International Journal of Future Generation Communication and Networking
Vol. 9, No. 7 (2016), pp. 13-22
http://dx.doi.org/10.14257/ijfgcn.2016.9.7.02

A Novel Approach For Elect A Zone Head On The Basis Of Energy And Distance Of Base Station In WSN

Ekta Chauhan

Department of computer science Engg.
Maharana Pratap College Of Technology
Gwalior, India
ektachauhan81@gmail.com

Abstract

Performance estimation is a most important study part in WSN and a prosperity of literature exists in this area. IN WSN, DOS attacks are known as threats that is an extremely serious threat due to the resources feature. Applications of the WSNs are transitioning to real-world, where they face attacks already skilled through the WAN and Internet. DOS is one form of attacks, which we will believe only become large common as accessible and sensor networks. WSN devices include limitations of the inherent resource, they are most receptive to the consumption and laying waste of these weak resources. In this paper on the basis of energy and distance of base station elect a zone head. The simulation of the proposed work concludes that the results of the approach are good it provides better results in terms of throughput and packet delivery ratio.

Keywords*: WSN; DOS; Sensor Management Protocol; ad-hoc networks, etc*

1. Introduction

WSN is generally nodes ad hoc network with capacities detecting. Such a large number of routing protocols proposed for ad hoc networks could likewise be utilized for WSNs. The attributes of WSNs are talked about from two viewpoints: from the nodes that make up the network, and from the network itself. Effective outline and usage of WSNs has turned into a hot range of exploration in recent years, because of the tremendous capability of sensor networks to empower applications that associate physical world to the virtual world. By networking administration substantial quantities of small sensor nodes, it is conceivable to acquire data about physical phenomena that was troublesome or difficult to get in more ordinary ways. In the coming years, as advances in micro-fabrication technology permit the expense of assembling sensor nodes to keep on, dropping, expanding organizations of wireless sensor networks are normal, with the networks inevitably developing to extensive quantities of nodes (*e.g.*, thousands). Potential applications for such huge scale WSNs exist in an assortment of fields, including medicinal monitoring [1-3], environmental monitoring [4-5], observation, home security, military operations, and mechanical machine monitoring. To comprehend the assortment of utilizations that can be bolstered by WSN, consider the accompanying two examples.

2. WSN Architecture

In an ordinary WSN, we see taking after network segments –Sensor nodes (Field devices) – Each sensor network node has ordinarily a few sections: a handset of the radio with an inner getting wire or association with an outside reception apparatus, electronic circuit and micro controller for

ISSN: 2233-7857 IJFGCN

a) Sensor interfacing and a vital source, additional often than not a battery or an installed energy harvesting type.
b) Gateway or Access Points – A Gateway empowers correspondence between Host application and field devices.
c) Network manager – A Network Manager is in charge of the setup of the network, planning correspondence between devices (i.e., designing super frames), routing tables administration and monitoring and reporting the network soundness.
d) Security administrator – The Security Manager is in charge of the era, and administration of k

The base stations are one or more recognized segment of the WSN with an excessive deal extra computational, vitality and correspondence assets. Other exceptional parts in routing based networks are routers, intended to figure, compute and convey the routing tables. Numerous methods are utilized to unite with the outside world, including mobile phone networks, satellite telephones, radio modems, high power Wi-Fi links and so on. [6]

