Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures

William Hurst, Nathan Shone, Quentin Monnet

Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures

William Hurst, Nathan Shone
School of Computing and Mathematical Sciences,
Liverpool John Moores University,
Liverpool, UK
{W.Hurst, N.Shone}@ljmu.ac.uk

Quentin Monnet
Université Paris-Est,
LACL (EA 4219), UPEC,
F-94010 Créteil, France
Quentin.monnet@lacl.fr

***Abstract*—Over the last decade, the level of critical infrastructure technology has been steadily transforming in order to keep pace with the growing demand for the services offered. The implementation of the smart grid, which relies on a complex and intelligent level of interconnectivity, is one example of how vital amenity provision is being refined. However, with this change, the risk of threats from the digital domain must be calculated. Superior interconnectivity between infrastructures means that the future cascading impacts of successful cyber-attacks are unknown. One such threat being faced in the digital domain is the Distributed Denial of Service (DDoS) attack. A DDoS has the goal of incapacitating a server, network or service, by barraging a target with external data traffic in the form of communication requests. DDoS have the potential to cause a critical infrastructure outage, and the subsequent impact on a network of such infrastructures is yet unknown. In this paper, an approach for assessing the future impacts of a cyber-attack in a network of critical infrastructures is presented; with a focus on DDoS attacks. A simulation of a critical infrastructure network provides data to represent both normal run-time and an attack scenario. Using this dataset, a technique for assessing the future impact of disruptions on integrated critical infrastructure network, is demonstrated.**

Index Terms—*Critical Infrastructure, Cyber-Attack Distributed Denial of Service, Simulation, Cascading Failure*

1. INTRODUCTION

Critical infrastructures present tempting targets for cyber-attackers. Society has a high reliance on the services provided and any disruption would have severe impacts on the economy, social well-being, and potentially even leads to loss of life [1]. Their service provision is becoming increasingly reliant on ICT networks, meaning they are more vulnerable than ever before to attacks emerging from cyber-space. Particularly, with the continued integration of wireless components and Internet enabled control system software, the last decade has seen a significant increase in the number of access points within infrastructure networks.

Traditionally, critical networks were closed to the outside world. However, the need for remote access within critical infrastructure networks has become increasingly crucial. This is predominantly due to their continuing growth, vast geographic distribution and increasing dependence on automation. In consequence, key service providers are increasingly reliant on the interconnectivity and remote access to centrally manage the component systems.

Presently, there is a growing level of interdependence between different critical infrastructures. For example, through the introduction of the smart grid, power plants, a once isolated infrastructure, have become intertwined with others to provide a more intelligent distribution service. There is also a physical dependence; critical infrastructures rely on each other to continue the provision of their own services. For example, civilians need to be able to access the emergency services at any time; however, the emergency services heavily rely on the availability of the telecommunications network; which in turn relies upon the provision of stable power supply.

Distributed Denial of Service (DDoS) attacks, in particular, pose a significant threat to critical infrastructures, companies and e-government services around the globe. A successful DDoS attack on an infrastructure has the potential, to not only impact the target, but cause a cascading effect. Often service provision crosses borders, meaning any impact would cause wide-spread devastation, affecting multiple countries.

The key challenge lies in the ability to block DDoS attacks, which are hard to identify. The nature of the attack means that a huge volume of traffic data originates from millions of different devices. As the devices are usually owned by law-abiding civilians, who are unaware of the event taking place, blocking the source of the traffic is a challenge. The attacks are caused by a hijacked network of computers, known as a botnet, controlled by a botmaster. They have the potential to be used for serious cyber-criminal activity; as this form of attack can be so powerful, the computing power of the target is exhausted [2]. As a result, the service provision is disrupted.

The reasons for a cyber-attack taking place vary. Frequently, the motivation is political, whereby key targets are taken down by activists or groups with a political message. Websites offer ideal targets for DDoS attacks, as they operate as the frontend and provide the customer interface, so the impact of an attack is noticeable. The effect is that users are unable to access the service due to the volume of traffic blocking access to the servers hosting the website. One example of this was the disruption to Wikileaks, caused by traffic at the level of 10 Gigabits per second [3]. Other high-

profile cases, such as the widely publicised attacks on Visa, MasterCard and the PlayStation network, show the real-threat being faced [4].

