IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 3, June 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

An Enhanced Security Approach to IoT Management on Information-Centric Networking

[1] Charles O. Muango; [2] Jairus O. Malenje; [3] Laban O. Matundura; [4] Qu Shaojian

[1, 2, 4] University of Shanghai for Science and Technology
Shanghai, 200093, China

[3] Masinde Muliro University of Science and Technology
Kakamega, 50100, Kenya

Abstract - Technology advancement has not only made the world a global village but also made it possible for people to interact with devices around them through the Internet of Things (IoT) and bring your own devices (BYOD) technology. Organizations have been caught up in this rush as many employees in corporations and students in learning institutions bring different devices (such as smartphones, smart watches, smart screens, tablets, smart wrist bands that measure activity of one's organs) with them and connect to the corporate networks. IoT/BYOD has greatly improved efficiency and has led to a happy work force since they can now perform their duties efficiently as much of activities orbiting around their social life are within grasp. However, the downside of this increase in connected mobile devices is a cocktail of security threats that makes cyber security management critical for business continuity. In this paper, we propose an enhanced security scheme in IoT by use of social network analysis to single out central nodes that have the greatest influence in attack propagation. Simulation results show that the proposed method can be used to deactivate the influential node in the network in case of an attack thereby reducing the catastrophic impact. The significance of our enhanced IoT security approach is its ability to detect nodes with suspicious activities and thereby take them off the grid.

.

Keywords - *IoT; Security; Gadgets; DDoS; Information-Centric Networking*

1. Introduction

Cyber Security is an area of great concern in the global arena of Information and Communication Technology (ICT).The risk of long term damage to organizations reputation through destruction of data that has taken years to accumulate is more real today. Currently, Information Systems security breaches have become a common phenomenon and the arrival of IoT technology has made the cyber security even more complex to manage considering the unique features of the devices that rival traditional computational systems [1]. The interconnectivity [2] [3] nature of these devices raises major security concerns in modern complex computing environments. Previously, mobile devices had many limitations due to restricted memory, processors and the operating systems that were more closed than servers and desktops. The situation has since changed; evidently, unknown to most users, some of the devices are so powerful and sophisticated such that they can rival personal computers in functionality and capacity. According to [4], mobile devices API and the software systems behind them are getting richer and more dominant, and their browsers are nearly as rich as their desktop counterparts.

The security challenges that come with the implementation of IoT technologies have not gone un-noticed by malicious individuals who can take advantage of inherent vulnerabilities. Given that these devices have the potential to discover nearby connections and independently establish connection with them, the security aspect in this kind of interaction has not been tackled adequately as it should. In Information-Centric Networking, content is retrieved by use of unique names enabling network replication of in addition to content based security. Content is accumulated, managed, and hived in the network for use say by IoT devices. With content-based security, the hosts are left vulnerable to attacks such as "man in the middle attack" [5]. Thus, as the interaction of IoT devices expands, the attacks are likely to get more complex and virulent [2]. Unfortunately, the inadequate knowledge by systems administrators and employees on the attack surface is contributing to the poor defensive posture of organizations. It is imperative for researchers to note this special kind of adjustments in technology [6]. In [7] , the growing presence of devices enables new attack methods and new attack surfaces for criminals and hackers to exploit, posing serious security and privacy issues. [8] underscores that we need shrewder and secure systems capable of detecting and quashing threats as they evolve.

According to [7], the increase in the number of devices that allow for communication among machines effectively reduces human control and people will have almost no control over what and with whom the devices transact.

This creates an avenue through which hackers can exploit as happened with recent attacks on IoT devices like the Mirai botnet as conferred by Marie. In the past, there have been efforts made by the security industry to counter a botnet known as Cut wail but the results were not satisfactory, instead, it led to disruption of services [6]. Since these IoT devices are inter-connected through the Internet forming what is called a social network, they pose real-world catastrophe, a big challenge with IoT security. With constrained memory and computing power, low power, low-cost, these devices can physically be accessed by intruders. Rafe [6]states further that attacks such as side-channel attacks (SCAs) can be deployed to extract vital information from them e.g. secret key. Despite all the challenges security experts are working hard to come up with solutions to mitigate the security flaws in IoT/BYOD devices. In spite of its disadvantages, Quantum-safe algorithm is one of the available solutions. According to [7], security should be looked at in both layers of IoT ecosystem: IoT devices themselves as the first layer, the communication between devices being second layer [8] and data storage and analysis as the third layer.