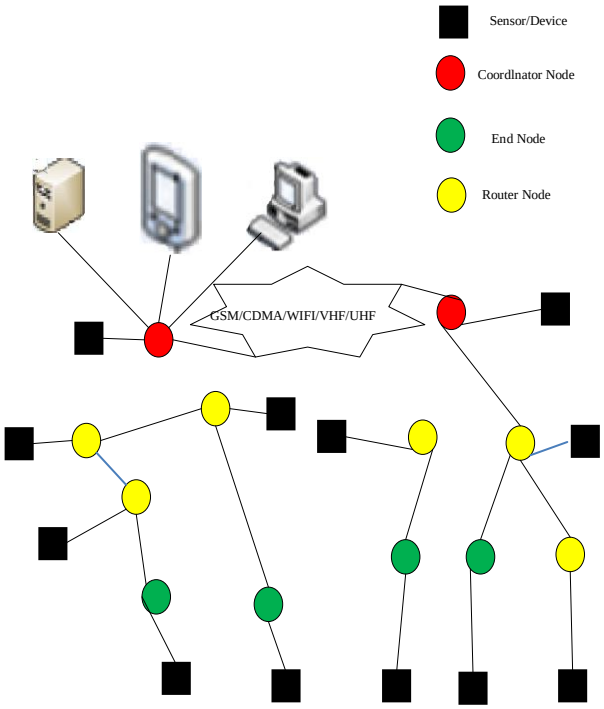

Figure 1. WSN Architecture

3. WSN Communication Protocol Architecture

Energy consumption of one sensor node is influenced by the structure of protocol layers and the way each layer manages the sensing data. The protocol layers stack used by the sensor nodes and a base station within the network includes the application layer, transport layer, network layer, data link layer, the physical layer, power management, plane mobility management plane and task management plane. Fig. 3 shows the protocol stacks and cross layer services.

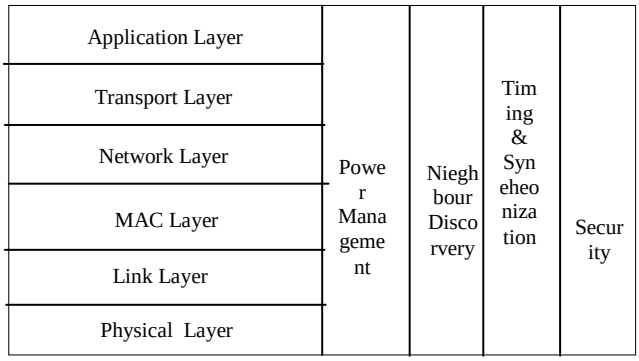

Figure 2. The Protocol Stacks and Cross-Layer Services

- **Application Layer**

This layer supports different software for applications depending on the sensing task. The three types of protocols are defined for this layer.

a) SMP- Sensor Management Protocol
b) TADAP-Task Assignment and Data Advertisement Protocol
c) SQDDP- Sensor Query and Data Dissemination Protocol

- **Transport Layer**

Transport layer helps to maintain the data flow when the application layer is in need. The development of protocols in this layer is a real task because sensors are influenced through numerous parameters and constraints for example limited power supply and memory.

- **Network Layer**

This layer allows routing of data through the wireless communication channel. There are several strategies to route data, such as routing power cost with available energy based on the energy metric and data centric routing based on attribute based naming and interest dissemination.

- **Data Link Layer**

The data link layer is responsible for data streams, data frame detection, Medium Access Control and error detection and correction multiplexing. The layer protocol design issues must take into account the various constraints for example power conservation, mobility management and recovery failure approach.

- **Physical Layer**

Physical layer is the lowermost layer and is in charge of frequency selection, carrier frequency generation signal location, and balance and data encryption

4. Characteristics of Wireless Sensor Networks

1. Large scale of deployment: A typical sensor network may consist of hundreds or thousands of heterogeneous nodes. In adding, sensor networks often contain numerous centralized control points known as base stations.

2. Resource scarcity*:* Particularly, a WSN is conceded to be formed of constrained-resource nodes, which must be small; therefore, they are limited in power, memory and processing capacity. Energy is the most precious resource for sensor networks so

communication is especially expensive in terms of power. For that reason, saving energy to prolong network life has a deep impact into the network architecture.

3. Multi-hop routing algorithm: A sensor network typically constitutes a wireless ad-hoc network, implying that every sensor bolsters a multi-hop routing algorithm.