In this paper, the potential effects of a disruption to a critical infrastructure network caused by a DDoS are presented. In a future, which contains inherent cyber-threat insecurities, the need to plan for attacks and improve the level of resilience is greatly needed. The remainder of this paper is structured as follows. Section 2 provides a background discussion on DDoS attacks. Section 3 presents a simulation of a network of critical infrastructures used for data construction. Section 4 provides an account of how the proposed framework uses data classification techniques to analyse subtle changes in critical infrastructure behaviours. Section 5 presents a discussion on the results and highlights, how the techniques can be used to plan for assessing the future impact of cascading failure. Finally, the paper is concluded in Section 6.

2. BACKGROUND

With the volumes of complex attacks starting to increase, there is a real present threat to critical infrastructures. In this subsection, the DDoS attack type is presented as a demonstration of the variety of attacks facing future critical infrastructure technologies.

2.1 DDoS

A DDoS attack involves overloading routers and intermediate links by sending them enormous volumes of network traffic [4]. It effectively functions as a cyber-army, which can span across the globe, without the user having to invest in their own hardware or own any physical components [5]. The popularity of the attack is due to the operator having an objectively high level of anonymity. There are numerous different types of DDoS, some of which include: SYN flood, peer-to-peer and permanent denial of service. Each of which is explained as follows:

- SYN Flood: Known as a Transmission Control Protocol Synchronised Flood (SYN Flood), the attack scenario involves exploiting the TCP connection establishment process [6]. Specifically, to establish a connection, a device sends and receives a SYN. The DDoS attack, in this case, functions by making the server unavailable and the SYN process is blocked.
- Peer-to-peer: This type of attack normally involves forcing clients of significant peer-to-peer file sharing centres, to connect to a victim after disconnecting from their own network. These attacks operate differently to a botnet and the bot computers are often controlled individually.
- Permanent denial of service: Often DDoS attacks can be so severe that the target hardware needs replacement as a result. This is known as a permanent denial of service (PDoS), where backdoors are exploited and used to target device firmware which is replaced by the attackers' own firmware.

The commonality in all types of DDoS attacks is that they are problematic to block, as distinguishing between good and bad requests to a server is a challenge. Finding a way to improve cyber-defences is of huge importance to safeguard the increasing use of wireless sensor networks (WSN) and dependence on interconnectivity in critical infrastructure networks. Consequently, in the following section, the vulnerabilities of WSNs are detailed.

2.2 DDoS and WSNs

Some specific architectures are particularly vulnerable to denial of service attacks. WSNs are one of those. Sensors are small devices spread over a monitored area, and they are expected to collect physical data upon their environment. Because they may be used in remote places or in hostile environments (hard to access areas, or battlefields for instance), they embed cheap hardware and are subject to strong limitations: they have low computation abilities, little available memory, and their battery is generally non-refillable. For these reasons, and because sensors communicate only through wireless protocols, WSNs are especially vulnerable to denial of service attacks [7].

DoS in WSNs embraces many different attacks, which can target all layers of the network [8]. Jamming the radio frequencies and disturbing the routing protocols are just two examples of ways to harm the network. Even jamming can actually be performed in a variety of ways [9]. In reaction to these, a number of solutions have been proposed [10]. Many solutions rely on trust models [11], [12]. Agents then apply a set of traffic rules [13] to assign a trust value to each of the nodes in the network. In that way, a simple detection system is constructed, which consists of a set of nodes called 'guarding nodes' that analyse traffic in a clustered network [14]. When detecting abnormal traffic from a given node, guarding nodes identify it as a compromised node and inform the cluster head (CH) of this fact. Upon receipt of reports from several distinct monitoring nodes (to prevent false denunciation from a compromised node), the CH virtually excludes the suspicious node from the cluster. The authors show the benefit of their method by presenting numerical analysis of detection rate. Although the method is efficient for detecting rogue nodes, the authors do not give details of the election mechanism for choosing the guardian nodes. Also, there is no mention in their study of renewing the election in time, which causes the appointed monitoring nodes to endorse heavier energy consumption over a long period.