There have been concerted efforts to introduce new security schemes to help users, who are the most vulnerable link in the IoT ecosystem, stay in control. One such tool has been developed by [9] where the authors have constructed an information security metric that informs end-users about the potential security problems with particular smart devices, thereby increasing the level of information security awareness. Their research is focused on the usage of these devices for smart homes and SOHO (Small Offices Home Offices). The constructed metric is based on known vulnerabilities and matching attack methods; it has a scaling mechanism for ease of understanding vulnerability levels and eventually a score is given for comparison of the various devices that provide almost identical services.

In organizations such as schools where you have a diverse mix of techno-savvy users, it is imperative to deploy a compact security system that can ensure safety for all. It is from this background that [10] try to address the security issue compounded with the use of carry-along devices attached to corporate networks using EZ-Net BYOD service management system. The author's show case a management system to control the logging in and out of the corporate network. It adds a fail-through authentication mechanism to the local Wi-Fi connection that ensures mobility control via numerous external authentication servers. The identification of the BYOD devices is done using the MAC-address since it is a unique identifier that can be easily used to separate or group users to particular domains. This is one of the steps towards enhancing security in the portable devices though it can only deal with attacks aimed at antagonizing the confidentiality and integrity of data but not availability of service.

[11] carried out a survey on the IoT security and the various threat they pose to their users and proposed some solutions to curb the emerging threats as a result of using the IoT devices. Of interest to our study is the threat categorized as node injection which is related to what our study seeks to get a solution to. They further used the monitoring verification scheme (MOVE) to check on malicious activity of nodes. However, the aim of our solution which goes beyond what they proposed, is to monitor, find and eliminate the most influential of the connected nodes in terms of propagation of malware.

Neighboring nodes in a network can influence each other in the process of information flow [12]. Applications have been proposed on how to identify the influencer nodes generally in networks but has fallen short of looking at the effect of centrality measures on other networks. Our work focused on testing and analyzing all the Centrality metrics since each has its own merits and demerits. By doing this, an informed decision on the node to be eliminated in case of an attack would be arrived at that is not biased to a particular centrality measure. Likewise, going by the current trends, attacks are no longer a likelihood but an inevitability [13]. Furthermore, the tests had not been done on an Information-Centric Network vis-a-vis getting the solution to DDoS attacks that is hideous with technology today [6] [14]. As a result, the aim of information security is to ensure confidentiality, integrity and availability; the latter being our key focus on this paper.

Getting an all in one solution to combating threats posed by the usage of IoT/BYOD is a daunting task considering the pros and cons of each solution. A framework has been proposed by [15]. They provide a general guideline on how to integrate BYOD into an enterprise environment. They propose the merging of the various solutions like Mobile Device Management, Cisco Smart BYOD solution and mobile virtual machines in the enterprise environment so as complement each other. They noted that a lot of solutions available concentrated so much on the confidentiality of data but ignored illegal data access. In conclusion, the authors proposed that in an organization, the most effective way to have leverage on security involving BYOD devices is to create virtual barriers that separate corporate space from personal space. This will make it possible to monitor corporate data, deny unauthorized and illegal access; better still organization's BYOD security policies should be followed to the letter.

From the studies reviewed above, there are ways of tackling the IoT devices security threats from a global perspective, but none looked at how to single out the ever increasing threat of DDoS which has become more destructive. Works reviewed all reiterates that IoT devices do not have standard security feature thus organization that integrate their usage expose their assets to an extensive threat surface due to their vulnerability nature. To identify key influencers in a network i.e. those that have a big impact in the spread of information and therein DDoS attack we have had to measure centrality scores in the network [16] [17]. This is based upon their physical characteristics when communication goes through the network. In this paper, we propose an enhanced IoT security scheme within organizations using Information-Centric Networks.

