International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Performance Analysis of Denial of Service (DoS) and Distributed (DDoS) Attack of Application and Network Layer of IoT

Hanumat Prasad Alahari, Suresh Babu. Yelavarthi

Abstract: ***In present days the Internet of Things (IoT) is fast-growing technology for the use of various internet services to connect with any component at anytime. This is used as a medium between the components that are self-organize; recognize themselves using (RFID) Radio frequency identification, Zig Bee and WSN etc. for efficient communication. IoT consists of the most unique features. IoT faces many complicated issues based on power, security, and connectivity. It is very important to adopt the IoT into various large networks which secure the personal data from the real threats. In this paper, analysis the DoS and DDoS attack of application and network layer of IoT. Moreover, this paper also analyze the performance with various metrics delay, number of packets lost, routing metrics that can improve the performance of the IoT.***

Keywords: DDOS, RFID, CoAP, XMPP, CARP, CORPL.

I. INTRODUCTION

IoT is a fast-growing field nowadays for secure in various fields. This acts as a medium for various domains. Today, this communication progressed to connect numerous smart devices to the Internet, characterized as Internet of Things (IoT), which is a most popular and trending technology that incorporate M2M (Machine to Machine) communication. This M2M communication device includes embedded sensors, RFID, Wi-Fi, data networks, actuators, LTE, WLAN etc. This merging capability of many kinds of devices in any network made IoT most useful for many applications. These devices process itself and exchange the data without the inclusion of human beings that empowered the physical world into a computerized network for greater accuracy and efficiency.

Moreover, IoT provides more attractive characteristics such as correspondence, union, unification, Green living, After all these improvements IoT still raises several problems and challenges which need to be considered. Previously there are much research is done on security issues of IoT. IoT security plays a major role in connecting the various devices and maintains the component securely. The other issues addressed is to decrypt the data which can be a store, tracking and analyzing the large amounts of data that will be generated.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Hanumat Prasad Alahari*, Research Scholar, Department Of Computer Science & Engineering, Acharya Nagarjuna University, Guntur. India hanuma.alahari@gmail.com
Dr. Suresh Babu. Yelavarthi, Prof . Department of Computer Science, J.K.C. College, Guntur, India. yalavarthi_s@yahoo.com

There will even be vital security challenges from the increasing quantity of information with the myriad of devices increasing security complexness. This, in turn, can have a control on obtainable needs, that are expected to extend, golf shot period of time business processes in danger.

II. LITERATURE SURVEY

This chapter explains the literature survey which is related to Attacks present in various layers of IoT for qualitative analyses proposed by various researchers. The author [4] explains the Secure Data Exchange Protocol (SDEP) which is used to make every sequence encoding rule and Hash rule and helps in maintaining user privacy and preventing the issues. RFID is the most advanced automatic technology which finds the objects by the RF signal and accesses the connected information. It contains 3 components like RFID tags, RFID readers and also the back server. This paper surveys on SDEP, which is supported by sequence encoding rule and Hash rule and additionally depends on the feedback register and it shows this protocol has each robust security and high sensible price.

All the wireless network square measure organized within the inauspicious space and square measure usually left-out and additionally a number of their routing protocols don't take into account security phase attributable to the resource constraints that have low communication vary, low process power, low power provide and low memory.

Richard Brooks in [6] gives us insight into sinkhole attack mechanism and reviewed 3 mechanisms used to suppress the Sleep Deprivation Attack namely, the random robin scheme, the round vote scheme, and the hash-based scheme. Among them, he named the hash-based scheme as a better countermeasure against the Sleep Deprivation Attack. “Towards an analysis of security issues, challenges and open problem in the internet of things” which mainly focused on open challenges and security issues of IoT. Everyone known that IOT is most popular and very fast growing technologies in the present world. IOT is spreading its technologies to all branches such as hospitality, construction, software development. But the security became a very major issue in that. In this paper several security problems and their solutions has been discussed. In addition to that interoperability of the objects and complete architecture of the IOT. WentaoShang [7] UCLA has surveyed on “Challenges in IOT networking via TCP\IP Architecture”. Networking and IOT are most trendy technologies in present days. IOT is widely spreading all over the world. In this paper, TCP\IP protocol stack is proposed for the IOT. IETF has done research to find out that protocol stack which mainly suite for IOT.