The most effective method of detecting a DoS attack in a WSN is simply to run a detection mechanism on each single sensor. Of course, this solution is not feasible in a network with constraints. Instead of equipping each sensor with such a mechanism, it is proposed in [15] to resort to heuristics in order to place several nodes equipped with detection systems at critical spots in the network topology. This optimised placement strategy enables distributed detection of DoS

attacks and reduces costs and processing overheads, since the number of required detectors is minimised. But those few selected nodes are likely to run out of battery power much faster than normal nodes. Some works examine the possibility of detecting the compromising of nodes as soon as an opponent physically withdraws them from the network. In the method that is developed in [16], each node keeps a watch on the presence of its neighbours. The Sequential Probability Radio Test (SPRT) is used to determine a dynamic time threshold. When a node appears to be missing for a period longer than this threshold, it is considered to be dead or captured by an attacker. If this node is later redeployed in the network, it will immediately be considered as compromised without having a chance to be harmful. Nothing is done, however, if an attacker manages to compromise the node without extracting the sensor from its environment. In [17], a revised version of the OLSR protocol is proposed. This routing protocol called DLSR aims at detecting distributed denial of service (DDoS) attacks and at dropping malicious requests before they can saturate a server's capacity to answer. To that end, the authors introduce two alert thresholds regarding this server's service capacity.

The authors also use Learning Automata (LAs), automatic systems, whose choice of next action depends on the result of its previous action. There is no indication in their work about the overhead or the energy load resulting from the use of the DLSR protocol. A novel broadcast authentication mechanism can also be deployed so as to cope with DoS attacks in sensor networks such as in [18]. This scheme uses an asymmetric distribution of keys between sensor nodes and the sink, and uses a Bloom filter as an authenticator, which efficiently compresses multiple authentication information. In this model, the sink, shares symmetric keys with each sensor node, and proves its knowledge of the information through multiple MAC values in its flooding messages. When the sink floods the network with control messages, it constructs a Bloom filter as an authenticator for the message. When a sensor node receives a flooded control message, it generates their Bloom filter with its keys and in the same way sink verifies message authentication.

2.3 Related Research

There are many concerns surrounding the resilience of future critical infrastructure networks, particularly when faced with DDoS attacks. One emerging type of critical infrastructure network is that of smart utility grids, with their increasing levels of complexity, interconnectivity and interdependence. Unfortunately, as with most new technologies, smart grid security is still in a juvenile stage [19] and there is currently a lack of defined standards. Hence, the effects that a DDoS attack will have on such dynamic and complex networks is extremely difficult to predict and therefore largely unknown.

Smart grids are highly complex networks comprised of millions of computing agents; the majority of which will be internet-facing. Unfortunately, this means that large parts of the grid will be exposed to DDoS attacks, which can ultimately lead to cascading failures throughout the infrastructure. In a smart electric grid, the predominant idea is to balance power distribution. For this, the Advanced Metering Infrastructure (AMI) is used, but its openness exposes many potential weak points within the network [20] that can be targeted by DDoS attacks to maximise impact and disruption throughout the grid. For example, targeting smart meter aggregators/gateways can prevent current energy consumption from being reliably measured. This in turn can affect the power availability of local and regional substations and ultimately the demand on the power stations. The potential repercussions of such attacks are highly significant, ranging from the interrupting the availability of individual components, to mass power outages or damage to infrastructures.

The security and resilience of future critical infrastructures is of vital significance to their success and functionality. The ease at which DDoS attacks can be launched and their high level of efficiency is concerning for safety of future critical infrastructures. This is particularly prevalent as the EU Commission aims to have at least 80% of Europe using smart electric meters by 2020 [21].

3. CRITICAL INFRASTRUCTURE SIMULATION

To counter the growing threat of DDoS attacks and predict the future impacts of other cyber-attack types, simulation presents an ideal tool to experiment with new and innovative security measures. In this paper, a simulation of a city, which is used to construct data and trace the effects of a DDoS attack in a network of critical infrastructures, is presented. The simulation consists of seven infrastructures, all interconnected by a network of cables and pipes, used for electricity, communication and water distribution. The infrastructures encompassed include: a power plant, an industrial infrastructure, a telecommunications infrastructure, a water distribution plant, residential housing and businesses. The software is based on object-oriented modelling, where each component is an individual object, which can be adjusted. When linked together, the system functions, as shown in Figure 1.

