Indian Journal of Science and Technology, *Vol 9(38), DOI: 10.17485/ijst/2016/v9i38/88145, October 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A QOS Parameter based Solution for Black hole Denial of Service Attack in Wireless Sensor Networks

S. S. Nagamuthu Krishnan[1]* and P. Srinivasan[2]

[1]Department of MCA, RV College of Engineering, Bangalore – 560059, Karnataka, India; ssnkrishnan@gmail.com
[2]VIT University, Vellore – 632014, Tamil Nadu, India; srinivasan.suriya@vit.ac.in

Abstract

Background/Objectives: A typical Wireless Sensor Network (WSN) is a collection of Sensor nodes with limited charge that get deployed in a range enabling different applications. Enormous potential is there for deployment of WSN in consumer centric applications, industry sector and defence. **Method:** WSNs are vulnerable to various types of attack, upon which black-hole, a type of Denial of Service (DoS) pose enormous challenge in detection and defence. The primary characteristic of the attack is that reprogramming done by attackers in the captured nodes block the packets received than forwarding to the base station. This results in information entering the black hole area not getting routed to the destination and degradation of QoS factors of delay and final throughput. In this study a comparative performance weighing of Star and tree topology setup of WSN nodes is carried out under the black hole scenario. In case, the parameter of delay is vital Mesh setup is chosen and in the requirement of throughput efficiency and fault tolerance Star topology is chosen. A methodology for choosing the topology depending on the required service parameter under black hole scenario is also devised. **Findings:** The vital parameters considered for the simulation study are delay in transmission of packets and throughput efficiency among the sensor nodes. The results prove a considerable reduction of the parameter of delay in transmission of packets if hybrid topology is followed and a reasonable increase in the QoS parameter of throughput as mesh topology is adopted during transmission in a black hole vulnerable network. **Improvements:** The vital parameters of negligible delay and throughput efficiency that contribute effective cooperation among the sensor nodes are taken into account while choosing the appropriate topology, and the results show the distribution of the parameter values for the particular topology chosen.

Keywords: Black Hole Attacks, Delay, Denial of Service, Throughput, Topology

1. Introduction

Wireless Sensor Networks offer the facility of deployment in an increased scale complex real-time data processing in messy environments. The applications facilitate in protection and monitoring of military based applications, environmental requirements, safety-critical aspects and domestic setup and facilities. It is highly essential to upkeep the availability of network in these prominent and safety centric facilities to reap the benefits. The profound reason for the requirement is Denial of Service attacks in such set up may permit practical damage to the well being and the aspect of safety of people. In the absence of protection and security measures, networks will be limited to localized environments, preventing to get benefited from promising benefits they hold. Ensuring availability in network becomes more complex given the limited capacity of individual sensor nodes to escape from failures or attacks. Sensor networks make the previously unrealizable information gathering highly feasible due to their dynamism, application oriented and ad-hoc nature. They are built to collate and make useful analysis of low-level data from an area of study. The goals are often satisfied based on cooperation of local nodes, summing up and production of information as individual nodes possess highly limited capabilities. The miniaturization

*Author for correspondence

of the nodes has resulted in them possessing limited or non-replenishing power storage and communicates in a wireless fashion and not having unique identity. They also have a tight requirement of forming volatile relationships in a crowded network having no existing standard setup. The protocols and procedures that operate in the network should facilitate a large-scale distribution, in most of the cases with only limited range interactions among nodes. The network should be able to offer its full service even in the event of failure of significant nodes meeting real-time processing expectations. Besides the limitations posed by application dependent files, as they reflect a periodically changing environment, the data gathered are valid for only a limited period of time. Sensor networks in military field may gather intelligent information in war field conditions, track opposition's troop movements, police a highly secured zone for activity or give a report on damage and casualties caused. Sensor networks also form a spontaneous communications network for rescue personnel at disaster recovery sites and by themselves help in locating life loss. They could also be deployed to monitor conditions at volcanic eruptions, through a faulty earthquake or at the sides a logged water reservoirs, provide real time monitoring of health for the aged and applied in detection of chemical or biological threat in a public utilities.

