IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

A Survey on Game Theory against Attack in Honeypot Enabled Networks for IoT

R. Sangeetha[1], M. Mohana[2]

PG Scholar, Srividya College of Engineering and Technology, Virudhunagar, India[1]

Assistant Professor, CSE, Srividya College of Engineering and Technology, Virudhunagar, India[2]

Abstract: At present the communication and information is increased by many devices that are associated to the internet. Growing, information technology and communication device require defense against intrusion. Now a day, network attacks are increasing gradually. Many of the intrusion detection are protected the network intrusion but it is not fully protect the current network attacks. Internet of Things (IoT) produces the honey pot technique for against the attacks. Honey pot techniques based on game-theoretic method with easily identify the network abnormal behavior data. The threshold frequency range classifies the attacker's action. The valuable intrusion detection system require low success rate of attacker, detection rate and accuracy is high. This paper presents a survey on Deceptive Attack and Defense Game in Honey pot Network for IoT. These successfully resist all type of attacks in networks for Internet of Things.

Keywords: Network attacks, Intrusion detection, Internet of Things, Honey pot, Game-theoretic, Deceptive Attack, Defense Game.

I. INTRODUCTION

With increasing the network service and application[6] makes network security is an essential research problem. Honeypots is one of the methodologies for network security in Internet of things. The internet of Things (IoT)[19] is an object or a thing that has a communication between internet and their demonstration. Internet of Things is the basis for a lot of services that depend on its accessibility and consistent operations. IoT provide the distinctive identifiers for automatic data transfer over a network.

The different field of IoT generally covers the smart grids, smart building, M2M (Machine to Machine) communication and smart cities. The fundamental motivation of IoT is provided the advanced solution to enterprise through modern technologies. Security is improved by network segment[18] that monitor and identify malicious traffic. IoT is a combination of constrained network of internet and hybrid network of internet. The protocols of IoT are i) lightweight security ii) Novel security iii) established protocol. The constrained environment like WSNs is provided by lightweit protocols. The IoT requirements[35] are specified by novel security. IoT use the characteristics of IDS and WSNs for security. But IoT characteristic has some drawbacks: i) no control point and centralized management ii) no message security iii) sensor nodes are identified by WSNs

The IP address is used for global identification of nodes in IoT. The challenge of IoT is global access, lossy link and constrained resources. The above drawback is overcome by RPL protocol.

Security of IoT[18]:
Confidentiality:
The message is transfer from source to destination. The message is attacked by attacker because the message is not hidden. The message is store with in the IoT device that provides the hidden service from encryption and decryption technique.

Data Integrity:
MIC (Message Integrity Code) provide the Data integrity service.

Source Integrity:
The message entity end points validate the identity of each message entity

Replay Protection:
The data packets are stored in intermediate node and replay the packet later. The replay packet holds a sensor reading for detect the duplication which is achieved by sequence number, integrity protected times tamp.

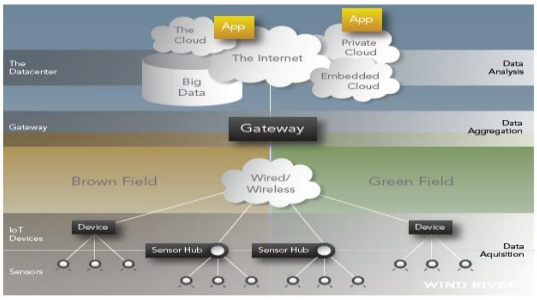

Figure.1. IoT Topology

DOI 10.17148/IJARCCE.2016.51051

IoT - standard security solutions[19]

IoT Layer	IoT Protocol	Security Protocol
Application	CoAP	User-defined
Transport	UDP	DTLS
Network	IPv6,RPL	IPsec,RPL security
6LoWPAN	6LoWPAN	None
Data-link	IEEE 802.15.4	802.15.4 security

Table 1. Security Solution of IoT.

Game Theory:
Computer network security is analyzed by game-theoretic model. Game theory is a division of applied mathematics. Game theory is a scenario of mufti person assessment. Game theory is suitable methodology[10] for security that provides the communication between the administrator and attacker that determines the strategy of counter measure for resist the attacks. Attacker and administrator[27] are the two- player and build the method for the game. The main objective of game theory is finding the suitable action for assessment maker based on situation and outcomes. The application of game theory is political science, economics, military and biology.