4. Static/dynamic environments*:* Where sensors are for the most part sent in static, predetermined areas with sensor readings taken at normal interims and multi hopped to a static sink for resulting examination and stockpiling. Portability expansion in every one of its structures speaks to a later research subject in sensor networking, that is, versatility of sinks, versatility of sensors and actuators and also the versatility of code, i.e. applications.

5. Node failure recovery: As sensors usually are deployed in remote and hostile surroundings, people cannot attend the sensor nodes. When some nodes fail due to exhausted batteries, faulted hardware and intrusion from attackers, these unattended nodes cannot be changed or repaired. Failed nodes may lead to network partition which decreases the cover ratio reducingthe availability of the network and even producing network failure. So, network topology should tolerate node-failure and activate self-configuring schemes to avoid network partition.

5. Security Issue in WSN

1. Availability:

The accessibility in WSN ensures the network administrations are possible, even in the subsistence of disavowal of service attacks. The security protocols perform the accessibility of data on the network with focus low vitality and capacity with reuse of code in the network. Inaccessibility, a few methodologies modify the code to reuse, however much code as could be expected and make utilization of additional correspondence to accomplish the same objective.

2. Self-Organization:

The WSN has numerous nodes for operations and sent in distinctive areas and fields. In self-association, the nodes are adaptable to act naturally arranging and self-recuperating in the network. The WSN is an Ad hoc network and all nodes are autonomous in network and without a framework. This natural trademark brings an extraordinary test for wireless network and security, also.

3. Time Synchronization:

Applications of WSN depend on some synchronization kind. The nodes have two states in the network on and rest and radio may be turned on or in rest mode for time frame. The sensor computes the end-to end deferral of a packet.

4. Secure Localization:

Wireless sensor network use area based data for recognizing the position of nodes in the network. Few attacks are connected with a sensor area by exploring for attacks. The attackers are seeking the header of packet and data for this reason. The safe restriction is an essential element amid actualizing security in the network.

5. Confidentiality:

The classification has limited data access to approved staff. The data ought not to spill crosswise over the nearby sensor network. At the point when one node sends the

exceptionally touchy data to the destination, it goes from numerous nodes in the network. For the procurement of security in data, network protocols are utilizing encryption strategy with a mystery key, the message is sent in encoded for to the channel. Data ought to encode to shield from activity analysis attack.

6. Authenticity:

Authenticity is basic in WSN, in light of the fact that a foe can without much of a stretch infuse messages. The collector node needs to ensure that data utilized as a part of any choice making procedure begin with trusted sources. The data validness is to ensure of the personalities of correspondence nodes. It is required in different organizational tasks.

7. Flexibility:

The sensor network situations are distinctive and relying upon natural conditions, risks and mission on the grounds that they are evolving as often as possible. Changing the mission objectives as often as possible need sensors to be diminished from settle nodes in the network.

6. Denial of Service Attack

A Denial of Service attack is an attack with the purpose that genuine users are unable of using a particular network resource which can be a website and whole system. The objective of a denial of service attack is to refuse legitimate user's accessibility to specific assets. In a DOS attack, the attacker basically transmits unnecessary messages asking the network or server to validate requests that have unacceptable return addresses. The network or server is incapable of determining the return address of the attacker when transmitting the verification approval, causing the server to wait before terminating the connection. When the server terminates the connection, the attacker transmits more verification messages with unacceptable return addresses. Consequently the process of verification and server wait will begin again, keeping the network or server occupied [3].

There are three main types of DOS attacks [5].
1) Utilization of inadequate, restricted or non-renewable resources
2) Damage or adjustment of composition information
3) Physical demolition or variation of network assets.