A. Simulation

During simulation run-time, the behaviour of one of the infrastructures has a direct impact on another. When a component failure occurs, the city is able to keep functioning, but the effects of the fault should be visible in the dataset. In addition, the effects of a cyber-attack are able to propagate as a result of interdependencies. For example, disruption of service provision from the power plant would directly affect telecommunications and water production, which rely on power to function. In the simulation, the individual *blue blocks* represent a visualisation of water flow. The *yellow blocks* represent units of energy generated by the power plant. The *green blocks* represent a network communication between infrastructures.

The system functions consistently during runtime. However, the output and behaviour differs slightly each time the simulation process takes place, resulting in variance in the datasets constructed.

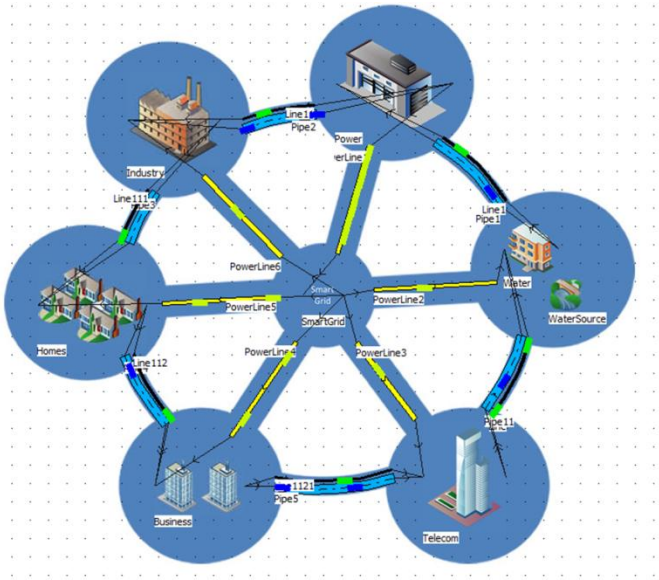

Figure 1 Critical Infrastructure Simulation Overview

The simulation presented is set in a format which is rudimentary to follow, for graphical purposes, and is used to construct granular data. Specifically, individual behavioural datasets for each of the critical infrastructures operating in the networked grid can be constructed.

B. Experiment Overview

As previously mentioned, the effects of a DDoS attack on one infrastructure may have the potential to cascade throughout the network of infrastructures. The aim of this research is, therefore, to propose a technique for identifying the cascading effects of a DDoS attack in particular. The ambition of the research is to develop a technique which can assist with the future planning and development of more resilient critical infrastructure interconnectivities. Often the impact of a minor disruption in one infrastructure on another may appear trivial and hard to identify; however, frequently the results can have a significant impact on service provision.

The data constructed from the simulation is used to present the effects of a DDoS attack, and propose a system for tracing its effects as its impact moves through the network. This research is noteworthy, particularly as countries, such as the UK, are migrating towards the use of the smart grid. The smart grid relies on an interconnectivity of services to offer a more intelligent utility distribution network. It is essential to plan for disruptions to technologies such as this, and predict how cyber-attacks will have a different impact in the future. As more digital and automation services are introduced, in order to match the growing demand for services offered by critical infrastructures, predicting the impact of a cyber-attack is vital.

In the simulation, an attack is introduced to the grid in a process which involves overloading the telecommunication plant with data requests. This acts as a simulation of a DDoS attack; disrupting how the infrastructures to communicate between each other. The attack threat is implemented through a direct connection to the telecommunications plant from an outside source. At this point, data is extracted from the simulation when functioning both normally and when under a cyber-attack. By completing this process, the dataset can be used to propose an approach for predicting the impact of attacks, which have the ability to cause a cascading effect. In the following section, the methodology and system framework is presented.

4. Methodology

As critical infrastructure datasets are significantly large, the proposed system operates through a serious of modules, which are based in a cloud environment for scalability purposes. The aim of the framework is to put forward a technique for the prediction of cascading effects in an interconnected network of critical infrastructures.