2. Materials and Methods

The usage of knowledge within Information-Centric Network to combat security problem in IoT devices is depicted in [18]. This proof of concept shows that it is possible to use information within the network to help a network/systems administrator make an informed decision when under attack[11]**}**.To better show how the interaction of nodes (IoT devices) in the network takes place we defined centrality measures as used in this work.

2.1 Betweenness Centrality

It is the ratio of all the geodesics (short paths) between pairs of nodes running through a particular node **u** in the network.

$$Bet(\mathrm{u}) = \sum_{x \neq u, y \neq \mathrm{u} \in \mathrm{V}} \frac{q_{x,y}(\mathrm{u})}{Q_{x,y}} \quad (1)$$

where $Q_{x,y}$ is the total number of shortest paths starting from source node x and destination node y, and $q_{x,y}(u)$ are the number of shortest paths that pass through node u (starting from source node x and destination node y).

2.2 Page Rank

This is used to quantify the importance of a particular web-page. Since our data was web data this would come in handy in terms of gauging the importance of all the pages visited within our network.

$$PR_{(p_i)} = \sum_{P_j \in \Psi P_i} \frac{PR_{(p_j)}}{L(P_j)} \quad (2)$$

where is the Page-Rank for page, is the set of web-pages that link to and is the number of outbound links on.

2.3 Closeness Centrality

Refers to the inverse of the sum of the shortest distances between each node in the network graph.

$$Clo(\mathrm{u}) = \frac{1}{|v|-1} \sum_{v \neq u \in V} dist(u,v) \quad (3)$$

where $dist(u,v)$ is the number of hops in the shortest path from node u to node v and V is the set of nodes in the network.

2.4 Degree Centrality

This measure refers to how many ties a node has to other nodes in the network. It can also be referred to as measure of actor activity.

$$Deg(u) = \frac{K(u)}{|V|-1} \quad (4)$$

where $K(u)$ is the number of edges of node u and V is the set of nodes in the network.

2.5 Proximity Prestige

Refers to how proximate a node **u** is to the nodes in its influence domain **I**. The influence domain **I** of a node is the number of other nodes that can reach it. That is to say how close are all the nodes to node **u.**

$$PP = \frac{\frac{1}{N-1}}{\sum \mathrm{d}(v,u) f \quad I} \quad (5)$$

where $\mathrm{d}(v,u)$ is the distance of nodes to u and $N-1$ is the total number of nodes in the influence domain I less the reference node u.

2.6 Influence Range Closeness Centrality

It is the standardized inverse average distance between node **u** and every other node reachable from it. It only considers distances from node u in its influence range **J.**

$$IRCC = \frac{\frac{|I|}{(n-1)}}{\frac{\sum d(u,j)}{|I|}} \quad (6)$$

where $\frac{|I|}{(n-1)}$ is the fraction of nodes reachable by **u** and $\frac{\sum d(u,j)}{|I|}$ is the average summation of the distance of nodes from **u.**

2.7 Information Centrality

It focuses on how information might flow through the various different paths. It uses all the paths between actors (nodes) weighted by strength of the bond and distance.

$$IC_i = \frac{n}{\sum_{j=1}^{n} \frac{1}{I_{ij}}} \quad (7)$$

where n is the number of nodes in the network and I_{ij} is the centrality of a path from node *i* to *j*

2.8 Eigen Vector Centrality

This refers to the centrality of each vertex that is proportional to the sum of the centralities of its neighbor's. A node is important if it is linked to by other important nodes.

$$EC(u_i) = \frac{1}{\lambda} \sum_{v_j \in V} a_{u_i v_j} EC(v_j) \quad (8)$$

where a_{ij} stands for the entry in the adjacency matrix **A** , **V** denotes the set of neighbors of v_j and $EC(v_j)$ denotes the Eigen centralities of nodes in V

As clients join the network they are authenticated and given unique IDs for the day to day operation and to the domains they can access. In this arrangement a device cannot stray into a domain it is not allowed in nor can it be allowed to search for the available IoT devices on the network to connect to.