As the cost involved and overhead is low, sensor networks find their deployment in civic-event monitoring, then discarded. Networks whose persistence level is more are refreshed from time to time by renewed deployments that in turn integrate with the existing set of networked sensors. Essential requirements of the network are they must be resilient in the event of individual node failure, as at any instance nodes could be smashed, lose their power or fail due to problems that persist in large-scale production processes.

A lot of work has be done in the recent past by many experts in research across the world and have come out with different rules and methods for protecting Wireless Sensor Networks for stopping the occurrence of DoS attacks. The methodology introduced in[1] computes the count of malicious packets from a voluminous set of packets and was based on probabilistic approach to thwart Denial of Service attack. This scheme helped them to reduce overhead than existing approaches. The mechanism proposed in[2] applies a game oriented way to stop such attacks in Wireless Sensor Networks. The approaches applied in the proposal were Utility based Dynamic Source Routing (UDSR) that brings in the summed up value of each route that the packets take and a solution based on a watch list in which each node exchanges a score from its neigh bouring nodes. The methodology applied in[3] introduced a novel mechanism for increasing the complexity of launching a low level Distributed Denial of Service attack (DDoS) in a Wireless Sensor Network by making use of a remote access structure that includes a implicit home and a DDoS Defence Server.

The form introduced in[4] uses the cluster adaptive rate limiting that uses an intrusion detection technique based on the host. This technique aims at reducing the power consumption to an appreciably lower level till the point the attack is subverted. The public key system introduced[5] stops a particular type of Denial of Service attacks that work to conduit the energy of sensor nodes in Wireless Sensor Networks. This proposal uses a Elliptic Curve Cryptography based key creation scheme in combination with the Denial of Service mitigation mechanism. The methodology covered in[6] introduces a multiuser Denial of Service limiting by including a signature oriented broadcast verification scheme. The proposal in[7] is for a distributed implementation Wireless Sensor Networks for preventing the possibility of Denial of Service attack when data element has been intercepted applying a broadcast key administration scheme. A good extent of hashing and numerical calculations is carried out to fake the first intercepted data packet. In spite of it the methodology achieves to reduce the time consumed for sending trusted messages over the entire network set up.

The protocol introduced in the scheme adopts *a* Key Distribution Server (KDS) that distributes a special key and a unique ID to each node in the network. The individual nodes compute the actual key applying a pseudo random function, the distributed special key and the unique ID. It also aims for cooperative authentication check between server and cluster nodes and from there on to sensor nodes. A secondary key is then generated for communication between server and cluster nodes. Then a tertiary key is computed for communication between server and sensor nodes through cluster nodes, followed by applying the secondary key the server pass information of the sensor nodes to every cluster node. Subsequently, the sensor nodes communicate their ID to the server using the tertiary key. Finally the sensor nodes that are members of a cluster communicate among them applying the tertiary key. In the event of total requests exceeding server's handling capacity it implements prevention of Denial of Service.

A cluster-based intrusion detection system proposed in [LC09] is to protect sensor networks from DoS attacks. The mechanism introduced here considers a specific group of nodes called "guarding Nodes" (gNodes) that observe, analyze the network traffic and report the abnormal event of DoS attacks to their cluster. For implementing this in each cluster is a combination of three types of nodes, gNode, the cluster head and sensor node. As any kind of nodes is liable be compromised this study devises a detection approach for various attack types and the responses for the attacks are explored for all possible node types.

Perrig et al. [AP02] proposed SPINS (Security Protocols for Sensor Networks) that is a combination of two proven symmetric key based building blocks viz. SNEP and μTESLA. The contribution made by SNEP is to ensure secrecy of data, two-way data authentication and freshness of data incurring lower overhead. MAC and a common counter between the sender and the receiver for the cipher block in counter mode which is incremented after each block for achieving two-party authentication and data accuracy are applied. μTESLA offers authenticated broadcast applying one-way key chains constructed applying secure hash functions.

