www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issues 8 Aug 2016, Page No. 17571-17576

Grid Base Cluster Aproach for Detection Of Sinkhole Attack in WSN

Rupali Prajapati, Nitin Manjhi
Department of Computer Science
SRCEM,Banmor
Gwalior,India
rupaliprajapati9@gmail.com
Department of Computer Science
SRCEM,Banmor
Gwalior,India
nitin.manjhi@gmail.com

***Abstract*— Wireless sensor network is most concerning area of research now a days, energy and attacks are most challenging task for sensor network. In this paper we study about prevention and detection of sinkhole attack in sensor network techniques have some drawback too. Overcome all the problems we propose a grid based technique in which we deploy mobile agent in each grid and on the basis of acknowledgement and dely of data we compute the time and then mobile agent send the information to base station and find out the malicious behavior of node. our result shows that by using our methodology network performance enhance.**

Keywords—wsn;mac;rreq;rrep;rssi.

I. Introduction

Wireless sensor networks (WSNs) are a multi-hop temporary autonomous system made from a group of mobile nodes with wireless transmitters and receivers. Not relying on any preset infrastructure, it would achieve automatic organization and running in arbitrary mesh topology. Together with micro-processing and wireless communication capabilities, they are widely used on occasions which require rapid deployment and dynamic networking, such as military tactical communications and emergency communications. They are becoming a research subject of critical significance in practical application [1].

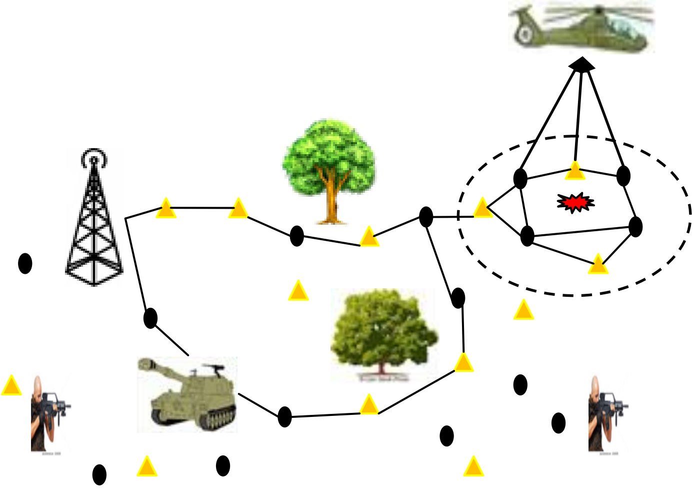


Figure 1. Wireless sensor network

Therefore, we need to utilize algorithms to obviate the security requirements of these networks in a way that it doesn’t draw excessive overhead on resources of sensor node [2]. WSNs security objectives conclude [2]:

• Data confidentiality: encrypting information to the render it imperceptible to illegal sensors is first security need of the sensor network.

• Data accuracy: these algorithms had been designed to make sure that the data have not been manipulated en route by means of other sensor nodes. In probably the most preliminary approach, MAC is calculated from the message and forwarded with the usual message. •

• Data freshness: it prevents resending old data from the adversary sensor nodes and ensures that the data received by the receivers is fresh.

• Resistance and fault tolerance: sensor networks need to be resistant against numerous attacks, and if a successful attack have been made, its impact should be local without disrupting the entire network.

II. Sinkhole Attack

Sinkhole attack is likely one of the severe attacks in wireless Ad hoc network. In the sinkhole attack, malicious node or compromised node presents incorrect routing knowledge to provide itself as a particular node and also receives whole network traffic. After receiving entire network traffic it modifies the secret information, equivalent to changes made to data packet or drops them to make the network complicated. A malicious node tries to draw the relaxed knowledge from all neighboring nodes. Sinkhole attacks impacts the performance of ad hoc networks protocols equivalent to AODV with the aid of utilizing flaws as maximizing the sequence number or minimizing the hop count [3]. In DSR protocol, sinkhole attack modifies sequence no in RREQ.