The algorithm of how the gateway incorporates IoT devices into the network is shown in Figure 1. Any client joining the network sends a freshness update request marked as Interest, of the anticipated Freshness Coefficient. The gateway then adds/updates its record with this request i.e. if request is above the minimum allowed for level of service it is set to the lowest value. A record having updated, re-evaluation of the freshness coefficient is done and set to lowest recorded requests and if no changes take place the gateway responds to the client with Data of the current freshness coefficient. If not Interest is send to the device for new configuration of the freshness coefficient and it gives feedback to the gateway with an update result. Notification Data is forwarded to the client.

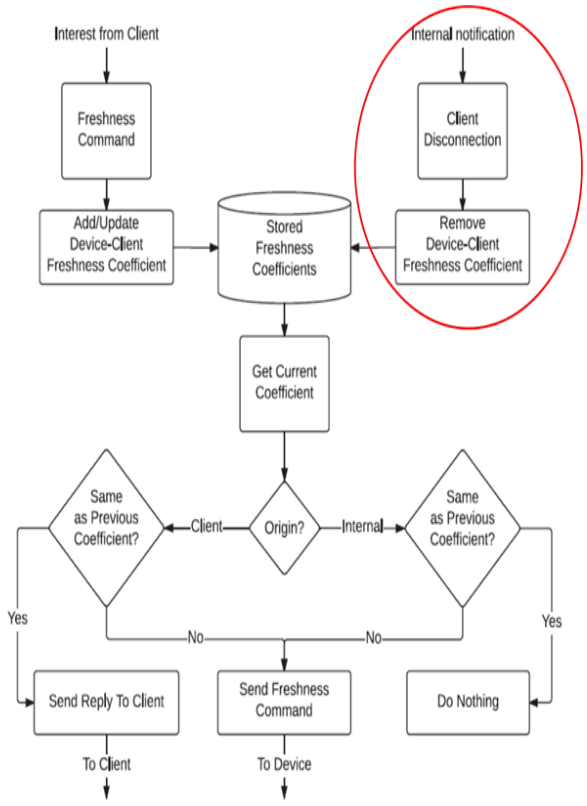

Fig 1. Freshness Control Algorithm Executed at the Gateway, Source-18]

When a device is no longer active, say after a period of time without active session key, the record connected to that particular device is removed. Security is one of the challenging issues in IoT due to its inherent wireless characteristic, the relevant information handled by IoT devices and the hostile environment where these devices are deployed. If the device wants to join a network again, it has to request for new freshness coefficient to be redone and special ID assigned to it. An Algorithm for secure IoT management architecture in an information centric environment has been presented in Fig. 1. What is missing in his concept is how to deal with DDoS attacks that compromise on availability of service in a network which the study did not focus on. Since the IoT devices when connected form a social network, it is therefore given that a social influence shall exist and that forms the basis of using centrality measure to single out the nodes. Our proposed enhanced algorithm for disconnection of a client procedure shall be implemented at the area cycled red in Fig.1. This shall be possible by adding a second procedure for permanent termination has presented in Fig 2.