Classification of Game theory:
The game theory is normally classified[28] into two types: i) Non – cooperative game - Its gives the detailed description of all play moves to players and ii) cooperative game – Its opposite to Non – co operative game that describes result only.

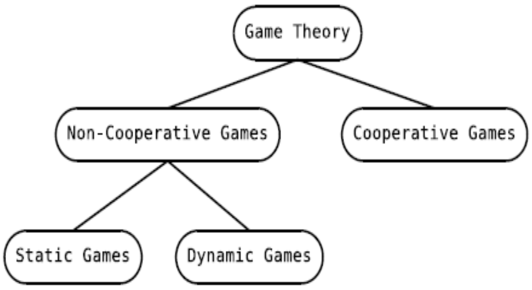

Figure 2 Game theory classification.

Non –cooperative game:
Non –cooperative game[9] is an interactive process, numbers of players are appeared and the result is determined by entity decision. The non co-operative game future classified into two types: Static game and Dynamic game based on player's moment.

Static Game: One-shot game [29]is static game. Simultaneous action plan is determined by players. The other player's knowledge is not considered. The game table is also called strategic form or normal form that represents the static game as diagrammatically.

Dynamic Game: Dynamic game [29]is also called Extensive game. This game has several stages in which all the players are considered the other players decisions. The static game problem of decision making is overcome by dynamic game. The dynamic game is represented by game tree that describes the all probable events taken by players. It also denotes the feasible outcome of every step in the game.

Congestion Game: It's also called potential game. The congestion game has two entities as resources and participants. The participants are depends on the resources. The same resources are selected by number of participants.

Stochastic Game: Stochastic is dynamic game[23] also has transitions function of probabilistic. The game has sequence stage and number of players. Players play the action; the other players get the payoff based on present state and selection of actions. This game is simplified by repetitive game and Markov decision method. The two-players of stochastic game are mostly used for analysis and model the unfamiliar situation. The application of Stochastic is biology, network security, economics.

Supermodularity: Supermodularity[21] is analyzing the player decision that affects the other player action. Its symmetric play game is based on payoff method. Multiple equilibrium is the fundamental property of supermodularity. The supermodularity function is utility. Sub modularity is the subset of Supermodularity function.

Components of a wireless network – game[42]

Components of game	Elements of network
Players	Nodes in the wireless network.
A set of strategies	Modulation scheme,Coding rate, transmit power level.
A set of payoffs	Performance metrics (delay, throughput)

Table 2. Component of network game.

Intrusion Detection:
The game theoretic model analyze and response to the intrusion detection system (IDS). The response of IDS[12] is alarm setting, monitoring the activity of user. Intrusion detection game provides the interaction between two players such as IDS[9][8] and attacker. The aim of attacker is to attacking the selected node through malicious message. The intrusion is detected by signaling game plan. It is multistage dynamic game and incomplete information. The intrusion detection game analyzes the node. The node selfish activity is not considered in game intrusion model. At a time the single node is attack by attacker so the malicious code collusion is not occurring. Signaling game model the players are source node, IDS and destination node. The sender node has two players as normal player and malicious player.

DOI 10.17148/IJARCCE.2016.51051

The IDS [25][26]detect either the player is attacker player or normal player. It is described by P 2[0, 1]. The decision choice of malicious player is malicious behavior or abnormal behavior. The designation has two messages as defend message and malicious message. The false alarm is raised by IDS when detecting the malicious message.

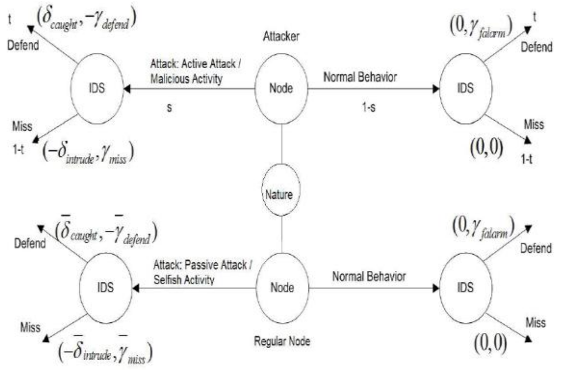
t
$(\delta_{caught}, -\gamma_{defend})$
Defend
Attacker
$(0, \gamma_{falarm})$
t
Defend
IDS
Attack: Active Attack / Malicious Activity
s
Node
Normal Behavior
1-s
IDS
Miss
1-t
$(-\delta_{intrude}, \gamma_{miss})$
Miss
$(0,0)$
1-t
Nature
Defend
$(\bar{\delta}_{caught}, -\bar{\gamma}_{defend})$
$(0, \gamma_{falarm})$
Defend
IDS
Attack: Passive Attack / Selfish Activity
Node
Normal Behavior
IDS
Miss
$(-\bar{\delta}_{intrude}, \bar{\gamma}_{miss})$
Regular Node
Miss
$(0,0)$