The aim of this paper is to solve the problems which are generated by the usage of this TCP\IP protocol stack and how to resolve those problems. In addition to it is also surveyed on the design functionalities of the transport layer protocols like CoAP, AMQP.

Network Attacks of IoT

This section initially presents the architecture of IoT that consist of three-layered architectures- application layer, network layer and perception layer.

The application layer is distributed as application layer and middleware layer, where application layer contains the various applications - smart grid, smart home, smart retail etc. while middleware layer provides management services like authentication, information development etc. The applications are connected to middle ware technology services. Middleware technology provides management services like authentication, service management, information management, technical management; Intelligent computer technology-SOA, Platform Enhanced Technology. Authentication means the system will check the incoming data and transmits it to the required user. These management services are carried using various protocols like CoAP, XMPP, AMQPetc..Over internet, this is connected to the network layer. Final layer is the context-aware that consists of various hardware technologies such as sensors, actuators, RFID devices. This device transmits the data through gateway interface for providing the external services for commercial and industrial oriented applications.

Network Layer Attack of IoT

Cognitive Routing Protocol for Low- Power and Loss Networks (CORPL)-The extension of RPL is CORPL named as Cognitive RPL that is designed for cognitive networks and uses (Destination-oriented directed acyclic graph) DODAG topology with two new changes to RPL. This utilizes the opportunistic forwarding while forwarding all the packets with multiple forwarders and chooses the best next hop to forward the packets. Channel-Aware Routing Protocol (CARP)-CARP refers to Channel-Aware Routing Protocol. It is a distributed routing protocol that is designed for underwater communications and can be used because of its lightweight packets. It also studies the link quality, which is computed depending upon old data transmissions (successful) that are collected from neighboring sensors, to select the forwarding nodes.6LoWPAN-6 Low WPAN refers to IPv6 over Low power Wireless Personal Area Network. It comprises low power devices that are adapted to IEEE 802.15.4 and offers header compression to decrease transmission overhead.

Attack of IoT Network Layer

This subsection discusses the various attacks against routing protocols of network layer of IoT before to discuss the DoS attack, which is one of the severe attack that degrade the performance of a network by disconnecting the host.

Sybil Attack: The Sybil attack occurs, when a single adversary is controlling multiple nodes on a network, which is not known to the network that the nodes are controlled by the adversarial node. In this attack, a single faulty entity presents multiple identities that control the significant part of the system.

Sinkhole Attack: Sinkhole attack is a type of attack where compromised node tries to attract network traffic by advertising its fake routing update. Because of this, the entire data flows through that particular node resulting in the loss of packets in that particular path. This leads to data discordance and interception. In this, attacker makes the system believe that all the data is received to the receiver .This whole process is unknown to the system.

Denial of service (DoS) Attack: DoS is one of the severe attacks that degrade the performance of a network by disconnecting the host, bandwidth depletion and resource depletion. This attack is not only used to gain unauthorized access but also to control the system unknowingly. Attackers are of many types such as; they can attack the network with the help of authentication by entering wrong passwords. If the security is high, the account or network locked and can block the attackers and prevent the various attacks within the network. This attack is very complicated and difficult to prevent because it is important to analyze the whole network.

Sleep Deprivation Attack: In wireless sensor networks, the sensor nodes are maintained with batteries of less life time. In order to sustain that, the nodes will follow sleep routines to prolong their lifetime. The Sleep Deprivation Attack will exploit this weakness and keeps all the nodes awake that leads to high consumption of battery. Due to high consumption, the lifetime of the battery will be decreased drastically; as a result nodes will get shut down. In addition the sleep deprivation attack increases the power consumption of sensor networks.