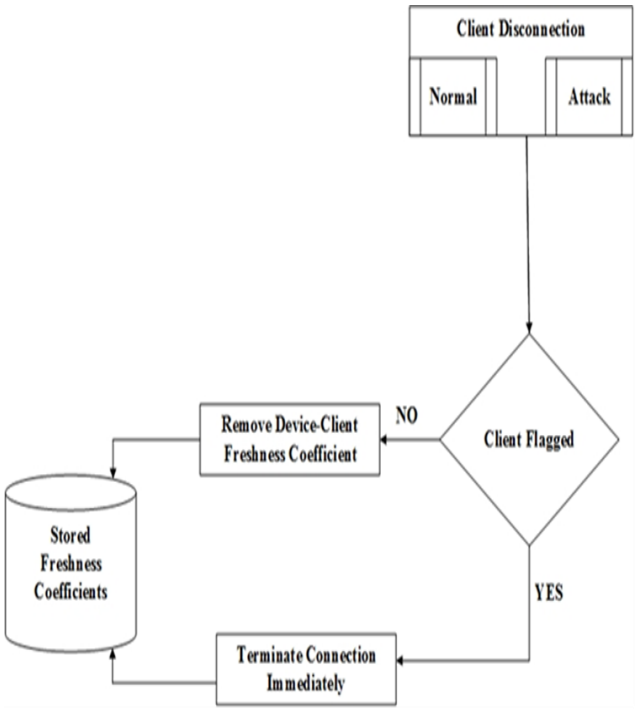

Fig.2: Enhanced Device Disconnection Algorithm

3. Simulation and Evaluation Results

We took a different approach in trying to solve DDoS attacks to ensure none disrupted communication on the network due to unavailability of services requested for by clients. Specifically, we address security in the network with respect to the roles each node plays in the event of a DDoS attack. We run a simulation of a real world scenario basing our result on assumption of an attack and thus single out the most culpable node in the system flagging it off for its connection to be terminated hence forth.

Data used in this simulation was retrieved from a learning institutions website using the SOCNetV-2.1 [19] web crawler (social networking analysis tool). It was then modeled using search engine indexing of all the visited pages as nodes and their real links to create a resemblance of an information centric network. This was viewed as a good case study by the researchers for an information-centric network domain since you have a good presentation of users constantly online and using the corporate network. Inter-relation and links between nodes is represented on the Fig. 3.

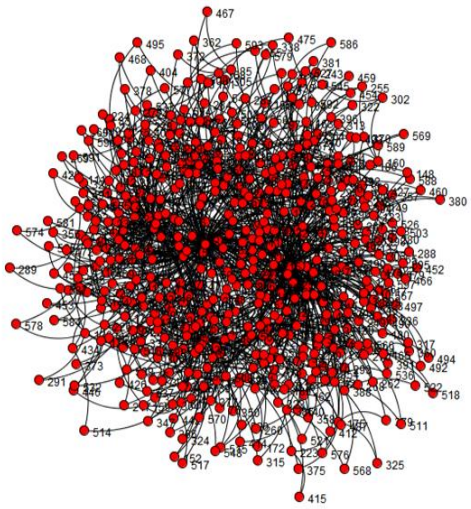

Fig.3: Schematic showing connected IoT devices

Since nodes in networks divulge social influence, DDoS attacks usually take advantage of these relationships to spread fast in the network. Nodes that intermingle frequently and whose activities influence each other more intensely share strong bonds, whereas nodes that don't interrelate often with each other are deemed to have weak links [16].

4. Discussion

In verifying our proposed scheme, we used centrality measures to carry our metric tests of the nodes in our network. The network under study in Fig. 4 presents a collaboration network where vertices represent IoT devices interacting in an Information-Centric Network. First we perform a drawing of this network using the basic graph drawing method using web crawling technique. The assumption made in this case is that the network is already infected with a DDoS attack and thus we need to isolate the central node. Information flowing through the network was extracted according to the transfer process and run through geodesics distance in the network. The centrality measures were tested and the results of the same are presented in Fig.4 and Fig.5.

