Software Defined Networking (SDN) paradigm to implement resilient design that ensures continuity of smart city application services. The framework integrates a sound mechanism that distinguishes AL-DDoS attack from legitimate flash crowd. This is a novel framework that addresses the flash crowd attack detection and mitigation in a smart city environment using SDN.

KEYWORDS

Smart city, Application level DDoS Attacks, Cyber Security, Flash crowd, Software Defined Networking

1 INTRODUCTION

A metropolitan city that can monitor and control its critical infrastructure including, roads, railways, subways, airports, seaports, power plants, communication systems, etc., using Information and communication technology (ICT) is considered to be a smart city[1]. Smart city can plan and optimize its resources, and provide efficient services to its citizens. All such services require the execution of several services under an orchestrated coordination. Smart city ICT infrastructure is unique in many respects. First, smart city is a highly complex system due to its enormous structure and heterogeneity. Second, smart city comprises extremely critical city systems. These systems are so vital that their destruction or service disruption can effect security, safety and economy of cities. Third, in smart city network traffic is highly dynamic and unpredictable. For instance, any emergency situation like, accidents or earthquakes, can cause impulsive load to networks. Fourth, smart city can become a prime target for terrorism and cyber-attacks because of the critical nature of services that it provides. Enemy nations can target smart city networks and application servers to paralyze the city almost instantly.

Cyber-attacks are nearly as old as the Internet itself and the problem has only grown more multifaceted over the period of time. Organizations continue to seek better means of attack prevention, detection and mitigation techniques[2]. Some experts believe that it was cyber-attack that caused the northeast blackout

of 2003 affecting more than 50 million people in a 9,300-square-mile area, and the massive 2008 Florida blackout that shut down large portions of the power grid[3]. Distributed denial-of-service (DDoS) attacks has become one of the major cyber security threats over the last decade[4][5]. DDoS attacks can consume vast amounts of computing, memory and network resources of the service provider. This, in turn, either causes performance degradation or disruption of services to legitimate users. Public web servers, in particular, has been the main target of DDoS attacks. Utilizing the services of cloud infrastructure providers, attackers are able launch massive attacks. Most recent attack against a Cloudflare[6] customer was estimated to be around 400Gbps[7]. DDoS attack is major cybersecurity threat that can have catastrophic impact on extremely critical smart city network. Besides, the traditional volumetric DDoS attack that leverage huge amount of traffic to bring down the network services, organizations are now faced with the challenge of low and slow application layer DDoS (AL-DDoS) attacks. AL-DDoS attacks exploits legitimate HTTP requests to overwhelm target resources. AL-DDoS attack are more challenging because it often mimics or occurs in the flash crowd events of popular websites[8][9].

The strategy to protect a city's cybersecurity is critical for managing risks and improving resilience. AL-DDoS attacks are primarily launched on web servers to disrupt their services [9][10]. Generally, smart city data centers will be hosting numerous web application servers to provide web based services to the citizens thereby, making smart city applications highly prone to AL-DDoS attacks. Smart city application services need protection from AL- DDoS attacks that could cause severe stoppages to critical services. Their continued operation will be vital for the well-being of the populace. Defending such a system from AL- DDoS attack is critical as the consequence of downtime may be disastrous.

AL- DDoS attack detection and mitigation is an enormous challenge due the distinct nature of smart city network traffic. Overwhelming volume, velocity and variety of traffic that is generated from across the city makes it a daunting task. Heterogeneity of networks, applications specific and dynamic security policies, emerging threats, high availability and scalability are the basic challenges that need to be accounted for when implementing a detection and mitigation mechanism for AL-DDoS attack in a smart city. Further, distinguishing AL-DDoS attack from legitimate flash crowd traffic in a smart city scenario is a significant challenge as AL-DDoS attack is easily misled by flash crowd traffic[10][11].

This research is motivated by the above mentioned challenges and requirements for a smart city. To this end, the purpose of this research is to propose an efficient mechanism for AL-DDoS attack detection and mitigation. The proposed framework for detection and mitigation of AL-DDoS attack is pragmatic for smart city network. As the framework is based on Software defined Networking (SDN) it exploits the key benefits of the technology, including handling heterogeneity issues, controlling key network components from a central controller, etc., inherently [12]. Likewise, separation of control plane from the data plane, in SDN, provides opportunity for implementing and updating of network policies at runtime, making it a prime choice for massive and dynamic smart city system.