Man in the middle attack: The man-in-the-middle attack may be described as a “Computer security breach in which a malicious user intercepts and possibly alters data in the network”. In this attack, a malicious attacker inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information transmitted between them. This attack is a type of eavesdropping where malicious attacker intercepts, send and receive the data that is meant for someone else without knowing them.

Malicious code injection: In today’s world code injection attack is a very big problem. Malicious codes are pieces of code that can affect the secrecy, the data and functionality, and control flow of a system. Code injection attacks are to take advantage of software loopholes and to insert fake code into target program. These injected fake codes are normally called malware. In this hacker compromises one node to inject malicious code in system which can also cause result in the network failure or in worst situation, the hacker can also get complete control on the network.

III. METHODOLOGIES OF DOS AND DDOS ATTACK:

Cyber-attacks became a reality of life, with information breaches of high-profile businesses and organizations creating headline news much on a day to day. One among the foremost common cyber threats is DoS that may be a denial of service, as per its name it makes websites and remaining on- line resources unavailable for proposed users. DoS attacks are of the many sorts some with directly aiming server design and a few others create use of vulnerabilities in communication and application protocols.

in contrast to different cyber-attacks, denial of service attack tries to create our servers and websites unavailable for legitimate users. In a number of the case, anyhow, denial of service is additionally used as a smokescreen for a few different malicious works, and for taking down security appliances, for instance, net application firewalls.
If a DoS attack is victorious, it willa extremely obvious event that impacts the complete on-line user base. Attributable to this, it has become a weapon of option to cyber vandals, extortionists, and hacktivists and for anyone trying to create a degree a cause. Denial of service attacks pre lasts for weeks, even months at a time that makes them severely damaging to any on-line organization. They result in loose customer trust, loss of revenues, and might force businesses to pay fortunes in compensations and additionally leads businesses to suffer long-term damage of reputation.

Distributed Denial of Service (DDoS) Algorithm

DDoS is a kind of DoS attack wherever multiple intermediate systems that concerned are often affected with a Trojan, are used for targeting one system inflicting a DoS attack. All systems maliciously used, systems that are controlled be assaulter in distributed attack and additionally finish targeted systems are the victims of a DDoS attack. In DoS attacks, the hacker makes servers and networks flood with traffic for overwhelming victim resources and for creating it not possible or troublesome for legitimate users to use them. Flooding attacks are tougher to live through, whereas associate server will usually be controlled with success by merely rebooting the system.
In this DDoS attack, the network traffic comes from many various attacking sources- from variety of thousands or additional. As a result of this, blocking single IP address makes it not possible to prevent the attack and additionally it's troublesome to differentiate legitimate traffic and malicious traffic once it's distributed over several points of origin. In typical DDoS attack, the assaulter starts through exploiting a vulnerability in one system and by creating it the DDos master .The master attacking system acknowledges different vulnerable systems and gains management on them either by infecting different systems through bypassing the authentication controls that's by estimating default parole on a wide used device or with malware. A system or a networked device underneath the management of an attacker is understood as a bit or a zombie. The individual that controls a larva net is usually referred as bot master. Botnets will comprise any range of bots; in botnets, there's no higher limit to their size as a result of, in present days
DoS are also characterized by the method that the attack uses.

- Application layer attacks create faux traffic flow to net application servers, particularly DNS (domain name server) or hypertext transfer protocol servers. In another way, DoS attacks depend upon flooding of the application servers with the network information, others rely upon misusing weaknesses either in the application protocol or in victim's application server.
- Buffer overflow attack may be an enclosure description most typically applied to Denial of Service attacks that sends additional flow to the network resource that is ever predictable by the developers.
- The ping-of-death attack misuses the ping protocol by creating request messages with outsized payloads, inflicting targeted systems to become weak, stop responding to legitimate requests.
- SYN flooding attack abuses (TCP) Transmission control protocol's
- Acknowledgement protocol so that a shopper creates a TCP reference to a server.