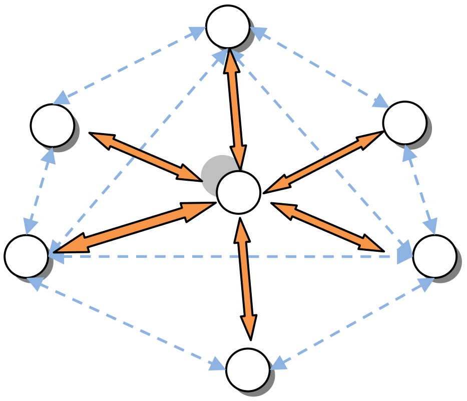


Fig.2 Example of Sinkhole attack

A. Effect of Sinkhole Attack on routing protocols

Routing protocols are need information packet need to transmitted from source node to the destination node by means of speaking with number of intermediate nodes. More than a few routing protocols had been proposed for such form of ad hoc networks. The studies on quite a lot of points of routing protocols were an active area of research for a long time. This paper analyzes the “Sinkhole Attack” that may be with ease employed in opposition to more than a few routing protocols. Routing protocols used in the wireless Ad hoc networks will also be categorized in the two different major types

- Table-driven routing protocols (Pro-Active)
- On-demand routing protocols (Reactive)

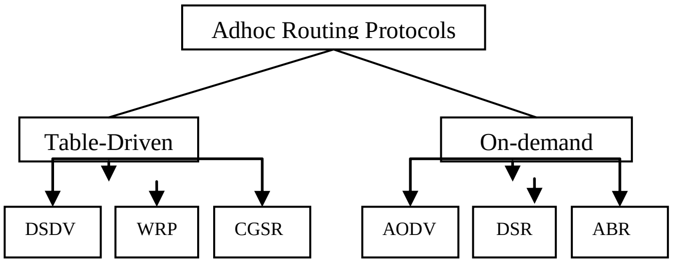


Fig.3 Ad hoc Routing Protocols

Table-driven routing protocols are improvements of the wired network routing protocols. They keep a table structure structure in order to retailer the routing information of each and every router. Table is continually up-to-date to maintain the correct information of network status [3]. Alternatively, on-demand routing protocols executes the path finding process when a path is required by a node.

III. COUNTERMEASURES AGAINGST SINKHOLE ATTACK

Data Consistency & Network Flow information Approach

The procedure provided in [4] includes the base station within the detection process, resulting in a high verbal exchange price for the protocol. The station of bottom floods network with request information containing affected nodes IDs. The affected nodes reply to BS with an information including their IDs, next hop id and related cost. The received data is then used from BS to construct a network flow graph for determining upon sinkhole. The performance of the proposed algorithm has been examined through each numerical evaluation and simulations. The results have tested the effectiveness and accuracy of the algorithm. They also endorse that its conversation and computation overheads are reasonably low for WSNs.

Hop Count Monitoring Scheme

A new IDS that notices the sinkhole attack presence is proposed in [4]. The scheme is established on hop depend monitoring. Because the hop-depend function is with ease obtained from routing tables, the ads (Anomaly Detection system) is modest to put in force with a small footprint. Additionally, the proposed advertisements are relevant to any routing protocol that dynamically continues a hop-count parameter as a measure of distance between destination and source nodes. The system can detect attacks with 96% accuracy and no false alarms utilizing a single detection system in the simulated network.

RSSI Based Scheme

A new technique of robust and lightweight answer for detecting the sinkhole attack founded on Received Signal strength Indicator (RSSI) readings of messages is proposed in [4]. The proposed answer needs collaboration of some Extra Monitor (EM) nodes aside from the ordinary nodes. It makes use of values of RSSI from 4 EM nodes to determine the role of all sensor nodes where the base Station (BS) is located at origin position (0, 0). This information is used as weight from the BS in an effort to become aware of Sinkhole attack. The simulation results exhibit that the proposed mechanism is lightweight as a result of the monitor nodes weren't loaded with any ordinary nodes or BS. The proposed mechanism does not motive the communication overhead.

Monitoring node’s CPU usage

A new algorithm for sinkhole attacks detecting for big scale WSNs is mentioned in [4]. The detection predicament is formulated as a change-point detection problem. The CPU utilization of every sensor node is monitored and analyzes the consistency of the CPU utilization. By using monitoring the CPU utilization of each and every node in constant time interval, the base station calculates the change of CPU utilization of each and every node. After evaluating the difference with a threshold, the bottom station would establish whether or not a node is malicious or now not. For that reason, proposed algorithm is able to variation between the legitimate and malicious nodes.

