JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-5 E-ISSN: 2347-2693

Performance Analysis of 802.11 and SMAC Protocol under Sleep Deprivation Torture Attack in Wireless Sensor Networks

Genita Gautam[1*] and Biswaraj Sen[2]

[1*,2]Department of Computer Science and Engineering, SMIT, SMU, India

www.ijcseonline.org

Received: May/07/2015 Revised: May/14//2015 Accepted: May/24/2015 Published: May/30/ 2015

Abstract— A Wireless Sensor Network (WSN) consists of a group of sensors which are geographically distributed and are capable of computing, communicating and sensing. One of the major challenges of WSN is to preserve energy. MAC protocols which operate at the data link layer have full control over the wireless radio; their design can contribute significantly to the overall energy requirements of a sensor node. The goal of the sensor MAC (S-MAC) protocol (Ye et al. 2002) is to reduce unnecessary energy consumption, while providing good scalability and collision avoidance. S-MAC adopts a duty-cycle approach, that is, nodes periodically transition between a listen state and a sleep state. The sleep deprivation torture attack also known as denial-of-sleep attack is a powerful attack in which an attacker prevents a sensor from going into sleep mode. It makes a device inoperable by draining the battery more quickly than it would be under normal usage. This paper provides a comparative study of 802.11 and SMAC protocol under this attack. A simulation has been carried out in NS2 and analysis shows that SMAC performs similar to 802.11 under such attack.

Keywords—Wireless Sensor Networks (WSN'S) , Media Access Control(MAC) , Sensor MAC (SMAC)

I. Introduction

Security is one of the most enormous challenges in WSN. This is because the applications served by these sensors make them attractive for intrusions and other attacks. Sensors are used in highly sensitive data applications such as battlefield, disaster relief, target tracking, rescue management, monitoring civil infrastructures such as tunnels and bridges and many more. Thus any breach of security or compromise of information for such kind of applications can have serious consequences.

One of the major constraints of sensors is its small size making them limited in their available memory and storage capacity. To overcome this challenge, a mechanism known as dynamic power management (DPM) is used, where a resource can be moved between different operational modes i.e. active, idle, and asleep by which the sensor node's battery life is extended. During sleep time the sensor nodes cannot receive messages from their neighbors nor can they relay for other sensors. Therefore, some WSN's use wakeup on demand strategies to enable nodes to wake up whenever required. This is done by the MAC protocols which operate at the data link layer.

If an attacker prevents the device from entering into the sleep mode by keeping it active, then the battery life can be drastically depleted. Such an attack is called the sleep deprivation torture attack. This is a very powerful attack as it drains the sensor battery very quickly then under normal condition.

Attacks can be categorized into two types based on the interruption of communication in the network, namely passive attacks and active attacks. During passive attacks fake data received from the attacker does not interrupt the network communication. Examples of this type of attack include eavesdropping, traffic analysis, and traffic monitoring. During active attacks fake packets received from the attacker disrupts the entire network. Example of this attack is jamming, replication, modification and denial-of-service (DOS).

The sleep deprivation torture attack is a type of denial-of-service attack.

II. MAC PROTOCOLS IN WSN

MAC protocols which operate at the data link layer are designed for fairness, i.e. All nodes are treated as equal. Any node can access the medium at any time and no special treatment is given to anyone. However in WSN, the nodes cooperate to achieve a common goal, thus fairness is of less importance. Instead, sensor nodes are concerned with energy consumption and sensing applications.

As discussed, sensor nodes must operate using finite energy source (batteries) due to their small size. Since MAC protocols have full control over the wireless radio, their design can contribute significantly to the overall energy requirements of a sensor node. Many networks can benefit from MAC schemes that don't require the nodes to be active always. They allow periodic access to the medium for transmission of data and to put their radios into low-power sleep modes between periodic transmissions. The amount of time a device spends in active mode is called the duty cycle. It is often very small due to the low frequency and small data transmissions occurring in many WSN's. Our aim here is to first understand how S-MAC is affected by this attack.