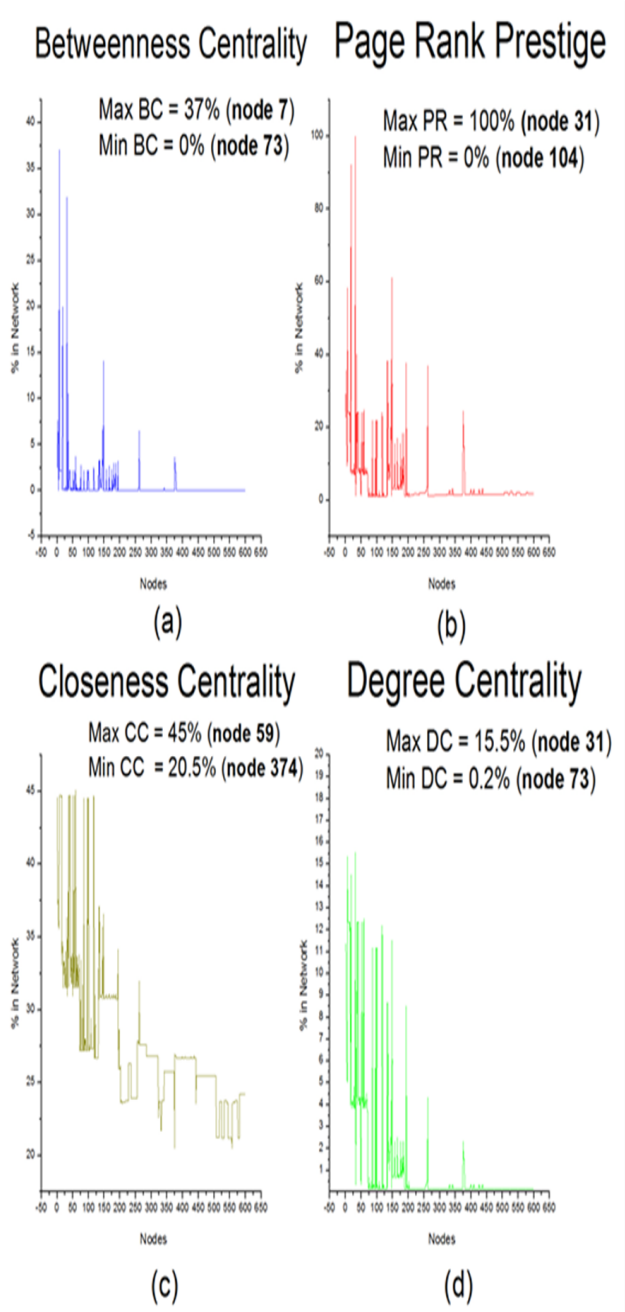

Fig 4: Result (A) showing distribution of Centrality Tests on Nodes

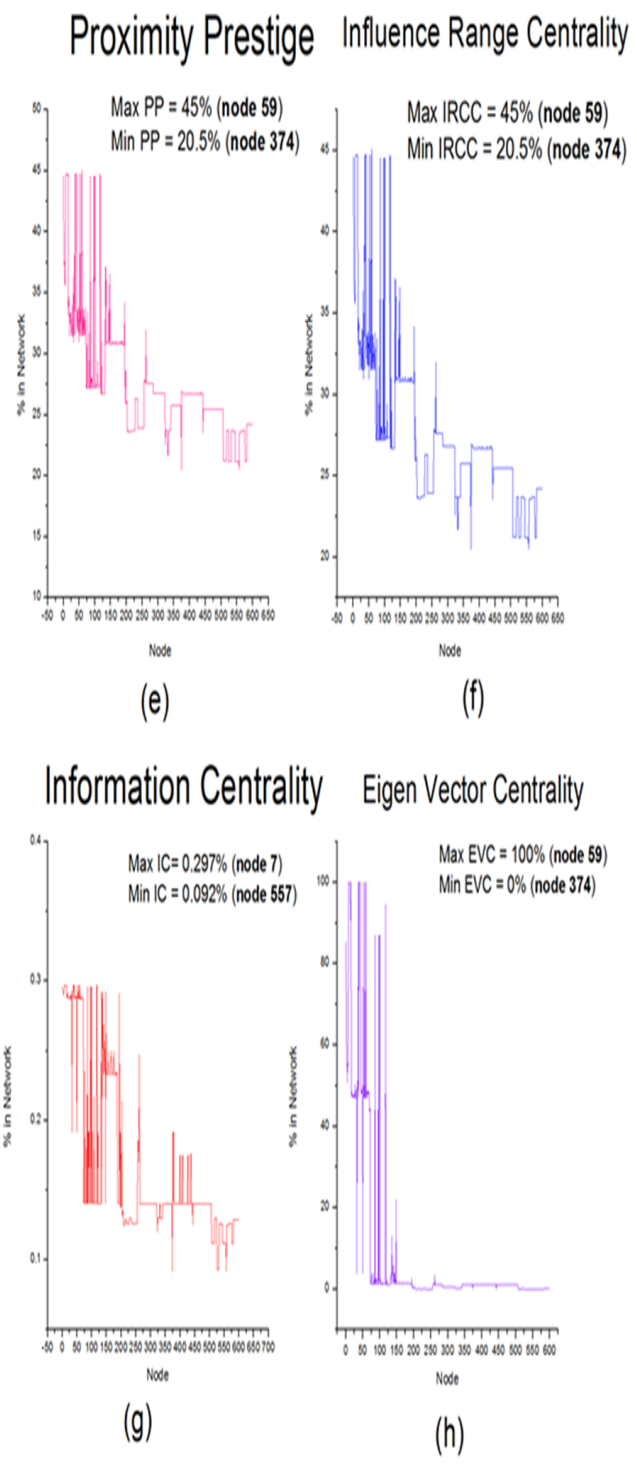

Figure 5: Result (B) showing distribution of Centrality Tests on Nodes

From the measures above we could not conclusively make a decision, we therefore had to explore other measures of centrality to ascertain that the node to be eliminated or rather whose connection needed to be terminated in the event of an attack. The proceeds from the calculations below are represented in Table 1 with their corresponding maximum and minimum nodes under each category.

Table 1: Summary Table of Node Centrality Measure

CENTRALITY MEASURES	NODES		HIGHEST TALLY
	MAX	MIN	
Betweenness Centrality	7	73	
Page Rank	31	104	
Closeness Centrality	**59**	374	
Degree Centrality	31	73	
Proximity Prestige	**59**	374	59
Influence Range Closeness Centrality	**59**	374	
Information Centrality	7	557	
Eigen Vector Centrality	**59**	374	

Table 1 shows the summary of both maximum and minimum nodes for each centrality measure. Comparison was made between the rankings of the nodes from highest to lowest with reference to the various centrality test done and node 59 ranked the highest. We narrowed our search to the node that is well-connected with the capability of linking to other important nodes; therefore, it is not surprising that node 59 was our target candidate for isolation from the network. Furthermore, Wang et al (2003) in their work about epidemic spreading in real networks, they prove that epidemic threshold is closely related to the largest Eigen value of the adjacency matrix of the network. Our node 59 had the highest score when Eigen Centrality measure was done thus further strengthening our choice for its removal. The epidemic threshold determines computer virus propagation on the network thus if value is 1 then like hood is high and vice versa

5. Conclusion

The aim of this paper was to use metrics to be able to identify a central node that is more active than the rest in the event of an attack then isolate it from the network. This was done by comparing values of the centrality measures from the simulation of our network. This means that when you have a network it is possible to get the epidemic threshold and the central nodes involved in malware spread through calculation and thereby being able to mitigate damage. The study used the centrality metrics to determine

the most influential nodes (IoT device) that an attacker could use to carry out a DDoS attack. Once the node is identified, it can then be disabled or cut off from the network to prevent the spread of an attack. However, further work needs to be done on the performance of the network when the central node(s) is removed. Furthermore, with the different types of networks research can be done to ascertain if this process suits them.

References

[1] Pwnie Express, "Internet of Evil Things," 2017.

[2] Afzal Shah Idris , Amin Malik Faizan , and Arshid Syed , "Enhancing Security in loT based Home Automation using Reed Solomon Codes," in IEEE WiSPNET 2016 conference, 2016.

[3] Marconot Johan , Pebay-Peyroula Florian , and David, "IoT Components LifeCycle based Security Analysis," in Euromicro Conference on Digital System Design, 2017.

[4] O'Neill Maire, "Insecurity by Design: Today's IoT Device Security Problem," Elsevier LTD, 2016.