Mobile Agent Based Approach

Method to the defend against sinkhole attacks creating mobile agents use is proposed in [4]. A mobile agent is a program segment which is the self-controlling. It uses mobile agents to collect information of all mobile sensor nodes to make every node aware of the complete community in order that a valid node is not going to hear the dishonest expertise from malicious or compromised node which results in sinkhole attack. It does no longer want any encryption or decryption mechanism to become aware of the sinkhole attack. This mechanism does no longer require more energy than normal routing protocols.

Using Message Digest Algorithm

Sinkhole attack detection in the WSNs creating message digest algorithms use is proposed in [4]. The predominant goal of the protocol is to realize the specified sink hole utilizing the one-way hash chains. In the proposed approach destination detects the attack most effective when the digest received from the trustable forward direction and the digest bought through the trustable node to the destination are unique. It also ensures the data integrity of the messages transferred utilizing the trustable route. The algorithm can be effective to handle cooperative malicious nodes that try and conceal the true intruder. Proposed algorithm functionality is tested in the MAT lab.

IV. CHALLENGES IN DETECTING SINKHOLE ATTACKS IN WSN

Based on our assessment of the literature on sinkhole attacks in WSNs, the following are the foremost challenges in the detecting WSNs sinkhole attack:

i. *Communication patterns in WSNs:* the entire messages from sensor nodes in a WSN are destined for the bottom station however as a rule routed via other nodes developing an opportunity for the sinkhole to an attack launch. established on that verbal exchange sample the intruder need simplest compromise nodes almost the base station rather of concentrating on all nodes within the network. It is a challenge since the communication pattern itself supplies the possibility for attack.

ii. *Dynamic nature of WSN:*

Sensor networks are ad hoc networks with routing patterns developed as sensors and BS come interanet. Low energy wireless signals are area to sporadic interference. Sensors will not be optimally positioned for communications, might not be invariably on and may, in some instances, transfer.

iii. *Specific sinkhole attacks depend on routing protocols:* In WSNs packets are transmitted founded on a routing metric which varies for different routing protocols [5]. For illustration the methods utilized by a compromised node in network that uses the TinyAODV protocol will likely be exceptional from the one used one more protocol such as the MintRoute protocol. Nevertheless, these protocols are generally established on how “close” a node is to the base station. An attacking node can take advantage of this to lie to its neighbors in order to launch a sinkhole attack. Then the entire data from its neighbors to the base station will go via the attacker node.

Iv. *Sinkhole attacks may be insider attacks;* outsider and Insider attacks are two different attacks classes on networks. An outsider attack adds a malicious node to network. In an insider attack the intruder compromises one of the most official nodes through tampering with it or by means of weak point within the victim’s system software; compromised nodes inject false understanding in the network or listen to secret information. A compromised node possesses adequate access privilege in the network and already has advantage bearing on the network topology which creates further challenges in detection. As a result of this concern, even cryptography won't totally defend in opposition to insider attack [5]. Therefore insider attacks pose a more serious threat to systems than outsider attacks.

v. *Resource constraints limit detection methods:* The limited power supply, low communication range, low memory capacity and low computational power of sensors are the basic constraints in WSNs that mechanisms of strong security hinder application. The strong cryptographic ways used in different networks can not be implemented in a WSN because of low memory capacity. Consequently weaker ways suitable with to be had resources have to be used.

vi. *Vulnerability to physical attack:* A WSN may be deployed in a adverse environment and left unattended. This provides an possibility for an intruder to attack a node physically and get entry to all necessary information [5].

vii. *Vulnerability to key compromises*: An adversary could also be equipped to crack the authentication key saved throughout the sensor node. It can be feasible to reverse engineer the chipset, find the important thing and crack it or use brute-force approaches.

V. LITERATURE SURVEY

1n [6] focuses on sinkhole problem, its consequences & presents mechanism for detection & prevention of it on the context of AODV protocol.

It additionally suggests performance of AODV without a sinkhole attack, below attack & after applying our mechanism in the type of simulation effect got for unique nodes variation in the network, through seeing that performance metrics as throughput, PDR, Packet loss & End to end delay. Simulation is implemented making use of widely used simulator NS2.

In [7] Mintroute protocol vulnerabilities to the sinkhole attacks are discussed and present manual rules used. The preliminary experimental outcomes with the real WSN testbed exhibit its facility in the detecting sinkhole attacks for small size WSNs. Subsequently, the sinkhole detection method design WSN is proposed.