Sensor MAC(SMAC)

SMAC stands for Sensor MAC. This protocol tries to reduce energy consumption due to overhearing, idle listening and collision. Each node has two states, listen state and sleep state. Any time frame in S-MAC is divided into two parts: one for listen period and the other for sleep period. Each node chooses its own schedule, though it is preferred when nodes synchronize their schedules such that they listen or sleep at the same time. In this case, nodes using the same schedule are considered to belong to the same virtual cluster, but no real clustering takes place and all nodes are free to communicate with nodes outside their clusters. Nodes periodically exchange their schedules with their neighbors using SYNC messages, that is, every node knows when any of its neighbor's will be awake. If node A wants to communicate with a neighbor B that uses a different schedule, A waits until B is listening and then initiates the data transfer. Contention for the medium is resolved using the RTS/CTS scheme. S-MAC divides a node's listen interval further into a part for receiving SYNC packets and a part for receiving RTS messages .Each part is further divided into small slots to facilitate carrier sensing. A node trying to send a SYNC or RTS message randomly selects a time slot (within the SYNC or RTS part of the interval, respectively) and senses the carrier for activity from when the receiver begins listening to the selected slot. If no activity has been detected, it wins the medium and begins transmissions.

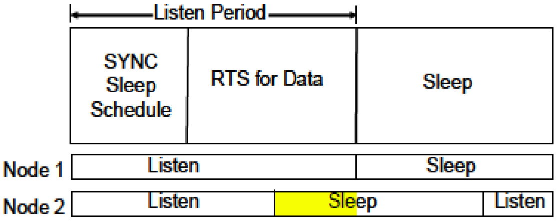


Fig 1: SMAC operation [2]
gfdgd

Categories of denial-of-sleep attack

The MAC-layer denial-of-sleep attacks on WSNs can be categorized based on the level of protocol knowledge required to initiate them and the level of network penetration achieved by an attacker [2].

Class 1—No Protocol Knowledge, No Ability to Penetrate Network:

With no knowledge of the MAC layer protocols, attacks are limited to physical-layer jamming and unintelligent replay attacks. In an unintelligent replay attack, recorded traffic is replayed into the network, causing nodes to waste energy receiving and processing these extra packets. If nodes in the network do not implement an anti-replay mechanism, this attack causes the replayed traffic to be forwarded through the network, consuming power at each node on the path to the destination. Undetected replay has the added benefit (to the attacker) of causing the network to resend data that could subvert the network's purpose. For example, replaying traffic in a military sensor network deployed to sense enemy movement could cause combat units to be misdirected.

Class 2: Full Protocol Knowledge, No Ability to Penetrate Network:

Traffic analysis can determine which MAC protocol lies being used in a sensor network. With this knowledge, an attacker could expand the attack types beyond those listed earlier to include intelligent jamming, injecting unauthenticated unicast or broadcast traffic into the network, or being more selective about replaying previous traffic. Intelligent jamming uses knowledge of link-layer protocols to reduce network throughput without relying on a constant jam signal, for example, by jamming only RTS packets. Such attacks improve over constant physical-layer jamming in that they preserve attacker energy, which can be important if attacking nodes have constraints similar to those of the target nodes. Even when attacker power consumption is not a factor, intelligent jamming might be used to make it more difficult for a network to detect an attack. If valid source and destination addresses are inserted by an attacker, unauthenticated traffic requires that nodes stay awake to receive packets, even if they are later discarded due to invalid authentication. If packets are encrypted, a node must receive the entire packet before decrypting and discarding it. The number of nodes impacted by unauthenticated broadcast traffic depends on the MAC protocol. For example, if the protocol uses a cluster head or gateway node to authenticate broadcast traffic before other nodes are compelled to receive it, then only the gateway node energy is impacted. Replay attacks can also be more cleverly executed with knowledge of the protocol, even if the messages cannot be deciphered. It has been shown that if the MAC layer protocol is known, traffic analysis can be used to distinguish data from control traffic. Depending on the protocol, effective denial-of-sleep attacks can be mounted by replaying specific control messages, even without the ability to decrypt the traffic. For example, properly timed SYNC retransmission in the S-MAC protocol could potentially prevent nodes from entering their duty/sleep cycle and could keep all nodes in receive mode until their batteries are depleted.