Time is divided into intervals and the sender associates each key of the one-way key chain with one time interval for performing cryptographic operations.

Sensor networks formed dynamic and periodical in hierarchical pattern apply clusters through the outcome of LEACH algorithm and facilitate distribution of liveliness and assigned work among sensor nodes. The security problem in such a type of of network is identified and solved by Oliveira et al. [LO08] that propose an improved version of LEACH. This combines together random key distribution beforehand and μTESLA. The purpose is to secure communications in a hierarchical network implementing dynamic cluster establishment. The running of a detection mechanism on every node in the network allows achieving a perfect detection against DoS attacks but it is not a feasible solution in a constrained network.

In [HI10], an optimized placement of detection nodes in a network for distributed detection of DoS attacks is proposed. In addition to placing detection nodes at critical points in a network, this proposition minimizes the number of these required nodes and therefore reduces the cost and processing overheads.

An effective and adaptive security design (SecCBSN) to safeguard cluster based communication in sensor networks is introduced in [MH08]. It is a combination of three modules that can detect malicious nodes by offering secure communication and authentication protocols between nodes. The head module in each cluster is responsible for scheduling of transmission and monitoring time cycles for its constituent sensor nodes. The primary security module works by assigning a certificate for existing nodes to authenticate new incoming nodes, acting for establishment of secure links and broadcast authentication information between its neigh bours. An intrusion detection module functioning in SecCBSN prevents the effect due to compromised nodes. For this it uses alarm return protocols, evaluation of trust value and distributing of black and white lists of nodes among the participating sensors.

Data summing up in Wireless Sensor Networks involves summarizing followed by combining data held at sensor nodes in order to reduce the volume of data transmitted in the network. In a cluster oriented sensor network, a head elected by the other sensor nodes is responsible for aggregation of data stored nearby and transmit the result of aggregation to the reporting station.

This process has to occur in a secure way to ensure data confidentiality and authentication. The methodology in Ozdemir and Xiao [OX10] explores the relationship between security and data aggregation process in Wireless Sensor Networks. An extensive literature review is presented here upon summarizing novel data aggregation protocols and based on this areas of future research are thrown open.

2. Problem Description

A good amount of work is already done on weighing the performance of WSN in various applications. In the paper the focus is on analyzing the performance of popular topologies of peer-to peer, tree and hybrid under black hole attack is carried out. A methodology is also developed for choosing the topology as per the required state of parameters.

2.1 Black Hole Attack Characterization

Black hole attacks occur in grid layer due to the pulling, capturing and blocking of packets by an attacker by means of reprogramming a set of nodes in the network instead of allowing them to pass to the base station resulting in making itself a sink node. This results in information capture in the black hole area. They can be easily constituted and

are capable of downgrading the performance of network by dividing the network, thus preventing important event information reaching the base stations. The key performance parameters that are affected due to the existence of black hole nodes are output per unit time and end-to-end delay introduced. The throughput factor abruptly goes down becoming very less and end to end delay shoots up abnormally.

Black hole attack in WSN is carried as in Figure 1.

Figure 1 shows a set up of six sensor elements (SN1, SN2, SN3, SN4 ----- SN6), two routers (R1, R2) and a coordinating element showing actual flow of packets. The nodes are responsible for sensing any physical trend, converting the same into interpretable information and sending it to router node R1 and R2. The first three sensor nodes (1, 2 and 3) report to routing element R1 and the last three nodes 4, 5 and 6 report to router R2. The routers R1 and R2 further forward the received information to the coordinator node.