2 RELATED WORK

Considering that the proposed framework comprises three major areas that has been extensively studied by researchers, the related work has been divided into three categories, that is, Smart City, Application level DDoS attacks and SDN based DDoS defense mechanisms.

2.1 Smart City

Smart city has been actively studied and researchers have come up with different definitions, frameworks, and implementations of smart city [13] [14],[15][16][17]. The key objective of almost all the research is to present a strategy to mitigate the problems generated by the urban population growth by using information and communication technology. Some researchers have addressed the smart city network and infrastructure requirement proposing cloud based solutions [18][19][20]. However, not much work has been found related to application level DDoS attacks on smart city application servers. This is a critical requirement for a smart city to remain functional.

2.2 Application Level DDoS Attacks

Application layer DDoS attacks are gaining momentum in the cyberspace. These emerging and more prevalent set of DDoS attacks are difficult to detect because it resembles the legitimate traffic.These attacks establish complete TCP connections with target server and then start flooding with several HTTP requests to overwhelm the victim or saturate the available bandwidth through illegitimate traffic. As these are slow and low attacks, it is very difficult to distinguish it from legitimate traffic. Therefore, application layer attacks are more successful tools for attackers to harm victims in current times. Moreover, the key challenge, to date, in this perspective is to differentiate between an attack and a flash crowd[21]. Flash crowd refers to sudden increase in legitimate connections on a server or website occurring at the same time or within a short period [22].The work of discriminating DDoS attacks from flash crowds has been explored for around a decade. Previous work [22], [23],[24] focused on extracting DDoS attack features, and was followed by detecting and filtering DDoS attack packets by the known features. However, these methods cannot actively detect DDoS attacks [21]. Other defense against flash crowd attacks is the use of graphical puzzles or CAPTACHA to differentiate between humans and bots [25]. Detecting anomalies by modeling legitimate behavior, using different statistical models is another common method for differentiating between flash crowd and DDoS attack. For example, XieandYu [26] used the hidden semi-markovmodel, and Awad and Khalil [27] employed the all-Kth Markov model to describe web browsing dynamics. Oikonomou and Mirkovic tried to discriminate mimicking attacks from real flash crowds by modeling human behavior [28].

2.3 SDN based DDoS Detection Techniques

Many researchers have proposed variety of solutions to overcome DDoS attacks in traditional computing environment however, the DDoS attacks are becoming more widespread. Software defined networking has emerged as a new paradigm in networking and has attracted the research community more recently[12] [29]. The capabilities of SDN that includes softwarebased traffic analysis, logical centralized control, global view of the network, and dynamic updating of forwarding rules complements DDoS attack detection and mitigation mechanisms. Braga[30] proposes a light weight detection mechanism based on traffic flow features implemented over a NOX based network. It uses Self Organizing Maps (SOM) [7], an unsupervised artificial neural network, to classify network traffic as either normal or abnormal, i.e. a potential attack, taking statistics about flows as parameters for the SOM computation. However the experiments were conducted on a small scale.
Radware[31] – a commercial cybersecurity solution provider has recently developed DefenseFlow[32] which is the first commercial SDN application that addresses DDoS attacks. Radware has furthermore contributed a simplified open source version of DefenseFlow, Defense4All[33], to the OpenDaylight[34]

project. DefenseFlow directs the network controller to collect specific flow statistics from forwarding devices in the network at a per second resolution. The application measures baseline traffic flows and then monitors for patterns suggestive of a DoS attack. In the event that a threat is detected, a traffic diversion mechanism programmatically redirects suspicious traffic to a dedicated behavioral analysis system for detailed traffic inspection, signature analysis, and threat neutralization. However, Radware does not provide any details of implementation. Also, Martin et al [35] does not considers DefenseFlow as pure SDN solution.