Class 3— Full Protocol Knowledge, Network Penetrated

Attacks in this category could be devastating to a WSN. With full knowledge of the MAC protocol and the ability to send trusted traffic, an attacker can produce traffic to gain maximum possible impact from denial-of-sleep attacks. The types of attacks that could be executed against each MAC protocol and the impact of such attacks can be analysed. This type of attack is very difficult to detect because it appears that the system is behaving normally, with the possible exception of the battery status indicator. Side effects that one would expect to see of these attacks if they are not implemented subtly include the CPU fan turning on while the user is performing some action that does not normally cause the fan to come on, the system becoming less interactive than usual, and the hard drive spinning up immediately after a spin down. A successful attack will likely cause the user to believe that the battery has become defective and will no longer keep a charge.

The type of attack implemented here is Class 3.

III. PROBLEM STATEMENT

The objective of this work is to investigate the performance of 802.11 and SMAC under sleep deprivation torture attack. Analysis has been done by calculating the average end-to-end delay, total energy consumed and average throughput of the network using PERL script and AWK script.

IV. SIMULATION ENVIRONMENT

The network model considers as wireless sensor network in two-dimensional (2D) plane with 64 sensors. These sensors are uniformly and independently deployed in a square area = (800m × 800m). The different simulation parameters that have been set up are given below:

Simulator	NS 2.35
Simulation Area	800m × 800m
No. of Nodes	64
Channel Type	Wireless
Radio Propagation Model	Two-way ground
Network Interface type	Wireless
MAC Type	802.11/SMAC
Maximum Packet in queue	50
Routing Protocol	AODV
Simulation Time	100 secs
Transmission Range	200/500 m
Communication Range	200/500m
Traffic	CBR
Packet Size	100 bytes
Rate	Variable

Table1: Simulation Parameters

In this WSN; every sensor reports its sensor data once every second to the cluster head. The cluster head aggregates the data and forwards it to the sink. The malicious node sends data to all the nodes that are in their communication range at an interval of 1 ms thus by making them busy consistently. Therefore they are continuously using energy to transmit or receive data. Thus, their battery gets depleted more rapidly than under normal conditions.

The first step of simulation is to implement Sleep Deprivation Torture Attack in a WSN without sleep cycles. i.e. by using 802.11 MAC protocol. There are three types of nodes. i.e. innocent, malicious and a sink shown in table 2. The sink node is the one who is having higher communication and sensing range i.e. 500m and also more initial energy. One of the innocent nodes who are closest to the node is elected as the cluster head. The cluster head aggregates the data and forwards it to the sink.

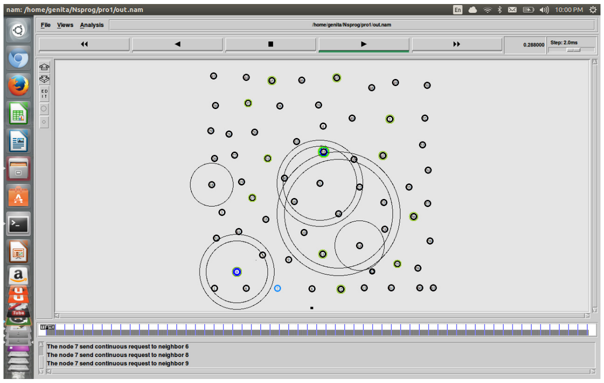
Type of Node	Communication Range(m)	Transmission Range(m)	Initial Energy(J)
Innocent	200	200	100
Malicious	200	200	100
Sink	500	500	200

Table 2: Types of nodes

The next step is to implement Sleep Deprivation Torture Attack in a WSN with SMAC. The WSN here is same as above. The duty cycle for each node is given as 10%. Rest of the time it will be in sleep mode. Without the presence of the intrusion detection model, these malicious nodes are not detected. Hence, the nodes do not allow the innocent nodes to go into sleep mode thus draining their battery more quickly than under normal conditions.