2.2 Attack Setup

Figure 2 points out black hole attacking setup. In the same set up of six sensor nodes, router nodes (R1 and R2) and a coordinator as the sensor nodes sense a physical fashion, transform it into interpretable form and send the same to routing elements R1 and R2. R2 a black hole attacker, blocks all the incoming data flow and doesn't forward to coordinating element. Here the node is represented with a dark background. This situation is very harmful as all packets are consumed by routing element R2 resulting in affecting of key network performance parameters through delay increment and decrement in throughput. This also happens to be an incoming way of an array of subtle

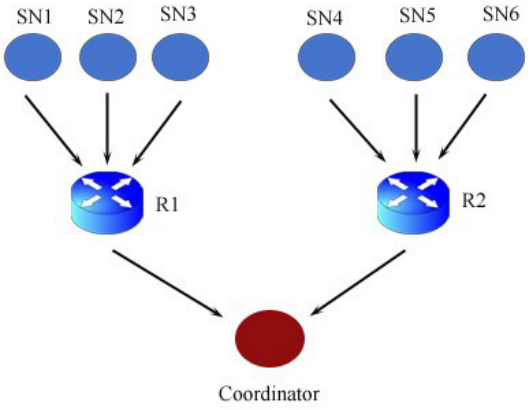

Figure 1. Normal flow of packets between sensor nodes [taken from[1]].

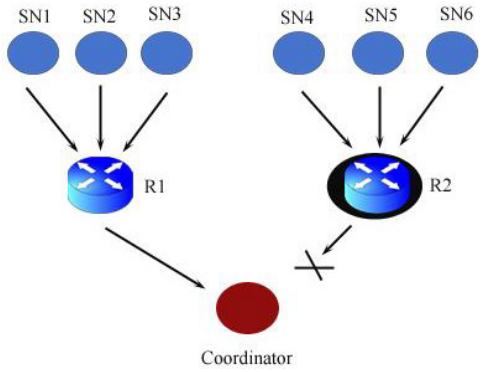

Figure 2. Black hole attack scenario, router R2 becomes attacker [taken from[1]].

attacks. Some of the defence mechanisms that are already available to tackle this scenario either apply message transfer between neighbourhood, message overhearing[7,9] or sharing information clandestine and introducing diverse path for information forwarding[10–12]. Methodologies that depend on neighbourhood message exchanges and overhear work under the supposition that the sensor nodes in the neigh bouring nodes of a black hole node remain un compromised and so remain scrutinizing and intimate the black hole node about alarming scenario. But, if many of the sensor nodes that lie in closeness conspire among them, they can easily tackle attacks based on overhearing ineffectively. The diversification of path and methodology based on clandestinely sharing information, although better, are still not highly successful in subverting black holes.

One of the common attacks in grid layer is said attack in which the attacker tries to direct all packages of the network towards itself. In other words, it tries to attract all the traffic towards itself. And in fact it tries to introduce itself as the sink. To accomplish this, the attacking node introduces itself as the closest node to the sink or advertises itself as a node with extraordinary capabilities. It does this to encourage the neigh bouring nodes to choose the enemy node for routing their data (D. Ganesan, 2001).

2.3 Popular Topologies in WSN

2.3.1 Tree based Topology

In tree topology implementation a central hub for each communion of sensor nodes acts as main communication routing element for that net worked setup. A root node element that integrates various localized communion is present one level higher than the central hubs in the levelling. The lower levels that are coordinated by the

individual central elements form Star network. The tree topology setup is arrived as a hybridization of Star and Peer to Peer topology set up[14].

Figure 3 points out the tree network topology. In such a set up the sensor nodes report to central connecting element which further report to root element that is considered as coordinator of the Wireless Sensor Network setup.

2.3.2 B. Mesh

Mesh networks enable transfer of packets between nodes making the network fault tolerant in nature. Each node can exchange information with every other node as data moves among nodes until it reaches the destination. This topology setup is one of the most complex implementations and causes a significant overhead to function it beneficially[14].

Figure 4 shows the setup in which sensor nodes exchange information with each other directly without the intervention or requirement of any routing element.