In [8] a proposal to offer protected communications in the sensible grid/utility metering networks utilizing RPL. The RPL protocol provides optimal routing performance in some wireless sensor networks and may become a strong standard in utility metering networks. However, protocol does many security flaws which should addressed prior to its critical infrastructure use for example AMI. Simulation results show that the proposed resolution provides good performance characteristics for use in utility grid networks.

In [9] In general, an intrusion detection system, referred to as INTI (Intrusion detection of SiNkhole attacks on 6LoWPAN for internet of things), to determine sinkhole attacks on routing services in the IoT. Furthermore, INTI objectives to mitigate antagonistic results discovered in IDS that disturb its efficiency, like false confident and negative, as good because the cost of the high valuable resource. System combines watchdog, reputation and trust approaches for attackers detection by analyzing devices performance. Results present INTI performance and its efficiency in attack detection rate phrases, various false negatives and false positives.

In [10] algorithm we investigated three scenarios with the trustability based on the beta distribution detecting those nodes in a WSN showing abnormal behaviour.

In addition, our algorithm can reward how weighting is an strong workable security measure within the specific WSN. Our proposed algorithm does not have any earlier information in regards to the target network when it's utilized to a WSN. It offers regular outcome, detecting malicious nodes with all reaching a trust value within a 0.003 variety within two hops of the assessing node in a WSN.

In [11] mechanism to launch sinkhole attack at WSNs. And then we reward some mechanisms to notice and defense this sort of attack. In the end, we do some experiments to verify our approaches.

In [12] The proposed IDS considers two varieties of sink mobility: periodic and random. Additionally, as the cell leaders don't activate their IDS agent at the same time, the further energy consumption incurred by the IDS is low. Simulation outcome exhibit the effectivity of the proposed IDS in terms of detection price, effectivity, and energy consumption.

In [13] muiltier intrusion detection system. Right here three tiers are application, routing and trust. The data transfer takes place between distinctive nodes. First a depended on connection is based between different nodes. second the routing policy is conformed for all nodes. Finally the application layer information is routed on the application kind. The node not following are believe or routing policy is observed a malicious node. In this research we have now simulated exclusive varieties of attacks and also provided pseudo code for one of a kind attacks like route invasion, eavesdrop, sinkhole. Then the performance of these attacks against the proposed algorithm has been calculated and result is displayed.

In [14] suggests an algorithm which firstly finds a group of suspected nodes by analyzing the consistency of data. Then, the intruder is recognized successfully within the group by checking the network flow information. The proposed algorithm's performance has been evaluated by using numerical analysis and simulations. Therefore, accuracy and efficiency of algorithm would be verified.

VI. COMPARISION TABLE

Techniques and Authors	Method of Study	Metrics Considered for Evaluation	Tools used
ACO-AD algorithm N.K. Sreelajaa et al	Simulation	Detection rate, False alarm rate and Number of searches	-
Redundancy Mechanism H.Shhafiei et al	Simulation	Detection rate, Mistake rate, Miss rate	NS2
Geostatistical Hazard Model Fang-Jiao Zhang et al	Simulation	Threshold. Number of monitors and Number of hops	OMNET++
Method using Request (rreq) and Response (rrep) for sequence number Tejindereep Singh et al	Simulation	Packet lost and Packet Received	NS2
Method using Base Station Maliheh Bahekmat et al	Simulation	Packet lost, Accuracy and Energy consumption	MATLAB
Method by analyzing network information Edith C.H. Nagai et al	Real Deployment	Accuracy and Energy consumption	-

Table 1 Comparison of Sinkhole Attack Detection Techniques [15]

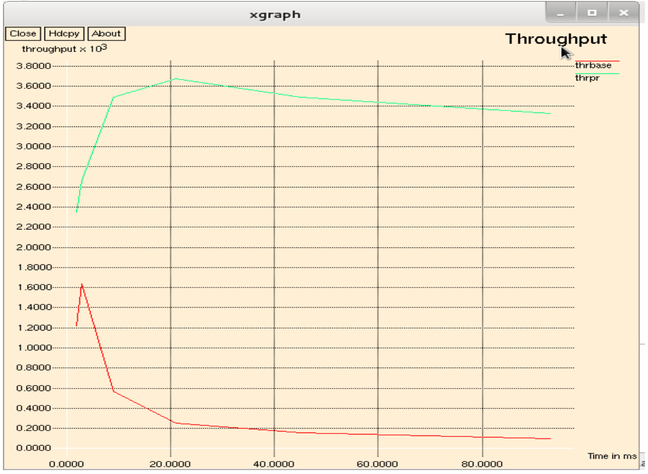
VII. PROPOSED WORK

WSN is an emerging knowledge and great potential to working in serious circumstances for example commercial and battlefields applications for example building, traffic surveillance, smart homes and habitat monitoring and numerous extra scenarios. One of the main challenges wsn face nowadays is security. While sensor node deployment in an unattended atmosphere produces networks vulnerable to a potential attacks variety, memory sensor and inherent power nodes limitations makes conventional security solutions unfeasible.