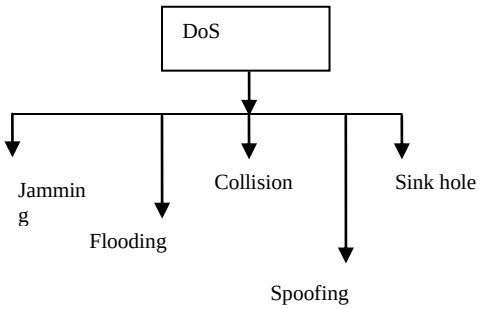

Figure 3. Types of Denial of service attacks

7. Literature Survey

Dharini et al (2015) in [7] proposed a detection scheme for detecting flooding attacks and gray hole attack. The proposed detection mechanism consumes less energy and also there is not much change in the throughput, packet delivery ratio and delay when

compared to ideal hierarchical wireless sensor network scenario. Thus the proposed detection mechanism is lightweight in nature, hence proving its efficiency.

P. V. Sawant et al (2015) in [8], introduced a detection framework for DOS attack utilizing elements, namely normalization and triangle area map procedures under Multivariate Correlation Analysis(MCA) which are helpful for precise movement depiction. Traffic Characterization is finished by separating the geometric connection between's system movement aspects.

Vikash Kumar et al (2014) in [9] devised a few security prerequisites for Wireless Sensor Network. Further, as security being key to the acknowledgment and utilization of sensor systems for some applications; it has made a depth threat examination of Wireless Sensor Network. Further proposed any security components against these threats in WSN.

Virmani et al (2014) in [10] studied about that Wireless sensor networks are prone to several potential attacks which block the normal functioning of the network. The security of a wireless sensor network is traded off on account of the random arrangement of sensor nodes in an open environment, memory restrictions, power constraints and unattended nature.

Venkatraman et al (2013) in [11] studied that a Group communications alludes to either point - to multi point (In which a packet is conveyed from a group member to alternate individuals) or multipoint-to multipoint communication (in which packet are sent from different individuals to different individuals concurrently). The attributes of distinctive wireless network - wireless infrastructure networks (WINs), ad-hoc networks (AHNs), and wireless sensor networks (WSNs) - are enormously diverse as far as group administration, packet sorts, and resources.

Priyanka Negi et al (2013) in [12] the proposed method, a modified CBF (Confidence Based Filtering) method is introduced to reduce the storage needs and to increase the processing speed on the server side. It is deployed at cloud data base. This technique is also based on correlation patterns.

Saman Taghavi Zargar and James Joshi et al (2013) in [13] have investigated the scope of DOS flooding attack issue and tried to defy it and categorize DOS flooding attack and characterize existing countermeasures relayed on where and when they anticipate, recognize, and react to the DOS flooding attack.

Hao Chen et al (2013) in [14] proposes real-time PSD converter based on FGPA to prevent shrew DDOS attacks which are low rate TCP targeted attacks. Here using component-reusable auto-correlation (AC) and adapted 2N-point real-valued DFT algorithm algorithm.

Maidamwar et al (2012) in [15] surveyed an effort to analyze threats to WSN and to report research variety efforts in studying a range of routing attacks that mark the network layer. The predominantly devastating attack is Wormhole attack-a Denial of Service attack, where attackers forming a low-latency link between two points in the network.

Akash Mittal et al (2011) in [16], defines various DDOS attack methods and countermeasures which include various approaches, for example, Bloom Filter, Trace Back method, Independent Component Analysis and TCP flow analysis. The paper also discusses different tools and software's used to perform DOS attacks in sensor networks.

Raymond et al (2009) in [17], have characterized the Lightweight Medium Access Control (LMAC) method. LMAC has turned out to be the most resistant protocol against energy effective attacks. LMAC is a decent illustrative of the TDMA classification. In LMAC time is separated into edges, which are further isolated into time slots. At first, it arranged Denial-of-sleep attack on WSN medium access control protocols taking into account attacker‟s information of the MAC convention and capacity to enter the network.

Jan Blumenthal, et al (2007) in [18] has acquainted Weighted Centroid Localization strategy by making it quick and simple for the algorithm to find devices in wireless sensor networks. The low complexity, the quick estimation and the insignificant asset necessities suggest WCL as localization algorithm in wireless strategy. WCL algorithm is derived

from a centroid determination which computes device's position through averaging known reference point's directions.