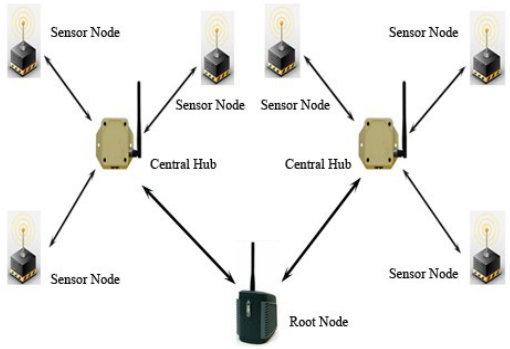

Figure 3. Tree network topology inside WSN [taken from[14]].

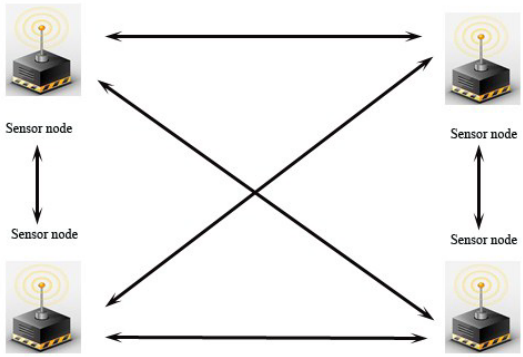

Figure 4. Mesh network topology inside WSN [taken from[14]].

2.3.3 C. Star

In Star topology set up the nodes are connected to a central communicating element. Here in this setup nodes cannot exchange information directly with each another and all message exchanges are routed through a centralized communicating element for that localized network. Each node will be a "client" and the central communicating element acts as server[14]. Figure 5 shows Star setup in which the nodes communicate among themselves through the central element.

2.3.4 D. Peer-to-Peer

Peer-to-Peer topology set up involves the nodes communicating directly with every other element without routing through a central element unlike Star set up. Here a Peer communication element works as both a "client" and "server" for other communicating elements that form the setup[13].

3. Proposed Methodology

The proposed methodology aims at black hole defence that protects the primary QOS parameters of delay in packet delivery, throughput efficacy and delay increment. The scheme works accordingly with the topology chosen and it could be appropriate to choose the topology for implementation of the sensor network as per the expected benefit by the value assigned for a parameter. The simulation study is performed by assuming a network size of twelve sensor nodes, four routers with normal flow and one coordinator node. Two routers among the four are assumed to be black hole nodes and the QoS parameters

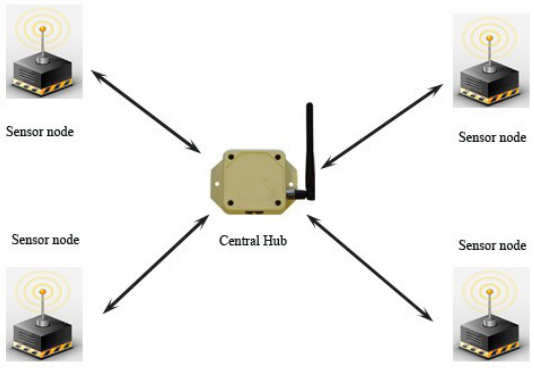

Figure 5. Star oriented topology inside WSN [taken from[14]].

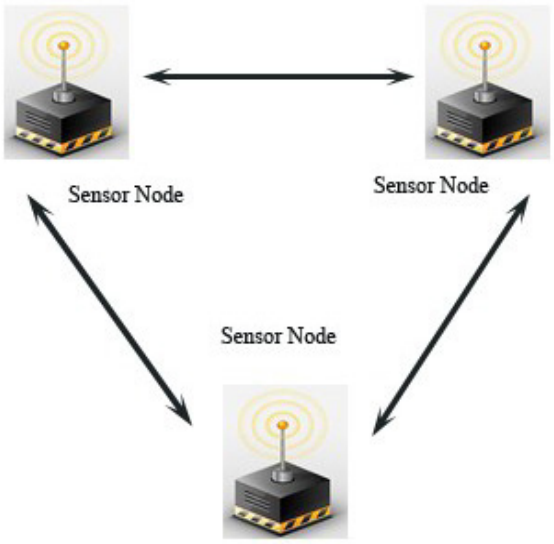

Figure 6. Peer-to-Peer network topology inside WSN [taken from[14]].

are analyzed with respect to the topologies of Peer-to Peer, hybrid and mesh.