The literature presented above provides a good starting point for understanding the limitations of existing solutions. Most of existing AL-DDoS solutions are tuned up for a specific application environment and are based on traditional networks. However, the research presented in this study focuses on smart city applications and addresses the diverse applications requirement. The proposed framework advocates a more structured attack detection and mitigation approach that leverages an architectural layering in SDNs. Likewise, almost no work has been found for distinguishing flash crowd from DDoS attack for smart city applications. The combination of following three domains, exclusively makes this work unique and inspiring:

- Smart city applications context
- Application level DDoS attack detection and mitigation for smart city application servers
- Distinguishing smart city applications legitimate Flash crowd from flash crowd attack

The novelty of this work lies in utilizing SDNs for detecting and mitigating AL-DDoS attacks, explicity identifying flash crowd attacks in smart city context. Moreover, this work presents a comprehensive framework for handling application specific security requirements dynamically.

3 PROPOSED FRAMEWORK

In order to address the aforementioned requirements, a proficient framework is required to detect and mitigate DDoS attacks in a smart city. Such a framework should not only ensure efficient detection and mitigation of DDoS attacks but also distinguish DDoS attack traffic from flash crowd. This work presents a novel framework where the capabilities of SDN are utilized for detection and mitigation of DDoS attack in a smart city environment. The framework, also includes, a dedicated module to distinguish a flash crowd attack traffic from a genuine flash crowd. The objective is to ensure the smooth functioning of smart city application servers by ensuring an efficient defense against DDoS attacks.

SDN has been proposed as a candidate of the next generation Internet architecture and organizations such as Google, Cisco, HP and Intel have already adopted SDN in their internal data centers and WANs [36][37][38]. This makes SDN an ideal choice for smart city network. The proposed framework exploits the inherent benefits of SDNs that are derived by the separation of control plane and data plane. Traditional networking paradigms fail to provide a logical centralized view of the network. The concept of SDN is actually a useful security technique, as it supports the customization of devices to the highest level at runtime. The configuration policies at a central controller can be implemented on all network devices instantly resulting in whole new layer of security.

The framework will efficiently analyze and filter the attack traffic flows from legitimate traffic flows. This will prevent the malicious traffic from impacting the performance of services. Legitimate traffic will be forwarded to complete the transactions without being

effected. Eventually, the business continuity will be maintained. The idea is to detect network attack patterns, by exploiting machine learning techniques, in real-time and to distinguish it from a flash crowd. The attack pattern once detected is shared with application service providers in the smart city. Application specific traffic patterns are accounted for when analyzing network traffic for attack. The proposed solution benefits from existing approaches implemented in traditional networks for DDoS attacks detection and mitigation and combines these with the advantages of SDN. The resultant framework provides comprehensive solution that addresses DDoS attack security requirements in a massive smart city network.

3.1 SDN based Controller Architecture for Smart City Application Servers

Understandably, a smart city network comprising hundreds of application servers is a huge network. Therefore, a single point controller cannot be practically efficient. The framework, illustrated in figure 1, lays down three-tier high level depiction of the application servers and controllers. Hierarchical approach is used to counter for application specific application requirements, sharing of threat information, to meet reliability and efficiency requirements, to maintain autonomy of each application service provider, and to follow resilience design approach.

3.1.1 Service Controller Layer

The Service Controller Layer (SCL) comprises of all the controllers. Each controller implements its own application specific security requirements. The AL-DDoS attack detection and mitigation module is tuned specific to the requirements of the hosted service. For instance, the live city traffic controller application server will have its own traffic patterns and thresholds based on the