Hung-Min Sun, et al (2007) in [19] have multi data flow topologies plan to diminish the influenced range brought on by the versatile jamming attack. Multi data flow is a topologies plan that can successfully protect the versatile jamming attack. The versatile jamming attack causes the energy utilization as well as breaks the routing on WSN furthermore demonstrates that the current guard component is not able to withstand this attack.

8. Proposed Work

The number of nodes used is 100 nodes. The xy-dimension is of size 2000X2000. The initial energy is 1 joules. The start of simulation is 0.1miliseconds and the end of simulation is 100.0miliseconds. NS-2 is abbreviated for the Network Simulator (Version 2) it is an event driven simulation tool that has demonstrated to study the active nature of communication networks. Ns2 simulator is used for both wireless as well as wired networks (*e.g.*, routing algorithms, UDP, TCP). NS-2 is very popular these days and its popularity increases day by day due to its elastic and advance nature. University of California and Cornell University developed the REAL network simulator; NS foundation is based only on this. DARPA (Defense Advanced Research Projects Agency) provides the full support to NS through which VINT (Virtual Internetwork Tested) project. National Science Foundation (NSF) has joined the development.

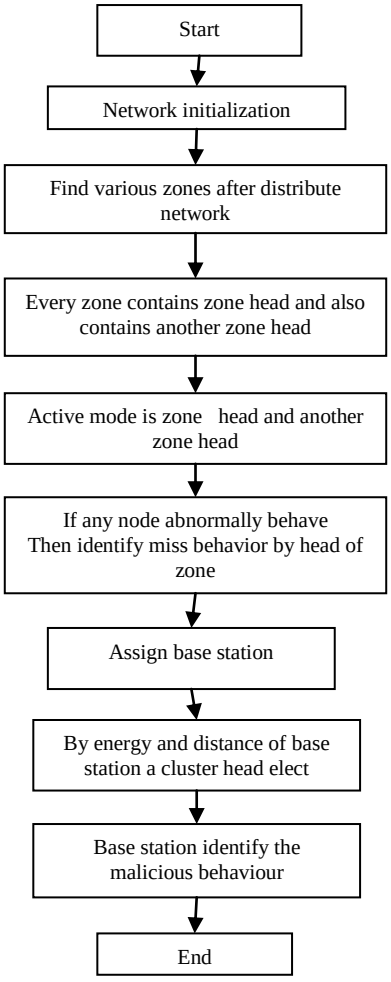

Figure 4. Proposed Work

9. Result Simulation

Throughput:

Per second transfer of data on bandwidth is known as throughput. The Fig.1 represents a throughput graph between base approach and proposed approach. The throughput of the proposed approach is better than the base approach.

Table 1. Base and proposed Throughput

Time	Base	Proposed
60	2885	3739
70	2726	3027
80	2522	4672
90	3340	4724
100	3527	4927

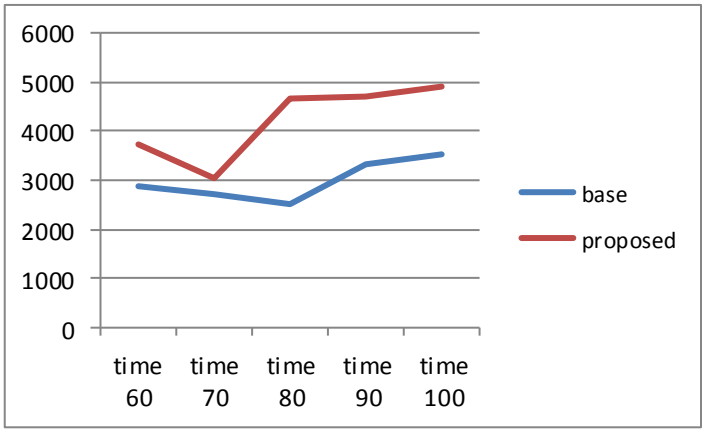

Figure 5. Base and proposed Throughput

Packet Delivey Ratio:

Defined as the ratio of packets delivered from source to destination. The Figure represents a PDR graph between base approach and the proposed approach. The packet delivery ratio of the proposed approach is better than the base approach.