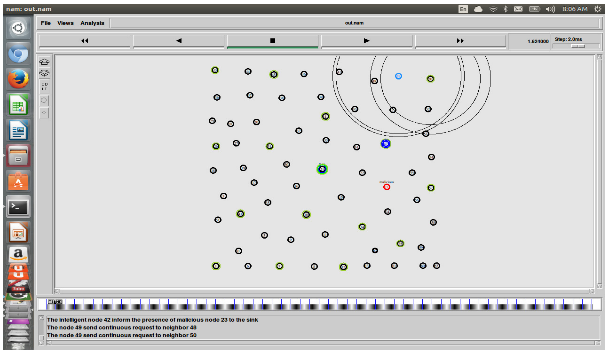
V. RESULTS AND DISCUSSIONS

The snapshot below show the shows the NAM output of 64 nodes in an area of 800m×800m. The localization technique used here is one-way Time of Arrival (ToA). The nodes in green colour are the cluster heads.


nam: /home/genita/Nsprog/prot/out.nam
File
Views
Analysis
/home/genita/Nsprog/prot/out.nam
0.288000
Step: 2.0ms
TIME

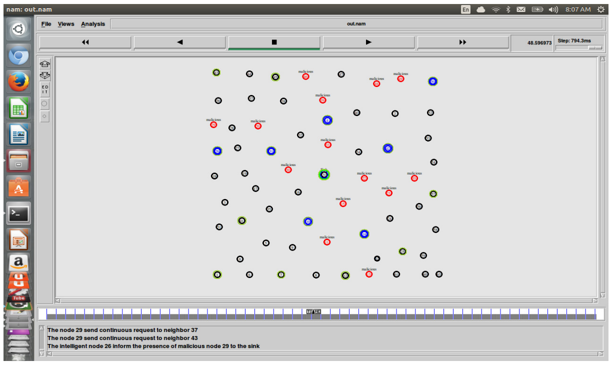
The node 7 send continuous request to neighbor 6
The node 7 send continuous request to neighbor 8
The node 7 send continuous request to neighbor 9

Fig 2: Nam output showing 64 nodes



The intelligent node 42 inform the presence of malicious node 23 to the sink
The node 49 send continuous request to neighbor 48
The node 49 send continuous request to neighbor 50

Fig 3: Nam output showing 1 malicious node



The node 29 send continuous request to neighbor 37
The node 29 send continuous request to neighbor 43
The intelligent node 26 inform the presence of malicious node 29 to the sink

Fig 4: Nam output showing n malicious nodes

A. Average end-to-end delay

Average End-to-End delay is a metrics used to measure the performance with time taken by a packet to travel across a network from a source node to the destination node. The average end to end delay of a data packet is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination.

End-to-End Delay=∑ (arrive time – send time) / ∑ Number of connections

The graph below show the average end-to-end delay in the network by varying the number of attackers in the network from 0% to 90%. It is observed that average end-to-end delay is higher in case of SMAC. This is due to the fact that because a message-generating event may occur during sleep time and a node can reply only in its active time. The average-end-to-end delay increases considerably under attack. This is because there is a large no. of packets flowing in the network and a large no. of packets is dropped and hence a large no. of retransmissions occurs.

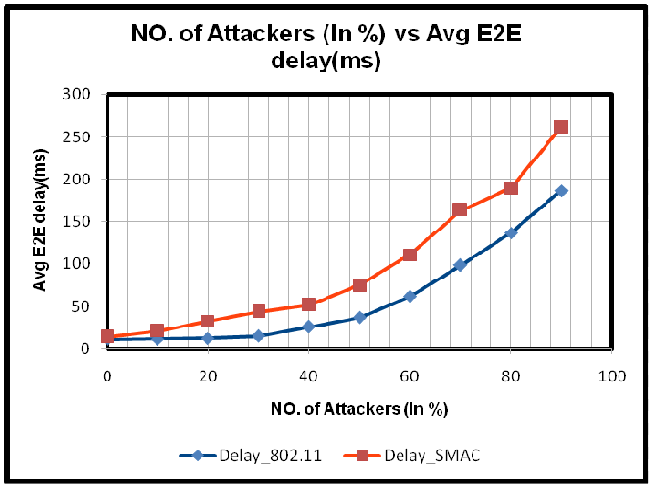


Fig 5: Graph showing Average End-to-End delay Vs the number of attackers in the system

B. Total Energy Consumption

Tx is the total amount of energy required to transmit and Rx is the total amount of energy required to receive data. Its unit is taken in milijoules.It is given by the formula below[20]:

Tx (k, d)= E_{elec} ** k +* E_{amp} ** k * d^2*
Rx(k)= E_{elec} ** k*
E_{elec}*=amount of energy consumption per bit in the transmitter or receiver circuitry = 50 nJ/bit = 0.001 mJ*

*k = Length of the message in bits= 100 * 8 bits= 800 bits.*

E_{amp}*=Amount of energy consumption of transmission amplifier = 100 pJ/bit= 100 * 10-6 mJ*

d = Distance between the nodes.