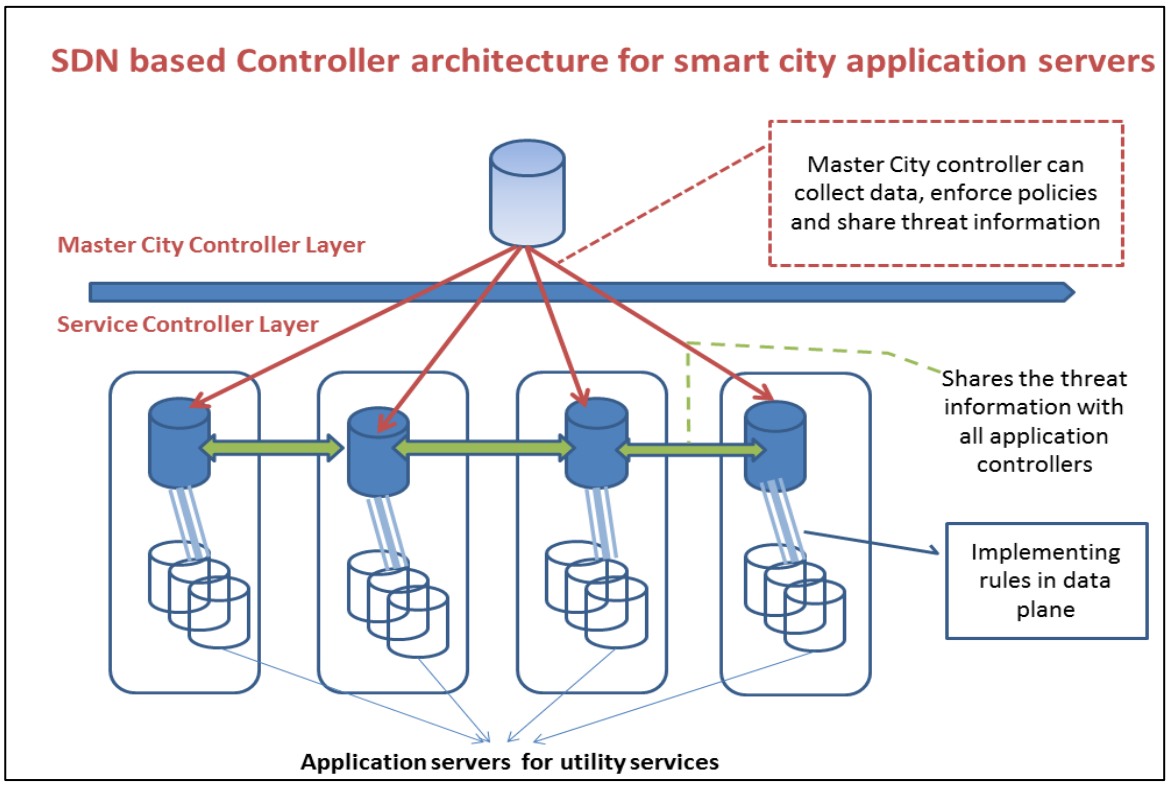

Figure 1: SDN based Controller architecture for smart city application servers

number of users. Similarly, smart grid users will have their unique characteristics with varying number of mobile and non-mobile users. Likewise, mitigation policy will also differ in each case. Therefore, each controller can independently implement and update their security policies across their application servers. Within a service controller layer, each controller can share the threat information with other controllers. This information sharing leads to efficient prevention of the possible attacks.

3.1.2 Master City Controller

Master City Controller (MCC) is basically used for recordkeeping, monitoring and overall threat analysis across whole city application services. The information collected at this server is critical for city administrators as it gives useful insights about cyber threats and development of city level cyber threat model. MCC can also share the threat information or any other information with SCL. Furthermore, threat model of MCC can be shared with other cities giving rise to country level threat model..