Figure 3 Signaling game - Intrusion Detection.

RRE:
RRE (Response and Recovery Engine)[4] is the game-theoretical engine of intrusion response. RRE is enabled by ART (Attack Response Tree) when the IDS send the inherent suspicions alerts. RRE is automation process that alert the intrusion discovered in the network. ART and RRE use Markov decision method for best response. This process is based on true/false method.

Honeyspot:
A honey pots is a computer system [3]that used for detecting and preventing the intruder. Honey pots tools easily understand the attacker's behavior and malicious attack. Honeypots is placed on network to attract the attacker attention. The basic operation of Honey pots is system log.

The data are not store in honey pot [36] system. The network security increased by two way:1)The intruder resource and time is waste by Honeypots. The intruder compromises the Honeypots system but the intruder does not hold the any valuable information. 2) The administrators examine the all events of attacker's and provide the better result for intrusion detection. Honeypots identify the attackers in different ways: Pure Honeypots, High interaction Honeypots, Low interaction Honeypots, Honeynets[27] and Honeyfarm .

The developed production system is called Pure Honeypots. The tap is used to monitor the attacker activity. High interaction Honeypots accesses attacker's root. So the great risks are easily managed in high interaction Honeypots network. Low interaction Honeypots imitate the services that are repeatedly embattled by attackers. So the low interaction Honeypots manages the low risk and complexity. More than one Honeypots network builds a Honeynet . The honey farm is the centralized gathering of Honeypots and tool analysis.

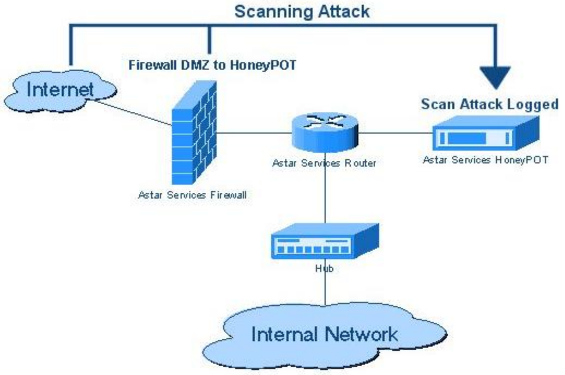

Figure 4 Honeypots security system.

Classification of Honeypots:
Honeypots are categories[28] into two type based on their design: 1) Production Honeypots 2) Research Honeypots.

Research Honeypots : Research Honeypots allow lock analysis for analyze the attacker activity. The system security is improved by attacker's activities. Data is located by unique identifier also analyze the attacked data and recognize relations between participants.

Production Honeypots : The production Honeypots is hold by production network. It is used to improve the overall network security. The production Honeypots is low – interaction Honeypots.

Honeypots Selection game:
The attacker decides to attack a system. In the Honeypots selection game the Honeypots is added to network and increase the probability. The attacker attacks the Honeypots system instead of computer system. The HSG is represented by tuple(d, a,n, k,D, p,I, f,A, u). The two players[10] are presented in Honeypots Selection Game (HSG) :bot master and Honeypots. The bot master does not know the nature of Honeypots. The bot master sends malicious message to Honeypots. The identity of Honeypots is identified by bot master to send a command to compromised to Honeypots and perform some process that are measured and controlled by sensor machine. The Honeypots have two stages for against the attack: Contribute stage: The bot master send attack command to Honeypots that command is executed. The Honeypots gather the information on bot master and allow the bot master to stay in long time to spend more resources. Not contribute stage – The bot master commands are not executed by Honeypots.