Table 2. Base and proposed Packet Delivey Ratio

Time	Base	Proposed
10	82	89
20	92	87
30	98	91
40	91	97
50	96	96

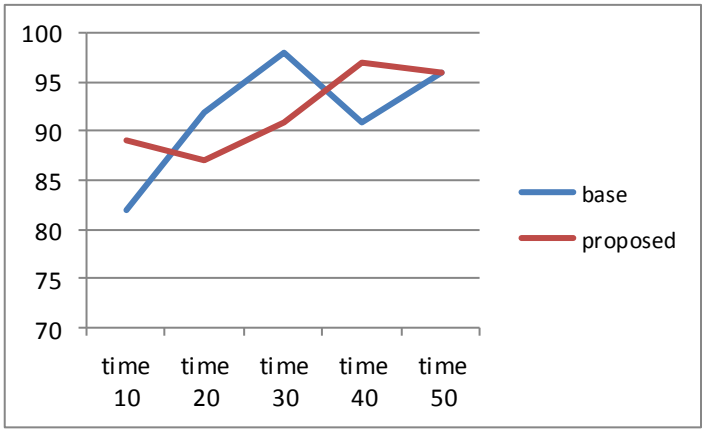

Figure 6. Base and proposed Packet Delivey Ratio

Routing Overhead:

The routing overhead is defined as data of data and flooding of data in the network transmitted by application, which utilizes a bit of accessible transfer rate of communication protocols. The Figure represents a routing overhead graph between base approach and the proposed approach. The overhead of the proposed approach is more than the base approach. Since the overhead should be minimum but as the routing increases in the proposed work the overhead also increases.

Table 2. Base and proposed Routing Overhead

Time	Base	Proposed
10	0.184	0.038
20	0.382	0.049
30	0.383	0.283
40	0.293	0.048
50	0.389	0.074

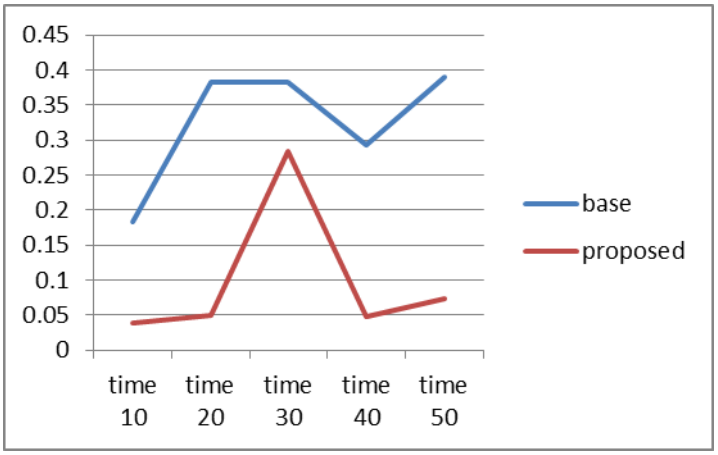

Figure 7. Base and proposed Routing Overhead

10. Conclusion

These consist two main key such as Security and Privacy that need to be considered when dealing with WSN control in an unattended atmosphere and carry sensitive data critical to the application. WSN are create of hundreds of problems based on sensors for solving real world sensitive applications. These nodes are strewed over an area to check

and record the information as desired by the application and to forward same to the midpoint node for further examination, which may generate an alert to control the situation. In current years, WSN has been grown very in the applications, resulted the require of a strong, consistent security mechanism. In this paper on the basis of energy and distance of base station elect a zone head. The simulation of the proposed work concludes that the results of the approach are good it provides better results in terms of throughput and packet delivery ratio.