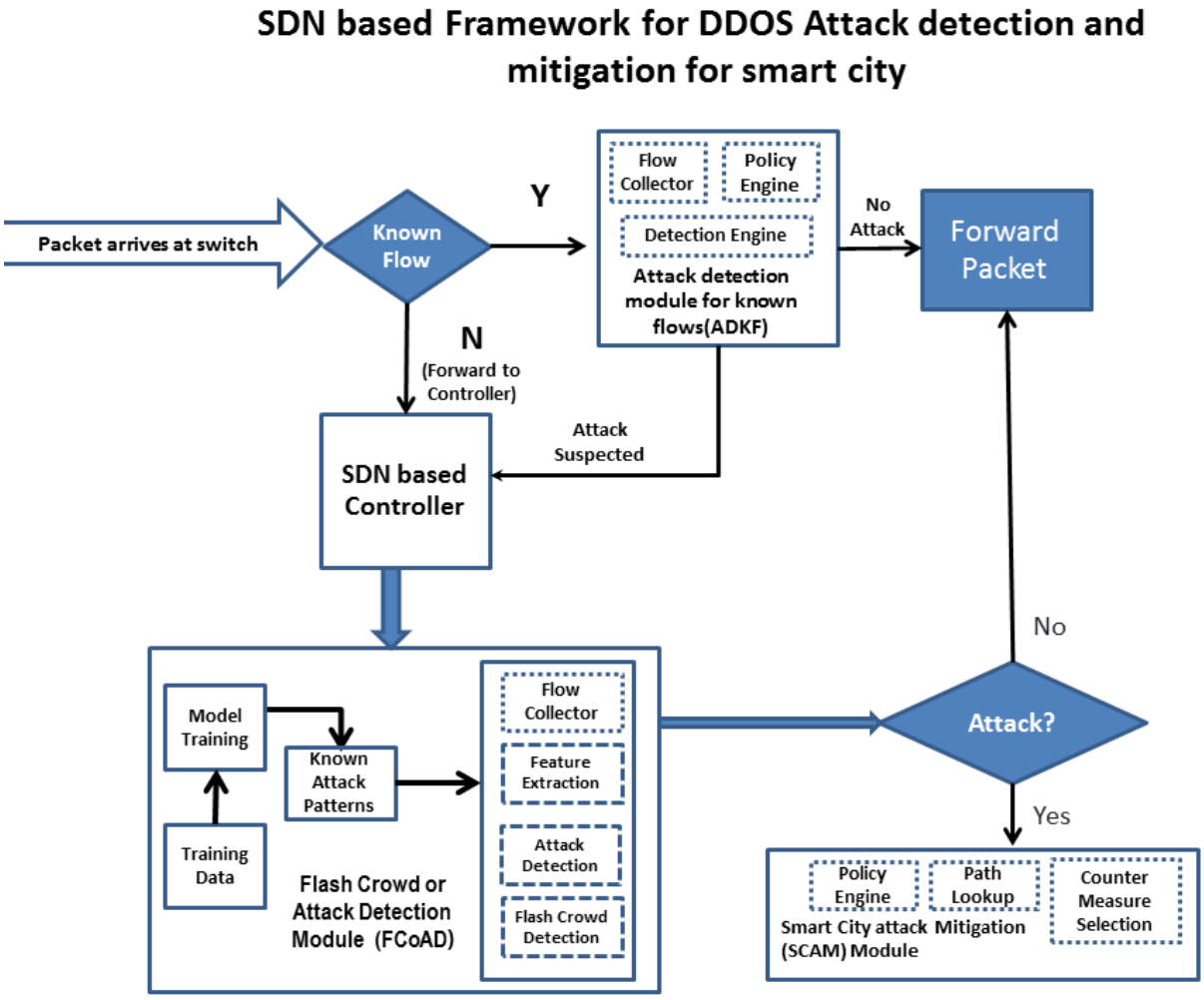

Figure 2: SDN based Framework for DDOS Attack detection and mitigation for smart city

3.2 Framework for DDOS Attack Detection and Mitigation for Smart City

The work flow of attack detection and mitigation module is depicted in figure 2. When a new packet arrives at the switch checks whether it belongs to existing flow. If so, it updates the flow statistics otherwise it is sent to the controller. Existing flow traffic is also monitored by Attack detection for known flows (ADKF) module. The packets marked as suspicious by ADKF module and the packets that does not have entries in switch flow tables are sent to controller. Controller queries the Flash Crowd or Attack Detection (FCoAD) Module for the packet flow. If the query result indicates an attack, FCoAD issues an alert to Smart City attack Mitigation (SCAM) Module. If the query result is normal, the packet is forwarded to its intended destination.

3.2.1 Attack Detection Module for Known Flows (ADKF)

ADKF consists of Flow Collector, Policy Engine, and Detection engine. Flow collector collects the flow statistics from switch for each flow. OpenFlow switches maintain counters for each flow table and flow entry. The module checks if amount of flow is within the permitted limits and does not violate Quality of service (QoS) parameters set up by policy engine. For e.g., if the flow ' A' exceeds the maximum transmission threshold defined by the policy engine the flow is sent to detection engine for further processing.