Network – Attacks :
MITM:
MITM is the Man-In-The-Middle attack[5], the attacker attack the message without knowledge of participants. The attacker successfully injects the attack based on the observation and message capture. The best example of MITM is cryptography security process in public key encryption.

DOI 10.17148/IJARCCE.2016.51051

Smurf Attack:
Smurf Attack is one type of DoS (Denial-of-Service)[5] attack. The fraud Echo request–message is transfer to all host in network. The smurf attack is prevented by 1) The destination address of data grams are not forward through router 2) configure the host that not reply the echo-request message.

Traffic Redirection:
The attacker compromises the router. The compromised router [5]sends the shortest path message to all nearby routers. The all nearby routers send the packet to compromised routers. The packet information is easily got from the compromised router.

Distributed Denial of Service :
DDoS attacker inserts the malicious program to all compromised system. The malicious programs control the system. The main aim of DDoS[5] is attack the bandwidth of network.
The attacker use any suitable methods like buffer overflow, unknown code installation to set the Trojan to target host and compromised system by root kit. The root kit isolates the malicious activities from system. The compromised system spread various type or same type of attack to the target system.

Defense against Network Attack
Configuration Management :
The most important aspect of defense against network is Tight configuration management[37]. Data backup is the important process in configuration management. Configuration management process is: Up-to-date backup and update - immediate process are done whenever the new patch or new service pack is released. All the files or application must have the sufficient protection. The default login allows third party to access the network resources. So login patterns are changed dynamically. Administrator or root password is implemented by tight security mechanism.

Firewall:
The most familiar network security [34]is firewall. The firewall stands between the internet and LAN. Firewall protection is based on filtering process that filters the unwanted packets from the network. The check point is created by firewall between LAN and internet. It is called as choke point.
The classification of firewalls are Packet filtering, Circuit Gateways, Application Proxies that are depends on Level filtering, Packet level filtering, Application level filtering and TCP session filtering. Packet filtering: It is based on IP packet level. The filtering is based on port number and address. Packet filtering successfully resists the Pspoofing attacks and DoS attacks.

Circuit Gateways: It is also known as Virtual Private Network (VPN). The function Circuit gateways function at transport layer. The packets are examined, reassemble and block in UDP or TCP connection. Application Proxies: it operates at application level. The applications are control or block the traffic. Application Proxies provide broad protection against threats provided by. The limitation of firewall is need perfectly configuration also reduce the performance speed when examines the traffics.

Encryption:
Encryption is another familiar technique of defense against attacks. The numbers of attacks are sniffer attack and eavesdropping is reduced by encryption techniques as PKI[11] (Private key Infrastructure), IPSec (Internet Protocol Security) and VPN (Virtual Private Networks). The most significant protocol of encryption is SSL. It's similar to human protection system and provides the protection at every point.

Secure Sockets Layer:
Symmetric key encryption and Asymmetric key encryption is used by Secure Sockets Layer (SSL)[31]. The data transfer is secure mode like encrypted tunnel. The confidentiality and integrity is provided by SSL with help of encryption and hashing algorithm. Protocol of SSL is TCP/IP.

Secure HTTP (SHTTP):
It's a substitute of HTTPS. The working principle and design is similar to HTTPS.SHTTP[31] function depends on application level. Secure tunnel is created for each message that are separately encrypted. The protocol of SHTTP is HTTP.

VPN:
Virtual Private Network (VPN)[20] is a method to transfer the unsecured network traffic. It uses the encryption, tunneling, authentication technique. The most common protocols of VPN is PPTP (Point-to-Point Tunneling Protocol), SOCKS, IPsec

(Internet Protocol Security), L2TP(Layer 2 Tunneling Protocol). The block website and bypass firewall are used for to transfer the data to target node without malicious attack.

Kerberos :
Kerberos is a validation protocol. The Kerberos[30]
provide the verification tokens that used for identify the system uniqueness with secure manner.
This protocol based on the assumption on machine participation that manage the loosely synchronization. The cryptographic protection resists the spoofing attack by mutual validation.

E-Mail Security:
Cryptography plays a main role in email security[7]. Emails are easily attack by attackers. The mail security is provided by standard mechanism like MIME (Secure multipurpose Internet mail extension), PGP, PEM, MSP (Message Security Protocol).

DOI 10.17148/IJARCCE.2016.51051

Hardware Development:
The hardware development [11]is new technology that denies the attacker access to network resources. The recent hardware technologies are smart cards and Biometric systems. Biometric is a significant role in network security.