A. Framework

This process includes various stages, such as: data collection, cleaning and normalisation of raw data, feature extraction, data classification and visualisation. Cleaning involves verifying that there are no missing values and smoothing out data which inconsistent. Noisy data, which refers to corrupt and meaningless values, are also removed. The features selected are unique for each critical infrastructure but they could include: overall water volumes, energy creation, water levels or speed of water flow. They are constructed by cataloguing the data into designated representations of the dataset. Classification is achieved using the features to train classifiers to detect subtle changes in system behaviours. This process is known as supervised learning. The classification results are then visualised in a graphical format and communicated to the user through a GUI. The system has its own user interface, which allows the operator to interact with the system. The framework is displayed in Figure 2 below.

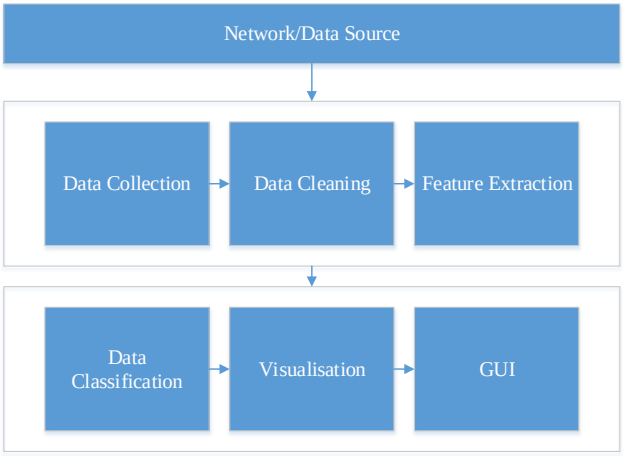

Figure 2 High Level Framework

B. Data Classification

The data classification is essential in order to identify variations in patterns of activity, which are often subtle and a challenge to identify. The evaluation process discussed in this paper uses supervised learning; this involves giving the classification algorithms the 'correct answer' to allow them to operate self-sufficiently. By using this method, classifiers are trained using features extracted from the dataset, to identify when anomalous behaviour has occurred in one critical infrastructure, as a result of a failure in another.

The approach involves specific data classification techniques, including: Uncorrelated Normal Density based Classifier (UDC), Quadratic Discriminant Classifier (QDC), Linear Discriminant Classifier (LDC), Polynomial Classifier (POLYC), k-Nearest Neighbour (KNNC), Decision Tree (TREEC), Parzen Classifier (PARZENC), Support Vector Classifier (SVC) and Naïve Bayes Classifier (NAIVEBC). Each of these classifiers was chosen as they have the ability to learn how to recognise abnormal values in a dataset. They also employ a supervised learning approach, which is a key part of the approach. In the following section, the classification evaluation techniques are presented. Each of the techniques provides an assessment of the classifiers' success or failure when classifying the data

5. EVALUATION

The dataset constructed from the simulation included a collection of 29 features and 12 records of data; 6 normal and 6 abnormal behaviour, for an initial case study. A sample of the data is presented in Table 1. The normal behaviour refers to when the critical infrastructures are functioning correctly and with no interferences.

Table 1. Data Sample

Label	Feature1	Feature2	Feature3	Feature4
Normal	13.556	13.556	3.6560	3.6560
Normal	19.427	19.427	5.4280	5.4280
Normal	24.488	24.488	7.0840	7.0840
Normal	30.475	30.475	8.7390	8.7390
Normal	37.265	37.265	8.3950	10.000
Normal	6.5170	6.5170	2.0000	2.0000
Attack	13.556	13.556	9.7120	19.136
Attack	19.427	19.427	17.195	20.907
Attack	24.488	24.488	22.563	22.563
Attack	30.475	30.475	24.219	24.219
Attack	37.265	37.265	10.000	23.875
Attack	6.5170	6.5170	5.2000	17.136

Abnormal behaviour refers to the city functioning in a cyber-attack scenario state. The dataset used for the classification process was constructed through running the simulation for a 24 hour period as normal and a 24 hour period under a DDoS attack on the telecommunications network. The dataset refers only to the effects of communication behavioural changes. As the dataset shows, in Table 1, some of the attack and normal behaviour values are the same for certain features. However, the changes in behaviour can be seen in others.