IV. SIMULATION RESULTS AND ANALYSIS

The results are analyzed and performance of Denial of Service (DoS) using Contiki Operating System in Cooja Simulation. Specifically, the attack analysis is performed on data messages that can reduce resources in the application and Network layer, while leaving the target's services unavailable. Contiki is an (OS) operating system is designed to focus on low-power wireless IoT devices and memory constrained devices which are software of open-source released with a BSD license. Applications of Contiki are sound monitoring for smart cities, systems for street lighting, alarms and radiation monitoring. Contiki was developed by Adam Dunkels, developers of Texas Instruments, Atmel, Cisco, Rednwire, RWTH Aachen University, Oxford University, SAP, Zoleritia, and many others.

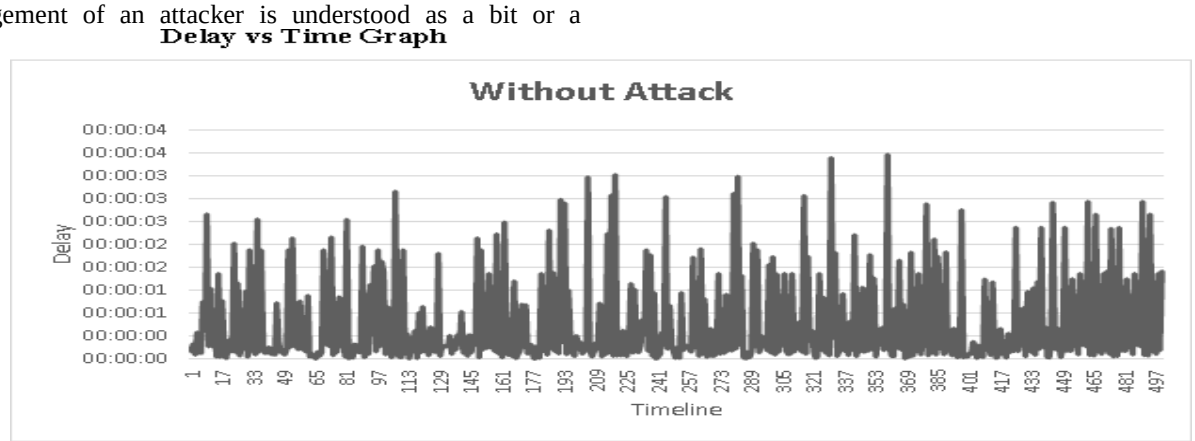

Figure-1: Delay vs Time without Attack

The following figure-1 shows the delay statistics obtained from our simulations for 25, 50, 75, 100motes without the presence of DoS and DDoS attack. It is observed that from the figure the average delay of 1.7s in the network application without the attack throughout the timeline.