*Total Energy Consumed (802.11)= Total no. of packets sent * Tx + Total no. of packets received * Rx+ Total time spend by the devices in idle mode ** T_I

Where $T_{I=}$ *Energy consumed in Idle mode= 0.01 pJ.*

*Total Energy Consumed (SMAC)= Total no. of packets sent * Tx + Total no. of packets received * Rx+ Total time spend by the devices in sleep mode ** T_s

T_s *= Energy consumed in Sleep mode= 0.001 pJ.*

SMAC improves total energy consumption in the network by introducing sleep cycles. But however when a node is under attack, it cannot go to sleep mode because an attacker sends continuous requests. Thus the amount of energy consumed in the network increases tremendously.

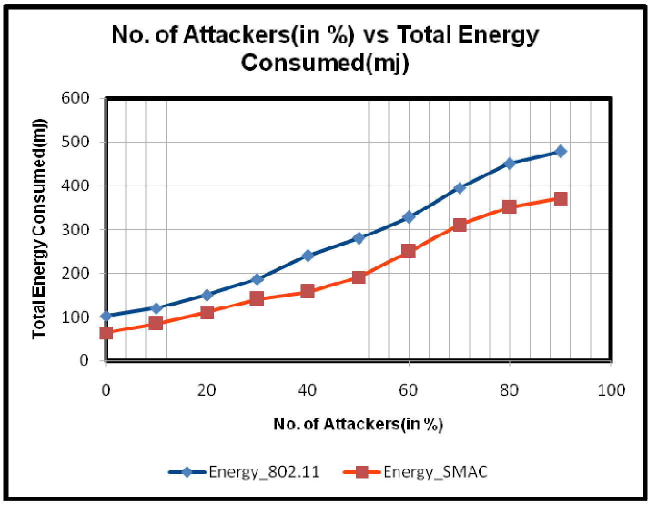


Fig 6: Graph showing total energy consumed Vs the number of attackers in the system

C. Average Throughput

Throughput of a network can be defined as the number of successfully delivered packets. The AWK script will count all the received application packets in a network such that we can calculate the network throughput. The code simply prints the observed throughput during the time interval throughout the simulation time by counting the no. of received packets.

Throughput(Kbps)=∑(recvdSize/(stopTime-startTime))(8/1000)*

The graph below shows that 802.11 give better throughput because when SMAC is used, only the active part of the frame is used for communication. However the average throughput of the network keeps decreasing as the no. of attackers increase in the network. This is because many packets get dropped in the network.

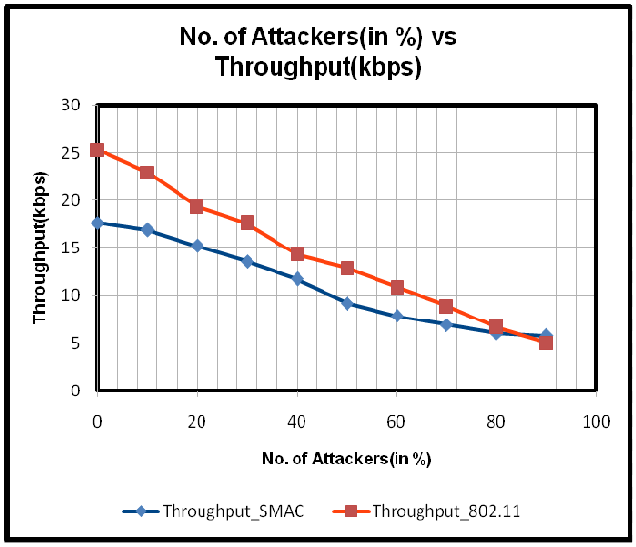


Fig 7: Graph showing average Throughput Vs the number of attackers in the system

VI. CONCLUSION

From the analysis it is observed that in the face of denial-of-sleep attack, SMAC also behaves similar to 802.11 as the sleep period of the nodes is disturbed. The amount of energy consumed in the network increases tremendously as the no. of attackers in the system keeps increasing. The throughput is reduced and the average end-to-end delay increases rapidly.