References

[1] C. Kidd, "The aware home: A living laboratory for ubiquitous computing research", Proceedings of the Second International Workshop on Cooperative Buildings (CoBuild), **(1999)**.
[2] S. Intille, "Designing a home of the future", IEEE Pervasive Computing, vol. 1, no. 2, **(2002)**, pp. 76–82.
[3] L. Schwiebert, S. Gupta and J.Weinmann, "Research challenges in wireless networks of biomedical sensors", Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (MobiCom), **(2001)**.
[4] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler and J. Anderson, "Wireless sensor networks for habitat monitoring", Proceedings of the ACM International Workshop on Wireless Sensor Networks and Applications (WSNA), **(2002)**.
[5] D. Steere, A. Baptista, D. McNamee, C. Pu and J. Walpole, "Research challenges in environmental observation and forecasting systems", Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), **(2000)**.
[6] V. Pahune, S. Khode, "Security Issues, Attacks And Challenges In Wireless Sensor Network", International Journal Of Engineering Sciences & Research Technology, **(2015)**.
[7] N. Dharini, Ranjith Balakrishnan and A. Pravin Renold, "Distributed Detection Of Flooding And Gray Hole Attacks In Wireless Sensor Network", International Conference On Smart Technologies And Management For Computing, Communication, Controls, Energy And Materials (ICSTM), **(2015)**.
[8] P. V. Sawant, M. P. Sable, P. V. Kore, S. R. Bhosale, "A System For Denialofservice Attack Detectionbased On Multivariate Correlation Analysis", Multidisciplinary Journal of Research in Engineering and Technology, **(2015)**.
[9] V. Kumar, A. Jain, P. N. Barwal, "Wireless Sensor Networks: Security Issues, Challenges and Solutions", International Journal of Information & Computation Technology, vol. 4, no. 8, **(2014)**, pp. 859-868.
[10] D. Virmani, A. Soni, S. Chandel and M. Hemrajani, "Routing Attacks in Wireless Sensor Networks:A Survey", International Journal of Computer Science and Information Technologies, vol. 5, no. 2, **(2014)**.
[11] K. Venkatraman, J. V. Daniel, G. Murugaboopathi, "Various Attacks in Wireless Sensor Network:Survey", International Journal of Soft Computing and Engineering, vol.3, iss.1, **(2013)**.
[12] P. Negi, A. Mishra and B. B. Gupta, "Enhanced CBF Packet Filtering Method to Detect DDoS Attack in Cloud Computing Environment", **(2013)**.
[13] S. T. Zargar, J. Joshi and D. Tipper, "Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE communications surveys, **(2013)**.
[14] H. Chen, T. Gaska, Y. Chen and D. H. Summerville, "An optimized reconfigurable power spectral density converter for real-time shrew DDoS attacks detection", Computers and Electrical Engineering, vol. 39, **(2013)**, pp. 295–308
[15] P. Maidamwar and N. Chavhan, "A Survey on Security Issues to DetectWormhole Attack In Wireless Sensor Network", International Journal on AdHoc Networking Systems (IJANS), vol. 2, no. 4, **(2012)**.
[16] A. Mittal, A. K. Shrivastava and M. Manoria, "A Review of DDOS Attack and its Countermeasures in TCP Based Networks", International Journal of Computer Science & Engineering Survey (IJCSES), vol. 2, no. 4, **(2011)**.
[17] D. R. Raymond and C. Randy, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols", IEEE Transactions on VehicularTechnology, vol. 58, no. 1, **(2009)**.
[18] W. Haining, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering", Networking, IEEE/ACM Transactions, vol. 15, **(2007)**, pp. 40-53.
[19] J. Blumenthal, R. Grossmann, F. Golatowski and D. Timmermann, "Weighted Centroid Localization in Zigbee-based Sensor Networks", IEEE International Symposium on Intelligent Signal Processing, (WISP 2007), **(2007)**.