Biometric scanner is used by workstation to identify the authentication access like log in. Many organization use Smartcard authentication. The pin is 4 digit characters and the pin is not modified by other users. It is verified by administrator and allows the authentication access.

Software Developments:
The anti virus software is one of the software development tools for resists the network attack[5]. The known attacks are against by digital signature. The cloud scanning provides the dynamic digital signature for against the attacks.

Routing Algorithm
Cooperative game for clustering based routing algorithm

DTTR: The standard algorithm [22]of Leach is foundation for DTTR. It uses the similar set of cluster and avoids the head rotation of cluster and re clustering. The game-theory establishes the model of network. It contains contributor, payoff and strategy. The selection of intermediate node depends on payoff value.

The payoff value set the rank for neighbor node. The data flow method of DTTR: 1) acceptance packet data node selects the next node hop by destination address. 2) The destination address is not selected the packet data sent based on maximum payoff value form queue. The advantage of DTTR is: High throughput, minimum standard deviation and less energy consumption.

DEEH: is the extended version of LEACH. The performance of DEEH [22]is high when the node has large density. The DEEH extend the network life also guarantee the topology strength.

PFDBG: is a type of repeat game. It has incomplete information and noticeable actions. The main aim of PFDBG [22]is set the power value of inference and transmits to neighbor node. The power value is based on information on adjacent node table. It has high throughput and less energy consumption.

CONCLUSION

This paper presented a survey on Deceptive Attack and Defense Game in Honeypot network for IoT. The game-theory provide the various game-model for detect the defense present in the network. The Honeypots with IoT system develops secure network transactions. The combination of both Honeypots and Game-theory model detect the intrusion and provide the fast response by RRE engine. This result is the efficient defense detection in network environment.

REFERENCES

[1] Shigen Shen, Yuanjie Li , Hongyun Xu, Qiying Cao," Signaling game based strategy of intrusion detection in wireless sensor networks", Computers and Mathematics with Applications Science Direct -2011.

[2] Cheolhyeon Kwon,Weiyi Liu and Inseok Hwang," Security Analysis for Cyber-Physical Systems against Stealthy Deception Attacks", American Control Conference (ACC)-2013.

[3] Nandan Garg and Daniel Grosu," Deception in Honeynets: A Game-Theoretic Analysis, "IEEE -2007.

[4] Anuvarsha.G and Rajesh kumar, "Intrusion Detection and Response Using Game Strategy and RRE Engine in Network Security" International Journal of Engineering and Computer Science, Volume 4 issue 3 march -2015.

[5] Natarajan Meghanathan," A Tutorial on Network Security: Attacks and Controls "International Journal on Communications Antenna and Propagation-2012.

[6] Quang Duy La and Tony Q.S. Quek," A Game Theoretic Model for Enabling Honeypots in IoT Networks " conference paper on Research gate may -2013.

[7] Ruchika Mehresh, and Shambhu Upadhyaya," A Deception Framework for Survivability against Next Generation Cyber Attacks ",International Conference on Security and Management (SAM), July 2012.

[8] Animesh Patcha and Jung-Min Park," A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks "IEEE -2004.

[9] Animesh Patcha and Jung-Min Park, "A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks", International Journal of Network Security, Vol.2 – 2006.

[10] Osama Hayatle, Hadi Otrok, Amr Youssef," A Game Theoretic Investigation for High Interaction Honeypots", IEEE-2012.

[11] Lidong Zhou and Zygmunt J. Haas," Securing Ad Hoc Networks", IEEE-1999.

[12] Tansu Alpcan and Tamer Bas," A Game Theoretic Analysis of Intrusion Detection in Access Control Systems" 43rd IEEE Conference on Decision and Control-2004.

[13] Suguo Du Xiaolong Li, Junbo Du and Haojin Zhu," An attack-and-defence game for security assessment in vehicular ad hoc networks", Springer Science and Business Media, -2012.

[14] Jürgen Markert and Michael Massoth, "Honeypots Wording and Definitions in Wireless Sensor Networks" 2nd international Electronic Conference on Sensors and Application, November-2015.