[5] Kavalaris Stylianos , Kioupakis Fragkiskos-Emmanouil , and Kaltsas Konstantinos , "Development of a Multi-Vector Information Security Rating Scale for Smart Devices as a Means of Raising Public InfoSec Awareness," Procedia Computer Science 65, pp. 500 – 509, 2015.

[6] Kao Yi-Chih , Chang Yung-Chia , and Chang Ruay-Shiung , "Managing Bring Your Own Device Services in Campus Wireless Networks," in Computer Science and Engineering Conference (ICSEC), 2015 International, 2015.

[7] Wang Yong , Wei Jinpeng , and Vangury Karthik , "Bring Your Own Device Security Issues and Challenges," in The 11th Annual IEEE CCNC- Mobile Device, Platform and Communication, 2014.

[8] Suarez Javier, Quevedo Jose, Vidal Ivan, Corujo Daniel, and Garcia-Reinoso Jaime, "A secure IoT management architecture based on Information-Centric Networking," 2016.

[9] Panda Mrutyunjaya , Dehuri Satchidananda , and Wang Gi-Nam , "Influencers in Social Networks," in Social Networking.: Springer.

[10] Wang Yang , Chakrabarti D., Wang Chenxi , and Faloutsos C. , "Epidemic spreading in real networks: an eigenvalue viewpoint," in 22nd International Symposium on Reliable Distributed Systems, 2003. Proceedings., 2003.

[11] Jaramillo David , Newhook Richard , and Nassar Nader , "Techniques and real world experiences in mobile device security," in IEEE SOUTHEASTCON 2014, 2014.

[12] Pilling Rafe , "Global threats, cyber-security nightmares and how to protect against them," Computer Fraud & Security, vol. 2013, pp. 14 - 18, 2013.

[13] Gandhi Meera and Muruganantham A. , "Potential Influencers Identification Using Multi-Criteria Decision Making (MCDM) Methods," Procedia Computer Science, vol. 57, pp. 1179 - 1188, 2015.

[14] Tyrer Andrew, "Can the UK cyber-security industry lead the world?," Computer Fraud & Security, vol. 2, pp. 5 - 7, 2015.

[15] McIntosh Chris , "Cyber-security: who will provide protection?," Computer Fraud & Security, vol. 12, pp. 19 - 20, 2015.

[16] SOCNETV: SOCIAL NETWORK ANALYSIS AND VISUALIZATION SOFTWARE. Social Network Visualizer. [Online]. http://socnetv.org/

[17] Peng Sancheng , Yang Aimin , Cao Lihong , Yu Shui , and Xie Dongqing , "Social influence modeling using information theory in mobile social networks," Information Sciences, vol. 379, pp. 146-159, 2017.

[18] Man Wing and Lam Wynne , "Attack-prevention and damage-control investments in cybersecurity," Information Economics and Policy, vol. 37, pp. 42 - 51, 2016.

[19] Arshad Sobia , Awais Azam Muhammad , Hassan Ahmed Syed , and Loo Prof.Jonathan, "Towards Information-Centric Networking (ICN) Naming for Internet of Things (IoT)," Proceedings of ICFNDS '17 Cambridge,United Kingdom, p. 6, 2017.

Authors -

Charles O. Muango Ph.D. Candidate, MSc.in Data Communication, BSc. In Computer Science. Currently am Employed at Masinde Muliro University of Science and Technology in the School of Computer and Informatics. Current research interests-Network Security, Cyber-Security, Social Networks, Deep learning & Human Computer Interaction.

Jairus O. Odawa Ph.D. Candidate, MSc. IT, BSc. in Computer Science. Assistant Lecturer at Masinde Muliro University of Science and Technology in the School of Computer and Informatics.

Laban O. Oenga Ph.D. Candidate, MSc. IT, BSc. in Computer Science. Assistant Lecturer at Masinde Muliro University of Science and Technology in the School of Computer and Informatics.

Qu Shaojian (Ph.D.) Prof at the University of Shanghai for Science and Technology in the School of Business Management.