A. Approach

The results of the classification process are calculated using a confusion matrix which determines the distribution of errors across all classes. The estimate of the classifier is calculated as the trace of the matrix divided by the total number of entries. Additionally, a Confusion Matrix provides the point where miss-classification occurs. In other words, it shows true positive (TP), false positive (FP), true negative (TN) and false negative (FN) values. Diagonal elements show the performance of the classifier, while off diagonal presents errors.

TP	FN
FP	TN

Using the confusion matrix, the success rate of each classifier can be evaluated by dividing the number of True Positive and True Negative results by the total number of feature vectors, as displayed in the following formula:

$$\frac{TP + TN}{TP + FP + TN + FN}$$

In addition to providing the success rate, the confusion matrix also provides the calculation of the sensitivity and specificity for each classification. Sensitivity is identification of positive results in a data set. This refers to accurately detected normal system behaviour and it is calculated using the formula:

$$\frac{TP}{TP + FN}$$

Whereas, Specificity is the identification of negative results and is calculated using the following formula. Again, in this paper, this refers to accurately detected normal and anomalous system behaviour.

$$\frac{TN}{TN + FP}$$

Using the confusion matrix, specificity and sensitivity results, it is possible to evaluate ability of each of the data classifiers abilities to detect anomalous behaviour.

B. Results

The results are displayed in Table 2. The classification process had mixed results, with an average classification success rate of 62.96%. SVC and PolyC were the most successful and able to classify 100% of the behaviour accurately. The results demonstrate how behavioural patterns can be analysed. A change in one infrastructure impacts another, and the impact can be identified using the SVC and PolyC classifiers.

Table 2. Classification Results

	AUC	Error	Sensitivity	Specificity
LDC	83.33	0.17	1.00	0.67
UDC	50.00	0.50	1.00	0.00
QDC	33.33	0.67	0.00	0.67
SVC	100.00	0.00	1.00	1.00
ParzenC	33.33	0.67	0.33	0.33
TreeC	66.67	0.33	1.00	0.33
KNNC	33.33	0.67	0.67	0.00
NaivebC	66.67	0.33	1.00	0.33
PolyC	100.00	0.00	1.00	1.00

C. Discussion

Critical infrastructures, which are seemingly separate, heavily rely on each other for an effective service provision. The technique presented, demonstrates how it is possible to assess the impact of a cyber-attack, in this case a DDoS attack in a network of infrastructures. Applying the above technique to individual critical infrastructure datasets demonstrates how the changes in behaviour of one infrastructure can be identified in the operation of another. This can be either through a direct or indirect connection. The results show that the classifiers are able to identify behavioural changes, with a mean average of 62.96%. The sensitivity results (normal behaviours), were relatively successful, with 6 of the 9 classifiers able to identify 100% of the normal behaviour. The specificity results, however (attack behaviour changes) were less-successful; with only 2, (SVC and PolyC) able to identify 100% of abnormal behaviour occurrences. For that reason, future work will focus on both classifiers for prediction.

6. Conclusion and Future Work

The aim of this research is to highlight an innovative approach for institutions to calculate the impact of cascading failures, and subsequently plan for resilience. The most ideal approach for countering the growing cyber-threat problem is to plan for the effects of a failure taking place in an interconnected network. It is essential to increase the level of resilience by ensuring that recovery plans are put in place in order to be prepared for when a cascading failure occurs. To expand on this work in the future, an enlarged dataset including more records will be used. A case study into the individual behaviour of one infrastructure, when a fault occurs in another, will also be investigated. The simulation of a critical infrastructure will be expanded, in order to incorporate a greater network or infrastructures and interconnectivities. Finally, the future work will also extend the experimentation to include data from a real smart grid network, and the processing of this data in a cloud environment.

References

[1] R. Poisel, M. Rybnicek, and S. Tjoa, Game-based Simulation of Distributed Denial of Service (DDoS) Attack and Defense Mechanisms of Critical Infrastructures, *Proceedings of IEEE 27th International Conference on Advanced Information Networking and Applications*, pp. 114–120, 2013.