The future work would be to provide a framework to defend against such kind of attacks in order to gain maximum throughput, less energy consumption and low end-to-end delay.

REFERENCES

[1] Chen C., Hui L., Pei Q., Ning L., Qingquan P, "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks", Proceedings of the 2009 Fifth International Conference on Information Assurance and Security, Vol. 02, IEEE CS, May 2009.

[2] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, "Effect of Denial of sleep attacks on wireless sensor network MAC protocols" published by IEEE , June 2008.

[3] Dharam Vir, Dr.S.K.Agarwal, Dr.S.A.Imam:"WSN Performance Evauation of power consumption",International Journal of Scientific and Research Publications, Volume 3, Issue 12, December 2013.

[4] Genita Gautam, Biswaraj Sen, "Survey on different types of Security threats in wireless Sensor Networks", International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, pp-770-774.

[5] Genita Gautam, Biswaraj Sen, "Design and simulation of Wireless Sensor networks in NS2", International Journal of Computer Applications, Vol. 113 (16) , 2015, pp-14-16.

[6] Jianliang Zheng and Myung J. Lee,"A Comprehensive Performance Study of IEEE 802.15.4", IEEE, Aug. 1999.

[7] Michael Brownfield, Yatharth Gupta, Mem and Nathaniel Davis IV :" Wireless Sensor Network Denial of sleep attack" , IEEE 2005.

[8] M. Riduan Ahmad, Eryk Dutkiewicz and Xiaojing Huang," A Survey of Low Duty Cycle MAC Protocols in Wireless Sensor Networks", www.intechopen.com, 07, February, 2011.

[9] P. Lin, C. Qiao, and X. Wang, "Medium access control with a dynamic duty cycle for sensor networks", IEEE Wireless Communications and Networking Conference, Volume: 3,March 2004.

[10] Rajesh Yadav, Shirshu Varma, N. Malaviya," A SURVEY OF MAC PROTOCOLS FOR WIRELESS SENSOR NETWORKS", UbiCC Journal, Volume 4, Number 3, August 2009..

[11] R. Rugin, G. Mazzini, "A simple and efficient MAC-routing integrated algorithm for sensor network", IEEE International Conference on Communications, Volume: 6, June 2006.

[12] S. Cui, R. Madan, A. J. Goldsmith, and S. Lall, "Joint Routing, MAC, and Link Layer optimization in Sensor Networks with Energy Constraints", to appear at ICC'05, Korea, May, 2005.

[13] Security Model Using NS2 "International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 4 Issue 1 May 2014.

[14] Shweta Agarwal, Varsha Jain, Kuldeep Goswami," ENERGY EFFICIENT MAC PROTOCOLS FOR WIRELESS SENSOR NETWORK", www.intechopen.com, 07, February, 2011.

[15] Shamneesh Sharma, Dinesh Kumar and Keshav Kishore,"Wireless Sensor Networks- A Review on Topologies and Node Architecture", International

Journal of Computer Sciences and Engineering", Vol 1 Issue 2, Oct 2013.

[16] Tapalina Bhattasali, Rituparna Chaki, Sugata sanyal: "Sleep deprivation Attack Detection in Wireless Sensor network", International Journal of Computer Applications, February 2012.

[17] Teerawat Issariyakul, Ekram Hossain,"Introduction to Network Simulator 2", Springer US,2008, pp 1-18.

[18] T.V. Dam and K. Langendoen, "An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks", The First ACM Conference on Embedded Networked Sensor Systems (Sensys'03), Los Angeles, CA, USA, November, 2003.

[19] Waltenegus Dargie and Christian Poellabauer," FUNDAMENTALS OF WIRELESS SENSOR NETWORKS", 2nd Edition ,John Wiley & Sons, Ltd, pp.25-30.

[20] Vidya M, Reshmi S, "Denial-of-service Attacks in Wireless Sensor Ndetworks", International Journal of Advanced Computer Theory and Engineering, Volume -3, Issue -2, 2014.