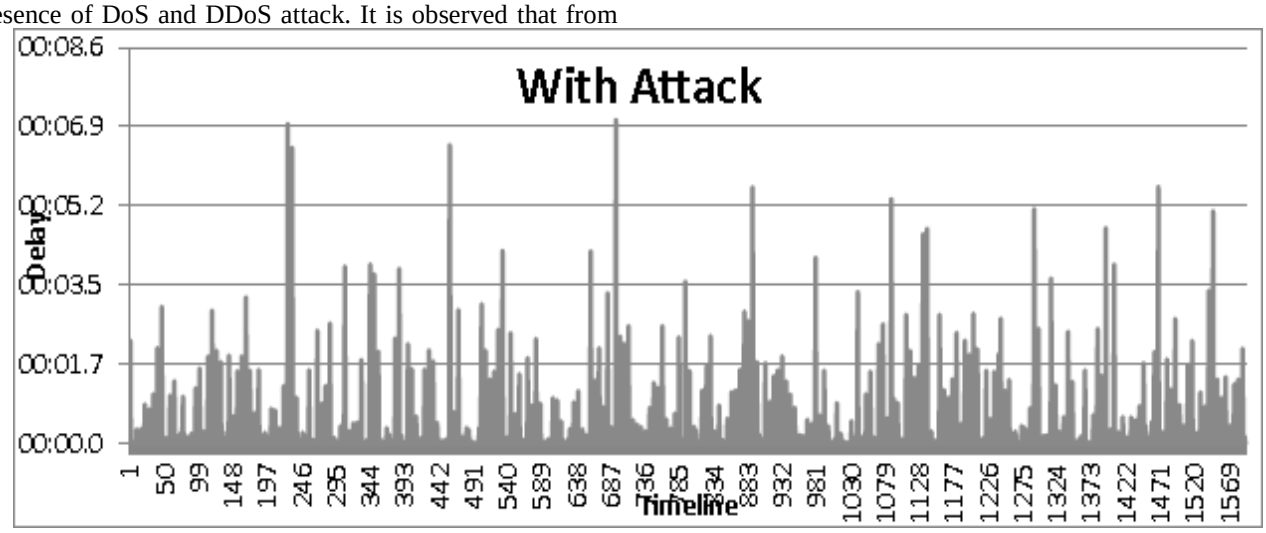

Figure-2 Delay vs time with DoS Attack

The following figure-2 shows the delay statistics obtained from our simulations for 25, 50, 75, 100motes without the presence of DoS and DDoS attack. It is observed that from the figure the average delay of 3s in the network with the presence of DoS and DDoS attack for the time of one hour.

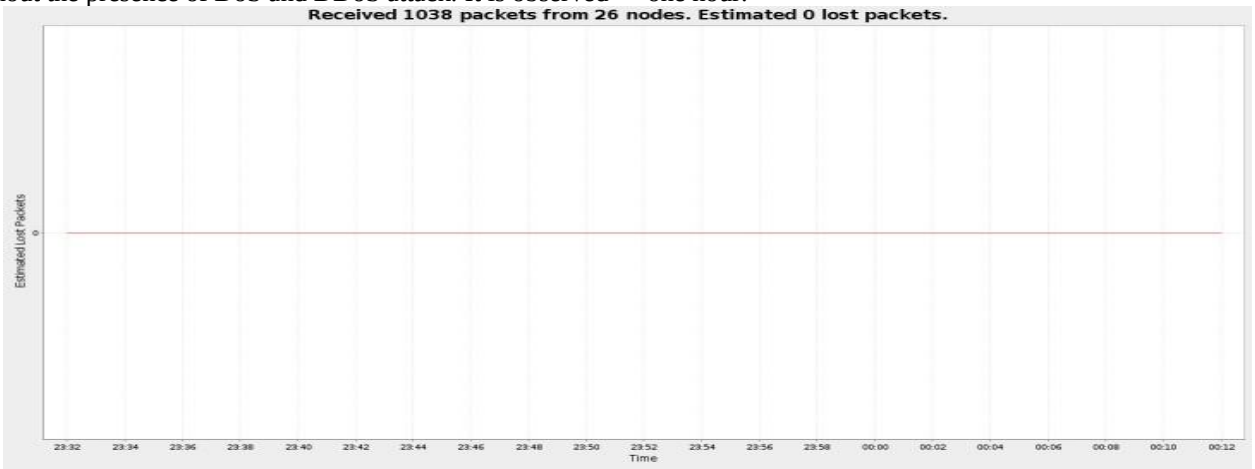

Figure 3 Estimated Lost Packets vs Time without DoS and DDoSAttack

The following figure-3 shows the delay statisticsobtained from our simulations for 25, 50, 75, 100motes without the presence of DoS and DDoS attack.It is observed that from the figure, that there is absolutely no packet loss in the network without the attack throughout the timeline.