[15] Radek Pbil, Viliam Lisy, Christopher Kiekintveld, Branislav Boksansk,and Michal," Game Theoretic Model of Strategic Honeypot Selection in Computer Networks", In proc. Decision and Game Theory for Security, Springer Berlin Heidelberg, 2012.

[16] Shyam Chandran and Resmi , "Optimal Game Theory for Network Security using IPDRS Engine",International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 1, January 2015.

[17] William Hurst and Chelsea Dobbins,"Guest Editorial Special Issue on: Big Data Analytics in Intelligent Systems", Journal of Computer Sciences and Applications, vol-3 - 2015.

[18] Shahid Raza," LIGHTWEIGHT SECURITY SOLUTIONS FOR THE INTERNET OF THINGS", School of Innovation, Design and Engineering -2013.

[19] Faheem Zafari, Ioannis Papapanagiotou, and Konstantinos Christidis, "Micro-location for Internet of Things equipped Smart Buildings ",IEEE -2015.

[20] Ruchika Mehresh and Shambhu Upadhyaya, " A Deception Framework for Survivability Against Next Generation Cyber Attacks", Springer international,2012.

[21] Ashiqur R and KhudaBukhsh," A Survey on Supermodular Games " - December 27, 2006.

DOI 10.17148/IJARCCE.2016.51051

[22] Zhi Ren, Shuang Peng, Hongjiang Lei and Jibi Li,” Game Theory-Based Routing Algorithms for Wireless Multi-hop Networks “,2nd International Conference on Computer and Information Application -2012.

[23] Kien C. Nguyen, Tansu Alpcan, and Tamer Bas¸ar,” Stochastic Games for Security in Networks with Interdependent Nodes “,International conference on Game Theory for Networks,2009.

[24] Jeffrey Pawlick and Quanyan Zhu,” Deception by Design: Evidence-Based Signaling Games for Network Defense”,May 16, 2015.

[25] Mohammad Masoud Javidi and Laya Aliahmadipour,” Game theory approaches for improving intrusion detection in MANETs”, Scientific Research and Essays Vol. 6(31), pp. 6535-6539, 16 December, 2011.

[26] Martin Rehak, Michal Pechoucek, Martin Grill, Jan Stiborek and Karel Bartos,” Game Theoretical Adaptation Model for Intrusion Detection System(Extended Abstract)”, Proc. of 10th Int. Conf. on Autonomous Agents and Multiagent Systems – Innovative Applications Track (AAMAS), 2011.

[27] Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya and Qishi Wu,” A Survey of Game Theory as Applied to Network Security “,Proceedings of the 43rd Hawaii International Conference on System Sciences – 2010.

[28] Yi Luo, Ferenc Szidarovszky, Youssif Al-Nashif and Salim Hariri,” Game Theory Based Network Security”, Journal of Information Security, 2010.

[29] Kong-wei Lye and Jeannette Wing,”Game Strategies in Network Security” International Journal of Information Security . 2005.

[30] Jon Oltsik,”Internet of Things: A CISO and Network Security Perspective”, Cisco Systems and is distributed under license from ESG,2014.

[31] KeyWhan Chung,Charles A.Kamhoua,Kevin A.Kwiat,Zbigniew T.kalbarczyk and Ravishankar k.Lyer” Game theory with learning for cyber security monitoring”, IEEE -2016.

[32] Dipak V Bhosale, Prajakta K Mitkal and Yogesh S Lonkar,” Cyber Security using Game theory”, - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 1, January 2016.

[33] Kartikey Agarwal, and Dr. Sanjay Kumar Dubey,” Network Security : Attacks and Defence”, International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE)Volume 1, Issue 3, August 2014.

[34] MS. Masroor Jahan Mohd.Mubeen Ansari,” Network Security: Attacks and Defence”, International Journal of Computer Science and Information Technology Research Vol. 3, Issue 2, pp: (959-963), 2015.

[35] internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security.

[36] searchsecurity.techtarget.com/definition/honey-pot.

[37] Kartikey Agarwal and Dr. Sanjay Kumar Dubey,” Network Security : Attacks and Defence”, International Journal of Advance Foundation and Research in Science & Engineering,2014.

[38] BADR BENMAMMAR, FRANCINE KRIEF,”Game theory applications in wireless networks: A survey” 13th International Conference on Software Engineering, Parallel and Distributed Systems (SEPADS '14),2014.

DOI 10.17148/IJARCCE.2016.51051