The following pseudo code gives a description of the implemented methodology for choosing the topology of implementation as per the expected state of the QoS parameters.

3.1 Procedure QOSBH

```
{
Topol_Unit = {Peer-Peer, Hybrid, Mesh}.
QOS_Parm = {Reasonable_throughput, negl_delay}.
if (Black hole vulnerable network && QOS_Parm = negl_
delay).
then
set Topology = Hybrid from Topology unit.
else if (Black hole vulnerable network && QOS_Parm =
Reasonable_throughput).
then
set Topology = Mesh.
else
set Topology = Peer-Peer .
}
```

The pseudo code given above works for choosing the topology as per the key QoS parameter of interest. In the attack scenario, if the delay factor is of greater importance, then the hybrid topology of mesh and Star will be of the preferred one as any node could be reached even if a particular router is under attack with acceptable delay.

If the throughput is of increased preference during attack then the mesh topology could be chosen as reasonable through put could be achieved following the topology and in the generalized case of considering reasonable importance to both the parameters the topology of Peer-Peer could be followed. The simulated performance measurement of the network as per the cases considered is carried out and the results are graphically shown.

4. Results and Interpretation

The following interpretation shows the results of the study undertaken with the simulation of the different scenarios considered as per the required parameters. The vital parameters considered for the study are delay in transmission of packets and throughput efficiency among the sensor nodes.

	Peer-Peer Topology	Peer to Peer Sensor Network Topology under Black Hole Attack	Hybrid Sensor Network Topology and Mesh topology under Black Hole Attack
Delay in Transmission (msec)	21.55	35.47	27.64
Throughput Efficiency (bps)	6236	5375	5970

The graphical illustration in Figure 7 shows a considerable reduction of the parameter of delay in transmission of packets if hybrid topology is followed in a black hole vulnerable network.

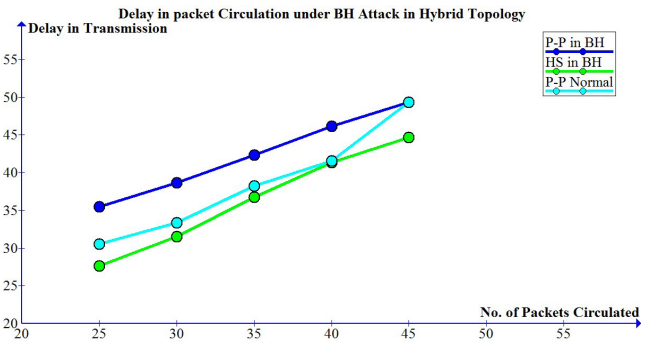

Figure 7. Delay in packet circulation under BH attack in hybrid topology.

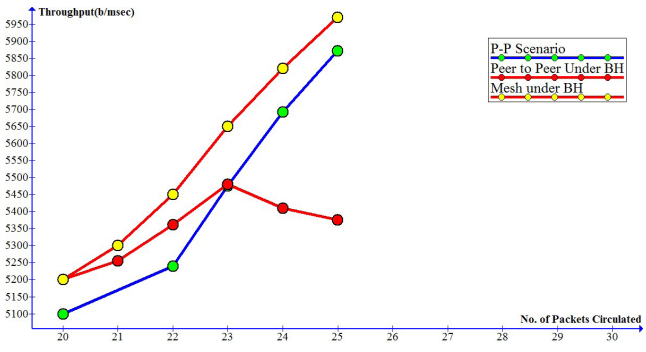

Figure 8. Throughput efficiency in mesh topology under black hole attacks.

Graphical illustration in Figure 8 shows a reasonable increase in the QoS parameter of throughput in transmission in a black hole vulnerable network.