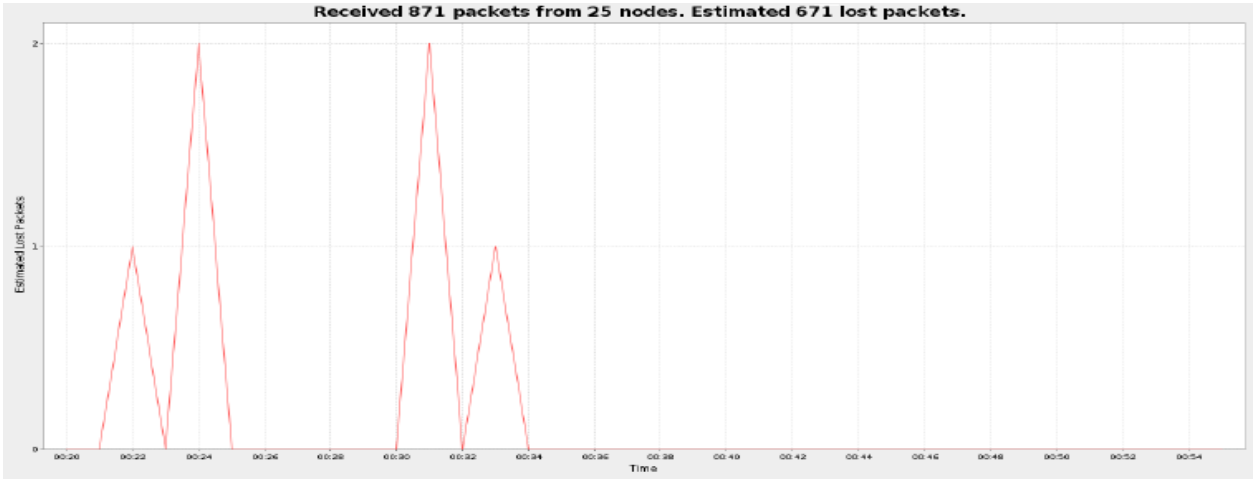

Figure-4: Estimated Lost Packets vs Time with DoS and DDoS Attack

The following figure-4 shows the delay statistics obtained from our simulations for 25, 50, 75, 100motes without the presence of DoS and DDoS attack. It is observed that from the figure that there are approximately 671 packets lost in the network with the attack for the time of one hour.

The following figure-4 shows the Routing path statistics obtained from our simulations for 25, 50, 75, 100motes.It is observed that from the figure that the number of decisions made by each node in the network in order to achieve best routing path to its destination