3.2.2 Flash Crowd Attack Detection (FCAD) Module

This module consists of many sub modules. Initially, training dataset is provided to tune up the system for normal and attack traffic patterns. Dataset will be updated regularly to improve the attack patterns. Feature Extractor module extracts the traffic flow features from the statistics collected by flow collector. On the basis of features, the traffic is either classified as attack traffic or legitimate traffic by Attack detection module. Flash Crowd detection module specifically deals distinguishing flash crowd attacks and genuine flash crowds.

3.2.3 Smart City Attack Mitigation (SCAM) module

This module receives the traffic that is classified as attack by FCAD module. Administrators can configure mitigation policies for each flow or group flows using Policy Engine. Based on these policies, counter measure is selected by the SCAM module. The path lookup is used to maintain a table of paths. Paths are assigned to flows based on the policies defined by policy engine. For e.g. Malicious flash crowd attack traffic is diverted to a path that lead to sinkhole.

4 Conclusion

Smart city network is a rapidly expanding network. User, applications and services will be increasing at fast pace. Hence, the AL-DDoS detection and mitigation mechanism must be effectively scalable. Secondly, the smart city network being enormous by nature will lead to dynamic network topologies. Nodes will be added or removed very frequently for maintenance, adding or upgrading of services, or any other reasons that cannot be foresighted. Furthermore, the smart city network comprises many critical systems with high availability requirements, like smart grid, smart traffic management, smart transportation, etc., each working autonomously. The infrastructure for all these systems cannot be in place at a time but will be added gradually. This will lead to heterogeneous network infrastructure which cannot afford any downtime. Likewise, diversity of applications is obvious in smart city systems, each application providing specific set of services to users. These applications will have varying level of network traffic and will need security policies according to their own

set of requirements. Moreover, these security policies will be highly dynamic. Changing city situations like, natural disasters, accidents or breaking news may require updating of security policies across the smart city network almost instantly. Efficiency of detection and mitigation mechanism along with low overhead is an inherent requirement of such a critical and large scale system. Therefore, it is desirable that DDoS detection and mitigation is lightweight, scalable and easy to manage. Additionally, intimation of threats information across all smart city systems will help in early detection and prevention of service disruption. This paper presents a novel SDN based framework for detection and mitigation of DDOS attack for the smart city application servers. The framework is designed to protect smart city services against known and emerging AL DDoS attacks that threaten the availability of real time services. Moreover, as smart city applications may experience flash crowds more frequently, distinguishing flash crowd attack from legitimate flash crowd traffic leads to more reliable attack detections.

References

[1] H. Chourabi, T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli, K. Nahon, T. a. Pardo, and H. J. Scholl, "Understanding Smart Cities: An Integrative Framework," *2012 45th Hawaii International Conference on System Sciences*, pp. 2289–2297, Jan. 2012.

[2] A. Bodhani, "Feeling lucky? [Special Report Cyber Security]," *Engineering & Technology*, vol. 10, no. 1, pp. 44–47, 2015.

[3] S. Harris, "China's Cyber Militia," *National Journal*, 2008. [Online]. Available: http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531.

[4] Z. Tan, a Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 447–456, 2014.

[5] J. Yuan and K. Mills, "Monitoring the macroscopic effect of DDoS flooding attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 4, pp. 324–335, 2005.

[6] Cloudflare, "Cloudflare Organization." [Online]. Available: https://www.cloudflare.com. [Accessed: 08-Aug-2015].

[7] S. Musil, "Record-breaking DDoS attack in Europe hits 400Gbps," *CNET*, 2014. [Online]. Available: http://www.cnet.com/news/record-breaking-ddos-attack-in-europe-hits-400gbps/.

[8] J. Choi, C. Choi, B. Ko, and P. Kim, "A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment," *Soft Computing*, vol. 18, no. 9, pp. 1697–1703, 2014.

[9] and C. L. Liao, Qin, Hong Li, Songlin Kang, "Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching," *Security and Communication Networks*, 2015.

[10] W. Zhou, W. Jia, S. Wen, Y. Xiang, and W. Zhou, "Detection and defense of application-layer DDoS attacks in backbone web traffic," *Future Generation Computer Systems*, vol. 38, pp. 36–46, Sep. 2014.