[2] C. Kavitha, Complete study on distributed denial of service attacks in the presence of clock drift, Proceedings of the International Conference on Information Communication and Embedded Systems, pp. 1–6, 2014.

[3] BBC Technology News, Wikileaks website back online after DDoS cyber-attack, [Available at: http://www.bbc.co.uk/news/technology-19255026], Accessed June 2015.

[4] Corero First Line of Defence, Corero Network Security Reports on Top 5 DDoS Attacks of 2011. [Available at: http://www.corero.com/company/newsroom/press-releases/-corero-network-security-reports-on-top-5-ddos-attacks-of-2011/]. Accessed June 2015.

[5] M. Feily, A. Shahrestani, and S. Ramadass, A Survey of Botnet and Botnet Detection, *Proceedings of the 3rd International Conference on Emerging Security Information, Systems and Technologies*, pp. 268–273, 2009.

[6] S. H. C. Haris, R. B. Ahmad, and M. A. H. A. Ghani, Detecting TCP SYN Flood Attack Based on Anomaly Detection, Proceedings of the 2nd International Conference on Network Applications, Protocols and Services, pp. 240–244, 2010

[7] I. Butun, S. D. Morgera, and R. Sankar, A survey of intrusion detection systems in wireless sensor networks, *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 266–282, 2013.

[8] A. Varshovi and B. Sadeghiyan, Ontological classification of network denial of service attacks: Basis for a unified detection framework., *Sci. Iran.*, vol. 17, no. 2, pp. 133–148, 2010.

[9] K. Pelechrinis and M. Iliofotou, Denial of service attacks in wireless networks: The case of jammers, IEEE Commun. Surv. Tutorials, vol. 13, no. 2, pp. 245–257, 2011.

[10] S. K. Singh, M. P. Singh, and D. K. Singh, A survey on network security and attack defense mechanism for wireless sensor networks, *Int. J. Comput. Trends Technol.*, 2011.

[11] M. Momani and S. Challa, Survey of trust models in different network domains, *Int. J. Ad Hoc, Sens. Ubiquitous Comput.*, vol. 1, no. 3, pp. 1–19, 2010.

[12] M. C. Fernández-Gago, R. Román, and J. Lopez, A survey on the applicability of trust management systems for wireless sensor networks, *In Proceedings of the 3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, pp. 25–30, 2007.

[13] M. R. Rohbanian, M. R. Kharazmi, A. Keshavarz-Haddad, and M. Keshtgary, "Watchdog-LEACH: A new method based on LEACH protocol to secure clustered wireless sensor networks.," *Adv. Comput. Sci. An Int. J.*, vol. 2, no. 3, pp. 105–117, 2013.

[14] G. H. Lai and C.-M. Chen, Detecting denial of service attacks in sensor networks, *J. Comput.*, vol. 4, no. 18, 2008.

[15] M. H. Islam, K. Nadeem, and S. A. Khan, Optimal sensor placement for detection against distributed denial of service attacks, *In Proceedings of the 2009 International Conference on Advanced Computer Control*, pp. 675–679, 2009.

[16] J.-W. Ho, Distributed detection of node capture attacks in wireless networks, *Smart Wireless Sensor Networks*, chapter 20, pages 345–360, 2010.

[17] P. Sudip Misra, V. Krishna, K. I. Abraham, N. Sasikumar, and F. S., An adaptive learning routing protocol for the prevention of distributed denial of service attacks in wireless mesh networks, *Math. with Appl.*, vol. 60, no. 2, pp. 294–306, 2010.

[18] J.-H. Son, H. Luo, and S.-W. Seo, Denial of service attack resistant flooding authentication in wireless sensor networks, *Comput. Commun.*, vol. 33, no. 13, pp. 1531–1542, 2010.

[19] Z Z. Lu, X. Lu, W. Wang, and C. Wang, Review and evaluation of security threat on the communication networks in the smart grid, in *Military Communications Conference*, pp. pp, 1830–1835, 2010.

[20] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, A Denial of Service Attack in Advanced Metering Infrastructure Network, *Proceedings of the International Conference on Communications*, pp. pp. 1029–1034,2014

[21] European Commission, Smart Grids and Meters, [Available at: *https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters]* Accessed June 2015.