5. Conclusion and Future Work

The methodology considered here works towards choosing of sensor network topology as it is established. The vital parameters of negligible delay and throughput efficiency that contribute effective cooperation among the sensor nodes are taken into account while choosing the appropriate topology and the results show the distribution of the parameter values for the particular topology chosen. This work could be further extended by analyzing the black hole scenario with a varied set of parameters that in turn prevent the sensor network from getting yielded to the attack.

6. References

1. Wazid M, Katal A, Sachan RS, Goudar RH, Singh DP. Detection and prevention mech anism for black hole attack in Wireless Sensor Network. International Conference on Communication and Signal Processing; India. 2013 Apr 3-5.
2. Blilat A, Bouayad A, el houda Chaoui N, ElGhazi M. Wireless Sensor Network: Security challenges. IEEE National Days of Network Security and Systems (JNS2; 2012. p. 68–72.
3. Yu YL, Li K, Zhou W, Li P. Trust mechanisms in Wireless Sensor Networks: Attack analysis and q countermeasures. Journal of Network Computer and Applications. Special Issue on Trusted Computing and Communications. Elsevier. 2012 May; 35(3):867–80.
4. Guechari M, Mokdad L, Tan S. Dynamic solution for detecting Denial of Service attacks in Wireless Sensor Networks. IEEE International Conference on Communications (ICC); 2012.
5. Schaffer P, Farkas K, Horvath A, Holczer T, Buttyan L. Survey secure and reliable clustering in Wireless Sensor Networks: A critical survey. Computer Networks: The International Journal of Computer and Telecommunications Networking. ACM; 2012 Jul.
6. Misra S, Bhattarai K, Xue G. BAMBi: Black hole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks. IEEE International Conference on Communications (ICC); 2011.
7. Mahmood AR, Aly HH, El-Derini MN. Defending against energy efficient link layer jamming Denial of Service attack in Wireless Sensor Networks. IEEE 9th IEEE/ ACS International Conference on Computer Systems and Applications (AICCSA); 2011.
8. Nanda R, Venkata Krishna P. A self enforcing and flexible security protocol for preventing Denial of Service attacks in Wireless Sensor Networks. IEEE Recent Advances in Intelligent Computational Systems (RAICS); 2011.
9. Modares H, Salleh R, Moravejosharieh A. Overview of security issues in Wireless Sensor Networks. 3rd International Conference on Computational Intelligence, Modeling and Simulation (CIMSIM '11), ACM; 2011.
10 Prathapani A, Santhananr L, Agrawal DP. Intelligent honeypot agent for black hole attack detection in Wireless Mesh Networks. IEEE 6th International Conference on Mobile Ad-hoc and Sensor System (MASS); 2009.
11. Tiwari M, Arya KV, Choudhari R, Choudhary. Designing intrusion detection to detect black hole and selective forwarding attack in WSN based on local Information. IEEE 4th International Conference on Computer Sciences and Convergence on Information Technology (ICCIT); 2009.
12. Gill K, Yang SH. A scheme for preventing denial of service attacks on Wireless Sensor Networks. IEEE 35th Annual Conference of Industrial Electronics, (IECON '09); 2009.
13. Medadian M, Mebadi A, Shahri E. Combat with black hole attack in AODV routing protocol. IEEE 9th Malaysia International Conference on Communications; 2009 Dec 15-17.
14. Raymond DR, Midkiff SF. Denial-of-Service in Wireless Sensor Networks: Attacks and defenses. IEEE Pervasive Computing; 2008. Jan-Mar.
15. Pathan ASK, Lee HW, Hong CS. Security in Wireless Sensor Networks: Issues and challenges. IEEE 8th International Conference on Advanced Communication Technology (ICACT); 2006.
16. Tanveer Z, Zomaya A. Security issues in Wireless Sensor Networks. IEEE International Conference on Systems and Networks Communications (ICSNC); 2006.