[11] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1073–1080, 2012.

[12] W. Xia, Y. Wen, S. Member, C. Heng Foh, D. Niyato, and H. Xie, "A Survey on Software-Defined Networking," *Ieee Communication Surveys & Tutorials*, vol. 17, no. 1, pp. 27–51, 2015.

[13] R. Giffinger and N. Pichler-Milanović, "Smart cities: Ranking of European medium-sized cities," 2007.

[14] S. Paroutis, M. Bennett, and L. Heracleous, "A strategic view on smart city technology: The case of IBM Smarter Cities during a recession," *Technological Forecasting and Social Change*, 2013.

[15] R. M. Kanter and S. S. Litow, "Informed and Interconnected: A Manifesto for Smarter Cities," *Working Paper*, vol. 09–141, pp. 1–28, 2009.

[16] S. Alawadhi and A. Aldama-Nalda, "Building understanding of smart city initiatives," *Electronic Government. Springer Berlin Heidelberg*, 2012.

[17] S. Idowu, "MASTER ' S THESIS A Development Framework for Smart City Services A Development Framework for Smart City Services."

[18] G. A. Zhang, J. Y. Gu, Z. H. Bao, C. Xu, and S. B. Zhang, "Towards a Smart City based on Cloud of Things, a survey on the smart city vision and paradigms," *European Transactions*

on Telecommunications, vol. 25, no. 3, pp. 294–307, 2014.

[19] R. Petrolo, V. Loscrí, and N. Mitton, "Towards a smart city based on cloud of things," in *Proceedings of the 2014 ACM international workshop on Wireless and mobile technologies for smart cities - WiMobCity '14*, 2014, pp. 61–66.

[20] N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, "Combining Cloud and sensors in a smart city environment," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1. p. 247, 2012.

[21] S. Yu, S. Member, S. Guo, and I. Stojmenovic, "Fool Me If You Can : Mimicking Attacks and Anti-Attacks in Cyberspace," vol. 64, no. 1, pp. 139–151, 2015.

[22] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites," in *Proceedings of the 11th international conference on World Wide Web (WWW '02)*, 2002, pp. 293–304.

[23] G. Carl, G. Kesidis, R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *Internet Computing, IEEE*, 2006.

[24] Y. Chen and K. Hwang, "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis," *Journal of Parallel and Distributed Computing*, 2006.

[25] S. Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz-4-sale: Surviving organized DDoS attacks that mimic flash crowds," *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation. USENIX Association*, vol. 2, pp. 287–300, 2005.

[26] Y. Xie and S. Yu, "A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors," *Networking, IEEE/ACM Transactions on*, 2009.

[27] M. A. Awad and I. Khalil, "Prediction of user's web-browsing behavior: Application of markov model," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 42, no. 4, pp. 1131–1142, 2012.

[28] G. Oikonomou and J. Mirkovic, "Modeling human behavior for defense against flash-crowd attacks," in *IEEE International Conference on Communications*, 2009.

[29] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, Jan. 2013.

[30] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS Flooding Attack Detection Using NOX / OpenFlow," pp. 408–415, 2010.

[31] Radware, "http://www.radware.com." .

[32] R. Meyran, "DefenseFlow: The First Ever SDN Application that Programs Networks for DoS/DDoS Security," 2013. [Online]. Available: http://blog.radware.com/security/2013/04/defenseflowdosddos-security/.

[33] Radware, "DefenseFlow NetFlow and SDN based DDoS Attack Defense," 2013. [Online]. Available: http://www.radware.com/Products/DefenseFlow/.

[34] Linux Foundation, "http://www.opendaylight.org." .

[35] M. Vizváry and J. Vykopal, "Future of DDoS Attacks Mitigation in Software Defined Networks," *Monitoring and Securing Virtualized Networks and Services. Springer Berlin Heidelberg*, 2014.

[36] S. Jain, A. Kumar, and S. Mandal, "B4: Experience with a globally-deployed software defined WAN," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, 2013.

[37] "Business Case for Cisco SDN for the WAN," *ACG Research*, 2014.

[38] S. H. Sterling Perrin, "Practical Implementation of SDN and NFV in the WAN," 2013.