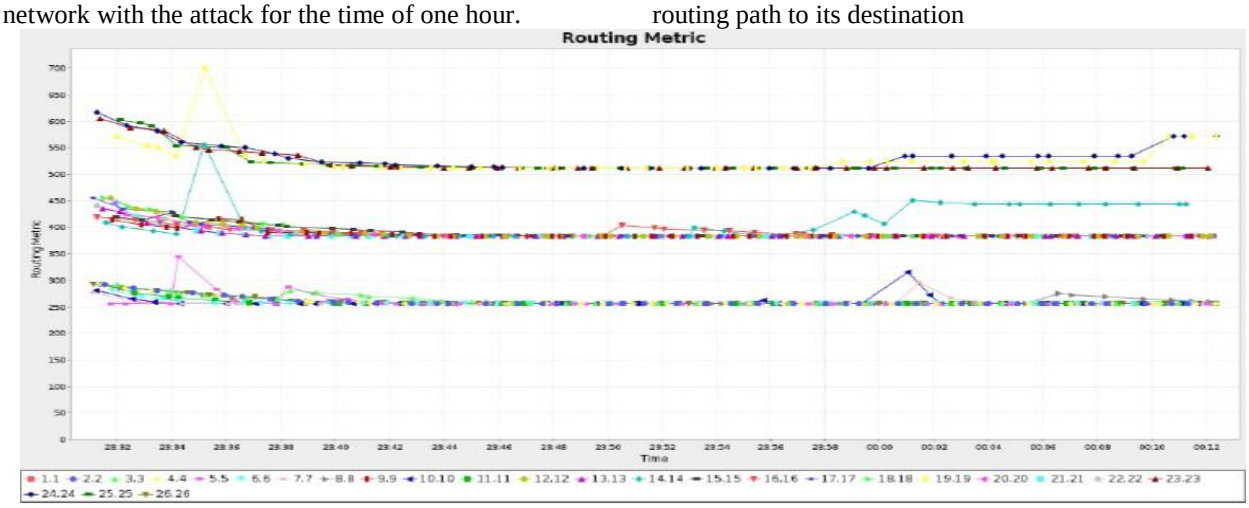

Figure-5 Routing Path

V. CONCLUSION

In this paper, the analysis is done on applications of DoS and DDoS attacks and also the network layer in IoT. In a real-time environment, the DoS is most challenging attack. If we try to analyze the attack and prevent it we can prevent the servers from crashes when they were overloaded with many users ,bots etc .Moreover, this paper also analyze the performance with various metrics delay, number of packets lost, routing metrics that can degrade the performance of the IoT.

REFERENCES:

1. Manish Gupta, Gayathri Gopala krishnan, and Raj Sharman, "Counter measures against Distributed Denial of Service", 11th, ASIA '16.
2. D. Swathi Gavaishnave, R. Sarala, "Detection of Malicious Code-Injection Attack Using Two Phase Analysis Technique", IJCA (0975 – 8887) Volume 45– No.18, May 2012.
3. M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man in the Middle Attacks," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, third quarter 2016.
4. Yaping Zhang, Lina Bo, and Qian Ma, "A Secure Data Exchange Protocol for the Internet of Things", SCST, Tianjin University, Tianjin, China.
5. George W. Kibirige, George W. Kibirige, "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network" Department of Informatics, SUA, Morogoro, Tanzania.
6. Matthewpirretti, sencunzhu, N. Vijay Krishnan, Patrickmcdaniel, and Mahmut kandemir, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense", IJDSN, 2: 267–287, 2006.
7. Lehtonen M., Ostojic D., Ilic A., Michahelles F. (2009) "Securing RFID Systems by Detecting Tag Cloning". In: Tokuda H., Beigl M., Friday A., Brush A.J.B., Tobe Y. (eds) Pervasive Computing. Pervasive 2009. Lecture Notes in Computer Science, vol 5538. Springer, Berlin, Heidelberg
8. T. A. Alghamdi, A. Lasebae and M. Aiash, "Security analysis of the constrained application protocol in the Internet of Things," FGCT, London, 2013, pp. 163-168.
9. Wentao Shang, Yingdi Yu, Ralph Droms and Lixia Zhang, "Challenges in IoT Networking via TCP/IP Architecture" NDN Technical Report NDN-0038, 2016. Revision 1: February 10, 2016.
10. Md. Mahmud Hossain, MaziarFotouhi, and Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", 2015 IEEE World Congress on Services.
11. MallikarjunTalwari "Routing Techniques and Protocols for Internet of Things: A Survey", Proceeding of NCRIET-2015 & Indian J.Sci.Res. 12(1):417-423, 2015.
12. Vasileios Karagiannis, Periklis Chatzimisios, Francisco Vazquez-Gallego, Jesus Alonso-Zarate2, "A Survey on Application Layer Protocols for the Internet of Things", Transaction on IoT and Cloud Computing 2015.

AUTHORS PROFILE

Alahari Hanumat Prasad, HOD, Dept of CSE at G.V.R&S college of Engineering & Technology, Budampadu, Guntur. He received M.Tech in Computer Science Engineering from Narasaraopet Engineering College and presently pursuing Ph.D From Acharaya Nagarjuna University. He gained 13 years Experience in Teaching and Administration. He attended various National and International Workshops and Conferences. He has published nearly 10 National and International papers.

Dr. Y. Suresh Babu, Prof, Dept of Computer Science,JKC college,Guntur. He holds a doctorate in Computer Science & Engg.Image Processing as specialization with a combined experience of 26 years in Academic & administration. He has published nearly 45 research papers in various National and International journals of reputed.