In existing work author find out malicious behavior on the basis of line of sight but if node does not exist in line we can't find malicious node. Overcome this draw back we propose a "**Grid Base Cluster Approach To Find Out Malicious Behavior In WSN",** in our propose work first we divide the network into grid, for cauterization if nodes are come into transmission range of each other they include in same cluster. After this process communication took place, and after send data if ACK does not receive by sender it wait for a particular time. Now active mobile node start moving in clusters and sender send information about ACK then mobile agent observe the behavior of nodes and count drop packets if miss ACK is more than threshold then mobile agent declare as malicious node and broadcast node-id of malicious node in network. Novelty of propose work we prove with the help of results.

```
Step1: initialize network ();
Step2: divide network into grid {
            if(node in transmission range){
                  node is in same cluster. }
            else{
                  node in different cluster
step3: cluster head selection
        if(node has highest energy || number of neighbors is high) {
```

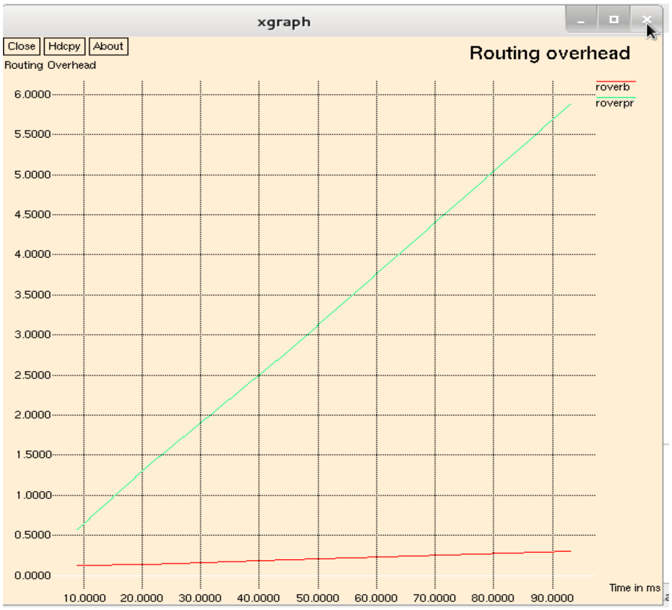
```
                    node become cluster head }
          else {
                    Node become normal node}
step4:  communication start
step5: check ack
              if(ackrcv!) {
                    active mobile agent in this area
                 if(node rapidly drop paket) {
                    agent sent info to cluster head
                         ch count number of miss ack
                  if(miss ack > threshold) {
                    sent info to base station and block node }
          } }
Step6: exit.
```



Graph:1 Throughput

Throughput:

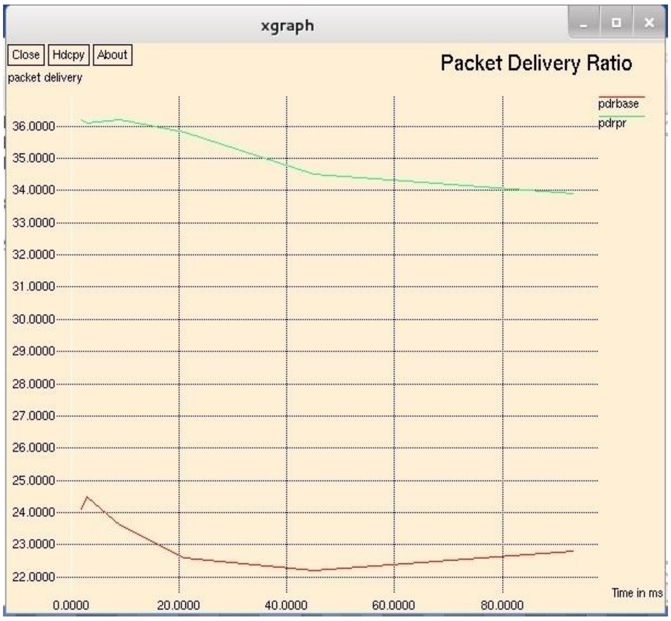
Per second transfer of data on bandwidth is known as throughput. The graph 1 represents a throughput graph between base approach and proposed approach. The throughput of the proposed approach is good than the existing approach.



Graph:2 Routing overhead

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 graph2 represents a routing overhead graph between base approach and 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.



Graph:3 Packet delivery ratio

Packet delivery ratio:

Defined as the ratio of packets delivered from source to destination. The graph3 represents a PDR between base approach and proposed approach. The packet delivery ratio of the proposed approach is good than the existing approach.

VIII. CONCLUSION

WSN is most concerning area of research in this paper we study about few prevention and detection technique of sink hole attack in wsn. Our propse work perform better compare to existing work, in future we apply optimization technique to enchance the result.

REFERENCES

[1] *Fang-Jiao Zhang et al. / Procedia Computer Science 31 (2014) 711 – 720*

[2] *Maliheh Bahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat Heydari Yazdi, and Sanaz Sadeghi," A Novel Algorithm for Detecting Sinkhole Attacks in WSNs", International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012,pp: 418- 421*

[3] *GAGANDEEP and AASHIMA," Study on Sinkhole Attacks in Wireless Ad hoc Networks", International Journal on Computer Science and Engineering (IJCSE) Vol. 4 No. 06 June 2012, pp: 1078-1085.*

[4] *Vinay Soni, Pratik Modi and Vishvash Chaudhri," Detecting Sinkhole Attack in Wireless Sensor Network", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 2, February 2013, Page 29-32.*

[5] *Junaid Ahsenali Chaudhry, Usman Tariq, Mohammed Arif Amin and Robert G. Rittenhouse," Sinkhole Vulnerabilities in Wireless Sensor*

Networks", International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.401-410 http://dx.doi.org/10.14257/ijsia.2014.8.1.37.

[6] *Nisarg Gandhewar and Rahila Patel," Detection & Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", 2012 Fourth International Conference on Computational Intelligence and Communication Networks, IEEE, pp: 714- 718.*

[7] *Murad A. Rassam, Anazida Zainal, Mohd. Aizaini Maarof, and Mohammed Al-Shaboti," A Sinkhole Attack Detection Scheme in Mintroute Wireless Sensor Networks", 1st IEEE International Symposium on Telecommunication Technologies 2012, pp: 71- 75.*

[8] *Clark Taylor and Thienne Johnson1," Strong Authentication Countermeasures Using Dynamic Keying for Sinkhole and Distance Spoofing Attacks in Smart Grid Networks", 2015 IEEE Wireless Communications and Networking Conference (WCNC): - Track 3: Mobile and Wireless Networks, pp: 1835- 1840.*

[9] *Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri Santos," Detection of Sinkhole Attacks for Supporting Secure Routing on 6LoWPAN for Internet of Things", 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM2015): Mini-Conference, pp: 606- 611.*

[10] *Dylan Cohen, Mark Kelly, Xu Huang and N. K. Srinath," Trustability Based on Beta Distribution Detectin Abnormal Behaviour Nodes in WSN", 2013 19th Asia-Pacific Conference on Communications (APCC), Bali - Indonesia IEEE, pp: 333- 338.*

[11] *Jin Qi, Tang Hong, Kuang Xiaohui and Liu Qiang," Detection and Defence of Sinkhole Attack in Wireless Sensor Network", 2012 IEEE.*

[12] *Mohamed Guerroumi, Abdelouahid Derhab and Kashif Saleem," Intrusion detection system against SinkHole attack in wireless sensor networks with mobile sink", 2015 12th International Conference on Information Technology - New Generations IEEE, pp: 307- 313.*

[13] *Sunil Phulre, Pratima Gautam and Sadhna K. Mishra," Implementation of Trusted Multitier method for Intrusion Detection in Mobile ad Hoc Networks with DSR Algorithm", Science and Information Conference 2014 August 27-29, 2014 London, UK, pp: 666- 673.*

[14] *Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala," Detection of Sinkhole Attack in Wireless Sensor Networks", Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013, Melaka, Malaysia.*

[15] *G.Keerthana and Dr.G.Padmavathi ," A Study on Sinkhole Attack Detection using Swarm Intelligence Techniques for Wireless Sensor Networks",IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 5, No5, October 2015*